PROGRAMA AVANZADO DE ESTUDIO:

SEGURIDAD EN SISTEMAS DE INFORMACIÓN

Versión Junio 2010 (*corregido y actualizado)*

"El Arte de la Guerra nos enseña que no debemos depender de la posibilidad de que el enemigo no venga, sino que debemos estar siempre listos a recibirlo. No debemos depender de la posibilidad de que el enemigo no nos ataque, sino del hecho de que logramos que nuestra posición sea inatacable."

El Arte de la Guerra, Sun Tzu

Este libro es el resultado de la recopilación exhaustiva de información de diversas fuentes, todas ellas incluidas en la bibliografía. Yo simplemente me he encargado de agrupar, ordenar, alimentar con mi propia experiencia y presentar en diferentes capítulos el presente libro, que pongo a disposición general. Cada capítulo tiene una sección de preguntas al final del mismo.

Este material, cubre todos los tópicos de la certificación CompTIA Security+, y gran parte de los tópicos de CompTIA Network+. Algunos temas y preguntas oficiales de certificaciones como CEH, CISSP, NSA, CISA, han sido incluidos también en la sección de preguntas de cada capítulo. Para más detalle remítase al índice y a la bibliografía.

"Nando" A. B. C.

Analista de Sistemas y Seguridad Informática

Venezuela. 2010

CAPÍTULO 1

1.1 SEGURIDAD DE LA INFORMACIÓN

1.1.2 ¿Qué es la seguridad de la información?

El termino Seguridad de Información, Seguridad informática y garantía de la información son usados con frecuencia y aunque su significado no es el mismo, persiguen una misma finalidad al proteger la Confidencialidad, Integridad y Disponibilidad de la información; Sin embargo entre ellos existen algunas diferencias sutiles. Estas diferencias radican principalmente en el enfoque , las metodologías utilizadas, y las zonas de concentración.

La Seguridad de la Información se refiere a la Confidencialidad, Integridad y Disponibilidad de la información y datos, independientemente de la forma los datos pueden tener: electrónicos, impresos, audio u otras formas.

Además, la seguridad de la información involucra la implementación de estrategias que cubran los procesos en donde la información es el activo primordial. Estas estrategias deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.

Cabe mencionar que la seguridad es un proceso continuo de mejora por lo que las políticas y controles establecidos para la protección de la información deberán revisarse y adecuarse, de ser necesario, ante los nuevos riesgos que surjan, a fin de tomar las acciones que permitan reducirlos y en el mejor de los casos eliminarlos.

Los Gobiernos, entidades militares, instituciones financieras, los hospitales y las empresas privadas acumulan una gran cantidad de información confidencial sobre sus empleados, clientes, productos, investigación y su situación financiera. La mayor parte de esta información es recolectada, tratada, almacenada y puesta a la disposición de sus usuarios, en computadoras y trasmitida a través de las redes entre los ordenadores.

En caso de que la información confidencial de una empresa, sus clientes, sus decisiones, su estado financiero o nueva línea de productos caigan en manos de un competidor; se vuelva pública de forma no autorizada, podría ser causa de la pérdida de credibilidad de los clientes, pérdida de negocios, demandas legales o incluso la quiebra de la misma.

Por lo que proteger la información confidencial es un requisito del negocio, y en muchos casos también un imperativo ético y una obligación legal.

Para el individuo común, la Seguridad de la Información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo.

El campo de la Seguridad de la Información ha crecido y evolucionado considerablemente en los últimos años. Convirtiéndose en una carrera acreditada a nivel mundial. La misma ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, Planificación de la continuidad del negocio, Ciencia Forense Digital y Administración de Sistemas de Gestión de Seguridad por nombrar algunos.

Por más de veinte años la Seguridad de la Información ha declarado que la confidencialidad, integridad y disponibilidad (conocida como la Tríada CIA, del inglés: "Confidentiality, Integrity, Availability") son los principios básicos de la seguridad de la información.

La correcta Gestión de la Seguridad de la Información busca establecer y mantener programas,

controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información, si alguna de estas características falla no estamos ante nada seguro. Es preciso anotar, además, que la seguridad no es ningún hito, es más bien un proceso continuo que hay que gestionar conociendo siempre las vulnerabilidades y las amenazas que se ciñen sobre cualquier información, teniendo siempre en cuenta las causas de riesgo y la probabilidad de que ocurran, así como el impacto que puede tener. Una vez conocidos todos estos puntos, y nunca antes, deberán tomarse las medidas de seguridad oportunas.

La **confidencialidad** es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

Para la Seguridad de la Información, **la integridad** es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.

La **Disponibilidad** es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

La información es uno de los recursos principales de las organizaciones. ¿Piense qué pasaría si roban la fórmula de alguna de las gaseosas internacionales? ¿cuánto representa esta información para la empresa? Es decir, cuidar la información es cuidar la propia existencia de la compañía. En el presente desarrollo, cada vez que se mencione Información se estará haciendo referencia a la Información que es procesada por un Sistema Informático; definiendo este último como el "conjunto formado por las personas, computadoras (hardware y software), papeles, medios de almacenamiento digital, el entorno donde actúan y sus interacciones."

La seguridad es un concepto abstracto difícil de definir, podríamos pensarla como una sensación de protección, que depende de varios factores (el contexto, nuestras fortalezas, nuestras debilidades, las amenazas). Si unimos las dos definiciones, podríamos intentar una definición de seguridad de la información, diciendo que es la sensación que perciben las personas sobre el nivel de protección de la información.

La seguridad de la información se encarga de protegerla de una amplia gama de amenazas, a fin de garantizar la continuidad comercial del negocio, minimizar los daños y maximizar el retorno sobre las inversiones y las oportunidades, normalmente se logra implementando un conjunto adecuado de controles que abarcan políticas y procedimientos, involucrando recursos humanos, hardware y software. Es decir, el término seguridad de la información cubre un amplio espectro de actividades, y parte de nuestro trabajo como profesionales de la seguridad, será hacer recomendaciones y tomar acciones para minimizar los riesgos y exposición de la información y demás activos. Estas actividades, muchas veces no son sencillas, pero deberemos realizarlas correctamente para tener una chance de mantener la seguridad de la información de la empresa dentro de niveles razonables.

"*La información es la sangre de todas las organizaciones y puede existir en muchas formas. Puede ser impresa o escrita en papel, almacenada electrónicamente, transmitida por correo electrónico, mostrada en películas o hablada en una conversación. En el ambiente de negocio competitivo de hoy, tal información está constantemente bajo amenaza de muchas fuentes. Éstas pueden ser internas, externas, accidentales o maliciosas. Con el uso creciente de la nueva tecnología, al almacenar, transmitir y recuperar la información, hemos abierto un gran número y tipo creciente de amenazas*".

"*Hay una necesidad de establecer una política comprensiva de seguridad de la información dentro de todas las organizaciones. Usted necesita asegurar la confidencialidad, integridad y disponibilidad de la información corporativa vital y de la información del cliente. El estándar para Information Security Management System (ISMS) BS 7799, ya ha sido rápidamente establecido por los vendedores de software más grandes del mundo*".

1.1.3 Conceptos

Seguridad Informática

La Seguridad Informática suele ser la forma más habitual con la que nos referimos a todo aquello que tiene que ver con la seguridad de los ordenadores y los sistemas. Es un concepto muy conocido pero que está obsoleto. Hace hincapié en la seguridad de los sistemas, teniendo en cuenta las amenazas de carácter fundamentalmente tecnológico.

La Seguridad Informática es un concepto de Seguridad que nació en la época en la que no existían las redes de banda ancha, los teléfonos móviles o los servicios de internet como las redes sociales o las tiendas virtuales. Es por ello que la Seguridad Informática suele hacer un especial énfasis en proteger los sistemas, es decir, los ordenadores, las redes y el resto de infraestructuras de nuestra organización. *La Seguridad Informática es un concepto fundamentalmente técnico.*

El problema del enfoque de la Seguridad Informática es que suele perder de vista otros aspectos importantes para una organización y, en la mayoría de las ocasiones, cuando nos hablan de Seguridad Informática nos parece algo completamente alejado de nuestra actividad diaria.

Seguridad TIC (*Seguridad de las Tecnologías de la Información y las Comunicaciones*)

Se trata de un enfoque más moderno, que incorpora el concepto de redes o infraestructura de comunicaciones. Hoy en día no concebimos el ordenador como un elemento aislado sino como un elemento conectado, y por otro lado, el ordenador ya no es el único elemento o dispositivo a proteger, sino que también hay que proteger las infraestructuras de comunicaciones, así como diversos dispositivos, como son los teléfonos móviles, PDA's, etc. La Seguridad TIC es un término mucho más amplio que la Seguridad Informática, pero sigue siendo de carácter fundamentalmente tecnológico.

Seguridad de la Información

Estamos ante el término más amplio y conceptual de los tres. Se basa en que lo fundamental es proteger la información y en base a esta premisa se desarrollan todas los demás aspectos relativos a la seguridad y a las medidas que necesitamos aplicar, así como el lugar donde hay que aplicarla. Es un concepto que tiene en cuenta, no solamente la seguridad tecnológica, sino también otras facetas de la seguridad, como son, la seguridad desde el punto de vista jurídico, desde el punto de vista normativo y desde el punto de vista organizativo.

De los tres conceptos el que más nos interesa es el de la Seguridad de la Información, puesto que es aquel que nos permitirá sacar el máximo provecho a la aplicación de la seguridad en nuestra organización. Además, es el más actual y el más amplio. Como veremos más adelante, abarca todos los aspectos relativos a la protección de la información. Por tanto, a partir de ahora y para todo lo que resta del libro, hablaremos de seguridad desde el punto de vista de la Seguridad de la Información o SI. *La Seguridad de la Información no tiene que ver únicamente con cuestiones tecnológicas, sino también legales u organizativas, es decir, puede ser aplicada desde tres puntos de vista: legal, técnico y organizativo*

La Tele-informática

Por definición, teleinformática o telemática es la asociación de técnicas propias de las

telecomunicaciones y la informática, con la que se realiza a distancia el intercambio de datos y el control de tratamientos automáticos, más concretamente podemos decir que la telemática proporciona a personas no especializadas la posibilidad de acceder a sistemas de comunicación e informaciones antes reservadas a especialistas. Juntas, estas técnicas constituyen un papel importante en la sociedad actual; la era de la información y las comunicaciones.

De esta manera se unen las funcionalidades de los sistemas informáticos, en cuanto a capacidad de procesar y almacenar grandes cantidades de datos y de las telecomunicaciones capaces de intercambiar información entre sistemas distantes.

La evolución de la electrónica y en especial de los semiconductores desde que en 1947 apareciera el transistor en los laboratorios Bell, ha posibilitado la realización de sistemas informáticos y redes cada vez más sofisticados, esto ha hecho que lo que en un principio podía parecer innecesario, unir ordenadores con redes telefónicas, cada vez haya ido adquiriendo mayor importancia, puesto que las redes se han hecho cada vez más complejas y veloces y los ordenadores (desde que apareciera el Eniac) más potentes, con mayor capacidad y mucho más pequeños.

La columna vertebral de la telemática está constituida por las redes de transmisión de datos, en un primer momento se utilizó la Red Telefónica Conmutada (RTC), compartiéndose las comunicaciones de voz con las de datos, para posteriormente ir evolucionando hacia redes dedicadas para datos. Estas redes para datos se diseñaron partiendo de la base de que sólo iban a manejar este tipo de tráfico (bits), así nacieron las que se conocen como redes de conmutación de paquetes.

Los servicios de telecomunicaciones son aquellas acciones tendentes a satisfacer una necesidad de comunicaciones mediante el intercambio, almacenamiento y tratamiento de información (audible, visible, texto...) requerida por un usuario.

Por servicio, en el ámbito de las telecomunicaciones, se entiende a la capacidad de transporte de información, que en algunos casos puede suponer el tratamiento y/o almacenamiento de la misma, ofrecida por un proveedor de servicios de telecomunicación a los usuarios a través de las redes de telecomunicación.

Seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada.

El termino Seguridad de Información, Seguridad informática y garantía de la información son usados con frecuencia y aun que su significado no es el mismo, persiguen una misma finalidad al proteger la Confidencialidad, Integridad y Disponibilidad de la información; Sin embargo entre ellos existen algunas diferencias sutiles. Estas diferencias radican principalmente en el enfoque , las metodologías utilizadas, y las zonas de concentración.

La Seguridad de la Información se refiere a la Confidencialidad, Integridad y Disponibilidad de la información y datos, independientemente de la forma los datos pueden tener: electrónicos, impresos, audio u otras formas.

A menos que la red que trata de proteger se encuentre en un cuarto cerrado con acceso controlado y no tenga conexiones desde el exterior, sus computadoras estarán en riesgo. Las entradas no autorizadas y violaciones de seguridad ocurren casi a diario en todo el mundo. Estos infractores no son sólo vándalos en Internet, sino que puede ser el empleado que sustrae tiempo o servicios de la computadora para su uso personal o mal intencionado.

En este capítulo se estudia la seguridad de la información, los objetivos que persigue y porqué hoy en día es una necesidad; por último se presentan las tendencias actuales que afectan la seguridad de manera que podamos tomar conciencia de la realidad a la que nos enfrentamos.

Desde los primeros días de la computación, siempre ha existido la necesidad de establecer algún tipo de control o protección sobre el equipamiento y eventualmente la información por ellos generada. No obstante dichos controles y niveles de protección, han evolucionado necesariamente, acompañando el avance en el campo de la informática y las comunicaciones.

Así como inicialmente, los únicos mecanismos de protección pasaban por ejemplo, por proteger físicamente el acceso al cuarto donde se albergaban los grandes computadores, con guardias de seguridad; conforme la computación fue evolucionando hacia equipos más pequeños y al alcance de mayor cantidad de usuarios, este modelo dejo de ser eficiente, debiendo complementar este tipo de controles físicos, con aquellos más relacionados con aspectos de seguridad lógica.

Del mismo modo, la proliferación de las redes de datos, requirió de nuevos cambios en los modelos de seguridad a aplicar por parte de las diferentes organizaciones, que preocupadas por la seguridad de la información relacionada con su actividad, requerían establecer ya no solo controles sobre los equipos, sino también sobre el transporte de datos. En tal sentido, sin dudas el mayor impacto respecto de la seguridad relacionada con computadoras hasta nuestros días, lo haya provocado el advenimiento de Internet y con el, la interconexión de redes mencionadas a menudo como “no seguras”, muchas veces más allá de nuestro propio control.

La nueva tendencia respecto de la implementación de gran cantidad de dispositivos móviles y redes inalámbricas como parte de la nueva infraestructura tecnológica, también ha requerido que los profesionales en seguridad, ajusten nuevamente sus procedimientos y desarrollen un conjunto de técnicas y controles capaces de velar por la seguridad de la información con ellos relacionada.

En resumen, la implementación de nuevas tecnologías indefectiblemente trae aparejado, el advenimiento de nuevas oportunidades de negocio, así como también riesgos, amenazas y nuevos vectores de ataque, siendo requerido como parte de un proceso continuo, la revisión constante de los modelos de seguridad y la adecuación de controles, de modo tal de mantener su vigencia.

1.1.4 Objetivos de la seguridad de la información

Mencionamos antes que la seguridad de la información se encarga de protegerla, más específicamente, podemos definir que lo logrará preservando la confidencialidad, integridad y disponibilidad de la información, como aspectos fundamentales y el control y autenticidad como aspectos secundarios . A continuación se describen estas características:

- La Integridad de la Información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.
- La Disponibilidad u Operatividad de la Información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada, con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.
- La Privacidad o Confidencialidad de la Información es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la información puede provocar severos daños a su dueño (por ejemplo conocer antecedentes médicos de una persona) o volverse obsoleta (por ejemplo: los planes de desarrollo de un producto que se “filtran” a una empresa competidora, facilitarán a esta última desarrollar un producto de características semejantes).
- El Control sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuándo y cómo permitir el acceso a la misma.
- La Autenticidad permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.

Adicional mente pueden considerarse algunos otros aspectos, relacionados con los anteriores, pero que incorporan algunas consideraciones particulares:

- Protección a la Réplica: mediante la cual se asegura que una transacción sólo puede realizarse una vez, a menos que se especifique lo contrario. No se deberá poder grabar una transacción para luego reproducirla, con el propósito de copiar la transacción para que parezca que se recibieron múltiples peticiones del mismo remitente original.
- No Repudio: mediante la cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.

1.1.5 Principios fundamentales de seguridad

Toda estrategia orientada a tratar aspectos de seguridad de la información, a menudo comprende diversos objetivos. Estos a su vez pueden ser grandes o pequeños, no obstante existen tres principios fundamentales, los cuales indefectiblemente suelen encontrarse direccionados en todo programa integral de seguridad de la información. Estos son conocidos individualmente como Confidencialidad, Integridad y Disponibilidad; y a menudo referidos en su conjunto como “CIA Triad” o “The Big Three”.

Si bien es cierto que el nivel de seguridad requerido para con cada uno de estos principios puede variar de organización en organización, debido principalmente a que cada una de ellas probablemente posea una combinación única de requerimientos, objetivos de negocio y requisitos de seguridad; por lo general cada uno de los controles, mecanismos y salvaguardas implementados en una organización, tienen por finalidad asegurar uno o mas de estos principios fundamentales.

Del mismo modo, cada uno de los riesgos, amenazas y vulnerabilidades identificados, suelen ser medidos o evaluados, respecto de su potencial capacidad de comprometer uno o varios de los principios de la Tríada.

Confidencialidad: El principio de Confidencialidad, asegura que el nivel necesario de secreto se encuentra asegurado en cada instancia del procesamiento de datos, de manera tal de prevenir su divulgación a personas no autorizadas a conocer los mismos. Dicho de otro modo, la Confidencialidad de la Información, a menudo es referida como la necesidad de que la misma sólo sea conocida por personas autorizadas.

Un aspecto de suma importancia a tener en cuenta cuando nos referimos particularmente a este principio, es que el nivel de Confidencialidad debe prevalecer no solo mientras que los datos residen en los sistemas y dispositivos dentro de la red, sino también durante su transmisión y almacenamiento en destino.

Varias son las amenazas que atentan contra la Confidencialidad: Usuarios pueden intencional o accidentalmente divulgar información sensible al no encriptar la misma antes de que esta le sea enviada a otra persona, pueden ser victima de algún tipo de ataque de ingeniería social en busca de secretos comerciales, información en tránsito puede ser interceptada por terceros que se encuentren en condiciones de realizar escuchas, etc.

La Confidencialidad, a menudo puede ser provista o reforzada, mediante la implementación de un estricto control de acceso, por medio de la encriptación de datos (ya sea al momento de almacenar o transmitir los mismos), la puesta en marcha de procesos de Clasificación de la Información, concientización y entrenamiento del personal. Cada uno de ellos suelen ser recursos de suma importancia a la hora de combatir efectivamente aspectos tales como la divulgación no autorizada.

Integridad: La Integridad de la Información es la característica que hace posible garantizar su exactitud y confiabilidad, velando por que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, de modo autorizado y mediante procesos autorizados. A su vez,

es de suma importancia que esta modificación sea registrada para posteriores controles o auditorias.

Una falla de integridad puede estar dada entre otros, por anomalías en el hardware, software, virus informáticos y/o modificaciones inesperadas. Precisamente, a fin de mantener su integridad, el conjunto de hardware, software y mecanismos intervinientes en el tratamiento de la información, deben ser capaces de trabajar de manera coordinada, a efectos de procesar, mantener y mover los datos a su destino previsto, sin que los mismos sufran cualquier tipo de alteración inesperada. Tanto los sistemas como la red, se deben proteger contra cualquier tipo de interferencia exterior que pueda permitir algún tipo de contaminación.

Ambientes en donde existen medidas que refuerzan el principio de Integridad en el tratamiento de la información, permiten asegurar que atacantes o cualquier tipo de error cometido por los usuarios, no serán capaces de comprometer la integridad del sistema o los datos.

Cuando un atacante distribuye un virus, una bomba lógica o un ***backdoor*** dentro del sistema, la integridad de este es comprometida. Este hecho puede afectar negativamente el principio de integridad de la información, debido a que la misma puede terminar por corromperse, ser contaminada mediante la introducción de datos erróneos/falsos o modificada con fines malévolos.

El control de acceso, los sistemas de detección de intrusos, la aplicación de chequeo de integridad, los procedimientos de control de cambios, la separación de funciones y la implementación del principio de “Menor Privilegio”, son solo algunos de los medios utilizados para prevenir problemas de integridad.

Disponibilidad: La Disponibilidad u Operatividad de la Información es su capacidad de encontrarse siempre disponible, para ser utilizada por las personas autorizadas. A fin de cumplir con este principio, los sistemas y redes deben proveer la capacidad adecuada de procesamiento, actuar de modo previsible y brindar un adecuado nivel de performance. A su vez, ellos deberían ser capaces de recuperarse de interrupciones de manera rápida y segura, a fin de que la productividad no se vea afectada negativamente.

Entre las amenazas que afectan el principio de Disponibilidad, se encuentran las fallas relacionadas con el software y hardware, aspectos relacionados con el entorno (calor, frío, humedad, electricidad estática, etc.), desastres naturales, denegaciones de servicios (DoS, DDoS), etc. A fin de prevenir inconvenientes que puedan afectar la Disponibilidad, deben ser implementados mecanismos de protección adecuados, con el fin de reforzar la estrategia de continuidad del negocio definida por la organización, previniendo de este modo amenazas internas o externas. En tal sentido deberían implementarse medidas de resguardo y recuperación, mecanismos redundantes, planes de contingencia, sistemas de prevención y/o detección de intrusos, procedimientos de ***hardening***, etc. A su vez puntos únicos de fallas deberían ser evitados.

1.1.6 La Necesidad de asegurar la información

Algunos indicadores atrás, mencionamos el hecho que a menudo solemos referirnos a los principios fundamentales de seguridad: Confidencialidad, Integridad y Disponibilidad, como “The CIA Triad” o “The Big Three”. Del mismo modo nos encargamos de describir cada uno de estos principios, de modo tal de comprender su importancia. Hemos visto como más allá del tipo de amenaza u ataque perpetrado contra un recurso cualquiera de información, este afecta indefectiblemente alguno de estos principios, todos o cualquier tipo de combinación entre ellos. Es por eso, que así como es posible identificar tres principios fundamentales de seguridad, también lo es identificar sus opuestos referidos como: Revelación (Disclosure), Modificación (Alteration) y Destrucción/Interrupción (Destruction/Disruption).

Una vez más, es importante recordar, que generalmente cuando se evalúa el daño producido por la concreción de una amenaza sobre un activo, dicha evaluación con frecuencia es realizada teniendo en cuenta el impacto causado sobre su confidencialidad, integridad y disponibilidad, a manos de algún

tipo de ataque que revela, altera, destruye o interrumpe.

La información y los sistemas de procesamiento, por un lado, y los sistemas de comunicaciones y las redes que le brindan apoyo son importantes recursos de toda empresa moderna. Hoy en día son esenciales para el normal desenvolvimiento de las tareas, es decir, si una empresa no tiene información se paraliza, piense que sucede si se corta el acceso a Internet en una empresa moderna, los usuarios, especialmente los gerentes, comienzan a impacientarse, porque no pueden enviar y recibir sus correos electrónicos, o porque no pueden consultar las últimas noticias de los mercados en la WEB, estos ejemplos bastan para darnos una idea de cuan necesaria es la información, entonces cuánto más necesaria es la seguridad de la información para garantizar que la empresa siga funcionando.

Los medios técnicos nos brindan un nivel de seguridad limitado, y debe ser respaldado por una gestión y procedimientos adecuados, es decir, la administración de la seguridad de la información, que exige la participación de todos los empleados de la organización y en algunos casos también puede requerir la participación de proveedores, clientes y accionistas. Asimismo, puede solicitarse el asesoramiento experto de organizaciones externas para garantizar un nivel de seguridad adecuado para nuestra organización.

La gran dependencia de las organizaciones actuales, respecto de los sistemas y servicios de información, denota que son más vulnerables a las amenazas concernientes a la seguridad. La interconexión de las redes públicas y privadas y el uso compartido de los recursos de información, incrementa la dificultad de lograr el control de los accesos. La tendencia hacia el procesamiento distribuido ha debilitado la eficacia del control técnico centralizado.

Por otro lado, encontramos gente ansiosa, dispuesta y calificada para tomar ventaja de cada debilidad en la seguridad, y continuamente descubrir y explotar nuevas debilidades.

Los millones de personas que participan en la liberalidad de la red no son conscientes de la realidad, como ejemplo presentamos a continuación algunos indicadores:

- El número de vulnerabilidades de los sistemas de información que se han comunicado a la base de datos Buqtraq se ha cuadruplicado desde el inicio de 1998
- El comité editorial conocido como "Common Vulnerabilities and Exposures" (CVE), formado por 20 organizaciones relacionadas con la seguridad, incluyendo fabricantes de software de seguridad e instituciones académicas, han publicado, en 1999, más de 1000 vulnerabilidades maduras y bien conocidas en la lista CVE
- El Instituto de Seguridad Informática (Computer Security Institute) y el FBI investigaron conjuntamente 643 casos de infracciones de seguridad informática realizadas contra empresas de los EE.UU., agencias estatales, instituciones financieras, centros médicos y universidades, comprobando que el 90% de las entidades analizadas habían sufrido ataques informáticos en el último año. 273 organizaciones informaron pérdidas financieras por este tema que ascendían a 270 millones de dólares ("2000 Computer Crime y Security Survey")

1.1.7 Seguridad en Internet

Intentar comunicar un secreto en un entorno con millones de testigos potenciales como Internet es difícil, y la probabilidad de que alguien escuche una conversación entre dos interlocutores se incrementa conforme lo hace la distancia que las separa. Dado que Internet es verdaderamente global, ningún secreto de valor debería ser comunicado a través de ella sin la ayuda de la criptografía.

En el mundo de los negocios, información como números de tarjetas de crédito, autenticaciones de

clientes, correos electrónicos e incluso llamadas telefónicas acaba siendo enrutada a través de Internet. Ya que gran parte de esta información corporativa no debe ser escuchada por terceras personas, la necesidad de seguridad es obvia.

Sin embargo, la Seguridad en Internet no es sólo una preocupación empresarial. Toda persona tiene derecho a la privacidad y cuando ésta accede a Internet su necesidad de privacidad no desaparece. La privacidad no es sólo confidencialidad, sino que también incluye anonimato. Lo que leemos, las páginas que visitamos, las cosas que compramos y la gente a la que hablamos representan información que a la mayoría de las personas no les gusta dar a conocer. Si las personas se ven obligadas a exponer información que normalmente desean ocultar por el hecho de conectarse a Internet, probablemente rechazarán todas las actividades relacionadas con la red.

Implementar la seguridad en el nivel de red tiene muchas ventajas. La primera de todas es que las cabeceras impuestas por los distintos protocolos son menores ya que todos los protocolos de transporte y de aplicación pueden compartir la infraestructura de gestión de claves provista por esta capa. La segunda sería que pocas aplicaciones necesitarían cambios para utilizar la infrastructura de seguridad, mientras que si la seguridad se implementara en capas superiores cada aplicación o protocolo debería diseñar su propia infrastructura. Esto resultaría en una multiplicación de esfuerzos, además de incrementar la probabilidad de existencia de fallos de seguridad en su diseño y codificación.

La desventaja principal de implementar la seguridad en la capa de red es la dificultad de resolver problemas como el de la imposibilidad de repudio o la autorización del usuario, ciertos mecanismos de seguridad extremo a extremo -en los routers intermedios no existe el concepto de "usuario", por lo que este problema no podría darse.

Los tipos de agresión a la seguridad de un sistema de computadores o de redes se caracterizan mejor observando la función del sistema como proveedor de información. En general, existe un flujo de información desde un origen, como puede ser un fichero o una región de memoria principal, a un destino, como otro fichero o un usuario.

Hay cuatro tipos de agresión:

- Interrupción: un recurso del sistema se destruye o no llega a estar disponible o se inutiliza. Ésta es una agresión de disponibilidad. Ejemplos de esto son la destrucción de un elemento hardware (un disco duro), la ruptura de una línea de comunicación o deshabilitar el sistema de gestión de ficheros.
- Intercepción: un ente no autorizado consigue acceder a un recurso. Ésta es una agresión a la confidencialidad. El ente no autorizado puede ser una persona, un programa o un computador. Ejemplos de agresiones a la confidencialidad son las intervenciones de las líneas para capturar datos y la copia ilícita de ficheros o programas.
- Modificación: un ente no autorizado no solamente gana acceso si no que deteriora el recurso. Ésta es una agresión a la integridad. Algunos ejemplos son los cambios de valores en un fichero de datos, alterando un programa para que funcione de una forma diferente, y modificando el contenido de los mensajes que se transmiten en una red.
- Fabricación: una parte no autorizada inserta objetos falsos en el sistema. Esta es una agresión a la autenticidad. Un ejemplo sería la incorporación de registros a un fichero.

Ataques pasivos: Las agresiones pasivas son el tipo de las escuchas o monitorizaciones ocultas de las transmisiones. La meta del oponente es obtener información que está siendo transmitida. Existen dos tipos de agresiones: divulgación del contenido de un mensaje o análisis del tráfico.

La divulgación del contenido de un mensaje se entiende fácilmente. Una conversación telefónica, un mensaje de correo electrónico o un fichero transferido pueden contener información sensible o confidencial. Así, sería deseable prevenir que el oponente se entere del contenido de estas

transmisiones.

El segundo tipo de agresión pasiva, el análisis del tráfico, es más sutil. Suponga que tenemos un medio de enmascarar el contenido de los mensajes u otro tipo de tráfico de información, aunque se capturan los mensajes, no se podría extraer la información del mensaje. La técnica más común para enmascarar el contenido es el cifrado. Pero incluso si tenemos protección de cifrado, el oponente podría ser capaz de observar los modelos de estos mensajes. El oponente podría determinar la localización y la identidad de los computadores que se están comunicando y observar la frecuencia y la longitud de los mensajes intercambiados. Esta información puede ser útil para extraer la naturaleza de la comunicación que se está realizando.

Las agresiones pasivas son muy difíciles de detectar ya que no implican la alteración de los datos. Sin embargo, es factible impedir el éxito de estas agresiones. Así, el énfasis para tratar estas agresiones está en la prevención antes que la detección.

Ataques activos: La segunda categoría de agresiones es la de las agresiones activas. Estas agresiones suponen la modificación del flujo de datos o la creación de flujos falsos y se subdivide en 4 categorías: enmascaramiento, repetición, modificación de mensajes y denegación de un servicio.

Un enmascaramiento tiene lugar cuando una entidad pretende ser otra entidad diferente. Una agresión de enmascaramiento normalmente incluye una de las otras formas de agresión activa. Por ejemplo, se puede captar una secuencia de autentificación y reemplazarla por otra secuencia de autentificación válida, así se habilita a otra entidad autorizada con pocos privilegios a obtener privilegios extras suplantando a la entidad que los tiene.

La repetición supone la captura pasiva de unidades de datos y su retransmisión subsiguiente para producir un efecto no autorizado.

La modificación de mensajes significa sencillamente que alguna porción de un mensaje legítimo se altera, o que el mensaje se retrasa o se reordena para producir un efecto no autorizado.

La denegación de un servicio impide o inhibe el uso o gestión normal de las facilidades de comunicación. Esta agresión puede tener un objetivo específico: por ejemplo, una entidad puede suprimir todos los mensajes dirigidos a un destino particular. Otro tipo de denegación de servicio es la perturbación sobre una red completa, deshabilitándola o sobrecargándola con mensajes de forma que se degrade su rendimiento.

Las agresiones activas presentan características opuestas a las agresiones pasivas. Mientras que una agresión pasiva es difícil de detectar, existen medidas disponibles para prevenirlas. Por otro lado, es bastante difícil prevenir una agresión activa, ya que para hacerlo se requeriría protección física constante de todos los recursos y de todas las rutas de comunicación. Por consiguiente, la meta es detectarlos y recuperarse de cualquier perturbación o retardo causados por ellos. Ya que la detección tiene un efecto disuasivo, también puede contribuir a la prevención.

1.1.8 Computer Crime y Delito Informático

Cuando hablamos de crimen relacionado con computadoras o “Computer Crime”, generalmente nos referimos a toda actividad criminal, donde una computadora o red de computadoras se encuentra involucrada ya sea como herramienta, objetivo o sitio para un crimen. Desde este punto de vista y en líneas generales, a menudo los crímenes suelen agruparse de acuerdo a sus características, en uno de los tres grupos dispuestos a continuación:

- Computer Assisted Crime: Crímenes cometidos utilizando una computadora (Fraude, Pornografía Infantil, etc.)
- Computer Specific / Targeted Crime: Crímenes cometidos contra una computadora, red o

sistema (DoS, Attacking passwords, etc.)

- Computer is Incidental: Computadora incidental al crimen (Listado del Clientes para un traficante)

Si bien muchos de los crímenes relacionados con computadoras, son novedosos y específicos, otros no son más que la evolución de crímenes para los cuales únicamente a cambiado el medio. De este modo por ejemplo, delitos comunes como el fraude han visto en la utilización de la computación y las redes de datos, el ámbito ideal donde potenciarse.

Para comprender el porque de la tendencia al alza en cuanto a los crímenes relacionados con computadoras, basta con revisar el rol que estas desempeñan hoy en día a nivel mundial. La información es considerada uno de los activos mas valiosos, esta es generada, manipulada y almacenada por medio de computadoras, pequeños dispositivos y redes de datos mientras que coincidentemente, las organizaciones se vuelven cada vez mas dependiente de los sistemas y servicios de información, por tanto no existe motivo por el cual pensar que estos datos pasarían desapercibidos por aquellos que buscan algún tipo de rédito en la concreción de un crimen.

El desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La cuantía de los perjuicios así ocasionados es a menudo muy superior a la usual en la delincuencia tradicional y también son mucho más elevadas las posibilidades de que no lleguen a descubrirse o castigarse. Delito informático, crimen cibernético o crimen electrónico, se refiere a actividades ilícitas realizadas por medio de ordenadores o del Internet o que tienen como objetivo la destrucción y el daño de ordenadores, medios electrónicos y redes de Internet. Sin embargo, las categorías que definen un delito informático son aún mayores y complejas y pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados. Con el desarrollo de la programación y de Internet, los delitos informativos se han vuelto más frecuentes y sofisticados. Existe una amplia gama de actividades delictivas que se realizan por medios informáticos: ingreso ilegal a sistemas, intercepción ilegal de redes, interferencias, daños en la información (borrado, deterioro, alteración o supresión de data), mal uso de artefactos, chantajes, fraude electrónico, ataques a sistemas, robo de bancos, ataques realizados por Hackers, violación de los derechos de autor, pornografía infantil, pedofilia en Internet, violación de información confidencial y muchos otros.

El delito informático incluye una amplia variedad de categorías de crímenes. Generalmente este puede ser dividido en dos grupos:

- Crímenes que tienen como objetivo redes de computadoras, por ejemplo, con la instalación de códigos, gusanos y archivos maliciosos (Spam), ataque masivos a servidores de Internet y generación de virus.
- Crímenes realizados por medio de ordenadores y del Internet, por ejemplo, espionaje por medio del Internet, fraudes y robos, pornografía infantil, pedofilia Internet, etc.

Un ejemplo común es cuando una persona comienza a robar información de websites o causa daños a redes de computadoras o servidores. Estas actividades pueden ser absolutamente virtuales, porque la información se encuentra en forma digital y el daño aunque real no tiene consecuencias físicas distintas a los daños causados sobre los ordenadores o servidores. En algunos sistemas judiciales la propiedad intangible no puede ser robada y el daño debe ser visible. Un ordenador puede ser fuente de evidencia y, aunque el ordenador no haya sido directamente utilizado para cometer el crimen, es un excelente artefacto que guarda los registros, especialmente en su posibilidad de codificar la data. Esto ha hecho que la data codificada de un ordenador o servidor tenga el valor absoluto de evidencia ante cualquier corte del mundo.

En todo delito de los llamados informáticos, hay que distinguir el medio y el fin. Para poder encuadrar

una acción dolosa o imprudente dentro de este tipo de delitos, el medio por el que se cometan debe ser un elemento, bien o servicio, patrimonial del ámbito de responsabilidad de la informática, y el fin que se persigue debe ser la producción de un beneficio al sujeto o autor del ilícito; una finalidad deseada que causa un perjuicio a un tercero.

A grandes rasgos, los delitos que de forma más frecuente se cometen en un medio tan ilimitado como es Internet son:

- Vulneración de la intimidad de las personas, invadiendo por ejemplo los correos electrónicos o interceptando el envío de documentos.
- Alteración, destrucción en datos, programas o documentos electrónicos ajenos. En este tipo delictivo se incluirían conductas como, por ejemplo, los actos de sabotaje contra soportes electrónicos, o la introducción de virus electrónicos para causar daños.
- El espionaje industrial informático, previsto con el fin de proteger los secretos empresariales.
- Las estafas informáticas, en las que se utiliza Internet como medio de comunicación anónimo: es un lugar ideal para cometer este tipo de delitos.
- La pornografía infantil, que se ha visto favorecida precisamente por ese anonimato que proporciona la red.
- Las injurias y las calumnias. Generalmente se cometen en foros o por correo electrónico.
- Los delitos contra la propiedad industrial e intelectual. Internet se muestra como un medio de lo más propicio para vulnerar los derechos de autor mediante, por ejemplo, la reproducción sin permiso de los contenidos que configuran una página web.

¿Quiénes cometen delitos informáticos? Las personas que cometen los "Delitos Informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los personas que tienen destreza para el manejo de computadoras y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos. Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que "entra" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes. Los delincuentes de la informática son tan diversos como sus delitos; puede tratarse de estudiantes, terroristas o figuras del crimen organizado. Estos delincuentes pueden pasar desapercibidos a través de las fronteras, ocultarse tras incontables «enlaces» o simplemente desvanecerse sin dejar ningún documento de rastro.

Los indicadores anteriores, nos han permitido conocer algunos datos generales respecto de la tecnología y sus problemas de seguridad asociados. Lo cierto es que cada nueva implementación de sistemas y tecnología, presupone riesgos. Parte del propósito de este capitulo, no es otro que el de formar profesionales que comprendiendo dichos riesgos, sean capaces de plantear estrategias eficaces con el fin de minimizar el mismo, afectando lo menos posible el propósito original para el cual dichos sistemas o tecnologías fueron creadas.

Un aspecto que a menudo es pasado por alto, radica en el hecho de que l**a seguridad debe ser incumbencia de todos y no tan solo de los especialistas**. Esto no solo es aplicable dentro de las organizaciones, sino que también debería serlo en relación al individuo como parte activa de la sociedad de la información.

La dependencia respecto de los sistemas de información a la cual nos refiriéramos anteriormente, provoca que por ejemplo el eventual ataque a los sistemas de un banco, no solo pueda impactar

negativamente en su propio negocio, sino que a su vez probablemente existan cientos de clientes que producto de dicho ataque, hayan visto comprometida por ejemplo su confidencialidad o privacidad. Del mismo modo, cuando un proveedor de software no toma en serio la seguridad de sus productos, deberíamos comprender que las implicancias de este tipo de asuntos, podría inclusive tener impacto a niveles de seguridad nacional, puesto que los gobiernos, al igual que cualquier organización del ámbito privado, a menudo utiliza en diferentes ámbitos el mismo software que el resto de las organizaciones. Que sucedería por ejemplo, si se distribuyera un nuevo gusano en condiciones de explotar una nueva vulnerabilidad en alguno de los sistemas operativos utilizados en el servicio de asistencia 911? cual sería el impacto de dicho servicio inoperable por horas o días?

En un mundo globalizado y altamente dependiente de la tecnología, todos debemos entender nuestro grado de responsabilidad respecto de los temas de seguridad de la información. Algunos desde posiciones de estado, otros desde la visión del profesional calificado en tareas relativas a seguridad de la información y otro tan solo como simples usuarios y/o consumidores de sistemas y tecnología.

Las infracciones de seguridad afectan a las organizaciones de diversas formas. Con frecuencia, tienen los resultados siguientes:

- Pérdida de beneficios
- Perjuicio de la reputación de la organización
- Pérdida o compromiso de la seguridad de los datos
- Interrupción de los procesos empresariales
- Deterioro de la confianza del cliente
- Deterioro de la confianza del inversor
- Consecuencias legales: en muchos estados o países, la incapacidad de proteger un sistema tiene consecuencias legales; un ejemplo es Sarbanes Oxley, HIPAA, GLBA, California SB 1386.

Las infracciones de seguridad tienen efectos de gran repercusión. Cuando existe una debilidad en la seguridad, ya sea real o sólo una percepción, la organización debe emprender acciones inmediatas para garantizar su eliminación y que los daños queden restringidos.

Muchas organizaciones tienen ahora servicios expuestos a los clientes, como los sitios Web. Los clientes pueden ser los primeros en observar el resultado de un ataque. Por lo tanto, es esencial que la parte de una compañía que se expone al cliente sea lo más segura posible.

1.2.1 ESCENARIO Y ELEMENTOS CLAVES

El trabajo en el área de seguridad de la información, no es nada fácil. La información sobre debilidades y vulnerabilidades en la mayoría de los sistemas comerciales son conocidas y están bien documentadas. Nuestros adversarios pueden utilizar motores de búsqueda para encontrar vulnerabilidades para virtualmente cualquier producto o sistema operativo. Se pueden comprar libros sobre Hacking de sistemas, o unirse a newsgroups en Internet y acceder a sitios web donde se detalla cómo explotar las debilidades de los sistemas. En muchas situaciones, se encontrará luchando con debilidades propias de los productos que está utilizando. Un buen consejo, debería asumir que su red está bajo ataque ahora mismo, mientras lee este libro.

Desde la perspectiva del profesional de la computación, el responsable se está enfrentando con situaciones que son mucho mayores que la simple protección contra virus informáticos. Está protegiendo muchos de los activos más importantes de la empresa de personas que están altamente motivadas para abusar de estos activos, des afortunadamente algunas de estas personas pueden

estar dentro de la organización.

Es muy importante que una organización realice un examen consciente de su actual situación respecto a la seguridad, este análisis permitirá tomar acciones en caso que el resultado indique que se encuentra en una situación comprometida. El examen implica los siguientes pasos:

- Identificación de activos
- Evaluación de vulnerabilidades
- Identificación de amenazas
- Estimación de los riesgos

Estas cuatro acciones le ayudarán a identificar cuales recursos vale la pena proteger, y a valorizarlos, debido a que algunos son más importantes que otros, además esta evaluación le ayudará a la hora de definir los recursos económicos y humanos destinados para su protección.

1.2.2 Activos

Cada organización tiene activos y recursos valiosos. La identificación de activos es el proceso por medio del cual una compañía intenta valuar la información y sus sistemas. En algunos casos, es tan simple como contabilizar las licencias de software; estas valuaciones de activos físicos son parte de un proceso de contabilización normal que una empresa debería realizar en forma rutinaria. La parte más dificultosa del proceso de identificación de activos es intentar asignarle un valor a la información. En algunos casos, podría ayudarnos si intentamos determinar qué sucedería en caso que la información se pierda o se vuelva no disponible. Si la ausencia de esta información provoca que el negocio se detenga, esta información es muy valiosa y se podrá valuar según el costo que le provoque a la empresa esta detención.

Es importante identificar todos los recursos de la red que podían verse afectados por un problema de seguridad. Podemos mencionar los siguientes ejemplos de activos asociados a sistemas de información:

Confidencialidad

- ***Recursos de información***: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, disposiciones relativas a sistemas de emergencia para la reposición de información perdida ("fallback"), información archivada.
- ***Recursos de software***: software de aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios.
- ***Activos físicos***: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PABXs, máquinas de fax, contestadores automáticos), medios magnéticos (cintas y discos), otros equipos técnicos (suministro de electricidad, unidades de aire acondicionado), mobiliario, lugares de emplazamiento.
- ***Servicios***: servicios informáticos y de comunicaciones, utilitarios generales, por ej., calefacción, iluminación, energía eléctrica, aire acondicionado.
- ***Recursos humanos.***

1.2.3 Vulnerabilidades

Probablemente las capacidades de seguridad del software y los sistemas utilizados en la organización es el área de mayor interés para el especialista de seguridad. A través del estudio de estas capacidades, podrá detectar las vulnerabilidades y fortalecer el sistema antes que los malintencionados se aprovechen.

Hasta hace poco tiempo, muchos desarrolladores de sistemas operativos no prestaban especial atención a las características de seguridad. Por ejemplo, un sistema operativo muy popular utiliza un esquema de seguridad que descansa en un logon y password, pero cuando aparece el mensaje de logon, en lugar de ingresar las credenciales, todo lo que tiene que hacer es un click sobre el botón Cancelar y el sistema le permitirá utilizar la mayoría de las capacidades de red y acceso local a todos los recursos. Esto es peor que no tener seguridad, porque muchos usuarios pensando en estas características supondrán que tienen un sistema seguro. Esto no es así, y como resultado ocurren muchos hurtos de información.

También encontramos vulnerabilidades en los protocolos, por ejemplo, el protocolo TCP/IP (Transfer Control Protocol/Internet Protocol) utilizado por la mayoría de las redes corporativas, fue diseñado para permitir comunicaciones en un ambiente confiable. Mientras es muy robusto en su manejo de errores, es por naturaleza inseguro. Por esta razón muchos ataques modernos ocurren a través del protocolo TCP/IP (En la Unidad 5 - Ataques y Contramedidas, se tratan los aspectos de seguridad relativos a este protocolo).

Los sistemas operativos y programas de aplicación han sido vulnerables a ataques internos y externos por mucho tiempo. Las compañías de software quieren vender software que sea fácil de utilizar, con interfaces gráficas, y fácilmente configurables. Los usuarios quieren lo mismo. Desafortunadamente, esta facilidad de uso y configuración generalmente crea problemas de seguridad adicionales. Por ejemplo, uno de los productos más populares en la actualidad permite que los e-mails y attachments puedan ejecutar programas embebidos en un mensaje. Esto permite crear mensajes de e-mail con fantásticas presentaciones, pero también permite que los mensajes puedan llevar virus que pueden dañar la computadora y desparramarse hacia otras redes. El desarrollador de este software ha desarrollado una actualización de seguridad, pero se observa que cada vez que se introduce una actualización, alguien encuentra una forma de saltearla.

Este problema se ha vuelto de tanta importancia que los desarrolladores han puesto a disposición de los clientes soporte de seguridad on-line. En el pasado, se ocultaban las vulnerabilidades, pensando que ayudaba a la seguridad del software; hoy en día se hacen públicas y se proveen las soluciones tan pronto como se descubren las vulnerabilidades. Esto, por otro lado, también ayuda a los Hackers quienes conocen que estos cambios no serán realizados en muchos sistemas por un tiempo. Es decir, el progreso hasta ahora ha sido la peor pesadilla del experto en seguridad, pero hay esperanzas que esto cambie en el futuro porque muchos desarrolladores de sistemas están replanteando las medidas de seguridad, porque han reconocido que los productos que entregan no pueden proteger a las organizaciones que los utilizan de la pérdida de datos o abusos.

1.2.4 Identificar las Amenazas a la seguridad

Una vez identificados los recursos que necesitan protección, deberá identificar cuáles son las amenazas a estos recursos, y poder determinar qué potencial de daño o pérdida existe. Por otro lado, deberá determinar de cuáles amenazas tratará de proteger a los recursos en función de la probabilidad de ocurrencia.

La implementación de una política de seguridad requiere que no solo se evalúen las amenazas, sino también el origen, así tendremos amenazas externas e internas. Por ejemplo, será poco provechoso implementar un ambiente de alta seguridad para proteger la empresa de los usuarios del exterior, si las amenazas provienen principalmente del interior. Si un miembro de nuestro grupo trae un diskette

con un documento que contiene un virus y lo abre en la PC de la oficina, el virus podría expandirse a través de toda la red, para este caso no hubieran servido de nada las mejores medidas de seguridad externas. Este es un problema muy común en las escuelas, y ambientes donde las personas utilizan recursos compartidos.

Entre las amenazas más comunes podemos encontrar, el eavesdropping o packet sniffing, acceso no autorizado, denegación de servicio, fraude y alteración de datos.

El modelo **STRIDE** de Microsoft proporciona una estructura para identificar las amenazas y los posibles puntos débiles:

TIPOS DE AMENAZAS	EJEMPLOS
Suplantación	• Falsificar mensajes de correo electrónico • Reproducir paquetes de autenticación
Alteración	• Reproducir paquetes de autenticación • Alterar datos durante la transmisión • Cambiar datos en archivos
Repudio	• Eliminar un archivo esencial y denegar este hecho • Adquirir un producto y negar posteriormente que se ha adquirido
Divulgación de información	• Exponer la información en mensajes de error • Exponer el código de los sitios Web
Denegación de servicio	• Inundar una red con paquetes de sincronización • Inundar una red con paquetes ICMP falsificados
Elevación de privilegios	• Explotar la saturación de un búfer para obtener privilegios en el sistema • Obtener privilegios de administrador de forma ilegítima

- La suplantación de identidades es la capacidad de obtener y usar la información de autenticación de otro usuario. Un ejemplo de suplantación de identidad es la utilización del nombre y la contraseña de otro usuario.
- La alteración de datos implica su modificación. Un ejemplo sería alterar el contenido del cookie de un cliente.
- El repudio es la capacidad de negar que algo ha ocurrido. Un ejemplo de repudio sería que un usuario cargue datos dañinos en el sistema cuando en éste no se puede realizar un seguimiento de la operación.
- La divulgación de información implica la exposición de información ante usuarios que se supone que no deben disponer de ella. Un ejemplo de divulgación de información es la capacidad de un intruso para leer archivos médicos confidenciales a los que no se le ha otorgado acceso.
- Los ataques de denegación de servicio privan a los usuarios del servicio normal. Un ejemplo de denegación de servicio consistiría en dejar un sitio Web inaccesible al inundarlo con una cantidad masiva de solicitudes HTTP.
- La elevación de privilegios es el proceso que siguen los intrusos para realizar una función que no tienen derecho a efectuar. Para ello, puede explotarse una debilidad del software o usar las credenciales de forma ilegítima.

Otros ataques podrían ser llevados a cabo únicamente con el propósito de que el sistema de destino incurra en gastos. Por ejemplo, se podría montar un ataque contra un servicio de fax o un teléfono celular para hacer un gran número de llamadas internacionales que supongan un gran costo.

1.3.1 RIESGO Y CONTROL

"Paso gran parte del tiempo volando alrededor del mundo y conversando con empresarios y profesionales de TI acerca de la seguridad de la información. Jamás dejo de asombrarme cuando escucho que algunos "expertos en seguridad", que cobran más de lo que deberían, pasan horas detallando cuán compleja es la seguridad. No lo es. La seguridad puede resumirse en dos palabras simples: Gestión de riesgos. No se trata de la eliminación de riesgos, se trata de la mitigación de riesgos."

Kai Axford, CISSP, Estratega en Seguridad Senior de Microsoft Trustworthy Computing Group

Los requerimientos a cubrir en el área de seguridad se identifican mediante una evaluación metódica de los riesgos de seguridad. Las erogaciones derivadas de la satisfacción de las necesidades de control deben ser equilibradas con respecto al impacto potencial de las fallas de seguridad en los negocios.

La evaluación de riesgos es una consideración sistemática de los siguientes puntos:

- impacto potencial de una falla de seguridad en los negocios, teniendo en cuenta las potenciales consecuencias por una pérdida de la confidencialidad, integridad o disponibilidad de la información y otros recursos.
- probabilidad de ocurrencia de dicha falla tomando en cuenta las amenazas y vulnerabilidades predominantes, y los controles actualmente implementados.

Los resultados de esta evaluación ayudarán a orientar y a determinar las prioridades y acciones de gestión adecuadas para la administración de los riesgos concernientes a seguridad de la información, y para la complementación de los controles seleccionados a fin de brindar protección contra dichos riesgos y reducirlos a un nivel aceptable.

Es importante llevar a cabo revisiones periódicas de los riesgos de seguridad y de los controles implementados a fin de:

- reflejar los cambios en los requerimientos y prioridades de la empresa;
- considerar nuevas amenazas y vulnerabilidades;
- corroborar que los controles siguen siendo eficaces y apropiados.

El análisis de riesgos implica determinar lo siguiente:

- ***Qué necesita proteger:*** Evaluación de los activos y su importancia
- ***De quién debe protegerlo***: Evaluación de amenazas y vulnerabilidades
- ***Cómo protegerlo:*** Evaluación de contramedidas

Los riesgos se pueden clasificar por el nivel de importancia y por la severidad de la pérdida. Esta valorización es muy útil, porque no debería llegar a una situación donde gasta más para proteger aquello que es menos valioso o aquello donde el costo de recuperarlo es inferior al de la pérdida.

Entre los factores que tenemos que considerar para realizar una correcta evaluación del riesgo,

encontramos:

- El riesgo de pérdida del recurso, que dependerá de las amenazas a las que está expuesto, las contra medidas implementadas para protegerlo y sus vulnerabilidades asociadas. Es un arte que depende del conocimiento y experiencia del evaluador.
- La importancia que representa el recurso para la empresa, evaluada según cada tipo, de acuerdo a los siguientes factores:
    - **Disponibilidad**: es la medida de qué tan importante es tener el recurso disponible todo el tiempo.
    - **Integridad**:es la medida de cuán importante es que el recurso o los datos del mismo sean consistentes. Esto es de particular trascendencia para los recursos de bases de datos.
    - **Confidencialidad**: es la medida de cuán importante es que los recursos sólo sean observados por las personas autorizadas.

1.3.2 Evaluación del riesgo de un recurso

Las técnicas de evaluación de riesgos pueden aplicarse a toda la organización, o sólo a partes de la misma, así como a los sistemas de información individuales, componentes de sistemas o servicios específicos cuando esto resulte factible, viable y provechoso. Vamos a presentar una técnica matemática para determinar el riesgo asociado a un recurso. Este es sólo un método entre muchos, cuál es el mejor de todos lo decidirá usted mismo a través de la experiencia.

Necesitaremos determinar los siguientes factores:

- Estimación del riesgo de pérdida del recurso (Ri)
- Estimación de la importancia del recurso (Wi)

Para realizar la cuantificación del riesgo de perder un recurso, podremos asignarle un valor numérico. Por ejemplo, al riesgo (Ri) de perder un recurso se le asigna un valor de cero a diez, donde cero indica que no hay riesgo y diez es el riesgo más alto. Este valor dependerá de los tipos de amenazas a las que está expuesto el recurso, de las contra medidas implementadas actualmente y de las vulnerabilidades conocidas. De manera similar, también se le puede asignar un valor entre cero y uno a la importancia que representa el recurso para la empresa (Wi), donde cero significa que no tiene importancia y uno la importancia más alta.

La evaluación general del riesgo (WRi) de cada recurso será entonces el producto numérico del valor del riesgo y su importancia. Es decir, WRi = Ri * Wi. También podemos calcular el riesgo general de la red, de la siguiente manera: WR = S (WRi) / S (Wi).

Supongamos, como ejemplo, una red simplificada con un router, un servidor y un bridge.

Los administradores de la red y de sistemas han producido las estimaciones siguientes para el riesgo y la importancia de cada uno de los dispositivos que forman nuestra red: Como se ve, a cada uno de los componentes del sistemas, se le ha asignado un cierto riesgo y una cierta importancia. Hay que destacar que estos valores son totalmente subjetivos, dependen exclusivamente de quien ó quienes están realizando la evaluación. Tenemos, entonces:

Router: R1 = 6

W1 = 7

Bridge: R2 = 6

W2 = 3

Servidor: R3 = 10

W3 = 10

El cálculo de los riesgos evaluados, será, para cada dispositivo:

Router: **WR1 = R1 * W1** = 6 * 7 = 42

Bridge: **WR2 = R2 * W2** = 6 * 3 = 1.8

Servidor: **WR3 = R3 * W3** = 10 * 10 = 100

La tabla que sigue a continuación, nos muestra cómo podríamos llevar a cabo esta tarea de una manera ordenada y los valores que contiene son los que hemos tratado:

Recurso del sistema		**Riesgo (Ri)**	**Importancia (Wi)**	**Riesgo evaluado (Ri * Wi)**
Número	**Nombre**			
1	Router	6	7	42
2	Bridge	6	3	18
3	Servidor	10	10	100

Vemos que, en este caso, el recurso que debemos proteger más es el Servidor ya que su riesgo ponderado es muy alto. Por tanto, comenzaremos por buscar las probables causas que pueden provocar problemas con los servicios brindados por él. Hay que tener muy en cuenta que, al realizar el análisis de riesgo,se deben identificar **todos** los recursos (por más triviales que parezcan) cuya seguridad está en riesgo de ser quebrantada. Ahora bien, ¿cuáles son los recursos? Los recursos que deben ser considerados al estimar las amenazas a la seguridad son solamente seis: Hardware, Software, Datos, Gente, Documentación, Accesorios.

Según el estándar ITIL, los servicios deben ser recuperables dentro de Los parámetros convenidos de confidencialidad e integridad.

1.3.3 Objetivos de la Gestión de Riesgo

La gestión del riesgo o “Information Risk Management”, no es otra cosa que el proceso de identificar, analizar, determinar y tratar el riesgo. Dicho proceso se encuentra principalmente compuesto por dos fases claramente definidas, siendo estas las mencionadas a continuación:

1. Análisis de Riesgos (Risk Assessment): Comprende la Identificación de vulnerabilidades y amenazas, el análisis de probabilidad de ocurrencia e impacto y el análisis de las medidas para aceptar, evitar o transferir el riesgo.
2. Tratamiento de Riesgos: Comprende las tareas de priorización, presupuestado, implementación y mantenimiento de medidas seleccionadas para la mitigación de riesgos.

Es importante conocer, que el principal objetivo de todo proceso de Gestión del Riesgo, es el de

reducir los riesgos hasta niveles de tolerancia aceptables para la organización. Cuando hablamos de niveles de tolerancia aceptables, nos referimos a aquel que la propia organización ha definido como aceptable. Puesto que cada organización persigue diferentes objetivos de negocio y a su vez este puede tener distintos requerimientos desde el punto de vista de la seguridad, es muy probable que el nivel que puede ser aceptable para una, pueda no serlo para otra.

Si bien no todos los riesgos a los que se enfrenta una organización se encuentran relacionados con la computación, cuando la gestión de riesgos se centra en seguridad de la información, es posible observar entre otros los siguientes riesgos que es necesario direccionar:

- Daño Físico: Fuego, agua, vandalismo, perdida de energía y desastres naturales.
- Acciones Humanas: Acción intencional o accidental que pueda atentar contra la productividad.
- Fallas del Equipamiento: Fallas del sistema o dispositivos periféricos.
- Ataques Internos o Externos: Hacking, Cracking y/o cualquier tipo de ataque.
- Pérdida de Datos: Divulgación de secretos comerciales, fraude, espionaje y robo.
- Errores en las Aplicaciones: Errores de computación, errores de entrada, buffers overflows

Estas amenazas necesitan ser identificadas, clasificadas por categoría y evaluadas para calcular la magnitud de perdidas potenciales. Si bien es cierto que el riesgo real es difícil de medir, la priorización de los riesgos potenciales, nos permitirá conocer cual de ellos necesita ser tratado en primera instancia.

1.3.4 Preguntas a responder

Muchas veces resulta más sencillo comprender el verdadero alcance de los procesos relacionados con la Gestión del Riesgo, viendo alguno de los componentes intervinientes en el proceso, como una serie de interrogantes que requieren de respuesta:

- *¿Que puede pasar? (Amenaza)*
- *¿Si Pasa, qué tan malo puede ser? (Impacto de la amenaza)*
- *¿Qué tan seguido puede pasar? (Frecuencia de la amenaza)*
- *¿Qué tan seguro estoy de las respuestas anteriores? (Falta de Certeza, Incertidumbre)*
- *¿Qué puedo hacer? (Mitigar el riesgo)*
- *¿Cuanto me costará? (Siempre calculado en forma anualizado)*
- *¿Dicho costo es efectivo? (Relación costo beneficio!)*

Sin dudas esta es una visión simplificada, pero no obstante nos permite observar claramente que tipo de información es la requerida a efectos de conocer el riesgo asociado a cada uno de los activos dispuestos en nuestra organización.

1.3.5 El equipo de Gestión de Riesgo

Ahora que conocemos cual es en líneas generales, el camino a recorrer en lo que a la evaluación de los riesgos se refiere, quizás sea necesario mencionar las características que debe poseer el equipo que se encontrará encargado de llevar adelante este proceso.

Sin embargo, antes es necesario mencionar la importancia de la existencia de una Política de Gestión de Riesgos, que alineada con la Política de Seguridad de la Información y con la Estrategia de la Organización contemple entre otros los siguientes puntos:

- Objetivos
- Definición de niveles aceptables de riesgo
- Procesos de análisis y tratamiento de riesgos
- Metodologías
- Definición de roles y responsabilidades
- Indicadores claves para el monitoreo de los controles implementados para la mitigación del riesgo

Ahora bien, el equipo de gestión del riesgo tiene como objetivo primario, garantizar que la organización se encuentra protegida ante los riesgos, teniendo en cuenta la relación costo-beneficio de la implementación de controles. Este equipo, deberá estar conformado por personal de las áreas sustantivas de la organización incluyendo IT y seguridad de la información.

Sus funciones se encontrarán relacionadas con la proposición y mantenimiento de la Política de Gestión de Riesgos, la redacción de procedimientos, las tareas de análisis de riesgos, la definición de métricas, la capacitación y concientización del personal, la elaboración de documentación y la integración de la Gestión de Riesgos al proceso de control de cambios, de modo tal que su política y procesos relacionados se encuentren siempre actualizados.

1.3.6 Tipos de Análisis de Riesgo

Existen básicamente dos tipos de *approaches* en lo que refiere al "Análisis de Riesgo": "*Cuantitativo*" y "*Cualitativo*".

El análisis de riesgo de tipo "**Cuantitativo**", intenta asignar valores reales y objetivos a cada componente de la evaluación de riesgos y a cada potencial perdida. Estos elementos pueden incluir costo de las contramedidas, valor de los activos, impacto en el negocio, frecuencia de la amenaza, efectividad de las contramedidas, probabilidades de explotación, etc. Cuando todos estos elementos son cuantificados, se dice que el proceso es "Cuantitativo". El análisis "Cuantitativo" provee a su vez porcentajes concretos cuando se trata de determinar la probabilidad de una amenaza. Cada elemento dentro del análisis es cuantificado e ingresado como un operador en ecuaciones, a fin de determinar el riesgo total y el riesgo residual.

Por su parte, el análisis del tipo "**Cualitativo**" utiliza elementos soft de la organización (opinión, mejores prácticas, intuición, experiencia, etc.) para ponderar el riesgo y sus componentes. Este es un modelo basado más bien en escenarios que en cálculos. En vez de asignar el costo exacto de las posibles pérdidas, en este escenario se ponderan en escala, los riesgos, los costos y efectos de una amenaza en relación del activo. Este tipo de procesos, conjuga: juicio, experiencia e intuición. Cada método posee sus ventajas y desventajas. La aplicación de análisis puramente "Cuantitativo", sencillamente no es posible. Principalmente debido a que parte de los ítems que se deberán evaluar como parte del análisis, son "Cualitativos" y por tanto no son certeros en cuanto a valores "Cuantitativos". En contra posición a ello, el análisis de riesgo puramente "Cualitativo" si es posible.

1.3.7 Tratamiento de Riesgo

Una vez concluida la primera fase del proceso de Gestión del Riesgo, y contando con la información arrojada por este proceso, es momento de iniciar la fase de "Tratamiento de Riesgos", que como

mencionáramos anteriormente, incluye las tareas de priorización, presupuestado, implementación y mantenimiento de los controles seleccionados a efectos de mitigar el riesgo. Al momento de analizar las contramedidas o controles, es de suma importancia observar si su relación costo beneficio es aceptable. Habiendo valuado los activos y conociendo el coste de un control determinado deberíamos ser capaces de asegurar que el costo del control no supera el costo del activo que se intenta proteger. Cuando iniciamos un proceso de análisis de controles o contramedidas, puede ser de utilidad conocer cuales son los aspectos a tener en cuenta en la estimación del costo anual de un control:

- *Costo de Adquisición*
- *Costo de diseño y planeamiento*
- *Costo de implementación*
- *Impacto en el entorno (Compatibilidad)*
- *Mantenimiento*
- *Pruebas*
- *Reparación, reemplazo, actualización*
- *Nivel de operación manual requerida*
- *Efectos sobre la productividad*
- *Habilidad de recupero*

Por ultimo, es de suma importancia recordar que una vez identificado, el riesgo puede ser “Mitigado” (por medio de la implementación de contramedidas, controles o salvaguardas), “Transferido” (mediante la adquisición de pólizas de seguro) o “Aceptado” (riesgo aceptable), pero nunca “Rechazado” o “Ignorado”.

1.3.8 Normativa

Por lo general, existe una relación directa entre los objetivos del negocio y las computadoras e información que con ellas es procesada. Debido a la importancia que la información y su procesamiento tiene para toda organización, directores y gerentes deberían hacer de la protección de sus activos de información un punto de máxima prioridad y proveer el soporte, tiempo, fondos y recursos necesarios, a efectos de garantizar que los sistemas, redes e información, se encuentran protegidos de la manera mas lógica posible (costo/beneficio).

Para que el plan de seguridad de una compañía sea implementado en forma exitosa, este necesita ser de incumbencia de la alta gerencia de la organización, definitivamente no debe circunscribirse al área de IT o al área de seguridad, y debe ser tratado con un enfoque del tipo TopDown. Esto significa que debe nacer o surgir desde los niveles más altos, pero ser útil y funcional en cada nivel dentro de la organización.

La gerencia debería comprender las regulaciones, leyes y responsabilidades que le afectan directa o indirectamente, así como también ser capaz de definir que necesita ser protegido y que no. Al mismo tiempo estos necesitan determinar que es lo que se espera del empleado en relación con la seguridad de la información y que consecuencias deberían asumir en caso de no cumplir con las normativas establecidas. Estas decisiones deberían ser tomadas por quienes de acuerdo a la posición que ocupan dentro de la organización, son considerados “el ultimo responsable”, en caso de que algo salga mal.

Un programa de seguridad, contiene todas y cada una de las piezas necesarias para proporcionar protección a la organización. A fin de proveer la coordinación necesaria para que estas piezas funcionen del modo esperado. Un programa de seguridad debe incluir políticas, procedimientos,

estándares, guidelines, baselines, un programa de concientización de usuarios, un plan de respuesta a incidentes, un programa de compliance, etc. El desarrollo de normativa, a menudo requiere de equipos multidisciplinarios. Departamentos de legales y recursos humanos necesitan involucrarse en el desarrollo de alguno de estos puntos, formando parte del equipo encargado del desarrollo de este conjunto de documentos.

1.4.1 CONCEPTOS

1.4.2 Exposición

Solemos referirnos bajo el termino “Exposición”, a la instancia en la cual la información o un activo de información, es susceptible a dañarse o perderse por el accionar de un “agente de amenaza”. La exposición, no significa que el evento que produce la perdida o daño del recurso “este ocurriendo”, solo significa que podría ocurrir dado que existe una amenaza y una vulnerabilidad que esta podría explotar. Una vulnerabilidad, “expone” a una organización a un posible daño. Si la administración de contraseñas en una organización es débil, y no existen reglas que regulen su fortaleza, la organización podría encontrarse expuesta a la posibilidad de que las contraseñas de sus usuarios sean adivinadas o capturadas, y utilizadas de modo no autorizado. Si una organización no realiza revisiones frecuentes, respecto del estado de su cableado eléctrico, y no posee controles efectivos contra incendios en el lugar, se expone a si misma a incendios potencialmente devastadores.

1.4.3 Contramedidas

Un proceso de suma importancia a la hora de asegurar cualquier sistema de información, es la selección de contramedidas. Formalmente, el término “Contramedida” o “Salvaguarda” es utilizado para referirnos a cualquier tipo de medida que permita detectar, prevenir o minimizar el riesgo asociado con la ocurrencia de una amenaza específica. Eventualmente las “Contramedidas” o “Salvaguardas” suelen recibir el nombre de “Controles”.

1.4.4 Hacker, Cracker y Script Kiddies

La concepción que la persona común tiene de los Hacker es alguien que penetra sistemas con el único fin de obtener un beneficio económico o por simple malicia. Según los propios Hackers, ellos son personas que gozan alcanzando un conocimiento profundo sobre el funcionamiento interno de un sistema, de un ordenador o de una red de computadoras, pero sin intenciones de causar daño u obtener un beneficio personal, más allá del reconocimiento dentro de su comunidad. Proclaman defender un sentido ético y una serie de principios contestatarios e inconformistas, pero nunca delictivos.

Cracker o "alguien que rompe", es un término acuñado por los Hackers hacia 1985 para defenderse contra la mala utilización que hacían los periodistas de la palabra Hacker. Los Crackers forman pequeños grupos, secretos y privados, se adentran en el terreno de lo ilegal, que tienen muy poco que ver con la cultura abierta que se describe en el mundo Hacker. Todos los Hackers tienen habilidades de sobra para convertirse en Crackers, pero han resistido la tentación y se mantienen dentro de la legalidad, e incluso rechazan frontalmente a los que se han convertido.

Mucho se ha escrito en la prensa acerca de los Hackers, y en rigor de verdad no todo lo que se lee en los periódicos es cierto. En el sentido si se quiere más romántico, un Hacker es aquella persona a la cual le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas. Ellos ven el Hacking, como un desafió intelectual. Así mismo, con frecuencia se utiliza el neologismo “Hacker”, para referirse a un experto/gurú en varias o alguna rama técnica relacionada con las tecnologías de la información y las telecomunicaciones: (Programación, redes, sistemas

operativos, hardware, etc.)

Lo más correcto sería utilizar definiciones provenientes del *Jargon File*, pero ya que la Wikipedia es un recurso universal utilizado por la mayoría de la gente, adoptaremos su breve definición acerca de lo que es un Hacker: Hacker es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con la informática: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etc. Se suele llamar *hackeo* y *hackear* a las obras propias de un Hacker. Y como muchos ya saben, esta palabra tan controvertida tiene sus orígenes en el MIT (Instituto Tecnológico de Massachussets), donde aparecieron por primera vez esas enormes computadoras que ocupaban habitaciones enteras y utilizaban tarjetas perforadas.

La historia de la informática y las comunicaciones, se encuentra llena de Hackers famosos, a quienes se les debe gran parte del desarrollo de la computación y las comunicaciones. Tim Vinton Cerf (inventor de los protocolos TCP/IP), Dennis Ritchie y Ken Thompson (Creadores de UNIX), Steve Jobs y Steve Wozniak (fundadores de Apple), Linus Torvalds (Desarrollador del primer kernel del sistema operativo GNU/Linux) y muchos otros.

Al margen de lo comentado y a nivel popular, en la actualidad el termino Hacker suele ser utilizado para referirse a los intrusos informáticos, mientras que el termino Cracker suele utilizarse a efectos de identificar a aquellos Hackers que utilizan su conocimiento, con el objeto de dañar sistemas ajenos u obtener algún tipo de rédito de sus acciones. Por lo general, el Cracker se distingue del hacker por sus valores morales. Otro termino que a menudo se relaciona con Hackers y Crackers, es el de Script Kiddies, término utilizado para referirse a aquellos Hackers quienes no poseen el skill necesario para llevar a cabo un ataque específico, sin para ello hacer uso de las herramientas (mayormente automáticas) que descargan de Internet o les son provistas por sus amigos. A menudo, el Script Kiddie no tiene conocimiento de cual es exactamente la vulnerabilidad que explota, ni que es lo que hace la herramienta que utiliza.

Es de suma importancia recalcar, que el Hacking es considerado un delito en muchos países, sin importar si el Hacker tuviera o no intenciones de dañar el sistema objetivo. Del mismo modo, en la literatura tradicional, suele referirse el término de Hacker, relacionado con el intruso que intenta lograr acceso no autorizado a un sistema.

1.4.5 Black Hat, Grey Hat y White Hat

En el indicador anterior, echamos un vistazo a términos como Hackers, Crackers y Script Kiddies. Adicionalmente, existe otra clasificación que a menudo es utilizada para identificar personas relacionadas con el Hacking.

Black Hat, es el término con el que se llama a aquellos quienes comprometen la seguridad de un sistema, sin el permiso de su propietario, usualmente con la intención de lograr acceso no autorizado a las computadoras de la red. Por su parte, el termino White Hat, suele ser utilizado para aquellas personas quienes se encuentran éticamente opuestas al abuso de redes y sistemas. Con frecuencia, los White Hat utilizan sus conocimientos con el objeto de proteger los sistemas de información, ya sea actuando como oficiales de seguridad, o reportando vulnerabilidades a los vendors.

Por ultimo Grey Hat, es el término que la comunidad utiliza para referirse a un Hacker que poseyendo el skill suficiente, algunas veces actúa legalmente (Tal como un White Hat) y otras no. Estos Hackers son un hibrido entre White Hat y Black Hat. Usualmente no hackean con el objetivo de obtener rédito económico, personal o causar algún tipo de daño, pero podrían o no cometer un crimen en el proceso de sus tareas o investigaciones.

1.4.6 Lamer y Wannabe

Lamer es un sinónimo de *Leecher* y de *Luser*, combinación de user (usuario), y looser (perdedor), empleado más frecuentemente entre los Crackers que entre los Hackers. Lo utilizan para hacer

referencia a aquella persona que se aprovecha de los recursos que ofrece la comunidad underground sin aportar nada a cambio. Es el que ingresa a un sitio y comienza a descargarse todas las utilidades, pero nunca desarrolla y sube una.

La comunidad Hacker también ha inventado el término wannabes, para designar a aquellos que podrán llegar a ser un Hacker, pero que aún le falta conocimiento para serlo. Todos los Hackers han pasado por esta etapa. Un Wannabe adquiere el estatus de Hacker cuando los veteranos consideran que ha acumulado méritos suficientes para ser considerado uno de los suyos.

1.4.7 Breve resumen histórico

1878: Menos de dos años después de que el sistema telefónico de Alexander Graham Bell empezara a funcionar, un grupo de adolescentes echó abajo la red.

1958: EE.UU. crea ARPA (Advanced Re search Projects Agency), ciencia y tecnología aplicada al campo militar.

1960: Los Hackers originales utilizaron los primeros mainframes del MIT para desarrollar habilidades y explorar el potencial de la informática. En esa época, Hacker era un término elogioso para los usuarios con un conocimiento exponencial de los ordenadores.

1969: La agencia de proyectos de investigación avanzados del Departamento de Defensa (DoD), construyó Arpanet.

1971: Antes del uso masivo de los ordena dores y de Internet, los phreakers utilizaron la extensa base de redes telefónicas. John Draper (Cap'n Crunch), descubrió que un simple silbato permitía a los usuarios entrar en los sistemas de facturación de las llamadas a larga distancia.

1973: Kahn desarrolla un nuevo protocolo, el TCP/IP (Transmisión Control Protocol/ Internet Protocol).

1976: Dos miembros del Homebrew Com puter Club lanzaron las llamadas blue box, que se utilizaban para Hacker sistemas telefónicos. La pareja (Steve Jobs y Steve Wozniak) con seguirían hacerse famosos después al fundar Apple Computer.

1983: Primer arresto de Hackers por el FBI después de que invadieran el centro de investigación de Los Alamos. Se estrena la película Juegos de guerra , que cambió la percepción del público con relación a los Hackers y estableció su prestigio.

1984: Se funda la publicación trimestral 2600 (nombrada como la frecuencia del silbato de John Draper), que ofrecía una plataforma a los Hackers y phreakers para expresar sus conocimientos y habilidades. Se forma Legion of Doom (LoD).

1987: Herbert Zinn, de 17 años de edad, es arrestado después de entrar en el sistema de AT&T. Los expertos afirman que estuvo a punto de bloquear todo el sistema telefónico norte americano. Se crea el primer virus conocido de MS-DoS, *Brain*. Los investigadores creen que se escribió en Pakistán. Infectaba el sector de arranque de los disquetes de 360 KB.

1988: Robert Morris bloquea 6.000 ordenadores a través de ARPANET con su famoso virus, que lanzó, según sus propias palabras, de forma accidental. Se funda la CERT (Computer Emergency Response Team). Aparece el primer software antivirus, escrito por un desarrollador de Indonesia.

1989: Primer caso de ciberespionaje en Alemania Occidental. The Mentor lanza el manifiesto Conscience of a Hacker , que finaliza con una frase inquietante: pueden detener a una persona, pero no pueden detenernos a todos.

1990: Se lanza el grupo de apoyo Freedom on the Internet . Aparecen sofisticados tipos de virus como los polimórficos (que se modifican a sí mismos cuando se expanden) o los de multipartición (que infectan diversas zonas de una máquina). El First National Citibank de Chicago sufre el primer robo informático reconocido por una cantidad de 70 millones de dólares. El Hacker Dark Dante, Kevin Lee Poulsen, es arrestado después de una búsqueda de 17 meses. Robaba secretos militares. Mitnick y Shimomura miden sus fuerzas.

1993: Se celebra la primera conferencia DefCon de Hacking en Las Vegas. Se suponía que el evento era una celebración única para decir adiós a las BBS (obsoletas por la Web), pero resultó tener tal éxito que se convirtió en un evento anual. DefCon es la conferencia de Hackers más importante del mundo, en la misma se reúnen los Hackers con conocimientos más avanzados con el fin de exponerlos al público, o de aplicarlos en las distintas competiciones que allí se realizan. En sus instalaciones hacen acto de presencia los agentes del FBI con el objetivo de llevarse nuevos fichajes para su plantilla (precisan a los mejores, y saben donde encontrarlos).

No obstante cabe aclarar, que como dijo Julio Cortázar: *la fama es una puta que se viste de verde*, y esta conferencia ha alcanzado tal reconocimiento que algunos Hackers o autodenominados Hackers, ven en ella una oportunidad para darse a conocer y conseguir aprobación entre el numeroso público. Esto es un arma de doble filo, porque tiende a una pérdida total del espíritu Hacker.

1994: Hackers atacan a los sitios web federales de los EE.UU., incluyendo la CIA, el Departamento de Justicia, la NASA y la Fuerza Aérea. No fue la mejor forma de hacerse popular entre los estamentos militares. Vladimir Levin, el legendario líder de un grupo de Hackers ruso, parece ser el cerebro del robo virtual de 10 millones de dólares del Citibank. Fue arrestado en Londres un año después y extraditado a EE.UU.

1995: El Departamento de Defensa de EE.UU. sufre 250.000 ataques en un año. Kevin Mitnick es arrestado bajo sospecha de robar 20.000 números de tarjetas de crédito. Es encontrado culpable un año después. La película Hackers llega a las pantallas de cine, difundiendo algunas ideas equivocadas sobre las actividades de los Hackers.

1998: Network Associates emite un anuncio anti-hacker durante la Superbowl en los EE.UU. En él, dos técnicos de misiles soviéticos destruyen el mundo, inseguros de saber si las ordenes vienen de Moscú o de los Hackers. Los Hackers afirman haber entrado en el sistema de satélites militares y amenazan con vender secretos a los terroristas. Se crea la NIPC (National Infrastructure Protection Centre) con un presupuesto multimillonario.

1999: Nacimiento del software anti-hacking. 2000: Se producen ataques de denegación de servicio (DoS) sobre los grandes nombres de la Red.

2001: XP, el Windows más seguro , es crackeado antes de su lanzamiento.

2002: Bill Gates, el jefe de Microsoft crea Trustworthy Computing. El ISP CloudeNine es hackeado hasta la muerte.

2007: Se producen varios ataques phishing específicos contra entidades españolas especialmente agresivos a través de un kit que comprende a muchos bancos españoles. Se produce un ataque masivo a través de un mensaje que invita a visualizar un supuesto vídeo en Youtube. El reclamo en esta ocasión es reproducir el célebre incidente entre el Rey de España y el Presidente de Venezuela con la famosa frase: ¿Por qué no te callas? .

2008: España ocupa el noveno puesto mundial en número de sistemas zombi, casi en empate técnico con Estados Unidos y Rusia. Se descubre una nueva forma de engañar a los servidores DNS para que den respuestas falsas, gracias a un fallo inherente del protocolo. No se han dado de talles técnicos sobre el problema. El descubridor Dan Kaminsky ha llevado en secreto su investigación durante meses, esperando a que todos los grandes fabricantes implicados se pusiesen de acuerdo para programar una solución y publicar los parches correspondientes.

1.5.1 AMENAZAS A LA SEGURIDAD

Las organizaciones, sus redes y sistemas de información enfrentan crecientes amenazas a su seguridad que incluyen el fraude asistido por computadora, actos de espionaje, sabotaje, vandalismo y hasta incendios e inundaciones.

En este contexto, amenaza informática es todo aquello capaz de manifestarse en forma de ataque a la red y provocar daños en los activos, por este motivo el profesional de seguridad debe conocer cuáles

son las posibles amenazas que existen en la actualidad, y mantenerse actualizado sobre las nuevas amenazas que aparezcan. Este conocimiento le permitirá realizar un correcto análisis de la situación respecto a la seguridad en la que se encuentra una organización.

Podemos realizar una clasificación de las amenazas según su origen, así encontramos las siguientes categorías:

Amenazas físicas: Las amenazas físicas se relacionan con la posibilidad de obtener acceso físico a los recursos. La mayoría de los sistemas de computación han desarrollado altos niveles de sofisticación para cuidarse de las amenazas externas. Sin embargo, estos sistemas generalmente son vulnerables a ataques, sabotaje y robos originados en el interior.

Los sistemas deben operar en un ambiente controlado, sobre todo debemos proteger el acceso físico a la consola de administración de los equipos, generalmente en los dispositivos de networking es un puerto particular y en los servidores la consola de administración se representa por el acceso desde el teclado conectado al servidor.

Estos accesos representan un punto crítico de vulnerabilidad, porque desde el puerto de consola se puede acceder a la mayoría de las funciones administrativas de los equipos.

Existen varias medidas que se pueden implementar para mantener a los intrusos fuera del alcance de los recursos, por ejemplo, puertas, locks, sistemas de vigilancia y sistemas de alarma, junto con técnicas biométricas para el control de acceso al sistema.

Generalmente se emplean técnicas denominadas, ingeniería social, para burlar los sistemas de vigilancia, a través de estas técnicas los intrusos se aprovechan de la confianza natural que posee el ser humano, por ejemplo, alguien ingresa a su edificio vestido con un uniforme y el logo correspondiente, se aproxima a la recepcionista y se identifica como técnico de la empresa mayorista que provee las impresoras y le dice que viene a realizar el servicio técnico preventivo correspondiente. En la mayoría de los casos la recepcionista le permitirá pasar y le indicará donde están las impresoras. El atacante ha conseguido ingresar a su organización y probablemente con el mismo truco pueda seguir accediendo a distintas áreas (en la Unidad 5 - Ataques y Contramedidas, se verá en mayor detalle este ataque y las formas de defendernos).

Catástrofes naturales: Desastres naturales son aquellos desastres provocados por la naturaleza como los tornados, inundaciones, terremotos o fuertes tormentas eléctricas. Generalmente ocasionan grandes pérdidas, principalmente porque su consecuencia casi inmediata es la interrupción del servicio informático, es decir la disponibilidad de la información. Para que tengamos una idea de la magnitud del problema, si nos situamos en los Estados Unidos, la pérdida horaria por interrupción de energía eléctrica es de más de u$s 100.000 en las transacciones de comercio electrónico, y asciende a u$s 8 millones para las operaciones de bolsa.

Fraude informático: Fraude informático se refiere a las defraudaciones provocadas en el ámbito de empresas o en Internet. Se considera como tal tanto al robo hormiga, como a la promoción de inversiones en sitios de Internet que nunca se concretan o la venta de productos y servicios informáticos que no existen. Debido a la magnitud que han adquirido estos delitos en los Estados Unidos y en el mundo, el FBI posee un departamento dedicado especialmente a los delitos informáticos. Los países mas industrializados encabezan la lista de denuncias. Esto se debe al hecho de que es en estos países donde existe mayor desarrollo tecnológico y donde encontramos la mayor cantidad de personas que accede a Internet para efectuar transacciones comerciales. La pérdida monetaria promedio causada a las víctimas de fraude informático es de u$s 600.

Error Humano: Es el que se produce por impericia o negligencia y el alcance del mismo es, de hecho,

impredecible. Esta afirmación es muy importante porque cualquier incidente de seguridad informática genera costos que se relacionan con el daño producido.

Algunos de los incidentes más comunes que podemos mencionar, son los siguientes:

- Exposición de datos personales de clientes.
- Olvido de hacer un backup o hacerlo mal.
- Codificar aplicaciones con errores involuntarios que las hacen vulnerables.
- Desconectar involuntariamente servidores que están brindando un servicio on-line.
- Brindar información sobre la organización a personas desconocidas.
- Elegir una password fácilmente vulnerada, o por otro lado, anotarla en un lugar de fácil acceso porque no la puede recordar.

Intriciones: Las intrusiones son ingresos no autorizados a los sistemas de comunicaciones, servidores, estaciones de trabajo, quebrando la seguridad de la empresa u organización.

Estos tipos de intrusiones son habituales en organismos gubernamentales, religiosos o militares, y en general persiguen varios objetivos entre los que encontramos venganza, desafío intelectual o técnico, poder, a través del acceso a información estratégica, ventaja competitiva, o simplemente la proclama de algún tipo de mensaje en contra de los organismos o la ridiculización de los mismos. Los delincuentes informáticos no solo persiguen los objetivos mencionados, sino también rédito económico. Por ejemplo, en un caso de intrusión al casino on-line de la empresa Cryptologic Gambling Software, los delincuentes modificaron el programa de ruleta de manera tal de poder jugar sin perder nunca y así llegaron a ganar u$s 1.9 millones.

Las pérdidas económicas producidas por los Hackers malintencionados no solo están relacionadas con las pérdidas directas producidas por los ataques, sino mucho peor aún, por la pérdida de confianza. Por ejemplo, los clientes de un grupo de Estados de USA que usaban la tarjeta Visa para sus transacciones electrónicas, se vieron afectados por delincuentes que interceptaban los datos de sus tarjetas y operaciones. Esto obligó a la reemisión de las tarjetas y generó enormes pérdidas a causa de la pérdida de confiabilidad en la institución.

La gran cantidad de delitos registrados en todos los ámbitos motivó la creación de grupos especiales dedicados a combatir a los ciberdelincuentes.

Software ilegal: Los programas de computadoras están protegidos por las leyes de derechos de autor y por los tratados internacionales. Mucha gente no se da cuenta de que usar software copiado ilegalmente es un hurto y que el uso de software ilegal puede acarrear consecuencias serias a una empresa, sus gerentes y sus empleados. Desafortunadamente, algunas veces se ignora el hecho de que el software tiene un valor económico. Sin embargo, el software es un elemento crítico de varios aspectos del funcionamiento de su empresa y por lo tanto debe administrarse y registrarse como cualquier otro activo. La adquisición y administración legal del software es un elemento esencial de los negocios, debido a que:

- Es una condición que la empresa debe cumplir para mantenerse dentro de un marco de legalidad.
- Si tiene cualquier problema con el software, recibirá soporte del fabricante y de sus distribuidores autorizados.
- Podrá recibir aviso de actualizaciones, este punto es muy importante debido a que continuamente se encuentran vulnerabilidades asociadas a los programas, el desarrollador se encarga de realizar una actualización que solucione este problema, y la hace disponible on-line para los usuarios registrados.

El software ilegal, o comúnmente llamado "software pirata" tiene muchas formas y puede entrar a su empresa de diversos modos, a continuación enumeramos las formas más comunes de piratería:

- **Copia en la oficina:** Tal vez la forma de piratería de software al nivel de usuario final es la copia sin licencia que ocurre en el lugar de trabajo. Típicamente, un negocio compra una o varias licencias de un producto y a medida que las necesidades de los usuarios crecen se hacen copias ilegales a partir de uno de los programas con licencia.
- **Piratería en la red:** Ocurre en redes de computadoras cuando un número mayor de usuarios que el permitido por la licencia accede al programa de computadora. Varios administradores de red fallan en reconocer que esto es una violación de las leyes de derechos de autor, y no controlan ni limitan adecuadamente el uso.
- **Piratería en Internet:** La piratería de software ha crecido dramáticamente con la expansión de Internet. Los programas pueden ser descargados o enviados por correo electrónico a individuos que no tienen una licencia.
- **Vendedores** : A menudo, el canal de ventas al público puede ser la fuente de software ilegal. Los vendedores de computadoras frecuentemente venden computadoras con software ya instalado. Desafortunadamente, en algunas ocasiones, estas computadoras han sido cargadas con software sin licencia.
- **Falsificación:** Los falsificadores tratan de engañar al consumidor para convencerlo de que está comprando un producto legítimo. Aunque el paquete y los manuales pueden tener la apariencia de un producto familiar, en realidad son falsificaciones. Para evitar esto deberá asegurarse de adquirir el software en compañías distribuidoras autorizadas.

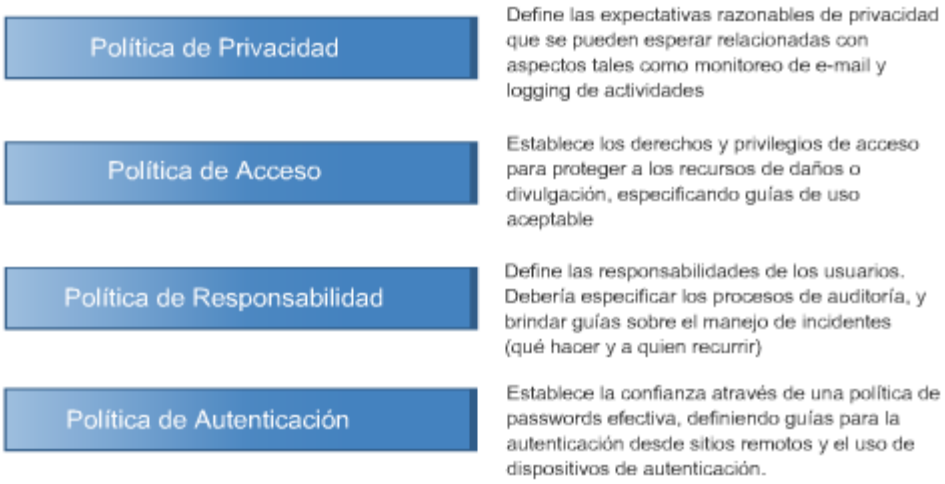
Código Malicioso: El código malicioso, es quizás la amenaza con mayor prensa y la más temida por todos los usuarios en general. Código malicioso es todo programa que genera algún tipo de problema en la computadora en la cual se ejecuta, ya sea robo o destrucción de información, pérdida de productividad, pérdida de privacidad, etc. Incluye a los virus, gusanos, caballos de Troya, espías, puertas traseras y software de control remoto subrepticio. Es de prever que el problema de código malicioso irá en aumento en el mundo ya que su propagación se ve facilitada por la conectividad de Internet. El código malicioso está evolucionando no en complejidad de técnicas de programación, sino respecto de las artimañas de que se vale para que el usuario ejecute el programa y lo active. Por supuesto que en muchos casos se explotan vulnerabilidades de los programas de correo electrónico, pero quienes programan este tipo de código suponen que los mensajes en los que está adjunto serán leídos mayoritariamente con sólo incorporar un asunto tal como "I love you". Este virus generó pérdidas por más de u$s 8.700 millones globalmente considerados. Si bien muchas empresas son afectadas por código malicioso, uno de los principales afectados por este tipo de ataques es Microsoft, quien a consecuencia de los daños provocados por Código Rojo y Nimda perdió importantes clientes que utilizaban IIS y que migraron a plataformas de Linux o Unix por considerarlas más seguras.

1.6.1 POLÍTICAS DE SEGURIDAD

En la sociedad, existen leyes que rigen el correcto comportamiento y mecanismos para encargarse de los problemas originados por su no cumplimiento. En las organizaciones, se utilizan las políticas para describir las reglas y expectativas, y los procedimientos para describir los cursos de acción para encargarse de los problemas. Estas políticas y procedimientos permiten que cada uno comprenda el punto de vista y la importancia que le otorga la organización a cada tópico, y que podría ocurrir si su comportamiento no se ajusta.

Las políticas no deberían ser documentos estáticos que permanezcan inalterables para siempre, deberán ser revisadas o revocadas conforme se produzcan cambios en el ambiente que dió origen a su creación. Por ejemplo, antes que Internet se vuelva popular, muchas empresas utilizaban BBSs (Bulletin Board Systems) para intercambiar información, cuando dejan este sistema para utilizar

Internet, la vieja política debería ser cancelada y reemplazada por una nueva política de acceso a Internet.



En particular, las Políticas de Seguridad se enfocan en la necesidad de proteger los datos y sistemas en una organización garantizando la confidencialidad, integridad y disponibilidad de la información. Es decir, no sólo incluye los archivos en un servidor, sino también el servidor mismo, y los dispositivos de comunicación que permiten a los usuarios acceder a los datos. Por ejemplo, se puede definir una política para tratar todo lo referente a seguridad física de un edificio de oficinas y la potencial amenaza de acceso no autorizado. Ésta, puede enunciar que el público en general debe permanecer en la recepción, frente al escritorio, pero los sitios mas allá de este punto son sólo para empleados. Además se deberán definir procedimientos que indiquen los pasos a seguir cuando no se cumple la política, por ejemplo, cuando se encuentra una persona no autorizada en una zona restringida.

Una Política de Seguridad, a menudo es referida como una declaración de alto nivel en la cual se establece el rol que se espera ocupe la seguridad de la información dentro de la organización. En una política de seguridad, la gerencia establece el modo en que un programa de seguridad de la información será llevado a cabo, presenta las metas del programa, asigna responsabilidades, demuestra el valor estratégico y táctico de la seguridad y se refiere a diferentes aspectos que se requieren a fin de reforzar la seguridad.

La Política de Seguridad, más allá de presentar directivas de alta gerencia, definir la filosofía organizacional de seguridad de la información y definir como se desarrollará el programa de seguridad, debe cumplir con ciertas premisas básicas entre las que se encuentran:

- *Debe ser independiente de la tecnología y las soluciones*
- *Debe definir responsabilidades y autoridades para la implantación de la seguridad informática*
- *Debe ser de carácter abreviado y de alto nivel*
- *Debe encontrarse alineada con la política general de la organización*
- *Debe determinar las normativas generales que deben cumplirse*

Al momento de establecer una Política de Seguridad de la Información, deben también ser tenidas en cuenta las siguientes consideraciones:

- *Esta debe ser dictada por un Comité de Seguridad*
- *Debe ser aprobada por las máximas autoridades*
- *Debe ser comunicada a todo el personal y terceros*

- *El personal y los terceros deben aceptar formalmente la Política*
- *Debe encontrarse integrada con la Política de Gestión de Riesgos*
- *Debe ser escrita en lenguaje claro y sin ambigüedades*
- *Debe ser consistente con las normativas legales y corporativas existentes*

1.6.2 Estándares

Bajo el término de Estándar, generalmente nos referimos a un tipo especial de documento, relacionado con la definición de acciones, reglas, actividades mandatorias y regulaciones. Los estándares pueden ser internos o de mandato externo a la organización (leyes del gobierno y regulaciones). En líneas generales, los estándares especifican la forma de poner en práctica un objetivo de la política, definen el uso de una determinada tecnología o la aplicación de una determinada solución de una manera uniforme. A fin de ejemplificar la diferencia entre política y estándar, podríamos imaginar por ejemplo, una sentencia de nuestra Política de Seguridad de la Información, en donde se especifica: "Se protegerá la red de la organización de accesos no autorizados desde redes externas" mientras que el Estándar refiriéndose al mismo punto, probablemente mencione algo así como: "Se implementarán equipos Firewall para el control de accesos a cada DMZ y a la LAN de la organización".

1.6.3 Baselines

Existen una serie de definiciones para describir el término Baseline. En el sentido más estricto, un Baseline, puede referir a un punto en el tiempo que pueda ser utilizado como una comparación con futuros cambios. Una vez que se han mitigado los riesgos y los sistemas han sido asegurados, un Baseline es formalmente revisado y aceptado, después de lo cual futuras implementaciones pueden ser comparadas contra lo expresado en este documento. Debido a sus características propias, un documento de Baseline suele ser utilizado como un punto de referencia constante. Los Baseline, también son utilizados para definir el mínimo nivel de protección requerido por un sistema, aplicativo o dispositivo. En el campo de la seguridad, Baselines específicos pueden ser definidos por tipo de sistemas, a efectos de documentar los seteos necesarios en relación al nivel de protección que se espera que estos provean.

Hemos mencionado que los Baselines determinan como deben ser configurados los distintos aspectos de seguridad de acuerdo a las diferentes tecnologías. Veamos cual sería en el ejemplo introducido en los indicadores anteriores, el rol del Baseline:

- ***Política***: "Se protegerá la red de la organización de accesos no autorizados desde redes externas"
- ***Estándar***: "Se implementarán equipos Firewall para el control de accesos a cada DMZ y a la LAN de la organización".
- ***Baseline***: "Permitir en el puerto XX el tráfico YY, etc"

1.6.4 Guidelines

Las Guidelines son acciones recomendadas y guías operacionales dirigidas a usuarios, al departamento de IT, al departamento de operaciones y a otros, cuando un estándar específico no es de aplicación. Las Guidelines pueden encontrarse relacionadas con metodologías respecto de cuestiones tecnológicas, del personal o de la seguridad física. Mientras que los estándares son reglas específicas y de cumplimiento obligatorio, las Guidelines suelen ser más generales y flexibles. En

resumen, las Guidelines no son otra cosa que definiciones generales establecidas para colaborar con el cumplimiento de los objetivos de las políticas, proporcionando un marco en el cual implementar controles adicionales. Es importante insistir en que debido a sus características, las Guidelines tienen carácter de “Recomendación” pero no son obligatorias.

- ***Política***: “Se protegerá la red de la organización de accesos no autorizados desde redes externas”
- ***Estándar***: “Se implementarán equipos Firewall para el control de accesos a cada DMZ y a la LAN de la organización”.
- ***Baseline***; “Permitir en el puerto XX el tráfico YY, etc”
- ***Guideline***; “Los administradores de red serán capacitados sobre la implementación y configuración de Firewalls”

1.6.5 Objetivo

El principal objetivo de una política de seguridad es hacer conocer al personal administrativo, gerentes, y demás usuarios, sus obligaciones respecto a la protección de los recursos tecnológicos e información. La política especificaría los mecanismos a través de los cuales se debería regir para cumplir estas responsabilidades. Otra finalidad es proporcionar una referencia a partir de la cual diseñar, configurar y/o auditar sistemas de computación y redes.

La política de seguridad también permite guiar y proporcionar apoyo gerencial para lograr los objetivos que la empresa desea en cuanto a confidencialidad, integridad y disponibilidad de la información. En consecuencia, si una organización comienza a implementar medidas de protección sin tener al menos una política de seguridad tácita o sobreentendida estaría cometiendo un grave error, porque los medios técnicos no bastan para brindar seguridad, sino que deben estar apoyados por las políticas y procedimientos correspondientes.

1.6.6 Responsabilidades

Como comentamos anteriormente, un aspecto importante de la política de seguridad es asegurar que todos saben cúal es su responsabilidad para mantener la seguridad.

La política debe garantizar que cada tipo de problema, aún aquellos desconocidos, está asociado con alguien que pueda manejarlo de manera responsable, de esta manera se evitarán incidentes o, al menos, se minimizará su impacto. Esto es muy importante, porque debemos ser conscientes que es difícil para una política de seguridad de red anticipar todas las amenazas posibles.

Asimismo, pueden existir varios niveles de responsabilidad asociados con una política, por ejemplo, cada usuario deberá ser responsable de guardar su contraseña. Un usuario que pone en riesgo su cuenta aumenta la probabilidad de comprometer otras cuentas y recursos. Por otro lado, los administradores de red y sistema son responsables de mantener la seguridad general.

1.6.7 Apoyo político

Para implantar con éxito una política de seguridad el nivel gerencial debe establecer una dirección política clara, demostrar apoyo y compromiso con respecto a la seguridad de la información, es decir debe respaldar la política para asegurar su cumplimiento. Una forma de demostrar este compromiso será asignar los recursos necesarios para garantizar su desarrollo y posterior mantenimiento.

Estos recursos no sólo deberán ser económicos, sino también humanos y de infraestructura, por ejemplo deberá garantizar un espacio físico y la colaboración de gerentes, usuarios, administradores,

diseñadores de aplicaciones, auditores y personal de seguridad, y expertos en áreas como legislación y administración de riesgos.

1.6.8 ¿Gasto o Inversión?

Históricamente asegurar los activos informáticos ha sido considerado como un gasto para muchas empresas, y fue así como varios proyectos millonarios de comunicaciones, ERP o bases de datos sufrieron posteriormente un costo por incidentes o ataques informáticos varias veces mayor al que hubiera correspondido a tomar los recaudos necesarios para minimizar los riesgos.

Se habla generalmente de este tema como un proceso de “tomar conciencia”, cuando en realidad la seguridad informática, en general, y el desarrollo y mantenimiento de la política de seguridad en particular no es ni más ni menos que otro proyecto al que hay que encontrarle la viabilidad económica para que se considere inversión y no gasto.

La pregunta siempre es ¿cuánto hay que invertir en asegurar los recursos?, es allí donde tenemos que utilizar un criterio simple que nos da la respuesta: si tenemos activos informáticos por un determinado valor, vamos a invertir más de este valor en asegurarlos?, evidentemente no. Lo importante entonces es conocer cuánto valen nuestros activos informáticos. Pero cuidado, porque tenemos valores intangibles que debemos considerar en la evaluación, piense por ejemplo, cuánto cuesta a la imagen de una compañía que ésta no pueda dar respuesta a sus clientes durante dos días porque “se cayo el sistema”. Este valor dependerá de la industria en la que la empresa se desempeña, no es lo mismo un banco que una pequeña empresa textil.

Entonces, debemos tener presente que el desarrollo de una política de seguridad y su implementación es una inversión, y las consecuencias de no tomar los recaudos necesarios pueden ser muy perjudiciales para el negocio, hasta llegar a casos extremos de quiebras.

1.6.9 Documentación de la Política de Seguridad

Los responsables del nivel gerencial deben aprobar y publicar un documento que contenga la política de seguridad y comunicarlo a todos los empleados, según corresponda. Éste debe poner de manifiesto su compromiso y establecer el enfoque de la organización con respecto a la gestión de la seguridad de la información. Como mínimo, debería contemplar los siguientes aspectos, que darán lugar a una serie de documentos que cubren aspectos específicos de la seguridad de la información:

¿Quién y Dónde? Una política debe especificar a cuáles personas o departamentos está dirigida. En muchos casos, se aplicará a todos los empleados, en otros casos se dirigirá a ciertas personas en determinadas circunstancias, por ejemplo, si todos tienen acceso a Internet, la política de acceso se aplica a todos. Por otro lado, la política de acceso debe especificar quién es el responsable de tratar los problemas y violaciones a esta política, en este caso las reglas sólo se aplicarían a una persona o departamento, por ejemplo, al departamento de tecnología.

¿Qué? La política debe expresar claramente el tema que está tratando. Por ejemplo, una política de Internet, puede contener reglas referidas al uso de e-mail e Internet, programas que están prohibidos durante las horas de trabajo (por ejemplo juegos en red), y sitios cuyo acceso se considera impropio (por ejemplo sitios pornográficos). En muchos casos ésta será la parte principal de la política.

¿Cuándo? En qué momentos tiene efecto la política. En algunos casos las políticas tienen una fecha de expiración; por ejemplo una política que defina el comportamiento durante el upgrade de un viejo sistema a uno nuevo no tendrá más sentido luego que el sistema nuevo esté implementado.

¿Por qué? Explica el propósito de la política, y lo que la organización espera conseguir a través de ella. Puede incluir una reseña de los aspectos que originaron la necesidad de la política.

¿Cómo? Es el procedimiento o metodología necesario para que la política funcione. Cuando una política incluye procedimientos, éstos detallan cómo se pone en práctica y se hace cumplir.

Una política de seguridad, generalmente está compuesta por un conjunto de documentos, que cubren aspectos específicos. A continuación presentamos un listado de aquellos que consideramos más importantes.

1. Una política de privacidad, la cual define las expectativas razonables de privacidad que se pueden esperar relacionadas con aspectos tales como monitoreo de e-mail, logging de pulsaciones de teclas, y acceso a archivos del usuario.
2. Una política de acceso, la cual define derechos y privilegios de acceso para proteger a los recursos de daños o divulgación especificando guías de uso aceptable. Debería contener guías para realizar conexiones externas, para conectar dispositivos a la red, agregar nuevo software, para utilizar Internet y el correo electrónico.
3. Una política de responsabilidad, la cual define las responsabilidades de los usuarios. Debería especificar los procesos de auditoría, y brindar guías sobre el manejo de incidentes (qué hacer y a quién recurrir)
4. Una política de autenticación, la cual establece la confianza a través de una política de passwords efectiva, definiendo guías para la autenticación desde sitios remotos y el uso de dispositivos de autenticación (ejemplo, one-time passwords y dispositivos que las generan)

1.6.10 Clasificación de la información

Bastante hemos hablado hasta aquí, en relación a todos aquellos procesos que en su conjunto nos permiten establecer un plan de seguridad integral efectivo. No obstante existe un proceso que al igual que los mencionados, resulta de suma importancia: La Clasificación de la Información. Evidentemente cualquier proceso de capa superior, previamente requiere de tareas tales como la identificación de activos, sin la cual procesos posteriores como la evaluación de riesgos sencillamente es impracticable. Suponiendo que como parte del proceso de identificación de activos, fuimos capaces de obtener una lista de recursos de información, los cuales requieren ser protegidos, es de esperar que el nivel de protección a otorgar a los mismos, se encuentre relacionado con el resultado obtenido en la evaluación de riesgos. No obstante, previamente es condición sin equanon, el conducir un proceso específico de clasificación de la información, con el objeto de identificar la criticidad que cada conjunto de datos tiene para el negocio, de modo tal que el tratamiento de los riesgos pueda ser discrecional y la selección de controles óptima en relación a su costo/beneficio.

1.6.11 Justificación

Varios son los motivos que justifican la puesta en marcha de un proceso de clasificación de información. El primero y mas evidente, es sin dudas el hecho de que no todos los datos/información tienen el mismo valor. Por su parte no todo el mundo debe acceder a todos los datos/información. Al margen de los motivos mencionados, cada vez con más frecuencia las organizaciones se encuentran obligadas a cumplir con aspectos legales o regulatorios, y por consiguiente a encarar un proceso formal de clasificación de de información, el cual les permita establecer en forma exacta el nivel de protección que debe ser otorgado a cada conjunto de datos. En nuestro país, la ley de Protección de Datos Personales o Habeas Data, es un claro ejemplo de este tipo de requerimientos, debido a que los controles o medidas de seguridad requeridos para las organizaciones que administren datos mencionados en la ley como “sensibles”, es superior al requerido a aquellas organizaciones que no lidien con este tipo de datos.

1.6.12 Beneficios de la clasificación de la información

Es cierto que los procesos de clasificación de información, a menudo requieren de un gran esfuerzo

por parte de la organización, no obstante una vez concluido dicho proceso, ésta sin dudas será capaz de visualizar los beneficios que el mismo le ha proporcionado.

El llevar a cabo la clasificación de la información existente en la organización, demuestra claramente el compromiso de esta hacia la seguridad de la información. Por otro lado, permite identificar que datos u información, son efectivamente más críticos para la organización. Es común, una vez finalizado el proceso de clasificación, sorprenderse del resultado que muestra que tal o cual recurso de información que se suponía de poco importancia, termina debiendo ser considerado como crítico. Más allá de los beneficios hasta aquí mencionados, quizás uno de suma importancia es aquel relacionado con la optimización en la inversión de controles. El correcto proceso de clasificación de información, sirve de soporte para la selección de controles, evitando que la organización invierta dinero en la implementación de salvaguardas, contramedidas o controles, sobre activos de información que no ameriten tal inversión.

1.6.13 Política de clasificación de la información

Del mismo modo que es necesaria una Política de Seguridad de la Información, lo es la elaboración de una Política de Clasificación de la Información, capaz de establecer declaraciones de alto nivel orientadas a ordenar el proceso de clasificación. A continuación se mencionan los principales puntos que deben ser contemplados, precisamente al momento de elaborar la Política de Clasificación de la Información de la organización:

- La Política de Clasificación de la Información
- Define la información como un activo de la organización
- Define los propietarios de información
- Define a los custodios de la información
- Define el proceso de clasificación de la información
- Establece las responsabilidades en el proceso de clasificación de la información
- Determina el criterio de clasificación de la información
- Establece los controles mínimos sobre la información para cada nivel establecido, en cumplimiento con normativas existentes

Por ultimo, es de suma importancia notar que como norma general, toda información que no sea de naturaleza pública, debe clasificarse.

1.6.14 Proceso de clasificación de información

Como todo proceso, a fin de llevar a cabo la Clasificación de Información en la organización, se requiere de la realización de una serie de pasos o tareas, que encontrándose claramente definidas permitirán implementar políticas de clasificación exitosas.

El proceso de clasificación al igual que cualquier otro tipo de proceso, debería documentarse y encontrarse disponible para su uso por parte de aquellas personas para las cual el mismo tenga incumbencia. A continuación, se detallan las tareas que habitualmente se encuentran incluidas en todo proceso de clasificación de información:

- *Definición de los niveles de clasificación*
- *Definición del criterio de clasificación*

- *Clasificación de la información por parte de los propietarios*
- *Identificación de custodios de la información*
- *Definir los controles de seguridad de la información para cada nivel*
- *Documentar excepciones a la clasificación*
- *Definir métodos de reasignación de la custodia de la información.*
- *Desarrollar un procedimiento de revisión periódica de la clasificación de la información y la definición de propietarios.*
- *Desarrollar un procedimiento para la desclasificación de la información.*
- *Introducir el proceso de clasificación de información en la concientización del personal.*

1.6.15 ¿Qué se debe tener en cuenta a la hora de clasificar información?

Al momento de llevar adelante un proceso de clasificación, uno de los primeros interrogantes que suelen presentarse, es precisamente cuales son los aspectos que deben ser tenidos en cuenta a la hora de clasificar información. Si bien las respuestas a dicha pregunta, pueden variar de acuerdo al entorno, existen una serie de tips que suelen ser de utilidad a tal efecto.

En primer lugar, un punto de importancia a la hora de decidir el nivel de clasificación de información, es su valor. Si bien con frecuencia puede resultar difícil calcular el mismo, aspectos tales como el tiempo en horas hombre, que requeriría volver a cargar información a un archivo de registro de ventas desde la propia factura física, ante la eventual perdida de tal información digital puede muchas veces ser un indicador del valor. Del mismo modo, eventualmente suele ser efectivo, asignar valor a nuestra información, en función de cuanto creemos que la misma podría valer en manos de la competencia.

Otro aspecto importante que podría influir en la clasificación a otorgar a determinado conjunto de datos o activo de información, es aquel relacionado con el impacto en función de que los mismos sean: divulgados, alterados o no se encuentren disponibles por un tiempo determinado. Por ejemplo, la no disponibilidad de información respecto de las cuentas de clientes, podría hacer que eventualmente un banco no pueda procesar pagos por un período de tiempo determinado, causando algún tipo de pérdida económica.

Por ultimo, pero no por eso menos importantes, podría existir información que si bien puede no tener un valor alto respecto de los procesos internos del negocio, su perdida podría acarrear serias implicancias legales terminado en multas o alguna otra penalidad que debería ser tenida en cuenta al momento de clasificar dicha información.

1.6.16 Criterios de clasificación

Un aspecto importante a definir cuando de clasificar información se trata, es el criterio que se utilizara en el proceso. Si bien es posible tanto técnica como teóricamente definir un sin numero de criterios diferentes, lo cierto es que habitualmente de acuerdo al ámbito de aplicación, a menudo este suele encontrarse restringido tan solo a dos, uno orientado al ambiente comercial o privado y el otro relacionado con el ambiente militar o gubernamental.

Modelo Comercial - Privado

- Público: Puede ser pública, su conocimiento no causa impacto negativo o adverso a la organización o el personal.
- Sensitivo: Requiere precauciones especiales. Ej.: información sobre proyectos.

- Privado: Información para uso interno de la compañía. Su conocimiento podría afectar negativamente al personal o la compañía. Ej.: información de RRHH.
- Confidencial: Sumamente Sensible, su conocimiento podría impactar fuertemente en la compañía. Ej.: estrategia comercial.

Modelo militar - Gubernamental

- Sin Clasificar: No Clasificada, Información que puede ser Publica.
- Sensitivo pero sin Clasificar: De Baja Sensibilidad. Si se hace publica, puede causar serios daños. Ej.: respuesta a tests.
- Confidencial: De conocerse, podría causar serios daños. Sólo para uso interno. Ej.: información de salud, código de programación.
- Secret: De conocerse, podría causar serios daños a la Seguridad Nacional. Ej.: desplazamiento de tropas.
- Top Secret: El grado más alto. De conocerse podría causar daño extremo en relación a la Seguridad Nacional. Ej.: planos de nuevo armamento, información de espionaje.

Es importante aclarar que estos modelos tradicionales, solo tienen en cuenta la sensibilidad de la información al momento de su clasificación. Por otro lado, también es de importancia conocer que una organización puede optar por utilizar tan solo dos niveles de clasificación, mientras que otra puede requerir más.

1.6.17 Difusión

Una vez escrita y acordada la política de seguridad, la organización debe asegurar que la declaración de la política se difunda y discuta en profundidad y a conciencia, para cumplir este objetivo, se disponen de varias herramientas, por ejemplo podrán utilizarse listas de distribución, publicación en la Intranet, o mediante educación interna, a través de seminarios de entrenamiento o charlas, de acuerdo al tamaño de la organización y las necesidades del momento. En definitiva, el objetivo es garantizar que todo el personal de la empresa conozca y comprenda los lineamientos de la política y se preocupe por su cumplimiento.

1.6.18 Cumplimiento

La organización debe garantizar que se lleven a cabo correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad. Esto implica una revisión continua de la manipulación de información que realizan los usuarios, a través de los logs que entregan los sistemas.

También se debe considerar la implementación de una revisión periódica in-situ de todos los procedimientos definidos en la política para garantizar su cumplimiento. De acuerdo al tamaño de la organización y la política de seguridad, se deberían considerar las siguientes áreas en el proceso de revisión:

- sistemas de información
- proveedores de sistemas
- usuarios
- gerentes

Por otro lado, además del objetivo enunciado anteriormente, se deberán verificar los sistemas operacionales a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados de acuerdo a las políticas y estándares.

1.6.19 Aspectos legales que involucran su incumplimiento

Se deben definir y documentar claramente todos los aspectos legales, normativos y contractuales relacionados con los objetivos de la política de seguridad (confidencialidad, integridad y disponibilidad) y las consecuencias legales en caso de incurrir en su incumplimiento. Estas consecuencias, pueden implicar diversos grados de sanciones de acuerdo a la responsabilidad sobre el recurso y al daño producido en la empresa. En general, la ley contempla sanciones para ciertos incidentes, como por ejemplo fraude, hurto, robo o espionaje. Pero por otro lado, no hay un consenso legal sobre las sanciones para ciertos incidentes, por ejemplo aquellos asociados con un mal uso de los recursos de la empresa, entre los que podemos mencionar utilizar el mail corporativo para fines personales, o visitar sitios no permitidos (juegos, pornografía). En este caso las empresas sostienen que de acuerdo a la gravedad del hecho y los apercibimientos recibidos, pueden ser motivo de despido con causa justificada. En todos los casos es conveniente procurar asesoramiento sobre los aspectos legales, de parte de los asesores jurídicos de la organización, o de abogados convenientemente calificados, sobre todo porque los requisitos legales varían según el país y en relación con la información que se genera en un país y se transmite a otro (por ejemplo, comunicaciones a través de Internet).

1.6.20 Revisión y evaluación

La política debe tener un propietario que sea responsable del mantenimiento y revisión periódica para detectar vulnerabilidades y garantizar la eficacia de los controles de hardware y software que hayan sido implementados. Este tipo de verificación debe ser realizada por personal especializado, en general con el apoyo de herramientas de software. Por ejemplo, se pueden realizar pruebas de penetración, donde básicamente se intenta penetrar el sistema como lo haría un intruso, por este motivo deberían ser realizadas por expertos independientes contratados específicamente para este propósito. Por otro lado, además de las revisiones anteriores, deberá estar alerta para realizar revisiones no programadas en respuesta a cualquier cambio en el contexto sobre el que se elaboró la política, por ejemplo, incidentes de seguridad significativos, nuevas vulnerabilidades o cambios en la infraestructura técnica de la organización.

Por otro lado, además de realizar revisiones de la política, también deberían programarse evaluaciones periódicas sobre la eficacia de la política, demostrada por la naturaleza, número e impacto de los incidentes de seguridad registrados. También es conveniente realizar una evaluación sobre el costo e impacto de los controles en el negocio, por ejemplo, para detectar una pérdida de productividad a causa de controles que no están de acuerdo con la filosofía de trabajo. Por último, se recomienda efectuar la evaluación del impacto en la política ante cualquier cambio tecnológico en el mercado, por ejemplo aparición de dispositivos que incorporan nuevos controles y pueden reemplazar a los existentes.

1.6.21 Background Checks

En indicadores anteriores tuvimos oportunidad de revisar algunos de los conceptos relacionados con la gestión del riesgo. Habitualmente, muchas tareas desarrolladas por los oficiales de seguridad, se encuentran relacionadas con la prevención de ataques provenientes del exterior. No obstante, es más común de lo que uno imagina, encontrar miles de casos en donde la amenaza no proviene del exterior sino que por el contrario se inicia en el interior mismo de la organización.

Si bien es cierto que ninguna compañía esta exenta de que un empleado disconforme cause algún

incidente de seguridad, probablemente el porcentaje sea menor, en aquellas que tomando en serio las cuestiones relacionadas con la seguridad de la información, trabajan en ello desde el inicio mismo del establecimiento de la relación laboral con sus empleados.

Bajo el término “Background Checks” se conoce al proceso por el cual se revisa información pública o se realizan tareas de verificación de la información dispuesta en los curriculums vitae de los candidatos. Este tipo de procesos, si bien deben llevarse a cabo idealmente para cualquier postulante, debería ser excluyente y probablemente más exhaustivos, al personal que vaya a desempeñar tareas críticas o manejar información sensible.

Mediante la conducción de procesos de “Background Checks”, la organización obtiene entre otros, los siguientes beneficios:

- Verificar que la información provista por el candidato es verdadera y actualizada
- Obtener una primera idea acerca del nivel de integridad del candidato
- Prevenir empleados no calificados
- Evitar incorporar personas con ética o moral alterados
- Prevenir posibles conflictos con el personal existente
- Prevenir posibles pérdidas por acciones fraudulentas
- Prevenir acciones legales (De parte de empleados despedidos, 3ras partes por negligencia en la contratación del personal, de parte de otros empleados por violencia, malos tratos, etc.)

1.6.22 Contratación y despido

Muchas veces las organizaciones suelen no poseer procedimientos formales respecto de los procesos de contratación y despido del personal. Acabamos de ver la importancia detrás de la ejecución de Background Checks y/o Security Clearances, al momento de realizar la contratación de empleados, pero que debe ser tenido en cuenta a la hora de su eventual despido? Claro esta que tal como en el proceso de Background Checks, este requiere de la participación activa del departamento de Recursos Humanos de la organización, quien con el asesoramiento de otros departamentos tal como el de Legales y obviamente el de seguridad de la información, deberían ser capaces de elaborar políticas y procedimientos donde se contemplen aspectos como los mencionados a continuación:

- Cómo manejar la salida del empleado
- Deshabilitación / Eliminación de su cuenta de usuario
- Reenvío de email y voice mail
- Cambios en las cerraduras y códigos de acceso
- Modificación de contraseñas de sistemas relacionados

1.6.23 Arquitectura de Seguridad de Información en la Empresa (EISA)

La Arquitectura de Seguridad de Información en la Empresa (EISA – *Enterprise Information Security Architecture*) es una parte de la arquitectura de la empresa que se centra en la seguridad de la información a lo largo de la empresa. Es la práctica de aplicar un método riguroso y comprensivo para describir una estructura actual y/o futura y el comportamiento de los procesos de seguridad de una organización, sistemas de seguridad de información y subunidades de personal y organizativas, para que se alineen con las metas comunes de la organización y la dirección estratégica. Aunque a

menudo se asocie estrictamente con tecnologías para la seguridad de la información, se relaciona en términos más generales con la práctica de seguridad de optimización del negocio, donde dirige la arquitectura de seguridad del negocio, la realización de gestiones y también la arquitectura de procesos de seguridad. La Arquitectura de Seguridad de Información en la Empresa está convirtiéndose en una práctica habitual dentro de las instituciones financieras alrededor del mundo. El propósito fundamental de crear una arquitectura de seguridad de información en la empresa es para asegurar que la estrategia de negocio y la seguridad de las tecnologías de la información (TI) están alineadas. Como tal, la arquitectura de seguridad de la información en la empresa permite la trazabilidad desde la estrategia de negocio hasta la tecnología subyacente. La arquitectura de seguridad de información en la empresa fue formalmente posicionada primero por Gartner Inc. en su libro blanco llamado Incorporando Seguridad en el Marco de la Arquitectura de la Empresa (Incorporating Security into the Enterprise Architecture Framework). Este fue publicado el 24 de enero de 2006. Desde su publicación, la arquitectura de seguridad ha pasado de ser un silo basado en arquitectura a una solución enfocada a la empresa que incorpora negocio, información y tecnología. La figura siguiente representa una vista unidimensional de la arquitectura de la empresa como una arquitectura orientada a servicios. También refleja la nueva suma a la familia de la arquitectura empresarial llamada "Seguridad" (Security). La arquitectura de negocio (Business), de información (Information) y de tecnología (Technology) suelen ser llamadas BIT para acortar. Ahora con la seguridad como parte de la familia de arquitecturas, se ha convertido en BITS.

Metas de EISA:

- Proporcionar estructura, coherencia y cohesión
- Debe permitir un alineamiento del negocio hacia la seguridad
- Principios inicio-fin definidos con estrategias de negocio
- Asegurar que todos los modelos e implementaciones pueden ser trazados hacia atrás hasta la estrategia de negocio, específicamente requerimientos de negocio y principios clave
- Proveer abstracción para que factores complicados puedan ser eliminados y reinstalados en niveles de detalle diferente sólo cuando sean requeridos
- Establecer un lenguaje común para la seguridad de la información dentro de la organización

Preguntas que responde la EISA:

- ¿Está la arquitectura actual apoyando y añadiendo valor a la seguridad de la organización?
- ¿Cómo podría una arquitectura de seguridad ser modificada para que añada más valor a la organización?
- Basándonos en lo que sabemos sobre lo que la organización quiere llevar a cabo en el futuro, ¿la arquitectura actual lo sustentará o lo entorpecerá?
- Implementar una arquitectura de seguridad de información en la empresa generalmente empieza documentando la estrategia de la organización y otros detalles necesarios tales como dónde y cómo opera. El proceso entonces desemboca en documentar competencias esenciales, procesos de negocio, y cómo la organización interactúa consigo misma y con partes tales como clientes, proveedores, y entidades gubernamentales.
- Habiendo documentado la estrategia y estructura de la organización, el proceso de arquitectura fluye entonces hacia la información diferenciada de los componentes tecnológicos tales como:
    - Cuadros de organización, actividades, y flujo de procesos sobre cómo la TI de la organización opera

- Ciclos, periodos y distribución en el tiempo de la organización
- Proveedores de tecnología hardware, software y servicios
- Inventarios y diagramas de aplicaciones y software
- Interfaces entre aplicaciones; esto es: eventos, mensajes y flujo de datos
- Intranet, Extranet, Internet, comercio electrónico (eCommerce), EDI links con partes de dentro y fuera de la organización
- Clasificación de datos, bases de datos y modelos de datos soportados
- Hardware, plataformas, hosting: servidores, componentes de red y dispositivos de seguridad y dónde se conservan
- Redes de área local y abiertas, diagramas de conectividad a internet

Donde sea posible, todo lo anterior debería estar relacionado explícitamente con la estrategia de la organización, metas y operaciones. La Arquitectura de Seguridad de Información en la Empresa documentará el estado actual de los componentes técnicos de seguridad listados arriba, así como un estado ideal futuro deseado (Arquitectura de Referencia) y finalmente un estado meta futuro resultado de los sacrificios y compromisos de ingeniería frente al ideal. Esencialmente el resultado es un conjunto de modelos anidados e interrelacionados, usualmente dirigidos y mantenidos con software especializado disponible en el mercado.

Semejante descripción exhaustiva de las dependencias de la TI se ha solapado notablemente con la metadata, en el sentido general de la IT, y con el concepto ITIL (Information Technology Infrastructure Library - Biblioteca de Infraestructura de Tecnologías de la Información) de la Configuración de los Gestores de Bases de Datos. Mantener la precisión de esa información puede ser un desafío importante. Junto con los modelos y diagramas se incluye un conjunto de mejores prácticas dirigidas a la adaptabilidad de la seguridad, escalabilidad, manejabilidad etc. Estas mejores prácticas de sistemas de ingeniería no son únicas a la Arquitectura de Seguridad de Información en la Empresa pero son esenciales sin embargo para su éxito. Conllevan cosas como modularidad, comunicación asíncrona entre más componentes, estandarización de identificadores clave y demás.

Aplicaciones exitosas de la Arquitectura de Seguridad de Información en la Empresa requieren una posición adecuada en la organización. La analogía con el plano de una ciudad es con frecuencia invocada en esta relación por ser instructiva. Un resultado intermedio de un proceso de arquitectura es un inventario extenso de la estrategia de seguridad del negocio, procesos de seguridad del negocio, cuadros organizacionales, inventarios de seguridad técnicos, diagramas de sistema e interfaz y topologías de red, así como de las relaciones explícitas entre ellos. Los inventarios y diagramas son simplemente herramientas que apoyan la toma de decisiones. Pero esto no es suficiente. Debe ser un proceso viviente. La arquitectura de Seguridad de Información en la Empresa es un componente clave del proceso de gobierno de tecnología de Seguridad de Información en cualquier organización de tamaño significativo. Cada vez más compañías están implementando procesos formales de arquitectura de seguridad en la empresa para respaldar el gobierno y la gestión de la TI. Sin embargo, como ya se indicó en el primer párrafo de este artículo, se relaciona perfectamente de forma más general a la práctica de la optimización del negocio en lo que se refiere a la arquitectura de seguridad del negocio, realización de la gestión así como de la arquitectura de seguridad de procesos. La Arquitectura de Seguridad de información de la Empresa está también relacionada con la gestión de la seguridad de la cartera de la TI y el sentido de la *metadata* en la empresa de TI.

1.6.24 Modelos de control de acceso

El comportamiento que proponemos para el sistema en cuanto a seguridad se ve fuertemente influenciado por las amenazas que el sistema debe afrontar y el tipo de sistema de que se trate. Es

muy diferente plantear un modelo para un entorno de alta seguridad, más preocupado por la posible filtración de información confidencial, que para un entorno comercial, más preocupado por asegurar la integridad y actualidad de la información. Son estos tipos de detalles los que nos guiarán a la hora de elegir el modelo. Una referencia importante en esta área es el denominado libro naranja (orange book), que durante años ha procurado un estándar para la evaluación de sistemas. Divide los sistemas en cuatro categorías (algunas se subdividen en clases) en función de los requerimientos que satisfacen. La categoría más baja es la D, que corresponde a sistemas que, tras ser evaluados, no satisfacen los requerimientos de las categorías superiores. La siguiente categoría, la C, se divide en dos clases, C1 y C2, e introduce controles de acceso discrecionales. La categoría B, con tres clases B1, B2 y B3, introduce controles de acceso obligatorios. La categoría A se reserva a sistemas que, aunque son funcionalmente equivalentes a los de la categoría B, disponen de completas especificaciones formales de diseño y en los que se han aplicado técnicas de verificación.

Cada una de las clases, excepto la D, especifica requerimientos en cuatro grandes áreas:

- ***Política de seguridad:*** conjunto de reglas que especifican si un sujeto puede acceder a un objeto.
- ***Gestión***: funciones de identificación, autenticación y auditoría.
- ***Compatibilidad***: criterios de evaluación del nivel de satisfacción de los restantes requerimientos (comprobaciones de seguridad, protección de los mecanismos de seguridad, etc.).
- ***Documentación***: especificación de los documentos requeridos para cada una de las clases y el contenido básico de cada documento (por ejemplo: Guía de Usuario de Capacidades de Seguridad, Documentación de Comprobación, Documentación de Diseño de Seguridad).

Aunque el *orange book* describe cuatro clases, realmente los divide en dos categorías: sistemas que incorporan controles de acceso discrecionales (categoría C), con seguridad limitada a un único nivel de seguridad, y sistemas que incorporan controles de acceso obligatorios, que permiten procesar información de diferentes niveles de seguridad (categorías A y B).

Los controles de acceso discrecionales exigen un proceso de identificación y verificación del usuario a la entrada al sistema. Una vez verificado que se trata de un usuario autorizado, este podrá acceder a toda la información que no tenga definidas restricciones de acceso. Un ejemplo de este tipo de controles es el mecanismo de permisos de UNIX: cuando un usuario crea un objeto, puede o no definir un conjunto de permisos de manipulación para él, su grupo y los restantes usuarios. Los controles de acceso obligatorios requieren múltiples niveles de seguridad. Los objetos y sujetos del sistema deben, obligatoriamente, tener un nivel de seguridad asociado. El sistema no debe permitir la creación de objetos o usuarios sin definir su nivel de seguridad, o que sean duplicados total o parcialmente con diferente nivel de seguridad. Cuando un usuario desea acceder a un objeto, el sistema comprueba los niveles de ambos y evalúa si se permite o no el acceso.

Modelo Bell-LaPadula: Uno de los modelos más conocidos, está basado en máquinas de estados finitos. De esta forma, el modelo consiste en la definición de un conjunto de variables de estado y funciones de transición y un estado inicial, considerado seguro. Así, si podemos probar que todas las transiciones son seguras y que nos llevan a estados considerados seguros, podemos mediante inducción demostrar que el sistema es seguro. el modelo de seguridad Bell-Lapadula , llamado así por sus creadores David Elliott Bell y Len LaPadula, consiste en dividir el permiso de acceso de los usuarios a la información en función de etiquetas de seguridad. Por ejemplo, en sistemas militares norteamericanos, categorizándola en 4 niveles: no clasificado, confidencial, secreto y ultra secreto. Este modelo se centra en la confidencialidad y no en la integridad. Se distinguen 2 tipos de entidades, sujetos y objetos. Se define estados seguros y se prueba que cualquier transición se hace de un estado seguro a otro. Un estado se define como estado seguro si el único modo de acceso permitido de un sujeto a un objeto está en concordancia con la política de seguridad. Para determinar si un

modo de acceso específico esta permitido, se compara la acreditación de un sujeto con la clasificación del objeto (más precisamente, la combinación de la clasificación y el conjunto de compartimientos) para determinar si el sujeto esta autorizado para el modo de acceso especificado. El esquema de clasificación/acreditación se expresa en términos de un retículo. El modelo define 2 reglas de control de acceso mandatorio (MAC) y una regla de control de acceso discrecional (DAC) con 3 propiedades:

1. Propiedad de seguridad simple: Un sujeto de un dado nivel de seguridad no puede leer un objeto perteneciente a un nivel de seguridad más alto.
2. Propiedad (Propiedad estrella): Un sujeto de un dado nivel de seguridad no debe escribir un objeto perteneciente a un nivel de seguridad más bajo. (También llamada propiedad de confinamiento)
3. Propiedad de seguridad discrecional: Se utiliza una matriz de acceso para especificar el control de acceso discrecional

Con Bell-La Padula, los usuarios pueden crear contenido solo en su nivel de seguridad o por encima (i.e, investigadores en el nivel secreto pueden crear archivos secretos o super secretos pero no archivos públicos). Inversamente, los usuarios pueden ver solamente contenido de su propio nivel o inferior. El principio de tranquilidad del modelo de Bell-La Padula establece que la clasificación de un sujeto u objeto no cambia mientras está siendo referenciada. Hay 2 formas para el principio de tranquilidad: el *principio de tranquilidad fuerte* establece que los niveles de seguridad no cambian durante la operación normal del sistema y el *principio de tranquilidad débil* establece que los niveles de seguridad no cambian de una manera que violen las reglas de una dada política de seguridad.

Modelo Brewer-Nash: llamado también muralla china(Chine Wall). Creado para proveer un tipo de control de acceso, capaz de cambiar dinámicamente dependiendo de las acciones previas realizadas por el usuario. Su principal objetivo es el de prevenir el conflicto de intereses.

Modelo Clark-Wilson: el modelo Clark-Wilson es un modelo que se basa en la jerarquización de aplicaciones para el manejo de información de parte de los usuarios. Este modelo se encuentra orientado a proteger la integridad de la información. Este modelo propone dos categorías de mecanismos para prevenir la modificación irrecuperable e incorrecta de la información, intencionada o no. El primero es el denominado de transacciones correctas y el segundo el denominado separación de obligaciones.

El mecanismo de transacciones correctas busca garantizar que un usuario no pueda modificar información arbitrariamente. Solamente permite la modificación en determinadas formas, restringiendo los posibles cambios incorrectos. Por ejemplo, un mecanismo de auditoría que recoja todas las transacciones de información, o un sistema en que solamente a un conjunto cerrado de programas se les permita modificar la información siguen este modelo.

El mecanismo de separación de obligaciones, por otra parte, trata de mantener la consistencia de la información separando todas las operaciones en diferentes partes que deben ser realizadas por diferentes sujetos. De esta manera, un usuario autorizado a iniciar una transacción no estará autorizado a ejecutarla o validarla. En comparación con el modelo de Bell-Lapadula, en este modelo no se definen niveles de seguridad para la información y en función de los mismos los datos que un usuario puede manejar, sino que se definen los programas que un usuario puede ejecutar, los cuales, a su vez, manejarán la información.

1.6.25 Seguridad por oscuridad

La seguridad por oscuridad, a veces llamada seguridad por ocultación, es un método que utiliza el secreto de diseño o implementación para asegurar que básicamente, por desconocimiento, no “se

encontrarán" los puntos débiles de dicho sistema. Cabe resaltar el conocido ejemplo de seguridad por oscuridad donde se menciona a los dueños de una casa que guardan una copia de la llave de entrada debajo del felpudo, medida utilizada para contrarrestar el caso de quedar "atrapados" fuera de casa por culpa de un olvido o pérdida de la llave de uso común. La vulnerabilidad teórica sería que alguien entrara a la casa con la copia de la llave escondida. Pero los dueños de la casa creen tener bajo control el tema de que la localización de la llave de repuesto no es conocida públicamente. Mantener este fundamento implica que la revisión de seguridad involucra solo unas pocas personas y a su vez confirma que si se llegara a conocer alguna vulnerabilidad en el sistema, sería fácilmente atacable por todos los conocedores de esta falla.

1.6.26 Seguridad del perímetro

La seguridad basada en la defensa perimetral apunta a reforzar los puntos de acceso o conexión de nuestra red privada con la red externa. Para ello se tiene que evaluar y planear qué tipos de acceso requiere el sistema, implementar sistemas de seguridad para bloquear el resto del tráfico (por ejemplo Firewalls o proxys), proteger esos únicos puntos vulnerables, y ahí mismo ubicar sistemas de monitoreo y detección de intrusos para que den aviso al administrador del sistema y así poder ejecutar acciones defensivas a tiempo. Cada computadora que se mueve o conecta y desconecta sin pasar por los accesos "oficiales" son el equivalente a puertas traseras por las que puede vulnerarse la seguridad de la red.

Ahora, ¿que impide que el sistema se "rompa" desde adentro?. Absolutamente nada. Hace años que el perímetro demarcado de nuestra red es demasiado difuso. Las personas conectan computadoras portátiles, PDAs o celulares en otras redes, como el ADSL de su casa, o la conexión wireless de algún café, y luego regresan al interior de la red corporativa listos a vulnerar el perímetro. Esto muestra que no se puede confiar en un único método para proteger el sistema, sino que debe implementarse una defensa de múltiples capas (múltiples perímetros) como si se tratara de una cebolla, para que la solución sea más fiable, además de que en cada componente de la red deben existir medidas de seguridad adicionales.

1.6.27 Seguridad en profundidad

La seguridad en profundidad asume que cada una de las medidas tomadas pueden ser rotas por algún atacante. Sin embargo, a medida que se agreguen capas en el sistema de seguridad, la probabilidad de que el atacante pueda esquivar todas y cada una de ellas sin ser descubierto disminuye proporcionalmente. Esta metodología está basada en un conjunto de reglas cada vez más restrictivas a medida que el objeto a defender se encuentre más cercano. Estas medidas están delimitadas por áreas o zonas de seguridad consideradas de la siguiente manera:

- Área de influencia: Es la zona más externa del sistema, donde es factible realizar acciones contra la integridad de ésta área.
- Área de exclusión: Es el espacio concéntrico exterior al área protegida, de utilización restringida o acceso limitado.
- Área protegida: Es el espacio delimitado por barreras físicas en el que se ejerce un cierto control de movimientos y permanencia.
- Área crítica: Es el espacio delimitado por barreras físicas, en el interior del área protegida, cuyo acceso y permanencia son objeto de especiales medidas de control.

Para reducir riesgo en un ambiente, se debe utilizar una estrategia de la defensa-en-profundidad para proteger recursos contra amenazas externas e internas. Defensa en profundidad (llamado a veces seguridad en profundidad o seguridad de varias capas) se toma de un término militar usado para

describir las contramedidas de la seguridad para formar un ambiente cohesivo de seguridad sin un solo punto de falla. Las capas de la seguridad que forman la estrategia de defensa-en-profundidad deben incluir medidas protectoras que implementen desde sus routers externos completamente a la localización de los recursos y a todos los puntos entre ellos.

Por capas múltiples se implementa seguridad, y se debe ayudar a asegurar una capa si se compromete la misma, Las otras capas proporcionarán la seguridad necesaria para proteger los recursos. Por ejemplo, el compromiso del Firewall de una organización no debe proporcionar acceso del atacante a los datos más sensibles de la organización. Cada capa debe proporcionar idealmente diversas formas de contramedidas para evitar que el mismo método de ataque sea utilizado en las diferentes capas. Se debe invertir en una protección multi-vendor contra virus si es posible. También es necesario asegurarse de que la protección de virus esté configurada en diversos puntos como gateway, server, clientes etcétera. Para reducir al mínimo la posibilidad de que un ataque contra una organización tenga éxito, se debe utilizar el mayor número posible de niveles de defensa. Defender una organización en profundidad implica el uso de varios niveles de defensa. Si un nivel se ve comprometido, ello no conlleva necesariamente que también lo esté toda la organización. Como directriz general, se debe diseñar y crear cada nivel de la seguridad bajo el supuesto de que se ha conseguido infringir la seguridad. Realizar los pasos necesarios para proteger el nivel en el que se esté trabajando.

Además, hay muchas formas de proteger cada nivel individual mediante herramientas, tecnologías, directivas y la aplicación de las recomendaciones. Por ejemplo:

- Nivel de directivas, procedimientos y concienciación: programas educativos de seguridad para los usuarios
- Nivel de seguridad física: guardias de seguridad, bloqueos y dispositivos de seguimiento
- Nivel perimetral: servidores de seguridad de hardware, software o ambos, y creación de redes privadas virtuales con procedimientos de cuarentena
- Nivel de red de Internet: segmentación de red, Seguridad IP (IPSec) y sistemas de detección de intrusos de red
- Nivel de host: prácticas destinadas a reforzar los servidores y clientes, herramientas de administración de revisiones, métodos seguros de autenticación y sistemas de detección de intrusos basados en hosts.
- Nivel de aplicación: prácticas destinadas a reforzar las aplicaciones y el software antivirus
- Nivel de datos: listas de control de acceso (ACL) y cifrado

Generalmente, los usuarios no tienen en cuenta la seguridad cuando realizan sus tareas diarias. Una directiva de seguridad para una organización debe definir:

- El uso aceptable.
- El acceso remoto.
- La protección de la información.
- La copia de seguridad de los datos.
- La seguridad del perímetro.
- La seguridad de los dispositivos y hosts básicos.

Una directiva debe comunicar consenso y proporcionar el fundamento para que el departamento de Recursos Humanos actúe en el caso de que se infrinja la seguridad. También puede ayudar a demandar a quienes logren infringir la seguridad.

Una directiva de seguridad debe proporcionar a la organización un procedimiento de tratamiento de incidentes apropiado. Debe definir:

- Las áreas de responsabilidad.
- El tipo de información que debe registrarse.
- El destino de esa información.
- Qué acciones emprender tras un incidente.

Una directiva de seguridad adecuada suele ser el fundamento del resto de prácticas de seguridad. Cada directiva debe ser lo suficientemente general para poder aplicarse en distintas tecnologías y plataformas. Al mismo tiempo, debe ser lo suficientemente específica para proporcionar a los profesionales de IT orientación sobre cómo implementar la directiva.

El ámbito de la directiva de seguridad de una organización depende del tamaño y complejidad de ésta. En muchas organizaciones hay consejos disponibles sobre cómo crear directivas de seguridad, por ejemplo, en http://www.sans.org/ y http://www.iss.net/.

Los intrusos pueden usar estratagemas sociales para aprovecharse de los usuarios que no son conscientes de los problemas de seguridad que pueden surgir en su lugar de trabajo o que los desconocen. Para los usuarios, muchas medidas de seguridad parecen innecesarias y, por lo tanto, no las siguen. Muchos ataques implican el uso de estratagemas sociales. Ciertos artificios sociales se aprovechan de la despreocupación por la seguridad con que la mayor parte de los usuarios actúan en su vida diaria. Un intruso puede emplear su tiempo de ocio o de trabajo en intentar conocer a los usuarios y ganarse su confianza. Aunque un intruso formule preguntas aparentemente inofensivas, la información que obtiene en conjunto le proporciona los medios para llevar a cabo o iniciar un ataque. Para contrarrestar estas amenazas de estratagemas sociales, las organizaciones deben implementar procedimientos claros y precisos, y procesos que deban cumplir todos los empleados, además de entrenarlos en el uso de estas directivas. Cada función que se desempeñe debe tener instrucciones claras y documentadas.

Siempre se requieren programas de aprendizaje sobre seguridad para detallar estos procesos y procedimientos. Las instrucciones deben formar una imagen completa de la seguridad de modo que los usuarios entiendan la necesidad de disponer de seguridad en todos los niveles y en todas las ocasiones. Una directiva de seguridad combina las necesidades de seguridad y la cultura de una organización. Se ve afectada por el tamaño de la organización y sus objetivos. Algunas directivas pueden ser aplicables a todos los sitios pero otras son específicas de ciertos entornos. Una directiva de seguridad debe equilibrar la posibilidad de control con la necesidad de productividad. Si las directivas son demasiado restrictivas, los usuarios siempre encontrarán formas de omitir los controles. Una organización debe demostrar un compromiso en la administración con respecto al grado de control definido en una directiva; de lo contrario, no se implementará correctamente.

1.6.28 Seguridad Física

Es muy importante ser consciente que por más que nuestra empresa sea la más segura desde el punto de vista de ataques externos, Hackers, virus, etc. la seguridad de la misma será nula si no se ha previsto como combatir un incendio. La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos tratados a continuación se prevén, otros, como la detección de un atacante interno a la empresa que intenta a acceder físicamente a una sala de operaciones de la misma, no. Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma. Así, la Seguridad Física consiste en la "*aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial*". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de

Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos. Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro.

Las principales amenazas que se prevén en la seguridad física son:

- Desastres naturales, incendios accidentales tormentas e inundaciones.
- Amenazas ocasionadas por el hombre.
- Disturbios, sabotajes internos y externos deliberados.

No hace falta recurrir a películas de espionaje para sacar ideas de cómo obtener la máxima seguridad en un sistema informático, además de que la solución sería extremadamente cara.

A veces basta recurrir al sentido común para darse cuenta que cerrar una puerta con llave o cortar la electricidad en ciertas áreas siguen siendo técnicas válidas en cualquier entorno. A continuación se analizan los peligros más importantes que se corren en un centro de procesamiento; con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos.

- Incendios
- Inundaciones
- Condiciones Climatológicas
- Señales de Radar
- Instalaciones Eléctricas
- Ergometría (*La Ergonomía es una disciplina que se ocupa de estudiar la forma en que interactúa el cuerpo humano con los artefactos y elementos que lo rodean, buscando que esa interacción sea lo menos agresiva y traumática posible*)

Instalaciones eléctricas: Trabajar con computadoras implica trabajar con electricidad. Por lo tanto esta una de las principales áreas a considerar en la seguridad física. Además, es una problemática que abarca desde el usuario hogareño hasta la gran empresa. En la medida que los sistemas se vuelven más complicados se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.

Picos y Ruidos Electromagnéticos: Las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios. También está el tema del ruido que interfiere en el funcionamiento de los componentes electrónicos. El ruido interfiere en los datos, además de favorecer la escucha electrónica.

Cableado: Los cables que se suelen utilizar para construir las redes locales van del cable telefónico normal al cable coaxial o la fibra óptica. Algunos edificios de oficinas ya se construyen con los cables instalados para evitar el tiempo y el gasto posterior, y de forma que se minimice el riesgo de un corte, rozadura u otro daño accidental. Los riesgos más comunes para el cableado se pueden resumir en los siguientes:

- Interferencia: estas modificaciones pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los cables de fibra óptica no sufren el problema de alteración (de los datos que viajan a través de él) por acción de campos eléctricos, que si sufren los cables metálicos.
- Corte del cable: la conexión establecida se rompe, lo que impide que el flujo de datos circule

por el cable.

- Daños en el cable: los daños normales con el uso pueden dañar el apantallamiento que preserva la integridad de los datos transmitidos o dañar al propio cable, lo que hace que las comunicaciones dejen de ser fiables.

En la mayor parte de las organizaciones, estos problemas entran dentro de la categoría de daños naturales. Sin embargo también se pueden ver como un medio para atacar la red si el objetivo es únicamente interferir en su funcionamiento. El cable de red ofrece también un nuevo frente de ataque para un determinado intruso que intentase acceder a los datos. Esto se puede hacer:

- Desviando o estableciendo una conexión no autorizada en la red: un sistema de administración y procedimiento de identificación de acceso adecuados hará difícil que se puedan obtener privilegios de usuarios en la red, pero los datos que fluyen a través del cable pueden estar en peligro.
- Haciendo una escucha sin establecer conexión, los datos se pueden seguir y pueden verse comprometidos.

Luego, no hace falta penetrar en los cables físicamente para obtener los datos que transportan.

Cableado de Alto Nivel de Seguridad: Son cableados de redes que se recomiendan para instalaciones con grado de seguridad militar. El objetivo es impedir la posibilidad de infiltraciones y monitoreos de la información que circula por el cable. Consta de un sistema de tubos (herméticamente cerrados) por cuyo interior circula aire a presión y el cable. A lo largo de la tubería hay sensores conectados a una computadora. Si se detecta algún tipo de variación de presión se dispara un sistema de alarma.

Pisos de Placas Extraíbles: Los cables de alimentación, comunicaciones, interconexión de equipos, receptáculos asociados con computadoras y equipos de procesamiento de datos pueden ser, en caso necesario, alojados en el espacio que, para tal fin se dispone en los pisos de placas extraíbles, debajo del mismo.

Sistema de Aire Acondicionado: Se debe proveer un sistema de calefacción, ventilación y aire acondicionado separado, que se dedique al cuarto de computadoras y equipos de proceso de datos en forma exclusiva. Teniendo en cuenta que los aparatos de aire acondicionado son causa potencial de incendios e inundaciones, es recomendable instalar redes de protección en todo el sistema de cañería al interior y al exterior, detectores y extinguidores de incendio, monitores y alarmas efectivas.

Emisiones Electromagnéticas: Desde hace tiempo se sospecha que las emisiones, de muy baja frecuencia que generan algunos periféricos, son dañinas para el ser humano.

Según recomendaciones científicas estas emisiones podrían reducirse mediante filtros adecuados al rango de las radiofrecuencias, siendo estas totalmente seguras para las personas. Para conseguir que las radiaciones sean mínimas hay que revisar los equipos constantemente y controlar su envejecimiento.

Acciones Hostiles

- Robo: Las computadoras son posesiones valiosas de las empresas y están expuestas, de la misma forma que lo están las piezas de stock e incluso el dinero. Es frecuente que los operadores utilicen la computadora de la empresa para realizar trabajos privados o para otras

organizaciones y, de esta manera, robar tiempo de máquina. La información importante o confidencial puede ser fácilmente copiada. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan menor protección que la que otorgan a una máquina de escribir o una calculadora. El software, es una propiedad muy fácilmente sustraíble y las cintas y discos son fácilmente copiados sin dejar ningún rastro

- Fraude: Cada año, millones de dólares son sustraídos de empresas y, en muchas ocasiones, las computadoras han sido utilizadas como instrumento para dichos fines. Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien pierden en imagen, no se da ninguna publicidad a este tipo de situaciones.
- Sabotaje: El peligro más temido en los centros de procesamiento de datos, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa. Físicamente, los imanes son las herramientas a las que se recurre, ya que con una ligera pasada la información desaparece, aunque las cintas estén almacenadas en el interior de su funda de protección. Una habitación llena de cintas puede ser destruida en pocos minutos y los centros de procesamiento de datos pueden ser destruidos sin entrar en ellos. Además, suciedad, partículas de metal o gasolina pueden ser introducidos por los conductos de aire acondicionado. Las líneas de comunicaciones y eléctricas pueden ser cortadas, etc.

Control de Accesos

El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.

- Utilización de Guardias
- Utilización de Detectores de Metales
- Utilización de Sistemas Biométricos (Definimos a la Biometría como "la parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos". La Biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas. La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a la persona por lo que es (manos, ojos, huellas digitales y voz).)
- Verificación Automática de Firmas
- Seguridad con Animales
- Protección Electrónica (Se llama así a la detección de robo, intrusión, asalto e incendios mediante la utilización de sensores conectados a centrales de alarmas. Estas centrales tienen conectadas los elementos de señalización que son los encargados de hacerles saber al personal de una situación de emergencia.)

1.6.29 Seguridad lógica

La Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."

Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe

estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica.

Los objetivos que se plantean serán:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Controles de Acceso

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario. Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados. Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso. Al respecto, el National Institute for Standars and Technology (NIST)(1) ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad en cualquier sistema:

- Identificación y Autentificación
- Roles
- Transacciones
- Limitaciones a los Servicios
- Modalidad de Acceso (Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información)
- Ubicación y Horario
- Control de Acceso Interno
- Control de Acceso Externo
- Administración

Niveles de Seguridad Informática

El estándar de niveles de seguridad mas utilizado internacionalmente es el TCSEC Orange Book, desarrollado en 1983 de acuerdo a las normas de seguridad en computadoras del Departamento de Defensa de los Estados Unidos. Los niveles describen diferentes tipos de seguridad del Sistema

Operativo y se enumeran desde el mínimo grado de seguridad al máximo.

Estos niveles han sido la base de desarrollo de estándares europeos (ITSEC/ITSEM) y luego internacionales (ISO/IEC). Cabe aclarar que cada nivel requiere todos los niveles definidos anteriormente: así el subnivel B2 abarca los subniveles B1, C2, C1 y el D.

- ***Nivel D:*** Este nivel contiene sólo una división y está reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad. Sin sistemas no confiables, no hay protección para el hardware, el sistema operativo es inestable y no hay autentificación con respecto a los usuarios y sus derechos en el acceso a la información. Los sistemas operativos que responden a este nivel son MS-DOS y System 7.0 de Macintosh.
- ***Nivel C1: Protección Discrecional:*** Se requiere identificación de usuarios que permite el acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso. Muchas de las tareas cotidianas de administración del sistema sólo pueden ser realizadas por este "super usuario" quien tiene gran responsabilidad en la seguridad del mismo. Con la actual descentralización de los sistemas de cómputos, no es raro que en una organización encontremos dos o tres personas cumpliendo este rol. Esto es un problema, pues no hay forma de distinguir entre los cambios que hizo cada usuario. A continuación se enumeran los requerimientos mínimos que debe cumplir la clase C1:
    - ***Acceso de control discrecional:*** distinción entre usuarios y recursos. Se podrán definir grupos de usuarios (con los mismos privilegios) y grupos de objetos (archivos, directorios, disco) sobre los cuales podrán actuar usuarios o grupos de ellos.
    - ***Identificación y Autentificación:*** se requiere que un usuario se identifique antes de comenzar a ejecutar acciones sobre el sistema. El dato de un usuario no podrá ser accedido por un usuario sin autorización o identificación.
- ***Nivel C2: Protección de Acceso Controlado:*** Este subnivel fue diseñado para solucionar las debilidades del C1. Cuenta con características adicionales que crean un ambiente de acceso controlado. Se debe llevar una auditoria de accesos e intentos fallidos de acceso a objetos. Tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización. Requiere que se audite el sistema. Esta auditoría es utilizada para llevar registros de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios. La auditoría requiere de autenticación adicional para estar seguros de que la persona que ejecuta el comando es quien dice ser. Su mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos. Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de administración del sistema sin necesidad de ser administradores. Permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.
- ***Nivel B1: Seguridad Etiquetada:*** Este subnivel, es el primero de los tres con que cuenta el nivel B. Soporta seguridad multinivel, como la secreta y ultrasecreta. Se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio. A cada objeto del sistema (usuario, dato, etc.) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, etc.) y con unas categorías (contabilidad, nóminas, ventas, etc.). Cada usuario que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa. Es decir que cada usuario tiene sus objetos asociados. También se establecen controles para limitar la propagación de derecho de accesos a los distintos objetos.
- ***Nivel B2: Protección Estructurada:*** Requiere que se etiquete cada objeto de nivel superior por ser padre de un objeto inferior. La Protección Estructurada es la primera que empieza a referirse al problema de un objeto a un nivel mas elevado de seguridad en comunicación con

otro objeto a un nivel inferior. Así, un disco rígido será etiquetado por almacenar archivos que son accedidos por distintos usuarios. El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas; y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.

- ***Nivel B3: Dominios de Seguridad:*** Refuerza a los dominios con la instalación de hardware: por ejemplo el hardware de administración de memoria se usa para proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos de diferentes dominios de seguridad. Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido. Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y testeos ante posibles violaciones. Este nivel requiere que la terminal del usuario se conecte al sistema por medio de una conexión segura. Además, cada usuario tiene asignado los lugares y objetos a los que puede acceder.
- ***Nivel A: Protección Verificada:*** Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema. Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. El software y el hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento.

1.7.1 SEGURIDAD EN REDES

Como se expresó anteriormente, la seguridad de la información se encarga de garantizar la confidencialidad, integridad y disponibilidad de la información. Para cumplir estos objetivos es necesario pensar la seguridad como un proceso, desarrollado a través de las siguientes etapas:

Prevención: Se refiere a prevenir la ocurrencia de infracciones a la seguridad de las computadoras o información, estas violaciones se conocen como incidentes. Generalmente, un incidente pone de manifiesto el fracaso de un procedimiento de seguridad . Los incidentes vienen en todas las formas y tamaños. Podemos clasificarlos como simples o mayores, un incidente simple puede ser una sesión bloqueada por un usuario que olvidó su contraseña, en cambio un incidente mayor sería la modificación del contenido de nuestro sitio web. Idealmente, la implantación de procedimientos y políticas de seguridad adecuados deberían garantizar que nuestra organización sea invulnerable a los ataques. Desafortunadamente, éste no es el caso, pero podemos asegurar que cuanto mejores sean las políticas de prevención, menor será la probabilidad de que ocurra un ataque exitoso.

Detección: Se refiere a la identificación de los incidentes. En muchas situaciones es muy complicada de realizar, porque involucra, no sólo la identificación de los activos afectados, sino además cómo ocurrió el ataque, y quién fue el autor. Dependiendo de la naturaleza del incidente, el proceso de detección puede ser llevado a cabo utilizando herramientas especiales de auditoría o un simple análisis de los archivos de registro de las aplicaciones (log files). Es recomendable que las actividades de detección sean parte de las políticas y procedimientos de seguridad.

Respuesta: Se refiere a desarrollar estrategias y técnicas que indiquen cómo proceder ante un incidente. El desarrollo de una respuesta apropiada involucra varios factores, por ejemplo, la naturaleza de los ataques y los posibles objetivos, es decir, la estrategia de respuesta no será la misma si el incidente fue sólo una exploración de nuestra red o la penetración de un sistema. Entonces, cuando ocurra un incidente, debemos contar con un plan de respuesta bien pensado y testeado, donde encontremos las estrategias de recuperación y neutralización de las amenazas.

La evaluación de estos objetivos, es una parte importante de los análisis que se realizan en las organizaciones para determinar el nivel de seguridad que posee. Si no se han tenido en cuenta en el desarrollo de su infraestructura probablemente se lleven una sorpresa en cualquier momento, esta sorpresa no será agradable, y seguramente sus efectos sean costosos de solucionar.

1.7.3 Marco de seguridad: *Security Wheel*

El incremento del acceso a recursos corporativos a través de Internet, así como la proliferación de aplicaciones que permiten la comunicación entre usuarios a través de canales no seguros, ha tenido como consecuencia, no sólo que el diseño de las redes tenga como punto central el concepto de seguridad, sino además que se considere la seguridad en redes como un proceso dinámico, continuo e iterativo.

A continuación vamos a desarrollar un modelo denominado Security Wheel (Rueda de Seguridad), que se basa en esta idea.

La Rueda de Seguridad (Security Wheel) hace referencia a un proceso no a un evento. Dada la complejidad, y naturaleza iterativa de la segurización de una empresa, el proceso nunca debería detenerse si la empresa desea estar protegida de las amenazas más recientes.

Este proceso incorpora los siguientes pasos:

1. Desarrollar una Política de Seguridad.
2. Proteger la información de la empresa en el nivel deseado.
3. Observar la actividad en los puntos de acceso críticos de la red.
4. Asegurar que las medidas de seguridad son suficientes para resistir los métodos de intrusión y herramientas actuales.
5. Agregar o actualizar las medidas de seguridad según sea necesario.

Este proceso es un esfuerzo continuo e iterativo de parte de la compañía por proteger sus recursos más importantes al costo más conveniente, mientras se reducen los riesgos al nivel apropiado.

1.7.4 Segurización

Después de desarrollar una política de seguridad, debe asegurar su red utilizando las tecnologías disponibles en el mercado (Firewalls, Sistemas de Detección de Intrusiones, Routers, VLANs).

Sin embargo, antes que pueda segurizar su red necesita analizar su conocimiento sobre los usuarios, los activos que necesitan protección, los servicios, la topología de red. Deberá tener en cuenta que las medidas de seguridad deben representar un balance entre un uso transparente para los usuarios y la máxima seguridad, a un costo razonable.

1.7.5 Monitoreo

Una vez que la red ha sido segurizada, se deberá monitorear la actividad en la red. Este proceso puede realizarse con herramientas sofisticadas como los sistemas de detección de intrusiones, que analizan el tráfico de la red en busca de patrones anormales y además, permiten recibir información de dispositivos similares ubicados en otros puntos de la red. Para completar el monitoreo sería conveniente activar y analizar todos los días los logs de los servidores y dispositivos de comunicación que tengamos en nuestra red. Cuando se detecta un incidente, se debe responder en forma rápida y apropiada, según lo que indique la política. Algunas de las acciones podrán estar configuradas en los dispositivos de manera que actúen en forma automática, sin nuestra intervención, por ejemplo los sistemas de detección de intrusiones podrían ejecutar una variedad de acciones, desde realizar un log del incidente, hasta reconfigurar las políticas de acceso en los dispositivos de comunicación (Router o Firewall) para impedir el ingreso del tráfico que generó el incidente.

1.7.6 Testing

Periódicamente deberá escanear la red en busca de nuevas vulnerabilidades, utilizando herramientas especialmente diseñadas para esta tarea. Está claro que lo mejor es actuar en forma proactiva, es decir, necesitamos encontrar las vulnerabilidades antes de que se produzca el ataque. Lamentablemente, es inevitable que aparezcan nuevos "agujeros de seguridad" en un ambiente creciente y cambiante como el de las redes actuales. Por esta razón deberá testear continuamente los recursos que han sufrido modificaciones, por ejemplo, instalación de nuevas aplicaciones, sistemas operativos, nuevos equipos de comunicaciones, Firewalls, routers, switchs, sistemas de detección de intrusiones, antivirus, etc.

1.7.7 Perfeccionamiento

Deberá analizar todos los resultados obtenidos a través de los anteriores pasos del ciclo de seguridad, luego implementar las contra medidas y mejoras necesarias en la política de seguridad de la red para estar protegido respecto a las últimas amenazas detectadas. No nos olvidemos del último paso, tan importante como los otros: comenzar nuevamente el ciclo de la Rueda de Seguridad.

1.7.8 Integración a la Política de Seguridad

En el centro de la rueda encontramos el elemento más importante, la política de seguridad. Vemos cómo se relaciona con cada paso del proceso, en un doble sentido, primero cada paso debe estar guiado según los lineamientos establecidos en la política, y por otro lado los resultados de una etapa pueden generar modificaciones en la misma.

Entonces a través de la política de seguridad podremos:

- Dirigir el desarrollo de las medidas de seguridad en la empresa
- Determinar cuáles activos son importantes
- Definir cuánto está dispuesto a invertir (en términos, de dinero, personal, y tiempo) para proteger los recursos que considera importante
- Determinar cuál es el nivel de riesgo admisible para cada amenaza

En cierta forma una política de seguridad es un plan de administración de riesgos, porque determina

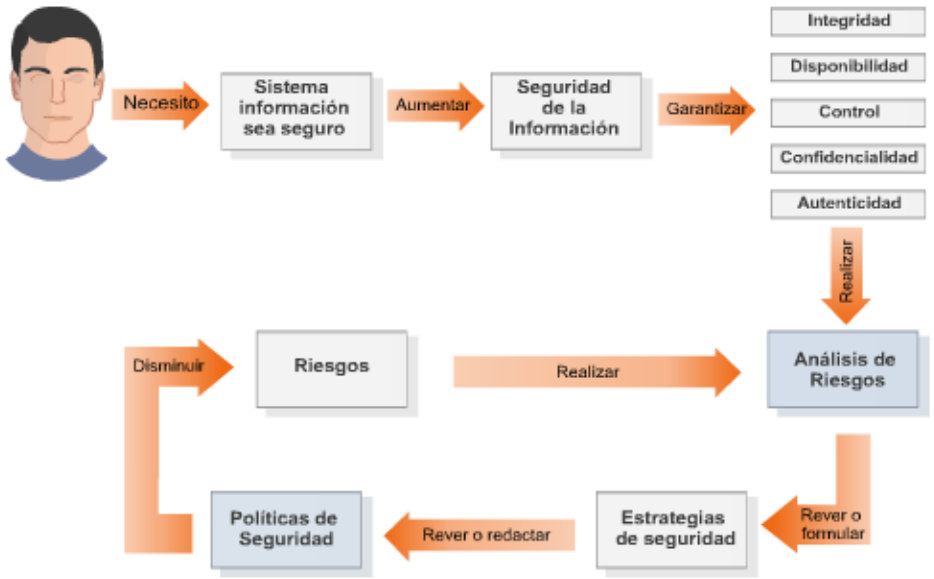
el umbral de riesgo que una organización está dispuesta a aceptar. Esto se debe a varios motivos, primero podemos afirmar que no existe una tecnología de seguridad que nos garantice un 100% de protección, pero aunque podemos acercarnos a un ideal, la mayoría de las organizaciones no tienen el presupuesto para implementar todas las medidas de seguridad requeridas. Entonces debemos implementar la mejor política de seguridad que nuestro presupuesto pueda pagar, para lo cual debemos centrarnos en los recursos más valiosos y aplicar medidas de protección de acuerdo a su importancia.

1.8 SÍNTESIS

Presentamos conceptos fundamentales de seguridad, en busca de la respuesta a las siguientes preguntas, ¿Qué es la seguridad de la información? y ¿Cuál es su objetivo? para responder estas preguntas debimos introducir un conjunto de conceptos asociados.

Definimos primero que una Amenaza es cualquier elemento que comprometa al sistema, definiendo este último como el conjunto formado por las personas, computadoras (hardware y software), papeles, medios de almacenamiento digital, información y el entorno donde actúan y sus interacciones.

En relación con las amenazas y los problemas de seguridad observamos que los técnicos en sistemas de información, normalmente, buscan medidas defensivas que no solucionan el problema de fondo, sólo lo transforma o retrasa, la amenaza o riesgo sigue allí. Entonces, podemos definir Riesgo como la proximidad o posibilidad de daño sobre un bien, ya se trate de actos naturales, errores u omisiones humanas y actos intencionales de vándalos. Luego, el Daño o Incidente es el resultado de la amenaza; aunque esto es sólo la mitad del axioma. El daño también es el resultado de la no acción, o acción defectuosa, del protector. El protector será el encargado de detectar cada una de las Vulnerabilidades, es decir, las debilidades del sistema que pueden ser explotadas y empleadas por la amenaza para comprometerlo. También será el encargado de aplicar las Contramedidas o técnicas de protección adecuadas.



Por último, la Seguridad de la información representa el índice en que un Sistema Informático está libre de todo peligro, daño o riesgo. Esta característica es muy difícil de conseguir en un 100%, en virtud de esto, normalmente se implementan medidas para acercarse al 100%.

Para garantizar que un sistema sea seguro se deberá garantizar las características de Integridad,

Disponibilidad, Confidencialidad, Control y Autenticidad. Será conveniente realizar un Análisis de Riesgos, para conocer ¿qué es lo que queremos proteger?, ¿de quién lo queremos proteger?, ¿cómo se puede lograr esto legislativa y técnicamente?; para luego concluir con la formulación de estrategias adecuadas de seguridad tendientes a la disminución de los riesgos, que se plasmarán en una política de seguridad.

No se debe confundir la seguridad de la información con la seguridad informática ya que la seguridad de la información abarca muchas más áreas mientras que la seguridad informática se encarga de la protección de las infraestructuras TIC que soportan el negocio. Por tanto la seguridad de la información abarca la seguridad informática.

1.9.1 PREGUNTAS Y TIPS

- **¿Qué es la seguridad de la información?** Es un índice que nos indica nuestra percepción del nivel de protección de nuestro sistema informático, es decir, que está libre de todo peligro, daño o riesgo.
- **¿Por qué es necesaria la seguridad de la información?** La información y los sistemas de procesamiento, por un lado, y los sistemas de comunicaciones y las redes que les brindan apoyo son esenciales para el normal desenvolvimiento de las tareas en las empresas modernas.
- **¿Cuál es el objetivo de la seguridad de la información?** Preservar las características de confidencialidad, integridad y disponibilidad de la información
- **¿Qué es una política de seguridad?** Es una declaración formal de las reglas que deben respetar las personas cuando acceden a la información y demás recursos tecnológicos de una organización.
- **La Seguridad de la Información se enfoca en proteger la información y no el hardware y software que la procesa.**
- **El modelo operacional de la Seguridad Informática nos dice que la protección se ofrece mediante prevención, detección y respuesta.**
- **"Host Security" se enfoca en proteger cada computador de forma individual, en vez de proteger toda una red entera.**
- **"Acceso" es la habilidad para interactuar con un objeto. "Control de Acceso" son los dispositivos o métodos usados para limitar el Acceso a objetos específicos**
- **¿Cuáles son tipos de documentación que deben ser contemplados durante el desarrollo de software?** Documentación técnica del proyecto, Manual de usuario
- **¿Cómo se denomina al hecho de incorporar la combinación de usuarios y contraseñas (o solo una de ellas) dentro del código?** Hardcoed
- **¿Cómo se denomina el mecanismo de control que implementa Java, respecto de lo que un programa puede o no hacer?** Sandbox
- **¿Cómo se denomina el manual que define un estándar de programación segura, liberado a través de ISECOM?** SPSMM
- **¿Cómo se denomina al proyecto open source para la seguridad de aplicaciones Web?** OWASP
- **¿Con qué término se conoce al canal de comunicación que permite la transferencia de información entre dos procesos, violando la política de seguridad del sistema?** Covert Channel
- **El desarrollo de código seguro implica el conocimiento de:** Comunicaciones, Hardware, Sistema operativo, Compiladores
- **Cual de los siguientes elementos no es un activo de información: Plantilla de la organización, Libros de contabilidad, Mobiliario?** El Mobiliario
- La información puede ser un activo tangible o intangible.
- Conseguir un nivel adecuado de seguridad en una empresa precisa de Responsabilidad, infraestructura e implicación de la dirección

CAPÍTULO 2

2.1 ELEMENTOS BÁSICOS DE NETWORKING

El estudio de las vulnerabilidades y seguridad en redes informáticas, exige la comprensión de los fundamentos de las redes, sus principales tecnologías y las recomendaciones de seguridad más apropiadas

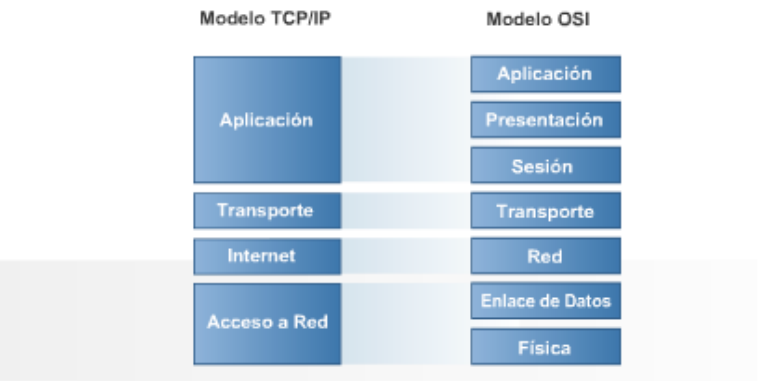
¿Qué es el modelo de referencia OSI? Esta considerado como el modelo principal para el análisis de las comunicaciones en una red. Fue liberado en 1984 y es utilizado por la ISO para describir el flujo de información en una red, basándose en el concepto de modelo estratificado en capas. Este modelo permite a los desarrolladores disponer de un conjunto de reglas que aseguren mayor compatibilidad e interoperatibilidad entre las distintas tecnologías de red producidas por empresas en el mundo entero.

¿Para que se utiliza IP? Es el protocolo que utiliza internet para encaminar la información entre dispositivos, por este motivo toda maquina que se conecte a Internet debe impremantar este dispositivo.

IP es el protocolo de capa de red de la familia de protocolos TCP/IP, interactúa en esta capa con un conjunto de protocolos subsiriarios que aportan mensajes de control y resolución de direcciones físicas a direcciones IP

¿Qué relación hay entre el modelo de referencia OSI y la pila de protocolos TCP/IP?

Ambos son modelos de networking divididos en capas. Su relación capa a capa se puede ver en el siguiente gráfico



¿Qué es Ethernet? Es la tecnología LAN más ampliamente utilizada. Define un acceso compartido al medio, ordenado por el protocolo CSMA/CD. Permite transmitir información sobre diferentes medio, Coaxial, Fibra óptica, par trenzado, con diferentes anchos de banda, desde 10 Mbps hasta 10 Gbps.

¿Qué significa la denominación EDI? La denominación EDI o intercambio electrónico de datos corresponde a una estructura común de documentos, por medio del cual las empresas que lo implementan pueden intercambiar información de negocios, bienes y servicios, utilizando

computadoras a través de redes privadas, empleando un formato estándar y minimizando los costos operativos. También es conocida con la denominación B2B (Bussiness to Business).

2.2 UN POCO DE HISTORIA

La idea de red de comunicaciones como infraestructura para ofrecer algún servicio de comunicación de información quizás se remonte muchos siglos atrás. Las redes basadas en el fenómeno de la electricidad se remontan a mediados del siglo XIX, con la invención del telégrafo. Pero las redes de comunicación de datos, digitales, surgen a partir de la invención del ordenador moderno, hacia la década de 1960 (aunque existieron máquinas de calcular bastante antes: el ábaco de los árabes, la máquina de Leibniz y ya en el siglo XX, el computador ENIAC, basado en válvulas de vacío).

Los primeros ordenadores con transistores eran equipos grandes y costosos en posesión de unas pocas empresas (los llamados centros de cálculo). Ofrecían los servicios a clientes que se desplazaban físicamente para entregar los datos de entrada y recoger los datos de salida. Es decir, al principio el acceso a los ordenadores era local, a través de terminales relativamente rudimentarios conectados a ellos (lectores de tarjetas perforadas con los programas y datos, impresores en papel continuo, teclados y pantallas de rayos catódicos, a lo sumo).

Con el fin de mejorar los servicios ofrecidos a sus clientes, los centros de cálculo habilitaron terminales en las ubicaciones de aquéllos para permitir el acceso remoto, usando módems y la red analógica de telefonía (la única realmente extendida en aquella época). Con el tiempo los ordenadores empezaron a conectarse entre sí para compartir datos y capacidad de proceso entre ellos, así como terminales de entrada/salida más sofisticados.

Ya tenemos las redes de ordenadores o de comunicación de datos. La conectividad entre ordenadores y terminales requirió la adición de hardware (los llamados front-end de comunicaciones) y software (los protocolos de comunicación). Cada fabricante de ordenadores escogió su propio camino, es decir, escogió su propia arquitectura de comunicaciones. Pero antes de definir con más exactitud eso, se hará un breve repaso a la historia de las redes de datos.

Postrimerías de la década de 1960: En EUA, ARPA (Advanced Research Projects Agency) promueve el desarrollo de una red específica para la comunicación entre los ordenadores de centros federales militares y de investigación. Dicha red debía ser robusta ante fallos de algunos de sus elementos (topología en malla con caminos redundantes) y adaptada al tráfico generado por los ordenadores (el paquete como unidad de información). Esa red, llamada ARPANet, fue el embrión de lo que hoy conocemos como Internet.

Principios de la década de 1970: IBM presenta su arquitectura de comunicaciones SNA (System Network Architecture). Poco después Digital presenta la suya DNA (Digital Network Architecture); Xerox, en sus laboratorios de Palo Alto (California, EUA) desarrolla una red de ámbito local y topología en bus bautizada como Ethernet para conectar estaciones de trabajo a elevada velocidad; en Canadá, DATAPAC significa una de las primeras redes públicas de datos.

Principios de la década de 1980: IBM, en sus laboratorios de Zurich (Suiza), desarrolla la red Token Ring, otra red de ámbito local con topología en anillo y filosofía de acceso diferente al de la red Ethernet. En 1985, la red SITA desarrollada por y para las compañías de transporte aéreo está ampliamente extendida.

En España: A principios de la década de 1970 la CTNE (Compañía Telefónica Nacional de España) presenta su red pública de datos IBERPAC; la compañía influye de forma notable en la definición, a nivel internacional en el CCITT, en la definición del estándar X.25 para dicho tipo de redes; en 1982 la red sufre un cambio de tecnología con la adopción de equipos propios de fabricación nacional (los sistemas TESYS).

Año 1978: La ISO (International Standards Organization) promueve el desarrollo de un modelo de referencia para el desarrollo de una arquitectura de comunicaciones para la interconexión de sistemas abiertos (OSI: Open Systems Interconnection).

Mediados de la década de 1990: “Explosión” de Internet y de las comunicaciones móviles celulares.

2.3 LAS TELECOMUNICACIONES

Una red de telecomunicaciones sirve para satisfacer la necesidad que tienen los usuarios de transferir información desde un punto origen a un punto destino; como ejemplo podemos citar una conversación telefónica, el envío de un fax, etc. A estas necesidades especificas de telecomunicación que tienen los usuarios se las denomina servicios finales o teleservicios.

Los servicios portadores son el resultado de la capacidad que tiene la red para transferir información extremo a extremo, independientemente del servicio final que soporte. Mediante estas capacidades portadoras de la red se prestan los servicios finales.

Los servicios suplementarios o servicios de valor añadido aportan información adicional al proceso de transferencia de información entre los puntos A y B, esta información adicional no es imprescindible para la comunicación. Algunos ejemplos son la tarificación detallada, información del número llamante, el contestador automático en red, etc.

Los servicios ofrecidos por la telemática se basan en unas redes de telecomunicaciones conectadas a unos centros de servicios que ponen a disposición de los usuarios bancos de datos o programas para la realización de tareas especificas. El usuario tiene acceso a estas redes mediante terminales apropiados que visualizan y/o procesan la información que transmiten las redes. Entre los servicios telemáticos podemos citar los servicios bancarios y el pago electrónico, en los que una red de oficinas se encuentran interconectadas por medio de una red de datos con los ordenadores centrales o centros de cálculo, desde donde se proporciona, actualiza y procesa la información que las transacciones bancarias requieran.

Desde sus orígenes, la industria de las telecomunicaciones nunca ha experimentado cambios tan drásticos como en la ultima década, donde la liberalización y la competencia son las causantes de una profunda reestructuración en el mercado de las telecomunicaciones.

Como ya hemos visto, para transportar información de un punto a otro ha de haber un camino físico entre el origen y el destino, a este medio se le denomina canal de comunicación. Para que la información enviada por un extremo de ese canal se reciba correctamente en el otro extremo, la información a transmitir tiene que sufrir un proceso de codificación y adaptación al medio, siendo necesario que cumpla una serie de requisitos como son la velocidad, la sincronización, etc. En las redes de comunicaciones de datos generalmente se trata de conectar a dos o más equipos informáticos para que se puedan transferir información entre ellos.

Partimos de la base de que los ordenadores y equipos de datos trabajan con información digital binaria, señal que solo puede tomar dos estados. Cuando estos ordenadores se quieran comunicar, porque tienen información de un usuario para otro, se enviarán mensajes que están compuestos por una secuencia de bits que tendrán que codificarse, de manera que el ordenador que los reciba pueda “entender” esa información y manejarla de la forma adecuada. Las señales que se transmiten por el canal de comunicación tendrán que cumplir una serie de requisitos como son el momento exacto y la velocidad adecuada para el envío de los datos previamente codificados.

2.3.1 Señales analógicas y digitales

Toda señal eléctrica está caracterizada por una serie de parámetros como son la amplitud de la señal, su frecuencia y la fase. La amplitud indica el valor de la magnitud física de la señal, por ejemplo el voltaje o la corriente; la frecuencia siempre que sea una señal periódica, es el número de veces que esta señal se repite en un periodo de tiempo de un segundo y la fase representa el avance o retraso del paso por cero de la amplitud de la señal con respecto al origen de tiempos.

Una señal analógica es aquella señal cuya variación de amplitud es continua en el tiempo, pudiendo tomar en cada instante de tiempo infinitos valores.

Una señal digital es aquella que solo puede tomar un número de valores discretos a lo largo del tiempo, en cada instante de tiempo solo puede tomar una serie de valores finitos. Su variación por tanto presenta discontinuidades en el tiempo.

2.3.2 Transmisión de señales

Para transmitir una información por un sistema de telecomunicaciones, existe la posibilidad de transmitir la señal de manera analógica o digital. Esta señal tendrá una atenuación en el medio de transmisión y además podrá sufrir una serie de perturbaciones, internas o externas al propio medio como pueden ser: distorsiones, diafonías, ruidos e interferencias, que harán que la señal se altere y no llegue exactamente la misma información al destino. Todas estas alteraciones las sufren por igual tanto las señales analógicas como las digitales, sin embargo no las afecta de la misma manera, caracterizándose cada una por tener sus ventajas e inconvenientes.

2.3.3 Líneas de transmisión

Es el medio utilizado para la unión entre distintos equipos de transmisión de información. En función de la naturaleza de las señales que transportan se pueden clasificar en analógicas y digitales.

Líneas analógicas en banda vocal: su margen de utilización está comprendido entre los 300 y los 3400 hercios, estando constituidas por pares metálicos que son las que normalmente llegan hasta el usuario, sistemas analógicos de transmisión utilizando la técnica de multiplexacción por división de frecuencias (MDF) y sistemas digitales de transmisión usando la técnica de multiplexación por división en el tiempo (MDT).

Líneas digitales: se utilizan para cualquier ancho de banda, estando formadas por pares metálicos hasta 2 Mbit/s, cable coaxial para velocidades iguales o superiores a 2 Mbit/s y distancias cortas, fibra óptica para velocidades superiores a 2 Mbit/s y distancias largas y los sistemas digitales de transmisión como la Jerarquía Digital Síncrona (JDS).

El envío de información entre dos dispositivos se puede realizar de diferentes formas teniendo en cuenta los siguientes parámetros y modos de transmisión que caracterizan el enlace de datos.

- **Transmisión serie:** Este modo de transmisión se caracteriza porque los datos son enviados uno a uno, bit a bit, uno a continuación de otro de manera secuencial y por un único canal de transmisión. Normalmente se utiliza cuando la distancia entre emisor y receptor es grande, ya que, a diferencia de la transmisión en paralelo, permite economizar circuitos físicos o canales de transmisión.
- **Transmisión paralelo:** En este modo de operación se envían en cada instante de tiempo varios datos simultáneamente, utilizando para ello varios circuitos entre el emisor y el receptor, tantos como datos se envían cada vez.

  Frente a la transmisión en serie tiene la ventaja de que multiplica la velocidad por el número de datos que se envían simultáneamente, pero tiene la desventaja de necesitar varios circuitos, estando recomendada para pequeñas distancias (del orden de unos metros como máximo).

2.3.4 Sincronismo

En la transmisión digital, para que el receptor pueda recuperar la información, es absolutamente

necesario que esté sincronizado con el emisor, esto es que tengan como referencia la misma base de tiempos.

- **Señal anisócrona:** Se llama anisócrona a una señal digital cuando los instantes significativos de la misma aparecen en cualquier momento, sin ninguna restricción; la duración de los impulsos que representan los datos no tienen porqué ser múltiplos.
- **Señal isócrona:** Se llama isócrona a una señal digital cuando los intervalos significativos son múltiplos de un determinado valor “T”

Normalmente las señales digitales son generadas teniendo como referencia un reloj o base de tiempos. Si una señal es generada por un único reloj todas las transiciones entre elementos serán múltiplos de un mismo valor “T”, siendo la señal resultante isócrona.

- **Transmisión síncrona:** En transmisión síncrona se envía, además de los datos la señal de reloj; de esta manera el receptor se sincroniza con el emisor y determina los instantes significativos de la señal que recibe. Los datos se transmiten de manera consecutiva entre el emisor y el receptor, con un flujo constante que viene determinado por la señal del reloj de sincronismo.

  Cuando se trata de transmisión de señales por pares metálicos en donde intervienen un terminal u ordenador (ETD) y un módem (ETCD), la señal o reloj de sincronismo del emisor puede generarse en cualquiera de estos dispositivos siendo común para ambos. En el receptor el módem es el encargado de generar la señal de sincronismo a partir de la señal que le llega por la línea.

  En la transmisión síncrona los datos que se envían se agrupan en bloques formando tramas, que son un conjunto consecutivo de bits con un tamaño y estructura determinados.
- Este tipo de transmisión es más eficiente en la utilización del medio de transmisión que la asíncrona, siendo también más inmune a errores por lo que se suele usar para mayores velocidades que la asíncrona.
- **Transmisión asíncrona:** Este modo de transmisión se caracteriza porque la base de tiempo del emisor y receptor no es la misma, empleándose un reloj para la generación de datos en la transmisión y otro distinto para la recepción.

  En este tipo de transmisión la información se transmite por palabras, bytes o conjunto de bits, estando precedidos estos bits por un bit de arranque o “start” y finalizando con al menos un bit de parada o “stop” pudiendo ser también 1,5 o 2 bits. A este conjunto de bits se le denomina carácter, pudiéndose transmitir en cualquier momento, es decir que entre dos informaciones consecutivas (al contrario de lo que ocurre en la transmisión síncrona) no tiene porqué haber un tiempo que sea múltiplo de un elemento unitario “bit”.

  En este tipo de transmisión, el receptor sincroniza su reloj con el transmisor usando el bit de arranque que llega con cada carácter.

2.3.5 Clasificación de los sistemas de transmisión

Los sistemas se pueden clasificar según su direccionalidad y momento en el que se efectúa la transmisión en los siguientes tipos:

- ***Símplex*** En este modo solo es posible la transmisión en un sentido, del terminal que origina la información hacia el que la recibe y procesa. Un ejemplo claro de este tipo son las emisoras de radiodifusión.

- ***Semidúplex*** (*half – dúplex*) Permite la transmisión en ambos sentidos de manera alterna. Un ejemplo de este tipo son las transmisiones efectuadas por radioaficionados.
- ***Dúplex*** (*full – dúplex*) Consiste en la transmisión en ambos sentidos de manera simultánea. Esta forma de trabajo es la más eficiente. Un ejemplo son las comunicaciones telefónicas.

2.3.6 Ancho de banda

El ancho de banda ocupado por una señal es la diferencia existente entre la frecuencia máxima y mínima de su espectro en frecuencias. Puesto que el espectro de muchas señales es infinito, el espectro efectivo se considera aquel en el que la señal tiene su mayor componente de energía. Suele considerarse aquel en el que la señal tiene el 90% de la energía.

El ancho de banda se define como la cantidad de información que puede fluir a través de una conexión de red en un período dado Es esencial comprender el concepto de ancho de banda al estudiar networking, por las siguientes cuatro razones:

- *El ancho de banda es finito*.
- *El ancho de banda no es gratuito*.
- *El ancho de banda es un factor clave a la hora de analizar el rendimiento de una red, diseñar nuevas redes y comprender la Internet*.
- *La demanda de ancho de banda no para de crecer*.

En los sistemas digitales, la unidad básica del ancho de banda es bits por segundo (bps). El ancho de banda es la medición de la cantidad de información, o bits, que puede fluir desde un lugar hacia otro en un período de tiempo determinado, o segundos. Aunque el ancho de banda se puede describir en bits por segundo, se suelen usar múltiplos de bits por segundo. En otras palabras, el ancho de banda de una red generalmente se describe en términos de miles de bits por segundo (kbps), millones de bits por segundo (Mbps), miles de millones de bits por segundo (Gbps) y billones de bits por segundo (Tbps). A pesar de que las expresiones ancho de banda y velocidad a menudo se usan en forma indistinta, no significan exactamente lo mismo. Se puede decir, por ejemplo, que una conexión T3 a 45Mbps opera a una velocidad mayor que una conexión T1 a 1,544Mbps. No obstante, si sólo se utiliza una cantidad pequeña de su capacidad para transportar datos, cada uno de estos tipos de conexión transportará datos a aproximadamente la misma velocidad. Por ejemplo, una cantidad pequeña de agua fluirá a la misma velocidad por una tubería pequeña y por una tubería grande. Por lo tanto, suele ser más exacto decir que una conexión T3 posee un mayor ancho de banda que una conexión T1. Esto es así porque la conexión T3 posee la capacidad para transportar más información en el mismo período de tiempo, y no porque tenga mayor velocidad.

El ancho de banda varía según el tipo de medio, además de las tecnologías LAN y WAN utilizadas. La física de los medios fundamenta algunas de las diferencias. Las señales se transmiten a través de cables de cobre de par trenzado, cables coaxiales, fibras ópticas, y por el aire. Las diferencias físicas en las formas en que se transmiten las señales son las que generan las limitaciones fundamentales en la capacidad que posee un medio dado para transportar información. No obstante, el verdadero ancho de banda de una red queda determinado por una combinación de los medios físicos y las tecnologías seleccionadas para señalizar y detectar señales de red. Por ejemplo, la actual comprensión de la física de los cables de cobre de par trenzado no blindados (UTP) establece el límite teórico del ancho de banda en más de un gigabit por segundo (Gbps). Sin embargo, en la realidad, el ancho de banda queda determinado por el uso de Ethernet 10BASE-T, 100BASE-TX, o 1000BASE-TX. En otras palabras, el ancho de banda real queda determinado por los métodos de señalización, las tarjetas de interfaz de red (NIC) y los demás equipos de red seleccionados. Por lo tanto, el ancho de banda no sólo queda determinado por las limitaciones de los medios.

2.3.7 Tecnologías y equipos de acceso a las redes de datos

Las señales de datos son generadas y almacenadas por dispositivos de procesamiento, generalmente ordenadores que trabajan de forma digital con datos binarios (bits). Para que estos dispositivos se puedan comunicar por medio de redes de datos es necesario el envío de la información digital a grandes distancias. Para posibilitar esa comunicación es necesario conectar a los ordenadores o controladores de comunicaciones (ETD) con equipos diseñados para realizar esta función (ETCD).

Para el transporte de datos las señales (bits) pueden ser enviadas de dos formas: de forma digital adaptando los niveles al medio de transmisión, o bien de manera analógica modulando y demodulando la señal que se envía. Según la técnica utilizada y las tecnologías empleadas para su desarrollo aparecen distintos dispositivos.

Los dispositivos ETCD más conocidos y más usados son los modems, que convierten la señal digital (fuente de datos) que tiene un gran ancho de banda, en una señal analógica con menor requerimiento de ancho de banda y apta para el envío a la línea de transmisión.

La mayoría de estos dispositivos siguen unas normas de estandarización propuestas por organismos internacionales como la UIT-T, para de esta manera poder conectar con otros equipos que cumplan las mismas normas aunque sean de distintos fabricantes.

Otros equipos que también trabajan con señales analógicas son los que utilizan tecnología xDSL (HDSL, ADSL, VDSL), dispositivos que últimamente están teniendo mucho auge, ya que multiplican la velocidad de la línea telefónica convencional (par de cobre) hasta valores impensables hace poco tiempo, permitiendo mantener conversaciones telefónicas simultáneamente al envío de datos, un hecho que no es posible con los módems tradicionales.

Otro equipo de acceso son las UTR (Unidades de Terminación de Red), en ocasiones llamados módems banda base; estos equipos envían señales digitales “adaptadas” a la línea de transmisión, conformando y filtrando los pulsos digitales con el objetivo de conseguir un requerimiento menor de ancho de banda que el de la señal original.

Un equipo más que también consigue velocidades muy elevadas es el módem-cable, estando orientado principalmente al mercado residencial. Utiliza una técnica de acceso compartido ya que el medio de transmisión, cable coaxial, se comparte con todos los usuarios de una zona, edificio o área geográfica; por este motivo y aunque la velocidad sea muy alta, la velocidad real que cada usuario obtiene depende del número que estén conectados en cada momento.

Esta tecnología hace la competencia en velocidad a los equipos ADSL.

Una ventaja añadida es que por el mismo cable se puede proporcionar a los usuarios varios servicios, como son la televisión normal y de pago, telefonía, acceso a Internet, además del acceso a otras redes de datos. Para realizar esto utiliza una tecnología denominada HFC (Híbrido de Fibra y cable Coaxial), que consiste en que los tendidos principales de estas redes, por la ciudad o entre distintas localidades, se realiza con cables de fibra óptica, consiguiendo con ello una capacidad de transmisión muy alta, para convertir posteriormente la señal en cada zona de la ciudad, pasándola a un cable coaxial que llega hasta la casa del usuario.

Otro equipo utilizado para acceder a las redes son los modems inalámbricos, que se caracterizan porque su medio de transmisión no es una línea o cable conductor sino que envían la señal al espacio en forma de ondas de radio a determinadas frecuencias. Estos aparatos se distinguen por la movilidad puesto que no es necesario que estén conectados a un punto de red. Su principal utilización es en entornos industriales, para oficinas móviles dentro de un área limitada como puede ser un edificio o bien para lugares donde la instalación de cables pueda resultar complicado o peligroso; de cualquier forma siempre su utilización está limitada a entornos reducidos.

También podríamos citar como equipo de acceso las tarjetas de Red de Area Local (LAN), que tienen la particularidad de utilizarse para acceso a redes que abarcan distancias cortas, como una oficina o

un edificio. Estas tarjetas utilizan como medio de transmisión el cable de pares o coaxial y es compartido por todas las tarjetas conectadas al mismo segmento de la red; por este motivo aunque la velocidad a la que funcionan es muy alta, hasta 1000 Mbit/s, la velocidad efectiva de transferencia de una tarjeta o estación de la red es muy inferior a la velocidad a la que puede trabajar la red.

Módem: La palabra módem viene de la contracción de dos palabras MOdulador y DEModulador. Este equipo con la información digital modula una señal para el envío a la línea de transmisión (generalmente un canal telefónico con un ancho de banda de 300 a 3400 Hz.) y en el otro extremo del canal la señal recibida se demodula recuperando los datos procedentes del origen.

UTR (Unidades de terminación de red): Por UTR se entiende a aquellos dispositivos (ETCD) de acceso a las redes por medio de pares simétricos, utilizando codificación en banda base.

El nombre de unidad de terminación de red se entiende por ser, para el cliente, el interfaz de acceso a la red y el punto donde termina para la operadora de la misma.

Las velocidades de transmisión llegan hasta 512 Kbps. y las distancias alcanzadas entre las dos UTR dependerán fundamentalmente de la velocidad de transmisión y de la calidad y calibre del par utilizado.

Las UTR también son conocidas como módem banda base, este término no es del todo correcto, ya que estrictamente hablando no modulan una señal para su envío a la línea de transmisión, sino que realizan una adaptación o transformación del código binario de entrada para enviarlo al medio de transmisión.

Esta adaptación tiene como fin que el ancho de banda de la señal resultante sea menor o su espectro en frecuencias sea más estrecho, de esta manera la señal sufre menos distorsión y atenuación en la línea. Las unidades de terminación de red, al contrario de lo que ocurre con los módems, no están normalizadas por la UIT-T.

Equipos xDSL: Los sistemas xDSL son utilizados para la transmisión de datos a altas velocidades, pudiendo llegar hasta 52 Mbps utilizando el par de cobre normal. De esta manera se consigue rentabilizar al máximo la planta exterior instalada, estando en disposición de llegar a cualquier domicilio o empresa sin necesidad de tender nuevos cables.

La primera especificación de la tecnología xDSL fue definida en 1987 por Bell Communications Research; al principio se pensó en esta tecnología para suministrar vídeo bajo demanda y televisión interactiva usando el par telefónico. La familia xDSL (“Digital Subscriber Line”, línea de abonado digital) está englobada por un conjunto de sistemas basados en la utilización del bucle de abonado como línea de transmisión y cuya diferencia estriba en la utilización del espectro de frecuencias y por supuesto de la velocidad que consiguen alcanzar.

Estos equipos utilizan Multiplexación por División en Frecuencia (MDF), usando portadoras de radiofrecuencia hasta de 1 Mhz, de esta manera separan el canal telefónico (300 a 3.400 hz) de los canales de bajada o recepción de datos y subida o transmisión.

Habitualmente se utiliza un dispositivo denominado “spliter”, compuesto de un filtro paso bajo y de otro paso alto para separar las señales de baja frecuencia de telefonía de las de alta frecuencia de datos.

Como ocurre con los módems, en estos equipos también existen varias formas de alterar la señal portadora de radiofrecuencia modulándola para enviarla a la línea de transmisión. Principalmente están siendo utilizados tres métodos de modulación que son: modulación en cuadratura (QAM), CAP (Carrierless Amplitude Phase) y DMT (Discrete Multi-Tone modulation), estos dos últimos basados en la modulación QAM.

ADSL: La UIT-T ha normalizado los dispositivos xDSL bajo la norma colectiva G.990. ADSL ("Asymmetrical Digital Subscriber's Line", línea de abonado digital asimétrica) G992.1 Es el formato original del que han derivado los otros miembros de la familia.

La denominación de asimétrica es debida a que las velocidades de transmisión y recepción son distintas. La máxima velocidad de bajada con la que llega la información a nuestro ordenador puede ser hasta de 8 Mbit/s; mientras que la velocidad de subida con la que enviamos información desde nuestro ordenador puede llegar a 800 Kbit/s.

El bucle local de abonado puede alcanzar rangos que van desde 1 Km. para una velocidad de 8 Mbit/s hasta 5 Km. para una velocidad de 2 Mbit/s.

Los equipos ADSL trabajan con un margen de frecuencias mucho mayor que los modems, desde los 24 Khz. hasta 1.100 Khz aproximadamente. Otra diferencia es que al utilizar un modo de transferencia asimétrico, el equipo situado en el extremo de la central es distinto al equipo del cliente, denominándose habitualmente ATU – R (ADSL Terminal Unit – Remote) el del lado del cliente y ATU – C (ADSL Terminal Unit – Central) el situado en la central telefónica.

Los servicios más comúnmente prestados por esta tecnología son el acceso a Internet a alta velocidad, correo electrónico, vídeo bajo demanda, etc. estando orientado principalmente al usuario doméstico y a pequeños negocios.

ADSL Lite. (G922.2) Es una versión simplificada de ADSL, en la que el módem del cliente tiene incluida una versión muy limitada del filtro. La velocidad de bajada en este caso se reduce con respecto a la versión ADSL normal, llegando 1,5 Mbit/s para una distancia de 3 a 4,5 Km. y la de subida llega hasta los 64 Kbit/s.

La ventaja que tiene es que su instalación es más sencilla, pudiendo hacerla un usuario no especializado como ocurre con cualquier módem.

HDSL (High speed Digital Subscriber's Line). (G922.1) Esta tecnología es simétrica, siendo por tanto iguales las velocidades en ambos sentidos entre el usuario y la red. Utiliza dos pares simétricos sin carga, uno para cada sentido de transmisión, obteniendo velocidades de 2 Mbit/s para distancias de 5 Km. Su principal utilización es para dar servicios de datos a empresas a velocidades E1/T1 (2 Mbit/s / 1,544 Mbit/s), también se puede usar para dar servicio a velocidades de N * 64 Kbit/s.

VDSL (Very high speed – DSL) Es un sistema asimétrico desarrollado para su uso en bucles locales muy cortos, en ocasiones es utilizado en el último tramo del bucle local para proporcionar un acceso directo a una fibra óptica que conecte con la red. Las velocidades de bajada comienzan desde 13 Mbit/s, pudiendo alcanzar hasta 52 Mbit/s, con 2,3 Mbit/s como canal de retorno hacia la red. El rango de distancias que puede abarcar va desde 1,3 Km. para una velocidad de 13 Mbit/s a 300 m. para 52 Mbit/s.

2.3.8 Arquitectura de Comunicación

Las arquitecturas de comunicaciones permiten ordenar la estructura necesaria para la comunicación entre equipos mediante una red de modo que puedan ofrecerse servicios añadidos al simple transporte de información, algunos tan importantes como la corrección de datos o la localización del destinatario en un medio compartido. En esta arquitectura, deben definirse ante todo algunos conceptos esenciales:

- *Proceso de aplicación:* cualquier proceso (programa de aplicación en ejecución) en un sistema informático que ofrezca alguna utilidad al usuario.

- *Sistema final:* sistema informático donde residen procesos de aplicación; en ciertos contextos se le llama acertadamente host (anfitrión). Son los antiguamente llamados mainframes, las estaciones de trabajo, los PCs, etc.
- *Sistema intermedio*: sistema que, en general, no posee aplicaciones de usuario y actúa como nodo de conmutación e interconexión en las redes; son los repetidores, puentes (bridges) y encaminadores (routers, gateways) cada uno de ellos con funcionalidades específicas.
- *Protocolo de comunicación:* Conjunto de reglas para el intercambio de información y de definiciones de los formatos de los mensajes para la interacción fructífera entre dos o más entidades. Por ejemplo, el popular protocolo IP, base de Internet.

Para estudiar las arquitecturas de comunicaciones es conveniente pensar que los objetos en comunicación son los procesos de aplicación y no los sistemas (finales) donde se alojan. Bajo esta premisa, ya puede intuirse que la tarea de poner en comunicación dichos procesos puede llegar a ser muy compleja.

Por eso, la mayoría de arquitecturas de comunicaciones están estructuradas en lo que suelen llamarse capas o niveles. Las principales ventajas de una estructuración de ese tipo son:

- la modularidad o independencia entre tareas. Permite resolver el problema general en pequeños problemas, más simples y resolubles individualmente.
- permitir varias alternativas para una misma tarea. Poder disponer de 2 protocolos, elegibles por la entidad de nivel superior, en función de los requisitos necesarios.
- la facilidad de cambios parciales. Por ejemplo, cambiar un protocolo por otro sin afectar al resto del funcionamiento. Una aplicación de ello podría ser la migración a una nueva versión de protocolo desde una anterior (pasar de IP versión 4 a IP versión 6, sin variar el resto de la torre de protocolos, obteniendo por tanto el beneficio del nuevo estándar en las funciones de las que específicamente sea responsable).

Para ilustrar mejor el concepto y la utilidad de una arquitectura de comunicaciones, se presentará a continuación una analogía ampliamente usada en la literatura sobre el tema.

Supongamos dos pensadores (filósofos) que viven en países distintos, con lenguas nativas distintas y que están interesados en establecer un intenso debate dialéctico. Ellos representarán los procesos de aplicación que desean intercambiar información al más alto nivel, sin preocupaciones secundarias. Para ellos debe diseñarse una arquitectura de comunicaciones que aborde básicamente dos problemas: la separación geográfica entre los filósofos y su separación idiomática (distinta forma de representar sus pensamientos).

La capa de adaptación sintáctica aborda el problema de la distinta forma en que los filósofos (*procesos de aplicación*) representan sus pensamientos (*información*), es decir, ofrece un servicio de intercambio de información transparente (independiente) al idioma en que está expresada. Con este fin, dicha capa se construye con dos entidades, *traductor1* y *traductor2*, colaborando entre sí, capaces de traducir a/desde el idioma de cada filósofo a otros idiomas comunes a ambos traductores (al menos uno de ellos).

La capa de comunicación aborda el problema de enviar cualquier información entre los sitios geográficos distintos donde residen los filósofos, es decir, ofrece un servicio de transporte de información entre sitios distantes, óptimo (en cuanto a rapidez, fiabilidad o coste) y transparente (independiente) a los problemas (extravíos, retrasos, desordenamientos, etc.) que puedan surgir en los envíos. A tal fin, dicha capa se construye con dos entidades, *ingeniero1* e *ingeniero2*, colaborando entre sí, con un conjunto de medios de comunicación (teléfono, fax, correo postal, correo electrónico, etc.) a su disposición para ponerse en contacto.

2.4 MODELO OSI

Durante la década de los 60, dentro del marco de la guerra fría, la Agencia de Proyectos de Investigación Avanzada del Departamento de Defensa de los Estados Unidos (DARPA) se planteó la posibilidad de que un ataque afectara a su red de comunicaciones y financió equipos de investigación en distintas universidades con el objetivo de desarrollar una red de ordenadores con una administración totalmente distribuida. Como resultado de la aplicación de sus estudios en redes de conmutación de paquetes, se creó la denominada red ARPANET, de carácter experimental y altamente tolerable a fallos. Más adelante, a mediados de los 70, la agencia empezó a investigar en la interconexión de distintas redes, y en 1974 estableció las bases de desarrollo de la familia de protocolos que se utilizan en las redes que conocemos hoy en día como redes TCP/IP.

El auge de las redes tuvo un comienzo desorganizado desde muchos puntos de vista. A principios de 1980 se experimentaron incrementos importantes en el número y tamaño de las redes. A medida que las compañías comprendían las ventajas de utilizar redes, se agregaban o expandían casi tan rápidamente como surgían y se introducían nuevas tecnologías de red.

A mediados de 1980, estas compañías comenzaron a experimentar problemas ocasionados por la rápida expansión. Entre las redes de compañías que utilizaron tecnologías privadas o propietarias surgieron dificultades de incompatibilidad al momento de querer interconectarse o evolucionar.

En un intento por solucionar el problema de la incompatibilidad, la Organización Internacional para la Estandarización (ISO) comenzó el desarrollo de un modelo de networking, paralelo a los modelos existentes, como DECnet, SNA y TCP/IP, para definir un conjunto de normas que sean aplicables a todas las redes; esto permitiría a los desarrolladores crear redes que sean compatibles y puedan intercambiar información.

Este desarrollo se denominó Modelo de Referencia OSI (Open System Interconnection), liberado en 1984, y es utilizado por la ISO para describir la comunicación en una red. Permite a los desarrolladores disponer de un conjunto de reglas que aseguren mayor compatibilidad e interoperabilidad entre las distintas tecnologías de red producidas por empresas en el mundo entero.

El modelo de referencia OSI se impuso como el principal modelo para las comunicaciones de red. Aunque existen otros modelos, la mayoría de los desarrolladores relacionaron sus productos al modelo de referencia OSI y lo utilizan para la capacitación de los usuarios en el uso de sus productos. El modelo OSI es considerado la mejor herramienta para la enseñanza sobre el envío y la recepción de datos en una red. El patrón para la Interconexión de Sistemas Abiertos se basa en un modelo de protocolos estratificados, cada nivel se desarrolla sobre el anterior, proporcionando un conjunto de servicios al nivel inmediatamente superior, por lo que el nivel más alto dispondrá de los servicios que ofrecen todos los niveles inferiores. La comunicación entre niveles equivalentes de distintos sistemas es una comunicación lógica horizontal.

Existen cuatro acciones, denominadas primitivas que son un conjunto de operaciones que sirven para ofrecer los servicios entre niveles, a estas primitivas acceden los niveles por medio de los Puntos de Acceso al Servicio (PAS, en inglés SAP “Service Access Points”). Este es un método que se utiliza para que los niveles se comuniquen entre sí. Estas acciones son:

- Solicitud.
- Indicación
- Respuesta
- Confirmación

Beneficios del modelo OSI:

- Reduce la complejidad
- Estandariza las interfaces
- Facilita la ingeniería modular
- Acelera la evolución
- Facilita la enseñanza y el aprendizaje

El intercambio de información entre capas se lleva a cabo por medio de un interfaz existente entre las mismas, este interfaz puede estar compuesto por elementos lógicos y/o físicos. Los protocolos de cada uno de los niveles pueden ser diferentes e independientes entre sí, lo único que necesitan es conocer los servicios que presta el interfaz con la capa inferior. El modelo OSI no especifica de forma exacta los protocolos y servicios que se utilizarán en cada nivel, únicamente indica las funciones que debe realizar cada capa, por lo que este modelo no se puede considerar como una arquitectura de red.

2.4.1 Modelo de red dividido en capas

El concepto de capas puede ser usado para describir las comunicaciones entre dispositivos de computación y resolver los problemas involucrados en este proceso. El mismo concepto puede ser aplicado también a cualquier tipo de flujo de información, desde la conversación de dos personas al flujo de datos en una red.

2.4.2 Funciones de las capas del modelo OSI

El Modelo OSI está formado por siete capas, cada una se concentra en una tarea específica. De manera que todas juntas permiten realizar la compleja tarea que involucra la transmisión de información entre sistemas de computación.

CAPA 7 Aplicación: *Aplicaciones de usuario*. Permite que las aplicaciones del usuario utilicen los servicios de red para acceder a recursos que no se encuentran accesibles localmente. Por ejemplo la aplicación navegador web, permite acceder a páginas que se encuentran en servidores en cualquier lugar del mundo. Algunos protocolos usados son HTTP, FTP, Telnet, SMTP, DNS, SNMP, DHCP, BOOTP, NTP, TFTP, NDS, etc.

CAPA 6 Presentación: *Formato de datos común*. Se encarga de garantizar que los datos sean legibles por el sistema receptor. Trabaja con la representación y estructura de los datos. En esta capa

se puede realizar la encriptación y compresión de datos. Permite codificar las imágenes, sonidos y videos en diferentes formatos. Los formatos más utilizados son:

- Audio: wav, mp3, midi
- Imágenes: jpg, bmp, gif
- Video: avi, swf

Algunos protocolos usados son LPP, XDR, NetBIOS, NCP, X.25 PAD, etc.

Se suele decir que el nombre más adecuado para la capa de Presentación hubiera sido el de capa de representación. Si el modelo OSI perseguía la interconexión de sistemas que fueran realmente abiertos, debía resolverse el problema de los diferentes formatos con que cada sistema representaba localmente su información (dependiente del fabricante del sistema, de su hardware y de su sistema operativo). Es ahí donde interviene la capa de presentación.

CAPA 5 Sesión: *Diálogos y conversaciones*. Permite establecer, mantener y finalizar en forma ordenada la comunicación entre las aplicaciones. Algunos protocolos usados son LDAP, RPC, SCP, SQL, etc. La capa de sesión fue una aportación relativamente nueva del modelo OSI de la ISO a las arquitecturas de comunicaciones. En efecto, podría pensarse que, dado el servicio perfectamente fiable que ofrece la capa de transporte, los procesos de aplicación no necesitarían nada más y podrían usar dicho servicio directamente.

De hecho, y siguiendo este razonamiento, la arquitectura TCP/IP carece de las capas de sesión y presentación explícitamente. Superados los errores de comunicación en la capa de transporte, la capa de sesión puede verse como un conjunto de herramientas, a disposición de los programadores, que permiten estructurar y enriquecer el diálogo entre los procesos de aplicación.

CAPA 4 Transporte: *Calidad de servicio y confiabilidad*. Proporciona un servicio de comunicación de extremo a extremo entre aplicaciones. Puede brindar un servicio orientado a la conexión, confiable, con control de errores y control de flujo, o un servicio no confiable. En el primer caso se encarga de establecer, mantener y terminar adecuadamente los circuitos virtuales que se utilizarán para la comunicación entre las aplicaciones de los sistemas finales. Algunos protocolos usados son TCP, UDP, SPX, NetBEUI, etc.

CAPA 3 Red: *Selección de ruta, direccionamiento y enrutamiento*. Se encarga de encaminar la información desde el sistema de computación origen hasta el destino, a través de la mejor ruta, utilizando un esquema de Direccionamiento Lógico o de Red. Podemos encontrar un ejemplo de protocolo de capa de red en el Protocolo Internet (IP), definido en el modelo TCP/IP. Algunos protocolos usados son IP,SLIP, ARP, OSPF, IGRP, GGP, EGP, BGP, RIP, ICMP, IPX, X.25, etc.

Esta capa, situada por encima de la de enlace, aprovecha los servicios brindados por esta y añade algunas características, como son Reenvío (*relaying*), Encaminamiento (*routing*), Control de congestión, Interconexión (adaptación) entre redes. La unidad de información en esta capa es el paquete o datagrama (para las redes de conmutación de paquetes). Puede decirse que la capa de red articula el conjunto de enlaces físicos, mejorados por la capa de enlace de datos, para constituir lo que propiamente se entiende por red de comunicaciones. Aunque la capa de Red está obviamente implementada en los sistemas finales, es en los sistemas intermedios donde ésta se encuentra realizada de forma completa.

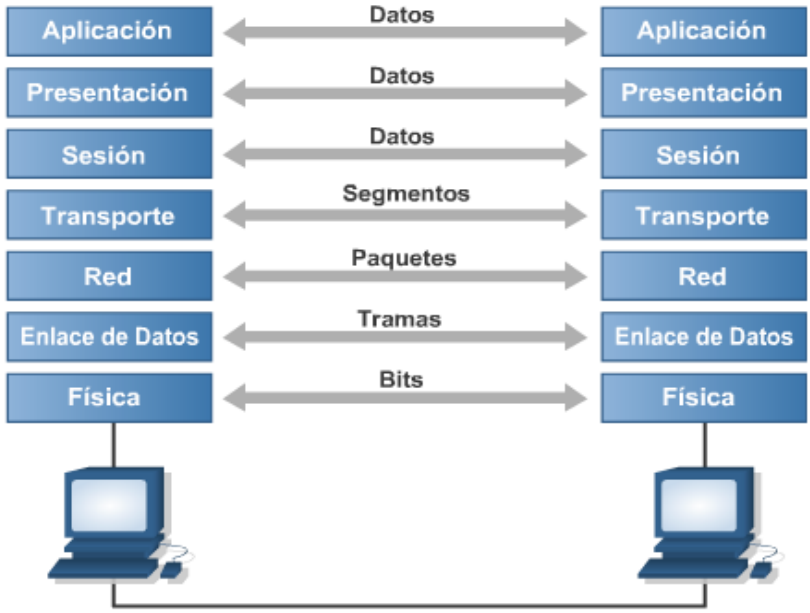
CAPA 2 Enlace de datos: *Tramas y control de acceso al medio*. Se encarga de realizar el traslado confiable de la información entre sistemas de computación físicamente contiguos, en su camino hacia

el destino final. Entre sus funciones debe garantizar el acceso ordenado de los sistemas al medio físico, control de errores y control de flujo. Para identificar los sistemas utiliza direccionamiento físico, en las tecnologías de LAN (Local Area Network) se denominan direcciones MAC. Define la topología lógica de una red. Las dos topologías lógicas utilizadas en redes LAN son redes de difusión y de traspaso de token. Algunos protocolos usados son IEEE 802.3 más conocido como Ethernet (CSMA/CD), IEEE 802.5 (token passing), FDDI token passing, VLANs, ATM Adaptation Layer, ISDN, Frame Relay, PPP, SMDS, HDLC, LAP-A, 802.2 (etiquetado de tramas).

CAPA 1 Física: *Señales y medios*. Se encarga del transporte físico de la información entre los sistemas de computación. En esta capa encontramos las definiciones eléctricas, mecánicas, funcionales y de procedimientos de los elementos que forman parte de las redes. Aquí encontramos los diferentes medios físicos, como cable UTP, coaxial, fibra óptica, etc. Define la topología física de la red, las más utilizadas son estrella, bus, y anillo. Son ejemplos de especificaciones de capa física: EIA RS-232C (para enlaces locales de datos entre computadores y periféricos), IEEE 802.3 (una parte de ella, para redes de área local Ethernet), CCITT I.430 (para el acceso básico a la RDSI), etc.

2.4.3 Comunicaciones de par a par

Al momento de llevar los datos de un origen a un destino, cada capa del modelo OSI en el origen debe comunicarse con su capa par en el destino. Esta forma de comunicación es llamada par - a - par. Durante este proceso, los protocolos de cada capa intercambian información llamada unidad de datos de protocolo (PDUs). De esta forma, cada capa en el host origen se comunica utilizando una PDU específica con su capa par en el host destino como puede ver en la figura



Aunque la transmisión lógica de la información se realiza entre capas pares, físicamente la información fluye en sentido descendente en las capas del dispositivo origen y en sentido ascendente en las capas del destino.

Después que las capas 7, 6 y 5 procesan la información, envían las PDU resultantes, llamadas "datos", a la capa 4; la capa 4 agrega más información y agrupa los datos en una PDU llamada "segmento".

La capa de red recibe los segmentos de la capa de transporte, le agrega información y los transforma

en "paquetes". Esta información contiene, entre otros elementos, las direcciones de red origen y destino que permitirán realizar el encaminamiento de los datos.

La capa de enlace de datos toma los paquetes y los transforma en "tramas", al agregar información necesaria para realizar sus funciones, por ejemplo, control de errores y acceso al medio. La capa física provee un servicio a la capa de enlace de datos codificando las tramas en patrones de 1s y 0s, denominados "bits" para su transmisión en el medio.

2.4.4 Encapsulamiento de datos

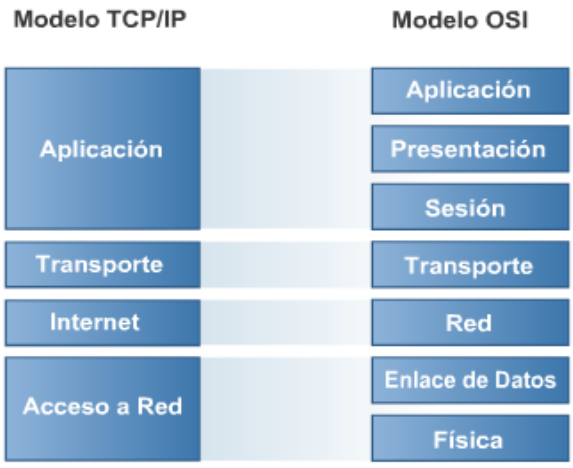
Las comunicaciones en una red son flujos de información entre un origen y un destino (que podría ser un host o un conjunto de hosts). Si un host quiere enviar datos a otro, los datos deben ser empaquetados a través de un proceso llamado encapsulación.

En este proceso, cada capa toma la PDU de la capa superior y la procesa, agregando información que será utilizada por la capa par del siguiente dispositivo de red, en el camino hacia el destino final. Básicamente, la información que se agrega será un encabezado, al comienzo de la PDU y en algunos casos una cola o terminador, al final.

El encabezado contiene, entre otros, información de direccionamiento, que permite reconocer la entidad de la capa que envía los datos, y la entidad de la capa par que deberá recibirlos. Además, en los casos que estén implementadas funciones de control de errores y control de flujo, se agrega información en el encabezado que permita realizar estas tareas.

2.4.5 OSI versus TCP/IP

El conjunto de protocolos más utilizado actualmente es TCP/IP. La pila de protocolos TCP/IP tiene cuatro capas: la capa de aplicación, la capa de transporte, la capa de internet y la capa de acceso de red . Algunas de las capas del modelo TCP/IP poseen el mismo nombre que las capas del modelo OSI pero esto no significa que cumplan funciones similares, por ejemplo, la capa de aplicación tiene diferentes funciones en cada modelo.



2.4.6 Funciones y vulnerabilidades de cada capa

Capa de aplicación: *Capas 5, 6 y 7 del modelo OSI*. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en esta capa, aquí se definen los protocolos de alto nivel, aspectos de representación y codificación de los datos y control de diálogo entre procesos.

La capa de aplicación presenta varias deficiencias de seguridad asociadas a sus protocolos. Debido al gran número de protocolos definidos en esta capa, la cantidad de deficiencias presentes también será superior al resto de capas. Algunos ejemplos de deficiencias de seguridad a este nivel podrían ser los siguientes:

- **Servicio de nombres de dominio**. Normalmente, cuando un sistema solicita conexión a un servicio, pide la dirección IP de un nombre de dominio y envía un paquete UDP a un servidor

DNS; entonces, éste responde con la dirección IP del dominio solicitado o una referencia que apunta a otro DNS que pueda suministrar la dirección IP solicitada.

Un servidor DNS debe entregar la dirección IP correcta pero, además, también puede entregar un nombre de dominio dada una dirección IP u otro tipo de información.

En el fondo, un servidor de DNS es una base de datos accesible desde internet. Por lo tanto, un atacante puede modificar lainformación que suministra ésta base de datos o acceder a información sensible almacenada en la base de datos por error, pudiendo obtener información relativa a la topología de la red de una organización concreta (por ejemplo, la lista de los sistemas que tiene la organización).

- **Telnet**. Normalmente, el servicio Telnet autentica al usuario mediante la solicitud del identificador de usuario y su contraseña, que se transmiten en claro por la red. Así, al igual que el resto de servicios de internet que no protegen los datos mediante mecanismos de protección, el protocolo de aplicación Telnet hace posible la captura de aplicación sensible mediante el uso de técnicas de sniffing.

  Actualmente existen otros protocolos a nivel de aplicación (como, por ejemplo, SSH) para acceder a un servicio equivalente a Telnet pero de manera segura (mediante autenticación fuerte). Aun así, el hecho de cifrar el identificador del usuario y la contraseña no impide que un atacante que las conozca acceda al servicio.

- **File Transfer Protocol**. Al igual que Telnet, FTP es un protocolo que envía la información en claro (tanto por el canal de datos como por el canal de comandos). Así pues, al enviar el identificador de usuario y la contraseña en claro por una red potencialmente hostil, presenta las mismas deficiencias de seguridad que veíamos anteriormente con el protocolo Telnet.

  Aparte de pensar en mecanismos de protección de información para solucionar el problema, FTP permite la conexión anónima a una zona restringida en la cual sólo se permite la descarga de archivos. De este modo, se restringen considerablemente los posibles problemas de seguridad relacionados con la captura de contraseñas, sin limitar una de las funcionalidades más interesantes del servicio.

- **Hypertext Transfer Protocol**. El protocolo HTTP es el responsable del servicio World Wide Web. Una de sus vulnerabilidades más conocidas procede de la posibilidad de entrega de información por parte de los usuarios del servicio. Esta entrega de información desde el cliente de HTTP es posible mediante la ejecución remota de código en la parte del servidor.

  La ejecución de este código por parte del servidor suele utilizarse para dar el formato adecuado tanto a la información entregada por el usuario como a los resultados devueltos (para que el navegador del cliente la pueda visualizar correctamente). Si este código que se ejecuta presenta deficiencias de programación, la seguridad del equipo en el que esté funcionando el servidor se podrá poner en peligro.

Capa de transporte *Capa 4 del modelo OSI*. La capa de transporte se encarga de la calidad de servicio, garantizando, cuando la aplicación lo requiera, confiabilidad, control de flujo, segmentación y control de errores en la comunicación. Se basa en dos protocolos, TCP (orientado a la conexión) y UDP (no orientado a la conexión). La capa de transporte transmite información TCP o UDP sobre datagramas IP. En esta capa podamos encontrar problemas de autenticación, de integridad y de confidencialidad. Algunos de los ataques más conocidos en esta capa son las denegaciones de servicio debidas a protocolos de transporte.

En cuanto a los mecanismos de seguridad incorporados en el diseño del protocolo de TCP (como las negociaciones involucradas en el establecimiento de una sesión TCP), existe una serie de ataques que aprovechan ciertas deficiencias en su diseño. Una de las vulnerabilidades más graves contra estos mecanismos de control puede comportar la posibilidad de interceptación de sesiones TCP establecidas, con el objetivo de secuestrarlas y dirigirlas a otros equipos con fines deshonestos. Estos ataques de secuestro se aprovechan de la poca exigencia en el protocolo de intercambio de TCP

respecto a la autenticación de los equipos involucrados en una sesión. Así, si un usuario hostil puede observar los intercambios de información utilizados durante el inicio de la sesión y es capaz de interceptar con éxito una conexión en marcha con todos los parámetros de autenticación configurados adecuadamente, podrá secuestrar la sesión.

Capa de Internet *Capa 3 del modelo OSI***.** El propósito de la capa de Internet es encaminar paquetes desde un origen hacia un destino. Se basa fundamentalmente en el Protocolo Internet (IP). En esta capa se puede realizar cualquier ataque que afecte un datagrama IP. Se incluyen como ataques contra esta capa las técnicas de sniffing, la suplantación de mensajes, la modificación de datos, los retrasos de mensajes y la denegación de mensajes. Pueden realizarse mediante aplicaciones que se conocen con el nombre de sniffers.

Cualquier atacante puede suplantar un paquete si indica que proviene de otro sistema. La suplantaci ón de un mensaje se puede realizar, por ejemplo, dando una respuesta a otro mensaje antes de que lo haga el suplantado.

En esta capa, la autenticación de los paquetes se realiza a nivel de máquina (por dirección IP) y no a nivel de usuario. Si un sistema suministra una dirección de máquina errónea, el receptor no detectará la suplantación. Para conseguir su objetivo, este tipo de ataques suele utilizar otras técnicas, como la predicción de números de secuencia TCP, el envenenamiento de tablas caché, etc. Por otro lado, los paquetes se pueden manipular si se modifican sus datos y se reconstruyen de forma adecuada los controles de las cabeceras. Si esto es posible, el receptor será incapaz de detectar el cambio.

Capa de acceso de red *Capa 1 y 2 del modelo OSI***.** Esta capa, también llamada host a red, se ocupa de todos los aspectos que involucren convertir un paquete en una trama y transmitirlo en el medio físico. Esta capa se encarga de las funciones de las capas física y de enlace de datos del modelo OSI.

Si se compara el modelo OSI con el modelo TCP/IP , se pueden ver que existen similitudes y diferencias. Los ejemplos incluyen:

Similitudes

- Se dividen en capas.
- Poseen una capa de aplicación, aunque incluyen servicios distintos.
- Las capas de transporte y red de ambos modelos cumplen funciones similares.

Diferencias

- TCP/IP combina las funciones de la capa de presentación y de sesión del modelo OSI en la capa de aplicación.
- En el modelo TCP/IP combina la capa de enlace de datos y la capa física del modelo OSI en una sola capa.
- El modelo OSI se desarrolló antes de que se inventaran los protocolos, respecto al modelo TCP/IP, los protocolos existían y el modelo fue una descripción de los mismos.
- El modelo TCP/IP no es general y no resulta apropiado para describir otra pila de protocolos distinta de TCP/IP.

En síntesis, el modelo OSI ha demostrado ser muy útil para estudiar las redes de computadoras. En contraste, los protocolos OSI no se han hecho populares. Lo contrario sucede con TCP/IP, donde el modelo prácticamente es inexistente, pero los protocolos se usan mucho, de hecho, la familia de protocolos TCP/IP es el estándar en torno al cual se desarrolló Internet.

Las vulnerabilidades de la capa de red están estrechamente ligadas al medio sobre el que se realiza la conexión. Esta capa presenta problemas de control de acceso y de confidencialidad.

Son ejemplos de vulnerabilidades a este nivel los ataques a las líneas punto a punto: desvío de los cables de conexión hacia otros sistemas, interceptación intrusiva de las comunicaciones (pinchar la línea), escuchas no intrusivas en medios de transmisión sin cables, etc.

2.5 PUERTOS

Sockets y Puertos son conceptos introducidos por los protocolos TCP y UDP, y son referencias lógicas respecto a por donde se conectarán determinados servicios o aplicaciones. Los Sockets son referencias lógicas creadas por las aplicaciones basadas en TCP/IP que sirven para que estas se comuniquen con su entorno, estas referencias lógicas requieren de tres parámetros que son: dirección IP del host, tipo de servicio (TCP con conexión, UDP sin conexión) y numero de puerto. Los puertos permiten entablar varias conexiones simultaneas por el mismo medio, por ejemplo cuando se abren dos sesiones simultaneas de un navegador con URL diferentes.

La IANA (Internet Assigned Numbers Authority) administra la asignación de puertos que van desde el 0 hasta el 65.536.

Los números de puerto se dividen en:

- Puertos bien conocidos
- Puertos definidos por el usuario.

Los puertos del 1025 hasta el 65.536 son asignados por las aplicaciones de los usuarios.

Los puertos bien conocidos van del 0 a 1024 y se asignan a aplicaciones publicas como http y a productos específicos de red. Por ejemplo:

Puerto	Servicio
21	FTP
23	TELNET
25	SMTP
53	DNS
80	HTTP
139	NetBIOS

Una de las técnicas de Hacking comunes consiste en explorar los puertos para saber si algunos de ellos están abiertos y a la escucha, y qué servicios vulnerables se están ejecutando en ellos. Los ataques mas sofisticados llevados adelante por Hackers experimentados se realizan a puertos determinados porque ya se sabe que servicio estará escuchando. Los puertos son también usados por los troyanos que activan esa vía de comunicación para permitir tomar el control de manera remota. De la misma manera que existen escaneadores de puertos abiertos con servicios a la escucha, también existen escaneadores de puertos de troyanos que permiten el ingreso y la administración remota.

2.6 ELEMENTOS DE UNA RED

Las redes se pueden dividir en dos grandes categorías de acuerdo a su área de cobertura:

- *Redes LAN (Local Area Networks - Redes de área local)*

- *Redes WAN (Wide Area Networks - Redes de área amplia)*

Las redes LAN generalmente se encuentran en su totalidad dentro de un mismo edificio o de un grupo de edificios. Las redes WAN cubren un área geográfica más extensa, por ejemplo, ciudades, países, o incluso el mundo entero .

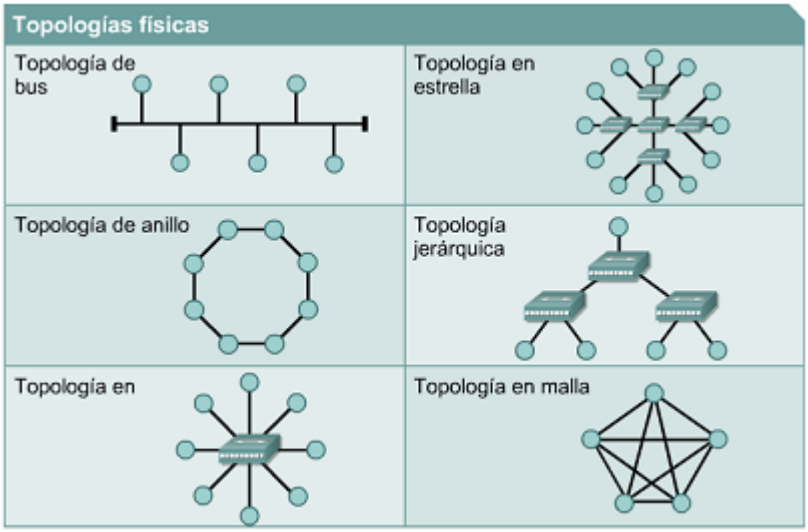
2.6.1 Redes de área local (LAN)

Las LAN permiten a las empresas compartir recursos informáticos y hacer un uso eficiente de los mismos, como por ejemplo acceder a una impresora que no esté directamente conectada o a un archivo almacenado en una máquina remota. Existen diferentes tecnologías de redes LAN, entre las que podemos destacar: Ethernet, Token Ring, FDDI. Por el contrario, las WAN se caracterizan por abarcar un espacio geográfico extenso, siendo Internet el ejemplo más claro de este tipo de redes, su velocidad de transmisión es baja en comparación a una LAN (64 Kbps, 128 Kbps, 512 Kbps, 1 Mbps, 2 Mbps, etc.), su tasa de errores es mayor que en unaLAN, siendo la empresa que proporciona el servicio de conexión la propietaria de los medios físicos. Una LAN le permite a una empresa compartir recursos informáticos, haciendo un uso eficiente de los mismos. Dentro de los diferentes dispositivos que interactúan para lograr este fin, encontramos: Switch, Router, Gateway, RAS, PBX, Firewalls, IDS

2.6.2 Topologías de Red

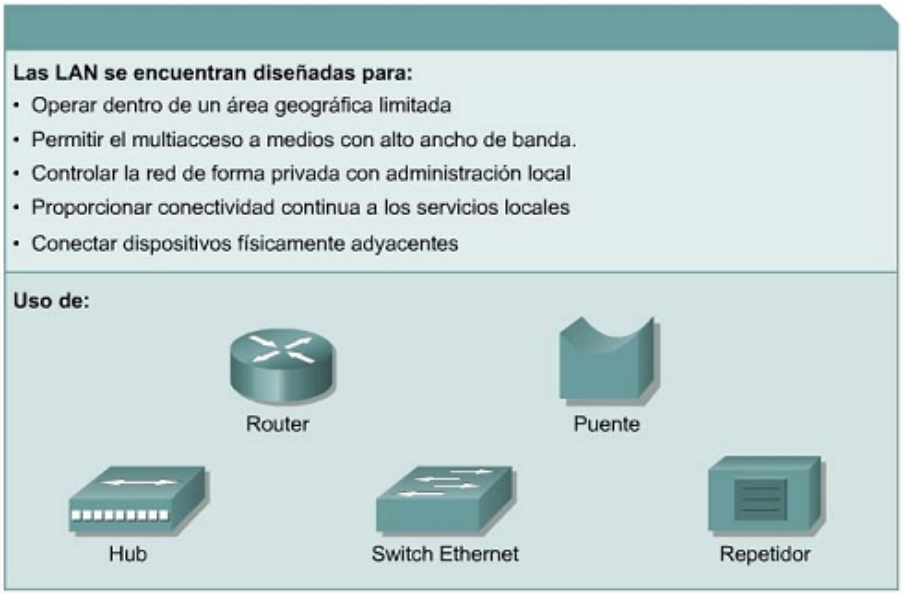
La topología de red es la disposición física y/o lógica de los elementos (enlaces, nodos) de una red. Así pueden definirse diversos modelos de topologías básicas:

- ***Malla***: Los distintos nodos están más o menos densamente unidos entre sí por enlaces directos (en general, de forma arbitraria y sin seguir ninguna jerarquía particular). Cuando cualquier nodo está unido directamente a todos los demás mediante un enlace directo, se dice que la red presenta una topología de malla completa.
- ***Estrella***: Los distintos nodos están unidos a un único nodo central.
- ***Árbol***: Los distintos nodos están distribuidos en forma de ramificaciones sucesivas a partir de un único nodo raíz.
- ***Bus***: Todos los nodos están unidos por un único enlace común.
- ***Anillo***: Los nodos están unidos en cadena, uno tras otro, cerrándose ésta sobre si misma (de manera circular).

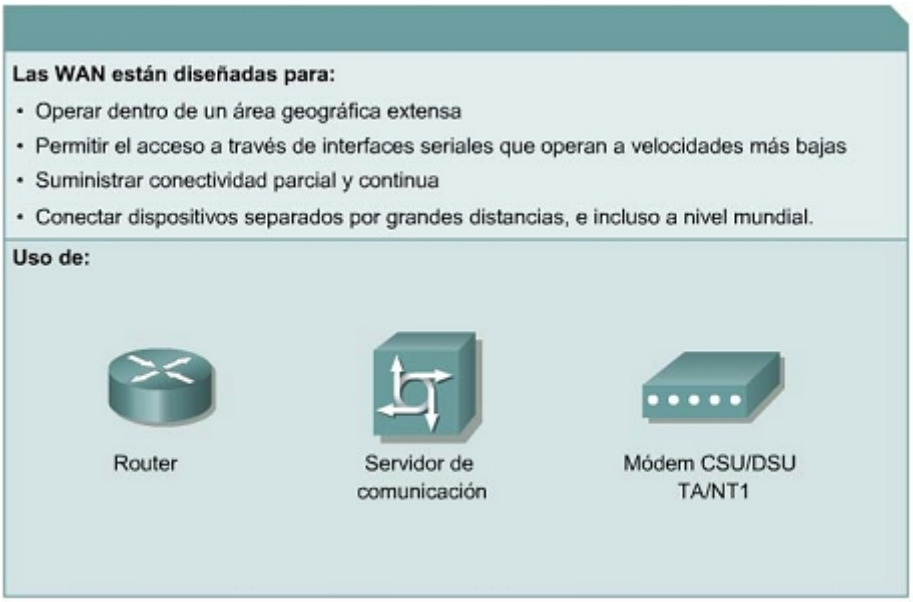


La topología lógica es la que define la forma en que las máquinas acceden a los medios. Los dos tipos más comunes de topologías lógicas son *broadcast* y transmisión de *tokens* o *testigos.*

La topología ***broadcast*** simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. Las estaciones no siguen ningún orden para utilizar la red, el orden es el primero que entra, el primero que se sirve. Esta es la forma en que funciona Ethernet La transmisión de ***tokens*** controla el acceso a la red mediante la transmisión de un token electrónico a cada host de forma secuencial. Cuando un host recibe el token, eso significa que el host puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, "pasa" el token al siguiente host y el proceso se vuelve a repetir. Esta es la forma en que funciona Token Ring.



2.6.3 Redes de área amplia (WAN)



Las WAN interconectan las LAN, que a su vez proporcionan acceso a los computadores o a los servidores de archivos ubicados en otros lugares. Como las WAN conectan redes de usuarios dentro

de un área geográfica extensa, permiten que las empresas se comuniquen entre sí a través de grandes distancias. Las WAN permiten que los computadores, impresoras y otros dispositivos de una LAN compartan y sean compartidas por redes en sitios distantes. Las WAN proporcionan comunicaciones instantáneas a través de zonas geográficas extensas. El software de colaboración brinda acceso a información en tiempo real y recursos que permiten realizar reuniones entre personas separadas por largas distancias, en lugar de hacerlas en persona. Networking de área amplia también dio lugar a una nueva clase de trabajadores, los empleados a distancia, que no tienen que salir de sus hogares para ir a trabajar.

2.6.4 Redes de área metropolitana (MAN)

La MAN es una red que abarca un área metropolitana, como, por ejemplo, una ciudad o una zona suburbana. Una MAN generalmente consta de una o más LAN dentro de un área geográfica común. Por ejemplo, un banco con varias sucursales puede utilizar una MAN. Normalmente, se utiliza un proveedor de servicios para conectar dos o más sitios LAN utilizando líneas privadas de comunicación o servicios ópticos. También se puede crear una MAN usando tecnologías de puente inalámbrico enviando haces de luz a través de áreas públicas.

2.6.5 Redes de área de almacenamiento (SAN)

Una SAN es una red dedicada, de alto rendimiento, que se utiliza para trasladar datos entre servidores y recursos de almacenamiento. Al tratarse de una red separada y dedicada, evita todo conflicto de tráfico entre clientes y servidores. La tecnología SAN permite conectividad de alta velocidad, de servidor a almacenamiento, almacenamiento a almacenamiento, o servidor a servidor. Este método usa una infraestructura de red por separado, evitando así cualquier problema asociado con la conectividad de las redes existentes.

2.6.6 Medios de Comunicación

El cable de cobre se utiliza en casi todas las LAN. Hay varios tipos de cable de cobre disponibles en el mercado, y cada uno presenta ventajas y desventajas. La correcta selección del cableado es fundamental para que la red funcione de manera eficiente. Debido a que el cobre transporta información utilizando corriente eléctrica, es importante comprender algunos principios básicos de la electricidad a la hora de planear e instalar una red.

La fibra óptica es el medio utilizado con mayor frecuencia en las transmisiones de punto a punto de mayor distancia y alto ancho de banda que requieren los backbones de LAN y las WAN. En los medios ópticos, se utiliza la luz para transmitir datos a través de una delgada fibra de vidrio o de plástico. Las señales eléctricas hacen que el transmisor de fibra óptica genere señales luminosas que son enviadas por la fibra. El host receptor recibe las señales luminosas y las convierte en señales eléctricas en el extremo opuesto de la fibra. Sin embargo, no hay electricidad en el cable de fibra óptica en sí. De hecho, el vidrio utilizado en el cable de fibra óptica es un muy buen aislante eléctrico. La conectividad física permitió un aumento en la productividad permitiendo que se compartan impresoras, servidores y software. Los sistemas tradicionales de red requieren que las estaciones de trabajo permanezcan estacionarias permitiendo movimientos sólo dentro del alcance de los medios y del área de la oficina.

La introducción de la tecnología inalámbrica elimina estas limitaciones y otorga portabilidad real al mundo de la computación. En la actualidad, la tecnología inalámbrica no ofrece las transferencias a alta velocidad, la seguridad o la confiabilidad de tiempo de actividad que brindan las redes que usan cables. Sin embargo, la flexibilidad de no tener cables justifica el sacrificio de estas características.

A menudo, los administradores tienen en cuenta las comunicaciones inalámbricas al instalar una nueva red o al actualizar una red existente. Una red inalámbrica puede empezar a funcionar sólo unos

pocos minutos después de encender las estaciones de trabajo. Se proporciona la conectividad a Internet a través de una conexión con cable, router, cablemódem o módem DSL y un punto de acceso inalámbrico que sirve de hub para los nodos inalámbricos. En el entorno residencial o de una pequeña oficina, es posible combinar estos dispositivos en una sola unidad.

Los cables tienen distintas especificaciones y generan distintas expectativas acerca de su rendimiento. • ¿Qué velocidad de transmisión de datos se puede lograr con un tipo particular de cable? La velocidad de transmisión de bits por el cable es de suma importancia. El tipo de conducto utilizado afecta la velocidad de la transmisión.

- ¿Qué tipo de transmisión se planea? ¿Serán las transmisiones digitales o tendrán base analógica? La transmisión digital o de banda base y la transmisión con base analógica o de banda ancha son las dos opciones.
- ¿Qué distancia puede recorrer una señal a través de un tipo de cable en particular antes de que la atenuación de dicha señal se convierta en un problema? En otras palabras, ¿se degrada tanto la señal que el dispositivo receptor no puede recibir e interpretar la señal correctamente en el momento en que la señal llega a dicho dispositivo? La distancia recorrida por la señal a través del cable afecta directamente la atenuación de la señal. La degradación de la señal está directamente relacionada con la distancia que recorre la señal y el tipo de cable que se utiliza.

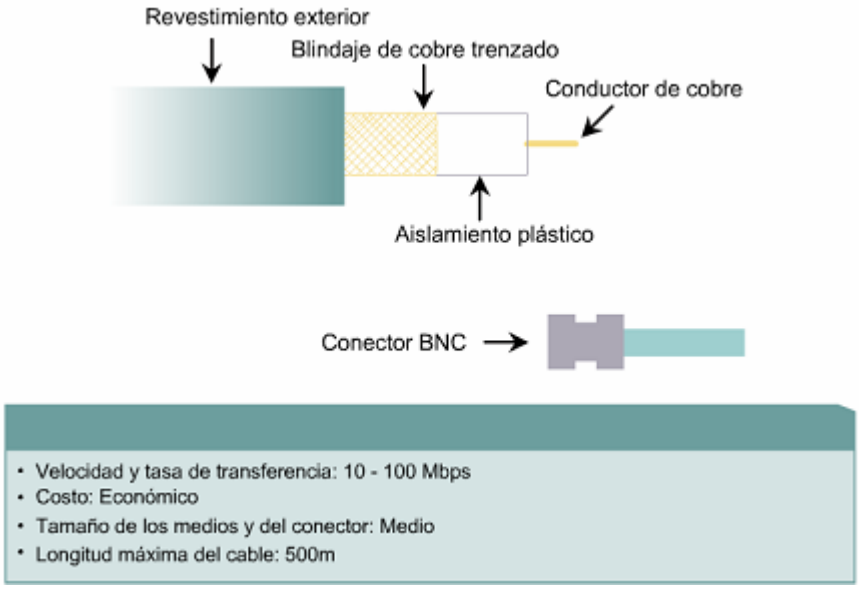
10BASE-T se refiere a la velocidad de transmisión a 10 Mbps. El tipo de transmisión es de banda base o digitalmente interpretada. T significa par trenzado.

10BASE5 se refiere a la velocidad de transmisión a 10 Mbps. El tipo de transmisión es de banda base o digitalmente interpretada. El 5 representa la capacidad que tiene el cable para permitir que la señal recorra aproximadamente 500 metros antes de que la atenuación interfiera con la capacidad del receptor de interpretar correctamente la señal recibida. 10BASE5 a menudo se denomina "Thicknet". Thicknet es, en realidad, un tipo de red, mientras que 10BASE5 es el cableado que se utiliza en dicha red.

10BASE2 se refiere a la velocidad de transmisión a 10 Mbps. El tipo de transmisión es de banda base o digitalmente interpretada. El 2, en 10BASE2, se refiere a la longitud máxima aproximada del segmento de 200 metros antes que la atenuación perjudique la habilidad del receptor para interpretar apropiadamente la señal que se recibe. La longitud máxima del segmeto es en reallidad 185 metros. 10BASE2 a menudo se denomina “Thinnet”. Thinnet es, en realidad, un tipo de red, mientras que 10BASE2 es el cableado que se utiliza en dicha red.

Cable coaxial consiste de un conductor de cobre rodeado de una capa de aislante flexible. El conductor central también puede ser hecho de un cable de aluminio cubierto de estaño que permite que el cable sea fabricado de forma económica. Sobre este material aislante existe una malla de cobre tejida u hoja metálica que actua como el segundo hilo del circuito y como un blindaje para el conductor interno. Esta segunda capa, o blindaje, también reduce la cantidad de interferencia electromagnética externa. Cubriendo la pantalla está la chaqueta del cable.

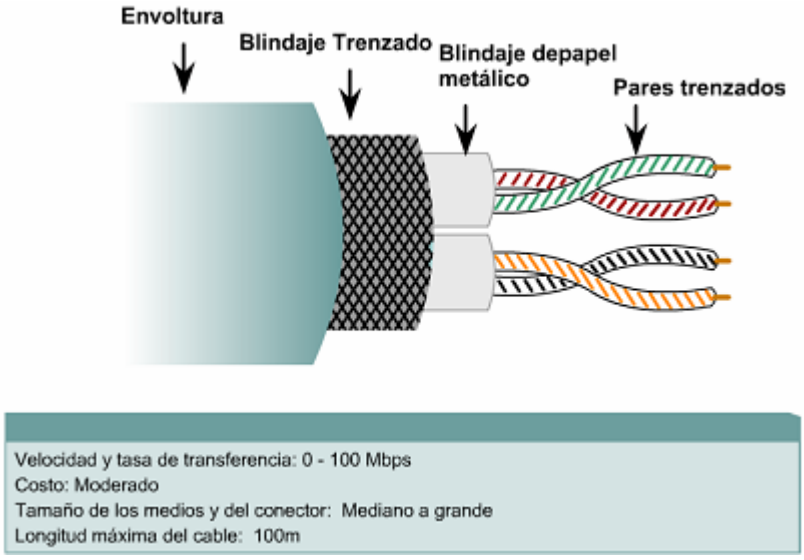
Para las LAN, el cable coaxial ofrece varias ventajas. Puede tenderse a mayores distancias que el cable de par trenzado blindado STP, y que el cable de par trenzado no blindado, UTP, sin necesidad de repetidores. Los repetidores regeneran las señales de la red de modo que puedan abarcar mayores distancias. El cable coaxial es más económico que el cable de fibra óptica y la tecnología es sumamente conocida. Se ha usado durante muchos años para todo tipo de comunicaciones de datos, incluida la televisión por cable.



Al trabajar con cables, es importante tener en cuenta su tamaño. A medida que aumenta el grosor, o diámetro, del cable, resulta más difícil trabajar con él. Recuerde que el cable debe pasar por conductos y cajas existentes cuyo tamaño es limitado. Se puede conseguir cable coaxial de varios tamaños. El cable de mayor diámetro es de uso específico como cable de backbone de Ethernet porque tiene mejores características de longitud de transmisión y de limitación del ruido. Este tipo de cable coaxial frecuentemente se denomina thicknet o red gruesa. Como su apodo lo indica, este tipo de cable puede ser demasiado rígido como para poder instalarse con facilidad en algunas situaciones. Generalmente, cuanto más difícil es instalar los medios de red, más costosa resulta la instalación. El cable coaxial resulta más costoso de instalar que el cable de par trenzado. Hoy en día el cable thicknet casi nunca se usa, salvo en instalaciones especiales.

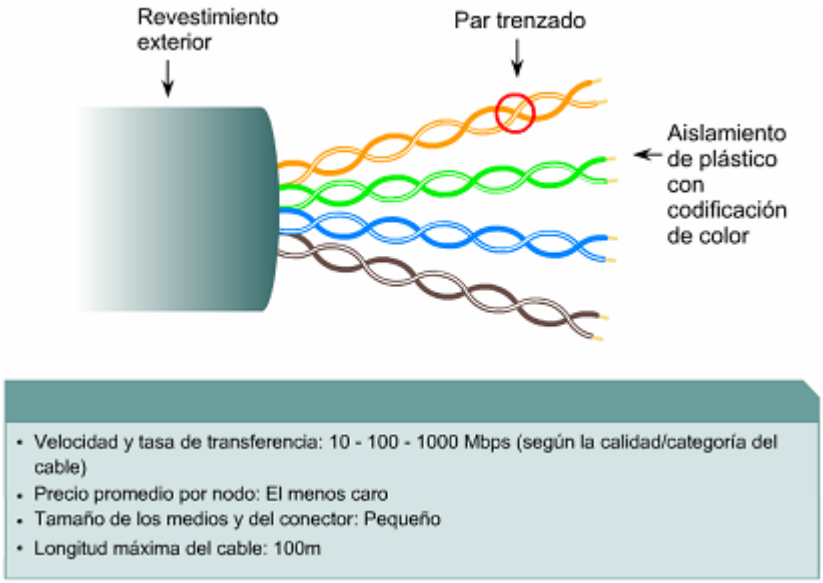
En el pasado, el cable coaxial con un diámetro externo de solamente 0,35 cm (a veces denominado thinnet o red fina) se usaba para las redes Ethernet. Era particularmente útil para las instalaciones de cable en las que era necesario que el cableado tuviera que hacer muchas vueltas. Como la instalación de thinnet era más sencilla, también resultaba más económica. Por este motivo algunas personas lo llamaban cheapernet (red barata). El trenzado externo metálico o de cobre del cable coaxial abarca la mitad del circuito eléctrico. Se debe tener especial cuidado de asegurar una sólida conexión eléctrica en ambos extremos, brindando así una correcta conexión a tierra. La incorrecta conexión del material de blindaje constituye uno de los problemas principales relacionados con la instalación del cable coaxial. Los problemas de conexión resultan en un ruido eléctrico que interfiere con la transmisión de señales sobre los medios de networking. Por esta razón, thinnet ya no se usa con frecuencia ni está respaldado por los estándares más recientes (100 Mbps y superiores) para redes Ethernet.

Cable STP El cable de par trenzado blindado (STP) combina las técnicas de blindaje, cancelación y trenzado de cables. Cada par de hilos está envuelto en un papel metálico. Los dos pares de hilos están envueltos juntos en una trenza o papel metálico. Generalmente es un cable de 150 ohmios. Según se especifica para el uso en instalaciones de redes Token Ring, el STP reduce el ruido eléctrico dentro del cable como, por ejemplo, el acoplamiento de par a par y la diafonía. El STP también reduce el ruido electrónico desde el exterior del cable, como, por ejemplo, la interferencia electromagnética (EMI) y la interferencia de radiofrecuencia (RFI). El cable de par trenzado blindado comparte muchas de las ventajas y desventajas del cable de par trenzado no blindado (UTP). El cable STP brinda mayor protección ante toda clase de interferencias externas, pero es más caro y de instalación más difícil que el UTP.



Un nuevo híbrido de UTP con STP tradicional se denomina UTP apantallado (ScTP), conocido también como par trenzado de papel metálico (FTP). El ScTP consiste, básicamente, en cable UTP envuelto en un blindaje de papel metálico. ScTP, como UTP, es también un cable de 100 Ohms. Muchos fabricantes e instaladores de cables pueden usar el término STP para describir el cable ScTP. Es importante entender que la mayoría de las referencias hechas a STP hoy en día se refieren en realidad a un cable de cuatro pares apantallado. Es muy improbable que un verdadero cable STP sea usado durante un trabajo de instalación de cable. Los materiales metálicos de blindaje utilizados en STP y ScTP deben estar conectados a tierra en ambos extremos. Si no están adecuadamente conectados a tierra o si hubiera discontinuidades en toda la extensión del material del blindaje, el STP y el ScTP se pueden volver susceptibles a graves problemas de ruido. Son susceptibles porque permiten que el blindaje actúe como una antena que recoge las señales no deseadas. Sin embargo, este efecto funciona en ambos sentidos. El blindaje no sólo evita que ondas electromagnéticas externas produzcan ruido en los cables de datos sino que también minimiza la irradiación de las ondas electromagnéticas internas. Estas ondas podrían producir ruido en otros dispositivos. Los cables STP y ScTP no pueden tenderse sobre distancias tan largas como las de otros medios de networking (tales como el cable coaxial y la fibra óptica) sin que se repita la señal. El uso de aislamiento y blindaje adicionales aumenta de manera considerable el tamaño, peso y costo del cable. Además, los materiales de blindaje hacen que las terminaciones sean más difíciles y aumentan la probabilidad de que se produzcan defectos de mano de obra. Sin embargo, el STP y el ScTP todavía desempeñan un papel importante, especialmente en Europa o en instalaciones donde exista mucha EMI y RFI cerca de los cables.

Cable UTP El cable de par trenzado no blindado (UTP) es un medio de cuatro pares de hilos que se utiliza en diversos tipos de redes. Cada uno de los 8 hilos de cobre individuales del cable UTP está revestido de un material aislante. Además, cada par de hilos está trenzado. Este tipo de cable cuenta sólo con el efecto de cancelación que producen los pares trenzados de hilos para limitar la degradación de la señal que causan la EMI y la RFI. Para reducir aún más la diafonía entre los pares en el cable UTP, la cantidad de trenzados en los pares de hilos varía. Al igual que el cable STP, el cable UTP debe seguir especificaciones precisas con respecto a cuánto trenzado se permite por unidad de longitud del cable.



El estándar TIA/EIA-568-B.2 especifica los componentes de cableado, transmisión, modelos de sistemas, y los procedimientos de medición necesarios para verificar los cables de par trenzado balanceado. Exige el tendido de dos cables, uno para voz y otro para datos en cada toma. De los dos cables, el cable de voz debe ser UTP de cuatro pares. El cable Categoría 5 es el que actualmente se recomienda e implementa con mayor frecuencia en las instalaciones. Sin embargo, las predicciones de los analistas y sondeos independientes indican que el cable de Categoría 6 sobrepasará al cable Categoría 5 en instalaciones de red. El hecho que los requerimientos de canal y enlace de la Categoría 6 sean compatibles con la Categoría 5e hace muy fácil para los clientes elegir Categoría 6 y reemplazar la Categoría 5e en sus redes. Las aplicaciones que funcionan sobre Categoría 5e también lo harán sobre Categoría 6.

El cable de par trenzado no blindado presenta muchas ventajas. Es de fácil instalación y es más económico que los demás tipos de medios para networking. De hecho, el UTP cuesta menos por metro que cualquier otro tipo de cableado para LAN. Sin embargo, la ventaja real es su tamaño. Debido a que su diámetro externo es tan pequeño, el cable UTP no llena los conductos para el cableado tan rápidamente como sucede con otros tipos de cables. Esto puede ser un factor sumamente importante a tener en cuenta, en especial si se está instalando una red en un edificio antiguo. Además, si se está instalando el cable UTP con un conector RJ-45, las fuentes potenciales de ruido de la red se reducen enormemente y prácticamente se garantiza una conexión sólida y de buena calidad. El cableado de par trenzado presenta ciertas desventajas. El cable UTP es más susceptible al ruido eléctrico y a la interferencia que otros tipos de medios para networking y la distancia que puede abarcar la señal sin el uso de repetidores es menor para UTP que para los cables coaxiales y de fibra óptica. En una época, el cable de par trenzado era considerado más lento para transmitir datos que otros tipos de cables. Sin embargo, hoy en día ya no es así. De hecho, en la actualidad, se considera que el cable de par trenzado es el más rápido entre los medios basados en cobre.

Medios típicos	Ancho de banda máximo teórico	Distancia máxima teórica
Cable coaxial de 50 ohmios (Ethernet 10BASE2, Thinnet)	10 Mbps	185 m
Cable coaxial de 50 ohmios (Ethernet 10BASE5, Thicknet)	10 Mbps	500 m
Cable de par trenzado no blindado de categoría 5 (UTP) (Ethernet 10BASE-T)	10 Mbps	100 m
Cable de par trenzado no blindado de categoría 5 (UTP) (Ethernet 100BASE-TX)	100 Mbps	100 m
Cable de par trenzado no blindado de categoría 5 (UTP) (Ethernet 1000BASE-TX)	1000 Mbps	100 m
Fibra Óptica Multimodo (62.5/125µm) (100BASE-FX Ethernet)	100 Mbps	2000 m
Fibra Óptica Multimodo (62.5/125µm) (1000BASE-SX Ethernet)	1000 Mbps	220 m
Fibra Óptica Multimodo(50/125µm) (1000BASE-SX Ethernet)	1000 Mbps	550 m
Fibra Óptica Monomodo (9/125µm) (1000BASE-LX Ethernet)	1000 Mbps	5000 m

Medios de fibra óptica La luz que se utiliza en las redes de fibra óptica es un tipo de energía electromagnética. Cuando una carga eléctrica se mueve hacia adelante y hacia atrás, o se acelera, se produce un tipo de energía denominada energía electromagnética. Esta energía, en forma de ondas, puede viajar a través del vacío, el aire y algunos materiales como el vidrio. Una propiedad importante de toda onda de energía es la longitud de onda. La radio, las microondas, el radar, la luz visible, los rayos x y los rayos gama parecen ser todos muy diferentes. Sin embargo, todos ellos son tipos de energía electromagnética. Si se ordenan todos los tipos de ondas electromagnéticas desde la mayor longitud de onda hasta la menor, se crea un continuo denominado espectro electromagnético. La longitud de onda de una onda electromagnética es determinada por la frecuencia a la que la carga eléctrica que genera la onda se mueve hacia adelante y hacia atrás. Si la carga se mueve lentamente hacia adelante y hacia atrás, la longitud de onda que genera es una longitud de onda larga. Visualice el movimiento de la carga eléctrica como si fuera una varilla en una charca. Si la varilla se mueve lentamente hacia adelante y hacia atrás, generará movimientos en el agua con una longitud de onda larga entre las partes superiores de las ondas. Si la varilla se mueve rápidamente hacia adelante y hacia atrás, los movimientos en el agua tendrán una longitud de onda mas corta. Como todas las ondas electromagnéticas se generan de la misma manera, comparten muchas propiedades. Todas las ondas viajan a la misma velocidad en el vacío. La velocidad es aproximadamente 300.000 kilometros por segundo o 186.283 millas por segundo. Esta es también la velocidad de la luz. Los ojos humanos están diseñados para percibir solamente la energía electromagnética de longitudes de onda de entre 700 y 400 nanómetros (nm). Un nanómetro es la mil millonésima parte de un metro (0,000000001 metro) de longitud. La energía electromagnética con longitudes de onda entre 700 y 400 nm recibe el nombre de luz visible. Las longitudes de onda de luz más largas que se encuentran cerca de los 700 nm se perciben como el color rojo. Las longitudes de onda más cortas que se encuentran alrededor de los 400 nm aparecen como el color violeta. Esta parte del espectro magnético se percibe como los colores del arco iris.

Guía de Onda (Wave Guide): La guía de onda es otro medio de comunicación también muy usado, el cual opera en el rango de las frecuencias comúnmente llamadas como microondas (en el orden de GHz). Su construcción es de material metálico por lo que no se puede decir que sea un cable. El ancho de banda es extremadamente grande y es usada principalmente cuando se requiere bajas perdidas en la señal bajo condiciones de muy alta potencia como el caso desde una antena de microondas a el receptor/transmisor de radio frecuencia. Las aplicaciones típicas de este medio es en

las centrales telefónicas para bajar/subir señales provenientes de antenas de satélite o estaciones terrenas de microondas. No todas las guías de onda son duras, también existen guías de onda más flexibles, existe un tipo de guía de onda que fabrica una compañía que se llama ANDREW, y a este tipo de guía de onda flexible se le conoce como Heliax.

Microondas terrestre: Un radioenlace terrestre o microondas terrestre provee conectividad entre dos sitios (estaciones terrenas) en línea de vista (Line-of-Sight, LOS) usando equipo de radio con frecuencias de portadora por encima de 1 GHz. La forma de onda emitida puede ser analógica (convencionalmente en FM) o digital.

Las principales aplicaciones de un sistema de microondas terrestre son las siguientes:

- Telefonía básica (canales telefónicos)
- Datos
- Telégrafo/Telex/Facsímile
- Canales de Televisión.
- Video
- Telefonía Celular (entre troncales)

Un sistema de microondas consiste de tres componentes principales: una antena con una corta y flexible guía de onda, una unidad externa de RF (Radio Frecuencia) y una unidad interna de RF. Las principales frecuencias utilizadas en microondas se encuentran alrededor de los 12 GHz, 18 y 23 Ghz, las cuales son capaces de conectar dos localidades entre 1 y 15 millas de distancia una de la otra. El equipo de microondas que opera entre 2 y 6 Ghz puede transmitir a distancias entre 20 y 30 millas. Las licencias o permisos para operar enlaces de microondas pueden resultar un poco difíciles ya que las autoridades deben de asegurarse que ambos enlaces no causen interferencia a los enlaces ya existentes.

El clima y el terreno son los mayores factores a considerar antes de instalar un sistema de microondas. Como por ejemplo, no se recomienda instalar sistemas en lugares donde no llueva mucho; en este caso deben usarse radios con frecuencias bajas (es decir menores a 10 GHz). La consideraciones en terreno incluyen la ausencia de montañas o grandes cuerpos de agua las cuales pueden ocasionar reflecciones de multi-trayectorias.

Radio Frecuencia (HF): Por convención, la radio transmisión en la banda entre 3 Mhz y 30 Mhz es llamada radio de alta frecuencia (HF) u ondas cortas. Las bandas de frecuencia dentro del espectro de HF son asignadas por tratados internacionales para servicios específicos como movibles (aeronáutico, marítimo y terrestre), radiodifusión, radio amateur, comunicaciones espaciales y radio astronomía. La radio de HF tiene propiedades de propagación que la hacen menos confiable que otras frecuencias; sin embargo, la radio de HF permite comunicaciones a grandes distancias con pequeñas cantidades de potencia radiada.

Las ondas de radio de HF transmitidas desde antenas en la tierra siguen dos trayectorias. La onda terrestre (groundwave) sigue la superficie de la tierra y la onda aérea (skywave) rebota de ida y vuelta entre la superficie de la tierra y varias capas de la ionosfera terrestre. La útil para comunicaciones de hasta cerca de 400 millas, y trabaja particularmente bien sobre el agua. La onda aérea propaga señales a distancias de hasta 4,000 millas con una confiabilidad en la trayectoria de 90 %.

La trayectoria de propagación de las ondas aéreas son afectadas por dos factores El angulo y la frecuencia Si la onda radiada entra en la capa ionizada con un angulo mayor que el (angulo crítico) entonces la onda no es reflejada ; pero si el angulo es menor que la onda será reflejada y regresara a la tierra. Ambos efectos son mostrados en las siguientes figuras.

El peso del capa de la ionósfera afectara gandemente la distancia de salto. La distancia tambien varia con la frecuencia de la onda transmitida. Ya que el peso y la densidad de la capas de la ionosfera dependen tambien la radiación solar, hay una significante diferencia entre la distancia de salto de las transmisiones diurnas y las nocturnas.

Las ondas terrestres en cambio tiene un alcance más corto comparadas con las ondas áereas. Las ondas terrestres tienen tres componentes: la onda directa, la onda de superficie y la onda reflejada. Las ondas terrestres son afectadas por la conductividad y las caracteristicas de la superficie de la tierra. A más alta conductividad mejor transmisión, asi las ondas terrestres viajan mejor sobre al agua del mar, agua dulce, aguas pantanosas, etc. Sobre terreno rocosos y desierto la transmisión es muy pobre, mientras que en zonas selvaticas es practicamente inutilizable. Las condiciones de humedad en el aire cercanas a la tierra afectan grandemente las ondas terrestres. Las características de propagación de la onda terrestre tambien son afectadas por la frecuencia de la onda.

Láser/Infrarrojo: Las transmisiones de láser de infrarrojo directo envuelven las mismas técnicas empleadas en la transmisión por fibra óptica, excepto que el medio en este caso es el aire libre. El láser tiene un alcance de hasta 10 millas, aunque casi todas las aplicaciones en la actualidad se realizan a distancias menores de una milla. típicamente, las transmisiones en infrarrojo son utilizadas donde la instalación de cable no es factible entre ambos sitios a conectar. Las velocidades típicas de transmisión a esas distancias son 1.5 Mbps. La ventaja del láser infrarrojo es que no es necesario solicitar permiso ante las autoridades para utilizar esta tecnología. Debe de tenerse mucho cuidado, en la instalación ya que los haces de luz pueden dañar al ojo humano. Por lo que se requiere un lugar adecuado para la instalación del equipo. Ambos sitios deben de tener linea de vista.

Para distancias cortas las transmisiones vía láser/infrarrojo son una excelente opción. Lo cual resulta en poco tiempo mas económico que el empleo de estaciones terrenas de microondas. Se utiliza bastante para conectar LANs localizadas en diferentes edificios.

Vía Satélite: La idea de comunicación global mediante el uso de satélites se debe a Arthur C. Clarke quien se basó en el trabajo matemático y físico de las Leyes de Isaac Newton publicadas en 1687 y las Leyes de Kepler, publicadas en el periodo 1609-1619, y lo unió con aplicaciones y tecnología existente en esa época (1940's). La propuesta de Clarke en 1945 se basaba en lo siguiente:

- El satélite serviría como repetidor de comunicaciones
- El satélite giraría a 36,000 km de altura sobre el ecuador
- A esa altura estaría en órbita "Geoestracionaria"
- Tres satélites separados a 120° entre sí cubrirían toda la tierra
- Se obtendría energía eléctrica mediante energía solar
- El satélite sería una estación espacial tripulada.

Casi todos estos puntos se llevaron a cabo unos años después, cuando mejoró la tecnología de cohetes, con la excepción del último punto. Este no se cumplió debido al alto costo que implicaba el transporte y mantenimiento de tripulación a bordo de la estación espacial, por cuestiones de seguridad médica y orgánica en los tripulantes, y finalmente por el avance de técnicas de control remoto. Un satélite actúa como una estación de relevación (relay station) o repetidor. Un transpondedor recibe la señal de un transmisor, luego la amplifica y la retransmite hacia la tierra a una frecuencia diferente. Debe notarse que la estación terrena transmisora envía a un solo satélite. El satélite, sin embargo, envía a cualquiera de las estaciones terrenas receptoras en su área de cobertura o huella (footprint). La transmisión por satélite ofrece muchas ventajas para una compañía. Los precios de renta de espacio satelital es más estable que los que ofrecen las compañías telefónicas. Ya que la transmisión por satélite no es sensitiva a la distancia. Y además existe un gran ancho de banda disponible.

Los beneficios de la comunicación por satélite desde el punto de vista de comunicaciones de datos podrían ser los siguientes:

- Transferencia de información a altas velocidades (Kbps, Mbps)
- Ideal para comunicaciones en puntos distantes y no fácilmente
- accesibles geográficamente.
- Ideal en servicios de acceso múltiple a un gran número de puntos.
- Permite establecer la comunicación entre dos usuarios distantes con
- la posibilidad de evitar las redes publicas telefónicas.

Entre las desventajas de la comunicación por satélite están las siguientes:

- 1/4 de segundo de tiempo de propagación. (retardo)
- Sensitividad a efectos atmosféricos
- Sensibles a eclipses
- Falla del satélite (no es muy común)
- Requieren transmitir a mucha potencia
- Posibilidad de interrupción por cuestiones de estrategia militar.

A pesar de las anteriores limitaciones, la transmisión por satélite sigue siendo muy popular. Los satélites de órbita baja (Low Earth Orbit LEO) ofrecen otras alternativas a los satélites geoestacionarios (Geosynchronous Earth Orbit GEO), los cuales giran alrededor de la tierra a más de 2,000 millas. Los satélites de este tipo proveen comunicaciones de datos a baja velocidad y no son capaces de manipular voz , señales de video o datos a altas velocidades. Pero tienen las ventajas que los satélites GEO no tienen. Por ejemplo, no existe retardo en las transmisiones, son menos sensibles a factores atmosféricos, y transmiten a muy poca potencia. Estos satélites operan a frecuencias asignadas entre los 1.545 GHz y los 1.645 GHz (Banda L). Los reflectores parabólicos (comúnmente llamados por error o por costumbre *antenas*) han sido el *símbolo* de las estaciones terrenas para comunicaciones por satélite. Existen además de los *reflectores paraboloides o Prime Focus* otros tipos de antenas muy ampliamente usados en campo de las comunicaciones, tales como los reflectores *Fuera de foco* (off-set)*, Casssegrain* y los platos tipos **Gregorianos**.

Ventajas de la Fibra Óptica	**Desventajas de la Fibra Óptica**	**Ventajas Satélite**	**Desventajas Satélite**
Gran ancho de banda	Cobertura limitada (del cableado)	Gran ancho de banda	Costo de operación mensual muy alto.
Inmunidad a la interferencia y ruido	Alto costo de operación mensual	Gran cobertura nacional e internacional	Retardo de 1/2 segundo
Bajo costo inicial en equipo de comunicaciones	Costos dependientes de la distancia	Costo insensible a la distancia	Inversión inicial en equipo de comunicaciones muy costoso (estaciones terrenas y demás dispositivos).
No requiere personal especializado	Requiere contratación de la línea ante una compañía telefónica		Muy sensible a factores atmosféricos
No hay costos por el mantenimiento de la línea.			Sensible a la interferencia y ruido

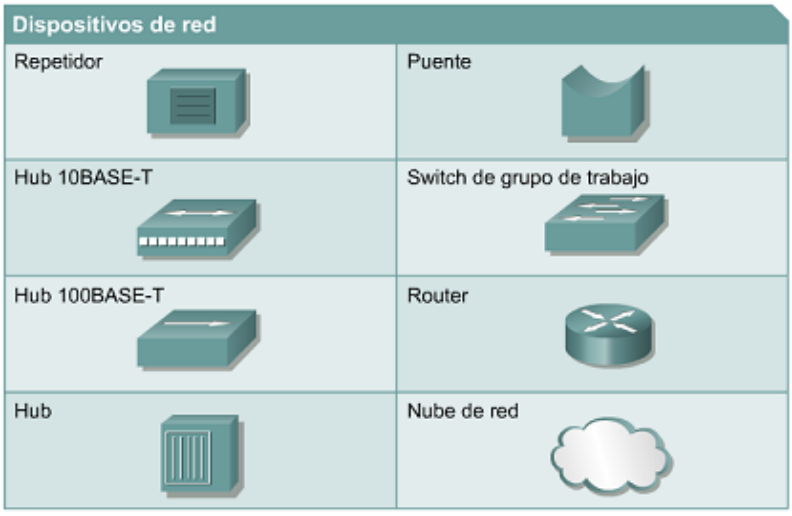
Ventajas de la Fibra Óptica	Desventajas de la Fibra Óptica	Ventajas Satélite	Desventajas Satélite
No usa el espectro radioeléctrico			Sensible a eclipses
No existe retardo			Requiere de personal especializado
			El mantenimiento corre a cargo del usuario
			No recomendable para aplicaciones de voz
			Hace uso del espectro radioeléctrico

Fibra óptica vs. Satélite

2.6.7 Dispositivos de Networking

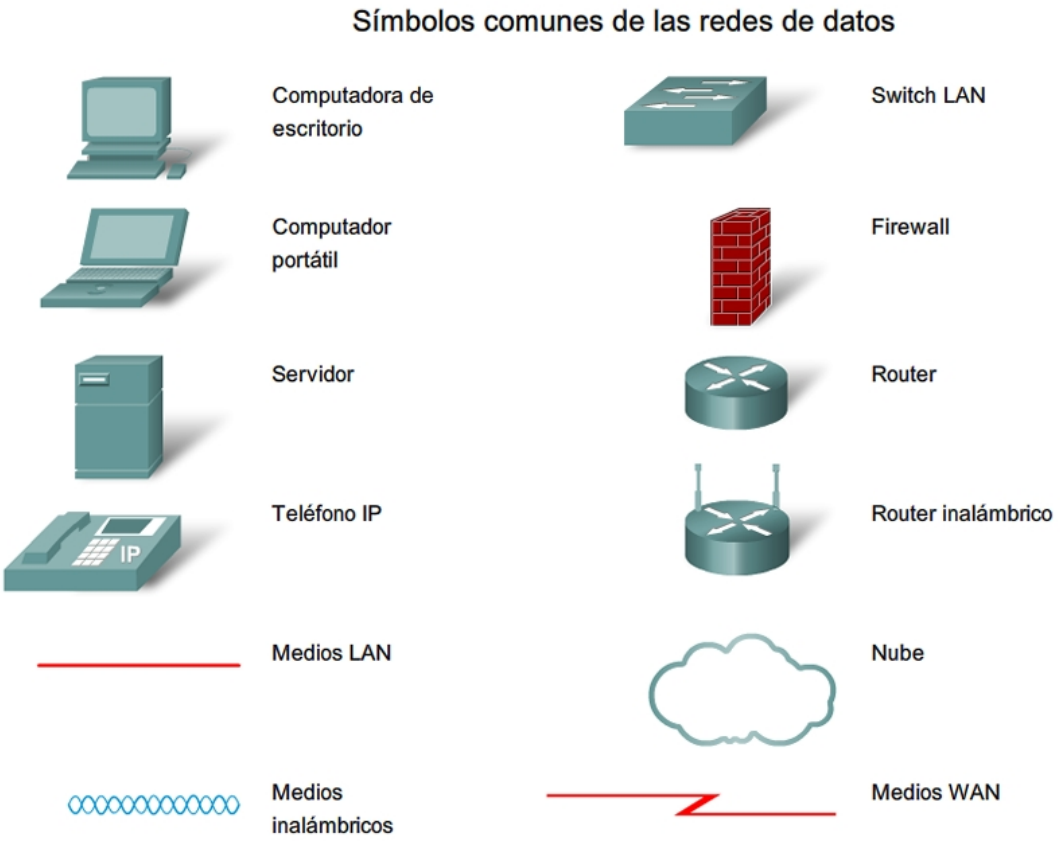
Los equipos que se conectan de forma directa a un segmento de red se denominan dispositivos. Estos dispositivos se clasifican en dos grandes grupos. El primer grupo está compuesto por los dispositivos de usuario final. Los dispositivos de usuario final incluyen los computadores, impresoras, escáners, y demás dispositivos que brindan servicios directamente al usuario. El segundo grupo está formado por los dispositivos de red. Los dispositivos de red son todos aquellos que conectan entre sí a los dispositivos de usuario final, posibilitando su intercomunicación.

Los dispositivos de usuario final que conectan a los usuarios con la red también se conocen con el nombre de hosts. Estos dispositivos permiten a los usuarios compartir, crear y obtener información. Los dispositivos host pueden existir sin una red, pero sin la red las capacidades de los *hosts* se ven sumamente limitadas. Los dispositivos *host* están físicamente conectados con los medios de red mediante una tarjeta de interfaz de red (NIC). Utilizan esta conexión para realizar las tareas de envío de correo electrónico, impresión de documentos, escaneado de imágenes o acceso a bases de datos.



Un NIC es una placa de circuito impreso que se coloca en la ranura de expansión de un bus de la motherboard de un computador, o puede ser un dispositivo periférico. También se denomina adaptador de red. Las NIC para computadores portátiles o de mano por lo general tienen el tamaño de una tarjeta PCMCIA. Cada NIC individual tiene un código único, denominado dirección de control de

acceso al medio (MAC). Esta dirección se utiliza para controlar la comunicación de datos para el host de la red. Tal como su nombre lo indica, la NIC controla el acceso del host al medio. Los dispositivos de red son los que transportan los datos que deben transferirse entre dispositivos de usuario final. Los dispositivos de red proporcionan el tendido de las conexiones de cable, la concentración de conexiones, la conversión de los formatos de datos y la administración de transferencia de datos. Algunos ejemplos de dispositivos que ejecutan estas funciones son los repetidores, hubs, puentes, switches y routers.



2.6.8 Clasificación de los tipos de conmutación de datos

La conmutación permite la entrega de información desde un nodo origen hasta un destino a través de un medio compartido, gracias a los nodos intermedios que actúan como elementos activos en el encaminamiento de la información, dirigiendo los datos. Existen diversas técnicas para llevar a cabo esta tarea, como son la conmutación de circuitos, de paquetes y de celdas, así como variantes específicas que a continuación son descritas.

- ***Conmutación de circuitos***: Modo de operación de una red en el que la comunicación entre dos terminales se produce a través de caminos establecidos al inicio de la comunicación, que no varían durante ésta y que se dedican en exclusiva a ella. Los caminos se construyen al inicio de la comunicación, por conmutación electro-mecánica o electrónica en los nodos intermedios, concatenando una serie de circuitos físicos (por ejemplo, una línea de par trenzado dentro de un cable de pares, un canal en un sistema de FDM o TDM, un canal de radiofrecuencia en el espacio o un canal luminoso en una fibra óptica). Las características más relevantes de las comunicaciones establecidas en este modo de operación son: a) su ancho de banda (B), o velocidad de transmisión (R), es fijo; b) su retardo (T) es bajo y constante. Dada la reserva exclusiva de recursos de red que implica, la conmutación de circuitos resultará rentable cuando se éstos aprovechen enteramente, es decir, para flujos continuos de datos. El

ejemplo más claro e importante de este modo de operación lo constituye la red telefónica bajo los estándares del ITU-T (con sus circuitos digitales full-duplex a 64 kbit/s dedicados a cada llamada telefónica).

- ***Conmutación de paquetes:*** Modo de operación de una red en el que la comunicación entre dos terminales se produce mediante los paquetes (unidades de información formadas por grupos de bits) que viajan a través de caminos, establecidos inicialmente o no, fijos o variables a lo largo de la comunicación, compartidos por paquetes de otras comunicaciones. El camino que sigue cada paquete se realiza, tras su análisis, por su conmutación digital en los nodos intermedios. Las características más relevantes de las comunicaciones establecidas en este modo de operación son: a) su ancho de banda (B) no está generalmente prefijado, es decir, la red proporciona capacidad según los paquetes asociados a cada comunicación vayan llegando (según su demanda) y en función de la disponibilidad de recursos; b) su retardo (T) es variable y mayor que en la conmutación de circuitos. Esta variabilidad en B y T es debida a que no se reservan recursos en exclusiva a las comunicaciones; por lo tanto, los tiempos de procesamiento y conmutación y la capacidad disponible varían continuamente en función de las comunicaciones y paquetes que existen en un momento dado. Algunos ejemplos de este modo de operación se encuentran en las redes de datos públicas o privadas que operan bajo estándares como X.25 (o Frame Relay) del ITU-T, TCP/IP de la comunidad internet, etc.

  Existen dos grandes familias dentro de la conmutación de paquetes clásica:

  - *Conmutación de paquetes en modo "circuito virtual":* El camino que siguen todos los paquetes pertenecientes a una comunicación se determina en su inicio y permanece invariable a lo largo de la comunicación como en la conmutación de circuitos. Aun así, sólo se determina el camino, no se hace una reserva de recursos (al menos no en exclusiva) como sucedía en la conmutación de circuitos. De ahí el nombre de circuito virtual.
  - *Conmutación de paquetes en modo "datagrama":* El camino que sigue cualquier paquete se determina individualmente, es decir, se determina en el momento en que un paquete llega a un nodo intermedio y solamente tiene validez para ese paquete en particular. De hecho, a nivel de la red, no existe la noción de comunicación (entendida como una asociación lógica en el tiempo entre dos terminales). Dicho de otro modo, cada paquete (que lleva toda la información necesaria para su "viaje" a través de la red) constituye en sí una comunicación.

- ***Conmutación de celdas:*** Es una variante evolucionada de la conmutación de paquetes en la que éstos son de longitud pequeña y fija (y usualmente llamados celdas). Su pequeña longitud permite una "granularidad" muy fina a la hora de asignar recursos a las comunicaciones y, por tanto, un buen aprovechamiento del ancho de banda. El tamaño fijo de las celdas facilita el uso de técnicas de conmutación muy rápidas (realizadas directamente por hardware). El ejemplo más relevante de este modo de operación se encuentra en las redes de banda ancha basadas en la tecnología ATM (Asynchronous Transfer Mode) (ver más detalles en el capítulo 6).

2.6.9 Clasificación del tráfico en clases

Con el único fin de perfilar los distintos tipos de tráfico que puedan ser transportados por una red, se pueden establecer una posible clasificación con las siguientes 3 clases de tráfico:

- Clase I (tiempo real): de mensajes largos o continuos, en tiempo real (no tolera retardos superiores, digamos, a 200 ms), admite errores, admite bloqueo, muy interactivo: hombrehombre (telefonía, videoconferencia), adecuado para la conmutación de circuitos.
- Clase II (interactivo, racheado): de mensajes cortos y racheados (a ráfagas), interactivo (tolera cierto retardo, de 1 a 3 s.), no suele admitir errores, admite cierto bloqueo, interactivo: hombre-máquina, máquina-máquina (terminal de datos, cajero electrónico, navegación web), adecuado

para la conmutación de paquetes.

- Clase III (pesado, diferido): de mensajes muy largos, no requiere tiempo real (tolera retardos elevados, hasta de minutos), no admite errores, no admite bloqueo, no interactivo: máquinamáquina (transferencia de archivos, correo electrónico), adecuado para la conmutación de paquetes o circuitos.

2.6.10 Hub

El hub es un dispositivo prácticamente fuera de uso, que opera en la capa 1 del modelo OSI. Su función es regenerar y retemporizar las señales de red. Los hubs toman los datos recibidos por un puerto y lo retransmiten por todos los otros puertos, por este motivo, se dice que este dispositivo "divide" el ancho de banda entre todas las estaciones conectadas. Forma un dominio de colisión entre todas las estaciones conectadas, esto permite que los datos enviados por cada estación sean recibidos por todas las demás. Los hubs concentran las conexiones. En otras palabras, permiten que la red trate un grupo de hosts como si fuera una sola unidad. Esto sucede de manera pasiva, sin interferir en la transmisión de datos. Los hubs activos no sólo concentran hosts, sino que además regeneran señales.

Los hubs en realidad son repetidores multipuerto. En muchos casos, la diferencia entre los dos dispositivos radica en el número de puertos que cada uno posee. Mientras que un repetidor convencional tiene sólo dos puertos, un hub por lo general tiene de cuatro a veinticuatro puertos. Los hubs por lo general se utilizan en las redes Ethernet 10BASE-T o 100BASE-T, aunque hay otras arquitecturas de red que también los utilizan. El uso de un hub hace que cambie la topología de la red desde un bus lineal, donde cada dispositivo se conecta de forma directa al cable, a una en estrella. En un hub, los datos que llegan a un puerto del hub se transmiten de forma eléctrica a todos los otros puertos conectados al mismo segmento de red, salvo a aquel puerto desde donde enviaron los datos.

Los hubs vienen en tres tipos básicos:

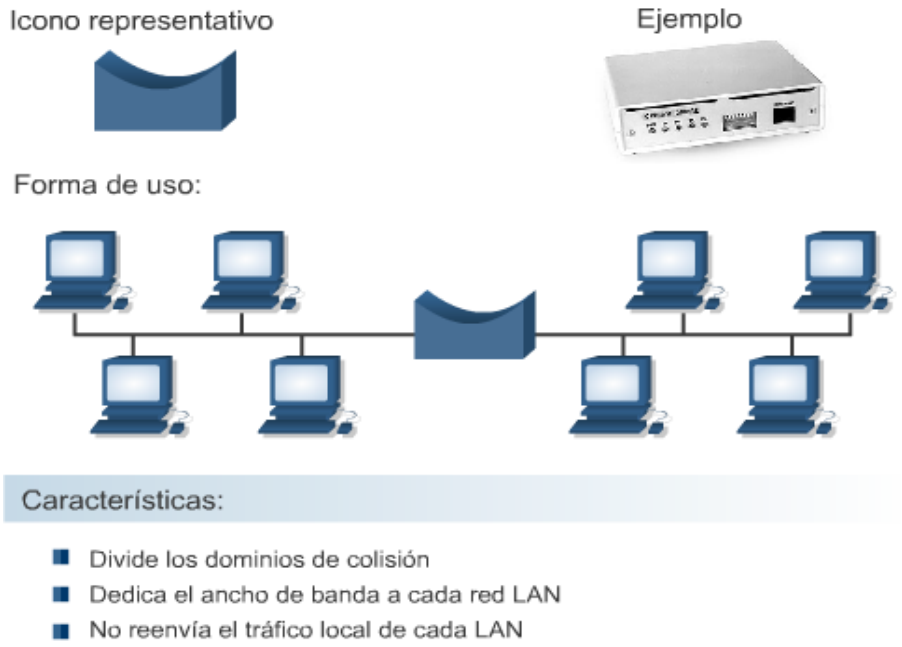
- Pasivo: Un hub pasivo sirve sólo como punto de conexión física. No manipula o visualiza el tráfico que lo cruza. No amplifica o limpia la señal. Un hub pasivo se utiliza sólo para compartir los medios físicos. En sí, un hub pasivo no requiere energía eléctrica.
- Activo: Se debe conectar un hub activo a un tomacorriente porque necesita alimentación para amplificar la señal entrante antes de pasarla a los otros puertos.

- Inteligente: A los hubs inteligentes a veces se los denomina "smart hubs". Estos dispositivos básicamente funcionan como hubs activos, pero también incluyen un chip microprocesador y capacidades diagnósticas. Los hubs inteligentes son más costosos que los hubs activos, pero resultan muy útiles en el diagnóstico de fallas.

Los dispositivos conectados al hub reciben todo el tráfico que se transporta a través del hub. Cuántos más dispositivos están conectados al hub, mayores son las probabilidades de que haya colisiones. Las colisiones ocurren cuando dos o más estaciones de trabajo envían al mismo tiempo datos a través del cable de la red. Cuando esto ocurre, todos los datos se corrompen. Cada dispositivo conectado al mismo segmento de red se considera un miembro de un dominio de colisión. Algunas veces los hubs se llaman concentradores, porque los hubs sirven como punto de conexión central para una LAN de Ethernet.

2.6.11 Puente

Un puente es un dispositivo que opera en la capa 2. Está diseñado para conectar dos segmentos LAN. El propósito de un puente es filtrar el tráfico de una LAN, de forma que sólo pase hacia la otra LAN lo que está dirigido a ella. Todo el tráfico que tiene origen y destino local, no se reenvía hacia la otra LAN. Para realizar su trabajo, el puente debe interpretar las tramas que son transmitidas en cada LAN y decidir si las reenvía de acuerdo a la dirección de destino. Se dice que este dispositivo "dedica" el ancho de banda a cada red LAN que interconecta. Cuando una estación envía una trama con destino broadcast, esta trama es reenviada a todas las LANs.



Los puentes convierten los formatos de transmisión de datos de la red además de realizar la administración básica de la transmisión de datos. Los puentes, tal como su nombre lo indica, proporcionan las conexiones entre LAN. Los puentes no sólo conectan las LAN, sino que además verifican los datos para determinar si les corresponde o no cruzar el puente. Esto aumenta la eficiencia de cada parte de la red.

A veces, es necesario dividir una LAN grande en segmentos más pequeños que sean más fáciles de manejar. Esto disminuye la cantidad de tráfico en una sola LAN y puede extender el área geográfica más allá de lo que una sola LAN puede admitir. Los dispositivos que se usan para conectar segmentos

de redes son los puentes, switches, routers y gateways. Los switches y los puentes operan en la capa de enlace de datos del modelo de referencia OSI. La función del puente es tomar decisiones inteligentes con respecto a pasar señales o no al segmento siguiente de la red.

Cuando un puente recibe una trama a través de la red, se busca la dirección MAC destino en la tabla de puenteo para determinar si hay que filtrar, inundar, o copiar la trama en otro segmento. El proceso de decisión tiene lugar de la siguiente forma:

- Si el dispositivo destino se encuentra en el mismo segmento que la trama, el puente impide que la trama vaya a otros segmentos. Este proceso se conoce como filtrado.
- Si el dispositivo destino está en un segmento distinto, el puente envía la trama hasta el segmento apropiado.
- Si el puente desconoce la dirección destino, el puente envía la trama a todos los segmentos excepto aquel en el cual se recibió. Este proceso se conoce como inundación.
- Si se ubica de forma estratégica, un puente puede mejorar el rendimiento de la red de manera notoria.

2.6.12 Switch

Un Switch, al igual que un puente, es un dispositivo de capa 2 (Enlace de Datos). De hecho, el Switch se denomina puente multipuerto. Los switches conmutan los datos sólo hacia el puerto al que está conectado el host destino. Se dice que este dispositivo "dedica" el ancho de banda a cada estación que interconecta. De la misma forma que los puentes, los switches retransmiten los broadcast por todos sus puertos. Cuando dos hosts realizan una transferencia, el switch realiza una microsegementación para comunicar los dos puertos donde están ubicados los hosts. Esta microsegmentación se mantiene mientras existe la transferencia y es independiente de otras transferencias. Esto permite mantener múltiples transferencia de manera simultánea e independiente. Los switches de grupos de trabajo agregan inteligencia a la administración de transferencia de datos. No sólo son capaces de determinar si los datos deben permanecer o no en una LAN, sino que pueden transferir los datos únicamente a la conexión que necesita esos datos. Otra diferencia entre un puente y un switch es que un switch no convierte formatos de transmisión de datos.

La conmutación es una tecnología que alivia la congestión en las LAN Ethernet, reduciendo el tráfico y aumentando el ancho de banda. Los switches pueden remplazar a los hubs con facilidad debido a que ellos funcionan con las infraestructuras de cableado existentes. Esto mejora el rendimiento con un mínimo de intrusión en la red ya existente. Actualmente en la comunicación de datos, todos los equipos de conmutación realizan dos operaciones básicas: La primera operación se llama conmutación de las tramas de datos. La conmutación de las tramas de datos es el procedimiento mediante el cual una trama se recibe en un medio de entrada y luego se transmite a un medio de salida.

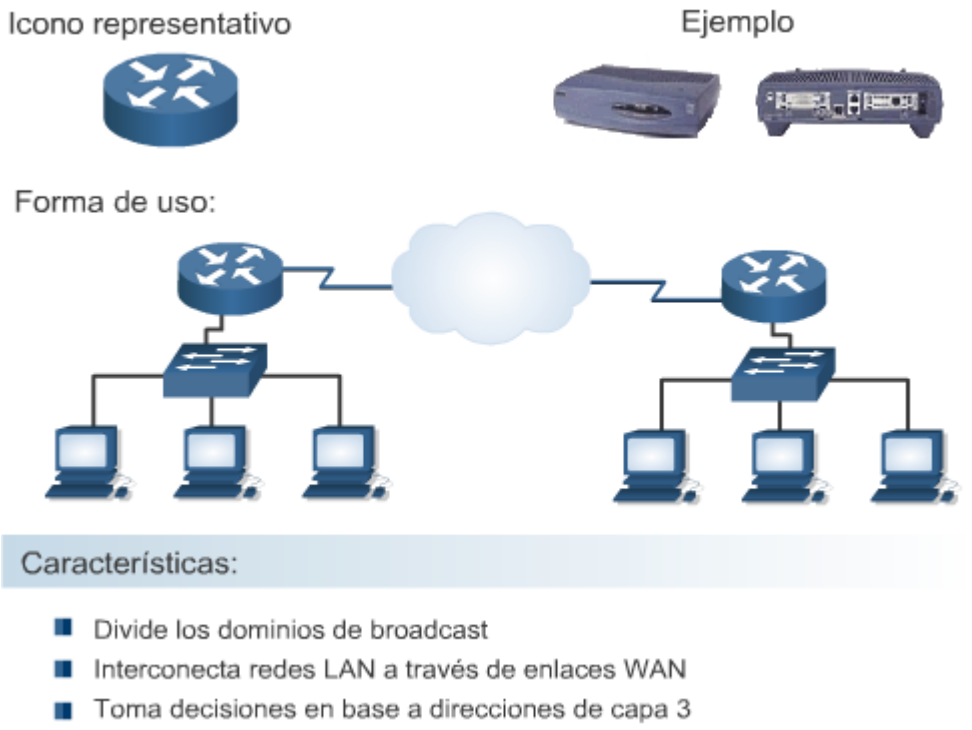
El segundo es el mantenimiento de operaciones de conmutación cuando los switch crean y mantienen tablas de conmutación y buscan loops. Los switches operan a velocidades mucho más altas que los puentes y pueden admitir nuevas funcionalidades como, por ejemplo, las LAN virtuales. Un switch se describe a veces como un puente multipuerto. Mientras que un puente típico puede tener sólo dos puertos que enlacen dos segmentos de red, el switch puede tener varios puertos, según la cantidad de segmentos de red que sea necesario conectar. Al igual que los puentes, los switches aprenden determinada información sobre los paquetes de datos que se reciben de los distintos computadores de la red. Los switches utilizan esa información para crear tablas de envío para determinar el destino de los datos que se están mandando de un computador a otro de la red.

Aunque hay algunas similitudes entre los dos, un switch es un dispositivo más sofisticado que un puente. Un puente determina si se debe enviar una trama al otro segmento de red, basándose en la dirección MAC destino. Un switch tiene muchos puertos con muchos segmentos de red conectados a ellos. El switch elige el puerto al cual el dispositivo o estación de trabajo destino está conectado. Los switches Ethernet están llegando a ser soluciones para conectividad de uso difundido porque, al igual que los puentes, los switches mejoran el rendimiento de la red al mejorar la velocidad y el ancho de banda.

Un switch Ethernet ofrece muchas ventajas. Un beneficio es que un switch para Ethernet permite que varios usuarios puedan comunicarse en paralelo usando circuitos virtuales y segmentos de red dedicados en un entorno virtualmente sin colisiones. Esto aumenta al máximo el ancho de banda disponible en el medio compartido. Otra de las ventajas es que desplazarse a un entorno de LAN conmutado es muy económico ya que el hardware y el cableado se pueden volver a utilizar.

2.6.13 Router

El Router es un dispositivo de capa 3 (Red). Toma sus decisiones de encaminamiento analizando las direcciones de red de los paquetes (PDU de capa 3). Los routers pueden conectar distintas tecnologías de Capa 2. La función de un Router es examinar los paquetes que recibe en una interfase, leer la dirección de destino de capa 3, elegir cuál es la mejor ruta y conmutar el paquete hacia el puerto de salida adecuado. Los routers no reenvían los broadcasts, por esto, se dice que "dividen" los dominios de broadcasts. Generalmente, los routers tienen una o más interfaces de LAN y una o más interfaces de WAN. Los routers poseen todas las capacidades indicadas antes. Los routers pueden regenerar señales, concentrar múltiples conexiones, convertir formatos de transmisión de datos, y manejar transferencias de datos. También pueden conectarse a una WAN, lo que les permite conectar LAN que se encuentran separadas por grandes distancias. Ninguno de los demás dispositivos puede proporcionar este tipo de conexión.



Tablas de enrutamiento: Los Routers utilizan protocolos de enrutamiento para crear y guardar tablas de enrutamiento que contienen información sobre las rutas. Esto ayuda al proceso de determinación de la ruta. Los protocolos de enrutamiento llenan las tablas de enrutamiento con una amplia variedad de información. Esta información varía según el protocolo de enrutamiento utilizado. Las tablas de enrutamiento contienen la información necesaria para enviar paquetes de datos a través de redes conectadas. Los dispositivos de Capa 3 interconectan dominios de broadcast o LAN. Se requiere un esquema de direccionamiento jerárquico para poder transferir los datos.

La tabla de enrutamiento se compone de información estática, proporcionada por el propio administrador de la red o dinámica, debido a la intervención de protocolos de enrutamiento tales como RIP, OSPF, IGRP, EIGRP, etc., quienes se encargan de actualizar el contenido de la tabla a medida que se van produciendo cambios en la topología, tales como: agregación o remoción de dispositivos, saturación de enlaces por exceso de tráfico, caídas de enlaces por interrupción de servicios, etc.

Los Routers mantienen información importante en sus tablas de enrutamiento, que incluye lo siguiente:

- Tipo de protocolo: el tipo de protocolo de enrutamiento que creó la entrada en la tabla de enrutamiento.
- Asociaciones entre destino/siguiente salto: estas asociaciones le dicen al Router que un destino en particular está directamente conectado al Router, o que puede ser alcanzado utilizando un Router denominado "salto siguiente" en el trayecto hacia el destino final. Cuando un Router recibe un paquete entrante, lee la dirección destino y verifica si hay concordancia entre esta dirección y una entrada de la tabla de enrutamiento.
- Métrica de enrutamiento: los distintos protocolos de enrutamiento utilizan métricas de enrutamiento distintas. Las métricas de enrutamiento se utilizan para determinar la conveniencia de una ruta. Por ejemplo, el números de saltos es la única métrica de enrutamiento que utiliza el protocolo de información de enrutamiento (RIP). El Protocolo de enrutamiento Gateway interior (IGRP) utiliza una combinación de ancho de banda, carga, retardo y confiabilidad como métricas para crear un valor métrico compuesto.

- Interfaces de salida: la interfaz por la que se envían los datos para llegar a su destino final.

Los Routers se comunican entre sí para mantener sus tablas de enrutamiento por medio de la transmisión de mensajes de actualización del enrutamiento. Algunos protocolos de enrutamiento transmiten estos mensajes de forma periódica, mientras que otros lo hacen cuando hay cambios en la topología de la red. Algunos protocolos transmiten toda la tabla de enrutamiento en cada mensaje de actualización, y otros transmiten sólo las rutas que se han modificado. Un Router crea y guarda su tabla de enrutamiento, analizando las actualizaciones de enrutamiento de los Routers vecinos.

Los routers, al igual que los switches, permiten la separación en dominios de colisión, pero no reenvían el tráfico broadcast, por lo que se los considera dispositivos que implementan la división de segmentos en dominios de broadcast. Generalmente los routers tienen una o más interfaces LAN y una o más interfaces WAN.

Dentro de la amplia gama de soluciones corporativas que podemos encontrar en el mercado, una de ellas la constituyen los routers denominados "apantallados" los cuales realizan el reenvío de los paquetes o un descarte de los mismos, basados en un conjunto de reglas provistas o configuradas por el administrador de la red.

La configuración en estos routers debe contemplar:

- Qué servicios se ofrecerán y en qué dirección.
- Las limitaciones respecto a la cantidad de PCs que tendrán acceso a los servicios y su posible agrupamiento.
- La existencia de equipos en la Internet que deban autenticarse con los equipos internos.

Parámetros a considerar para crear las reglas o políticas:

- Dirección IP origen y destino.
- Protocolo de capa 3 (IP).
- Protocolo de capa 4 (TCP/UDP).
- En los segmentos TCP, el bit de ACK.
- Tipo de mensaje para el caso de protocolo ICMP.
- Puertos origen/destino de TCP y UDP.

Routers Apantallados (Screening router) o routers que filtran información: Previo al análisis de una implementación con screening routers, recordemos que la redirección ordinaria solamente tiene en cuenta hacia dónde se dirige cada paquete de información, y selecciona cuál es la mejor vía para llegar a su destino. Este tipo de redireccionamiento no tiene en cuenta las políticas de seguridad o si la ruta es potencialmente segura o insegura. Únicamente su objetivo es el de llevar la información a su destino.

El "screening router", en cambio, analiza el paquete de información al detalle y establece si puede ser enviado a su destino en función de las políticas de seguridad del sistema.

En el supuesto caso de que fuera el único sistema de protección, y ante su posible falla, la red o el equipo puede verse expuesto a las amenazas del exterior. El "screening router" puede dar acceso a un servicio (o denegarlo). Pero, de haberse producido el acceso no autorizado, no puede realizar protecciones individuales dentro del mismo.

¿Cómo filtra paquetes? Un Firewall filtra o discrimina paquetes de información o de datos que va redirigiendo entre los host internos y externos del sistema, gracias a una selección que realiza

siguiendo las políticas de seguridad establecidas. Este redireccionamiento se conoce con el nombre técnico de "screening router". La finalidad de esta redirección puede considerar algunos de los siguientes elementos:

- Bloqueo de todas las conexiones externas, salvo aquellas que trabajen bajo SMTP, para permitir la recepción de correo electrónico.
- Bloqueo de todas las conexiones que puedan considerarse potencialmente inseguras.
- Permitiendo el servicio de correo electrónico y de FTP, aunque manteniendo el bloqueo a servicios potencialmente peligrosos como TFTP, RPC, servicios del tipo "r": rlogin (acceso por clave no verificado), etc.

Políticas de seguridad en los routers apantallados (screening routers)

Existen una serie de elementos de seguridad que son similares a todos los Firewalls:

- Un criterio de filtro de paquetes, que se establece para los puertos del dispositivo. Esta regla se conoce como "filtro de paquetes".
- Cuando un paquete de información llega al puerto establecido, cada uno de sus encabezados se analiza. Generalmente atañe a los del tipo IP, TCP o UDP.
- Las reglas de filtro de paquetes se guardan en un orden preciso para que cada una de ellas se ejecute en ese mismo orden, en función del tipo de paquete de información que llegue al sistema de red o al equipo.
- En el caso de que una regla (o parte de ella) se vea vulnerada, o no cumpla los requisitos establecidos, el paquete de información podrá recibirse en el sistema, pero, éste avisará mediante alertas de cuáles han sido los protocolos y normas que no cumple.
- Si la política de seguridad lo permite, la transmisión de los datos continúa y se recibe el paquete.
- Si un paquete no cumple ninguna de las reglas, se manda un aviso al sistema, que impide su acceso.

En función de los enunciados mencionados anteriormente, quedaría definida la importancia del mantenimiento adecuado del orden de las reglas para el firewall, ya que la aplicación las va leyendo una a una. Un Firewall NO es un sistema autónomo que pueda ir de una regla a otra sino que las va procesando según el orden marcado por el administrador del sistema o por el usuario.

Si las reglas se establecieran en un orden equivocado, podría no permitir el acceso de servicios que serían válidos, y permitir el acceso a otros servicios nocivos.

Un "Screening Router" puede ser un router (enrutador) comercial o un nodo con capacidad de enrutamiento que posee aptitudes de filtrado de paquetes, teniendo la funcionalidad de bloquear o permitir el tráfico entre redes o nodos basados en direcciones, puertos, protocolos, interfaces, etc.

Screened Host: Arquitectura del mismo.

Una arquitectura del tipo "Screened Host" provee servicios desde un sistema que está en la red interna, usando un router separado. La principal seguridad está dada por el filtrado de paquetes.

Definido por algunos autores como "Bastion Host", el mismo, podría estar situado en la red interna. Los paquetes filtrados por el "screening router" son procesados de tal manera que el "Bastion Host" es

la única máquina de la red interna a la que los host de Internet pueden abrir conexiones, donde solo cierto tipo de conexiones son permitidas. Por lo tanto, cualquier sistema externo que intente acceder al sistema interno deberá conectarse con este host, el cual requiere tener un alto nivel de seguridad.

El filtrado de paquetes, también, debe permitirle al "Bastion Host" abrir conexiones al mundo exterior. La configuración del filtrado de paquetes en un "screening router", debería contemplar las siguientes aproximaciones:

- Permitir que hosts internos se conecten con hosts de Internet para ciertos servicios (servicios permitidos por medio de paquetes filtrados), y
- No permitir todas las conexiones desde los hosts internos (forzar a esos hosts a usar el servicio de proxy via el "Bastion Host").

Estas aproximaciones se pueden combinar para brindar diferentes servicios: algunos pueden ser permitidos directamente filtrando paquetes, mientras que otros directamente vía proxy. Existen algunas desventajas en una implementación de este tipo; la principal es que si un ataque vulnera el "Bastion Host", ésto no es notado por la red interna. Así mismo, el router también presenta un punto de falla, si el mismo es comprometido, la red entera está disponible para ser atacada. El router puede ser el primer elemento a utilizar en la estrategia de defensa perimetral, si bien el mismo debe contar con recursos de seguridad e inspección para mejorar su rendimiento. En los temas subsiguientes veremos, como esta instancia se potencia con los Firewalls.

2.6.14 Gateway

El término gateway se utiliza generalmente para todo software ejecutándose sobre un dispositivo, que permite la conexión entre dos diferentes entornos actuando como un traductor. Usualmente un gateway es necesario cuando un entorno, que utiliza un determinado protocolo, se comunica con otro que emplea un protocolo distinto.

Un gateway puede traducir paquetes IPX (Novell) en paquetes IP, aceptar correos que provienen de un tipo específico de servidor y formato, y entregarlos en formato compresible para otro tipo diferente de servidor o conectar enlaces de datos de distintas tecnologías, como Ethernet y Token Ring. Un gateway ejecuta tareas mucho más complejas que otros dispositivos de conexión como switches o routers, sin embargo muchas personas designan a un router como un gateway, cuando éste es utilizado para conectar dos tecnologías de enlace diferentes, tales como Ethernet a Frame Relay, Ethernet a MPLS, Ethernet a Token Ring, etc. Otro ejemplo lo constituye un gateway de voz sobre IP (VoIP), dispositivos utilizados para la digitalización de la voz a fin de poder transmitir la misma a través de redes digitales.

2.6.15 RAS

Remote Access Services (Servicios de Acceso Remoto) es un término utilizado para describir el proceso de conexión entres sistemas remotos, básicamente entre una estación de trabajo que utiliza la red telefónica pública por medio de un módem, a una red que utiliza un servidor RAS.

Un RAS típico es el ofrecido por Microsoft Windows, el cual facilita la comunicación entre computadoras situadas a grandes distancias. La conexión puede estar materializada por diferentes tecnologías, como ser PSTN, ISDN, DSL o Cablemodems. Dependiendo los protocolos que se utilicen en su implementación, dichas conexiones pueden ser en texto claro (sin seguridad) o protegidas mediante el empleo de algoritmos de encriptación.

2.6.16 PBX

Las compañías telefónicas emplean tecnologías de conmutación, para trasmitir los llamados telefónicos que realizan los abonados a sus correspondientes destinos. Una empresa telefónica posee switches que conectan localidades, ciudades y áreas metropolitanas, a través del uso de anillos de fibra óptica, por ejemplo.

Una Private Branch Exchange (PBX) es un switch telefónico privado que está situado dentro de la empresa y es propiedad de la misma. Permite conectar a sus usuarios por medio de líneas locales, facilitando las comunicaciones entre ellos sin tener que salir a la red pública y cursando el tráfico externo a través de enlaces troncales proporcionados por una prestataria externa.

Entre sus componentes más importantes, encontramos:

- El conmutador (switch) y sus elementos asociados
- Los equipos terminales (digitales o analógicos)
- El cableado interno y el distribuidor general de líneas
- Los sistemas de alimentación
- Los enlaces troncales a la red pública

Entre las facilidades típicas que brindan, podemos mencionar:

- Conectar terminales de datos
- Permitir la transmisión de datos a la Red Telefónica Pública (PSTN)
- Conectar líneas tanto digitales como analógicas
- Sistema de control de gastos
- Guía telefónica electrónica integrada
- Integración con servidores de fax
- Utilización de una red de teléfonos inalámbricos
- Conexión a redes de VoIP
- Servicios extendidos, como ser: identificación de llamada, llamada en espera, transferencia de llamadas, desvío, conferencia, marcado abreviado, rellamada, etc.

Muchos sistemas PBX tienen password de administración por defecto que nunca son cambiadas. En consecuencia, un Phreaker (Hacker telefónico) que tiene conocimiento de las passwords típicas de cada fabricante de sistemas operativos para PBX, puede hacer uso de ellas para producir enrutamiento de llamadas, reconfiguración de switches o ganar acceso para realizar gratuitamente llamadas locales e internacionales. De allí la importancia de cambiar siempre las passwords por defecto de estos dispositivos.

2.6.17 Firewall

Un Firewall constituye la primer línea de defensa de una red y es empleado para restringir el acceso a una red desde otra red. La mayoría de las compañías utilizan Firewalls para restringir el acceso a sus

redes desde Internet, aunque también pueden ser usados para restringir tráfico interno desde un segmento de red a otro.

El propósito de los Firewall es aislar una red de otra y están disponibles a través de implementaciones de software, como funcionalidad adicional en otro tipo de dispositivo (funciones de Firewall en un Router) o como hardware dedicado (appliance específico).

Un Firewall permite aplicar la política de seguridad de red de la compañía, inspeccionando el tráfico entrante y saliente a la misma, permitiendo sólo los servicios autorizados mediante el análisis de las direcciones IP de origen y destino, los puertos de origen y destino y otros parámetros de inspección como ser: números de secuencia, campos de control, comandos específicos, etc., según las capacidades del sistema operativo del Firewall, filtrando los paquetes que no cumplen con la política vigente.

La instalación de un Firewall en la topología de red de la empresa debe ser tal, que todo flujo de tráfico debe pasar sin excepción a través del mismo, a fin de poder implementar su política de inspección.

Un Firewall puede ser un sistema (software o hardware), es decir, un dispositivo físico (hard) que se conecta entre la red y el cable de la conexión a Internet, como en el caso del CISCO PIX 535, o bien un programa (soft) que se instala en el sistema que tiene el módem (u otro dispositivo) que conecta con Internet, como el Firewall-1 de CheckPoint. Incluso podemos encontrar PCs muy potentes y con softwares específicos que lo único que hacen es monitorear en tiempo real las comunicaciones entre redes.

Es posible configurar un Firewall de forma que permita sólo tráfico de correo, de modo de proteger de cualquier ataque sobre la red destino. Generalmente, están configurados para proteger contra "logins" sin autorización expresa desde cualquier parte del mundo. Esto, ayuda principalmente, a prevenir ataques en máquinas y software de nuestra red.

También, permiten bloquear el tráfico "desde Internet hacia la empresa", admitiendo que los usuarios del interior, se comuniquen libremente con los usuarios del exterior. Pueden protegernos de cualquier tipo de ataque a la red, siempre y cuando se configuren para ello. Esto proporciona un sistema simple para auditar la red.

Siempre que disponga de una red privada que vaya a conectarse a una red pública, se necesita la protección que este recurso ofrece. Incluso en el caso de los usuarios particulares que se conectan a Internet mediante un módem resulta recomendable, ya que permite estar protegido contra los ataques que se puedan sufrir, así como moverse por la red de forma anónima. De esta manera, los datos estarán a salvo y la privacidad quedará asegurada.

Beneficios e inconvenientes de un Firewall

Como claros beneficios, se pueden citar la seguridad frente a cierto nivel de ataques externos y la oportunidad de permitir acceder a determinados recursos de la red pública sólo a ciertas personas. De esta manera, el administrador sabe a qué elementos se accede y quién lo hace.

Tener uno de estos sistemas implica ciertas restricciones para los usuarios, que no suelen ser aceptadas con agrado. Además, puede constituir un cuello de botella en el acceso a ciertos recursos, debido a que todo el tráfico entre la red privada y la pública debe ser analizado y registrado por si se necesita un análisis posterior de estos datos.

También, hay que tener en cuenta que si falla ambas redes podrían quedar virtualmente aisladas con todos los inconvenientes que ello pueda acarrear. No obstante, las alternativas son la falta de seguridad o la incapacidad de acceso a las redes públicas, y ninguna de estas posibilidades resulta aceptable.

SI bien son cada vez más necesarios en nuestras redes, "todos los expertos recomiendan que no se usen en lugar de otras herramientas, sino junto a ellas"; cualquier firewalls, desde el más simple al

más avanzado, presenta dos consideraciones de seguridad:

Por un lado, centralizan todas las medidas en un único sistema, de forma que si éste se ve comprometido y el resto de nuestra red no está lo suficientemente protegido, el atacante consigue amenazar a toda la subred simplemente poniendo en jaque a una máquina.

El segundo punto, relacionado con éste, es la falsa sensación de seguridad que proporciona: generalmente un administrador que no disponga del mismo, comúnmente, va a preocuparse de la integridad de todas y cada una de sus máquinas, pero en el momento en que lo instala y lo configura asume que toda su red es segura, por lo que se suele descuidar enormemente la seguridad de los equipos de la red interna.

Esto, como acabamos de comentar, es un grave error, ya que en el momento que un pirata acceda al Firewall en cuestión (recordemos que es un sistema muy expuesto a ataques externos) automáticamente va a tener la posibilidad de controlar toda la red objeto del ataque.

Como veremos más adelante (y esto es algo de sentido común), evidentemente no protege contra ataques que no pasan por él: incluyendo todo tipo de ataques internos dentro del perímetro de seguridad, pero también otros factores que a priori no deberían suponer un problema. El típico ejemplo de estos últimos son los usuarios que instalan sin permiso, sin conocimiento del administrador de la red, y muchas veces sin pensar en sus consecuencias, un simple módem en sus PCs o estaciones de trabajo; esto tan habitual en muchas organizaciones, supone la violación y la ruptura total del perímetro de seguridad, ya que posibilita accesos a la red no controlados por el Firewall.

Otro problema de sentido común es la reconfiguración de los sistemas al pasarlos de una zona a otra con diferente nivel de seguridad, por ejemplo al mover un equipo que se encuentra en el área protegida a la DMZ (veremos más adelante lo que estas siglas significan); este acto [que en ocasiones no implica ni tan siquiera el movimiento físico del equipo, sino simplemente conectarlo en una toma de red diferente] puede ocasionar graves problemas de seguridad en nuestra organización, por lo que cada vez que un cambio de este estilo se produzca no sólo es necesaria la reconfiguración del sistema, sino la revisión de todas las políticas de seguridad aplicadas a esa máquina.

2.6.18 IDS

Un Intrusion Detection System (Sistema de Detección de Intrusos) cumple una función diferente a un Firewall, debido a que son diseñados para detectar anormalidades de seguridad, como ser el uso no autorizado o abuso de un recurso, o bien un intento de ataque sobre los mismos. Estos recursos pueden ser computadoras (servidores), redes o infraestructura de comunicaciones.

Un IDS está diseñado para ayudar a mitigar el daño que puede causar a los recursos un incidente de seguridad. Su función consiste en detectar tráfico sospechoso y reaccionar enviando alarmas o reconfigurando dispositivos con el objeto de finalizar conexiones.

Las herramientas generales de IDS pueden implementarse, al igual que los Firewalls, sobre dispositivos dedicados (appliance) o mediante software. Aunque existen diferentes tipos de productos, la mayoría tienen en común tres componentes:

- Sensores • Analizadores
- Interface de administración

Los sensores se encargan de recolectar el tráfico y los datos propios de la actividad de los usuarios, enviando esta información al analizador. Éste controla el tráfico recolectado en busca de actividades sospechosas. Si detecta una actividad programada como maliciosa, envía inmediatamente una alarma a la pantalla de la interface de administración, a fin de alertar en forma oportuna al administrador de seguridad, sobre la ejecución de un posible ataque.

2.6.19 Comparación del modelo IEEE con el modelo OSI

El Instituto de Ingeniería Eléctrica y Electrónica (IEEE) es una organización profesional que define estándares de red. Los estándares IEEE 802.3 y 802.5, son los estándares de LAN más conocidos y predominantes del mundo actual. Los estándares IEEE abarcan sólo las dos capas inferiores del modelo OSI. A diferencia del modelo OSI, los estándares IEEE dividen la capa de enlaces de datos en dos subcapas , llamadas subcapa MAC (Medium Access Control - Control de Acceso al Medio) y subcapa LLC (Logical Link Control - Control de enlace Lógico) .

La IEEE define con un estándar la subcapa LLC, denominado IEEE 802.2. La subcapa MAC comparte la definición del estándar con la capa física, así nos encontramos con los estándares IEEE 802.3, 802.11 que definen, además de un método de acceso, los medios y conectores que se deberán utilizar para interconectar los dispositivos

802.1x es un estándar del IEEE que está diseñado para proporcionar acceso a una red. 802.1x realiza la autenticación de los clientes a nivel de puertos, utilizando la información contenida en las credenciales únicas de cada cliente.

El proceso de autenticación define tres roles :

- **Suplicante (Supplicant)**: Consiste en el extremo que solicita acceso a la red. Un suplicante puede ser tanto un usuario final como un dispositivo.
- **Autenticador (Authenticator):** Es el dispositivo al cual el suplicante está directamente conectado y a través del cual obtiene el permiso para acceder a la red. Actúa como un gateway del servidor de autenticación.
- **Servidor de Autenticación (Authentication Server)** Es el responsable final de la autenticación del suplicante.

El proceso de autenticación basado en puertos, es soportado en dos topologías:

- ***Punto a punto***
- ***Wireless LAN***

Dicho proceso consiste en el intercambio de mensajes EAP (Extensible Authentication Protocol) utilizando también el protocolo RADIUS. Este intercambio ocurre entre el suplicante y el servidor de autenticación. El autenticador se desempeña como un relay transparente para este intercambio y consiste en el punto de aplicación de las instrucciones de seguridad que el servidor de autenticación le envía como resultado del proceso de autenticación.

Entre los tipos más utilizados de EAP encontramos:

- ***Cisco LEAP***
- ***EAP-TLS***
- ***PEAP***
- ***EAP-MD5***

Al implementarse sobre un switch ocurre lo siguiente: El cliente, una estación de trabajo por ejemplo, le solicita acceso al dispositivo de conmutación, es decir, al Switch, quien reenvía al servidor de autenticación (RADIUS) dicha solicitud actuando como un proxy, bloqueando mientras tanto el acceso a la red por parte del cliente. Este servidor de autenticación valida la identidad del cliente y notifica al Switch si el cliente está autorizado o no para acceder a la LAN

Una alternativa de seguridad para wireless LAN usando este estándar, consiste en proporcionar autenticación centralizada y distribución dinámica de claves. Este enfoque del 802.11 utiliza 802.1x e EAP para lograr esta funcionalidad, la cual comprende:

- Autenticación mutua entre el cliente y el servidor de autenticación (RADIUS)
- Claves de encriptación que son derivadas dinámicamente luego de la autenticación
- Control centralizado de políticas, donde al expirar el tiempo de sesión se inicia un proceso de reautenticación y una nueva generación de las claves de encriptación.

Al implementarse, un cliente wireless que se asocia al access point no puede obtener acceso a la red hasta que el usuario ejecuta el proceso de logon. Al hacerlo, se intercambian mensajes EAP entre el cliente y el servidor de autenticación (RADIUS) para realizar una autenticación mutua, donde el cliente verifica las credenciales del servidor y viceversa. Un suplicante EAP es usado en el dispositivo del cliente para obtener sus credenciales. Luego de realizarse con éxito la autenticación mutua, se obtiene una clave que va a ser empleada por el cliente durante su sesión. La password del cliente y la clave de sesión nunca es transmitida en texto claro a través del enlace.

2.6.20 Conectividad del Host

La función de una NIC es conectar un dispositivo host al medio de red. Una NIC es una placa de circuito impreso que se coloca en la ranura de expansión de un bus de la motherboard o dispositivo periférico de un computador. La NIC también se conoce como adaptador de red. En los computadores portátiles o de mano, una NIC tiene el tamaño de una tarjeta de crédito. Las NIC se consideran dispositivos Capa 2 porque cada NIC lleva un identificador exclusivo codificado, denominado dirección MAC. Esta dirección se utiliza para controlar la comunicación de datos para el host de la red. Posteriormente se suministrarán más detalles acerca de la dirección MAC. Tal como su nombre lo indica, la tarjeta de interfaz de red controla el acceso del host al medio.

En algunos casos, el tipo de conector de la NIC no concuerda con el tipo de medios con los que debe conectarse. Un buen ejemplo de ello es el router Cisco 2500. En el router, se ve un conector AUI. Ese conector AUI necesita conectarse a un cable Ethernet UTP Categoría 5 Para hacer esto, se usa un transmisor/receptor, también conocido como transceptor. El transceptor convierte un tipo de señal o conector en otro. Por ejemplo, un transceptor puede conectar una interfaz AUI de 15 pins a un jack RJ-45. Se considera un dispositivo de Capa 1, dado que sólo analiza los bits y ninguna otra información acerca de la dirección o de protocolos de niveles más altos. Las NIC no se representan con ningún símbolo estandarizado. Se entiende que siempre que haya dispositivos de networking conectados a un medio de red, existe alguna clase de NIC o un dispositivo similar a la NIC. Siempre que se ve un punto en un mapa topológico, éste representa una interfaz NIC o puerto que actúa como una NIC.

2.6.21 Comunicación de par a par

Al usar tecnologías LAN y WAN, muchos computadores se interconectan para brindar servicios a sus usuarios. Para lograrlo, los computadores en red toman diferentes roles o funciones entre si. Algunos tipos de aplicaciones requieren que los computadores funcionen como socios en partes iguales. Otro tipo de aplicaciones distribuyen sus tareas de modo que las funciones de un computador sirvan a una cantidad de otros de manera desigual. En cualquiera de los casos, dos computadores por lo general se comunican entre si usando protocolos petición/respuesta. Un computador realiza una petición de servicio, y el segundo computador lo recibe y responde. El que realiza la petición asume el papel de cliente, y el que responde el de servidor.

En una red de par a par, los computadores en red actúan como socios en partes iguales, o pares.

Como pares, cada computador puede tomar la función de cliente o de servidor. En algún momento, el computador A pedirá un archivo al computador B, el cual responderá entregándole el archivo al computador A. El computador A funciona como cliente, mientras que el B funciona como servidor. Más tarde, los computadores A y B cambiarán de papel. En una red de par a par, los usuarios individuales controlan sus propios recursos. Los usuarios pueden decidir compartir ciertos archivos con otros usuarios. Es posible que los usuarios requieran una contraseña antes de permitir que otros tengan accesos a sus recursos. Ya que son los usuarios individuales los que toman estas decisiones, no hay un punto central de control o administración en la red. Además, en caso de fallas, los usuarios individuales deben tener una copia de seguridad de sus sistemas para poder recuperar los datos si estos se pierden. Cuando un computador actúa como servidor, es posible que el usuario de ese equipo note que el rendimiento es menor, ya que el equipo cumple las peticiones realizadas por otros sistemas.

Las redes de par a par son relativamente fáciles de instalar y operar. No se necesita más equipo que un sistema operativo adecuado en cada computador. Como los usuarios controlan sus propios recursos, no se necesitan administradores dedicados. A medida que la red crece, las relaciones de par a par se hacen cada vez más difíciles de coordinar. Una red de par a par funciona bien con 10 computadores o menos. Ya que las redes de par a par no se adaptan bien a mayores tamaños, su eficiencia disminuye a medida que el número de computadores en la red aumenta. Además, los usuarios individuales controlan el acceso a los recursos de sus computadores, lo que implica que la seguridad se hace difícil de mantener. El modelo cliente/servidor de networking se puede usar para superar las limitaciones de la red de par a par.

2.6.22 Modelo Cliente/Servidor

En una disposición cliente/servidor, los servicios de red se ubican en un computador dedicado denominado servidor. El servidor responde a las peticiones de los clientes. El servidor es un computador central que se encuentra disponible de forma continua para responder a las peticiones de los clientes, ya sea de un archivo, impresión, aplicación u otros servicios. La mayoría de los sistemas operativos adoptan la forma de relación cliente/servidor. En general, los computadores de escritorio funcionan como clientes y uno o más computadores con potencia de procesamiento adicional, memoria y software especializado funcionan como servidores.

Los servidores están diseñados para cumplir con las peticiones de muchos clientes a la vez. Antes de que un cliente pueda acceder a los recursos del servidor, se debe identificar y obtener la autorización para usar el recurso. Esto se hace asignando a cada cliente un nombre de cuenta y una contraseña que un servicio de autenticación verifica. El servicio de autenticación actúa como guardián para proteger el acceso a la red. Con la centralización de las cuentas de los usuarios, de la seguridad, y del control de acceso, las redes basadas en servidores simplifican la administración de grandes redes. La concentración de recursos de red como archivos, impresoras y aplicaciones en servidores hace que sea más fácil hacer una copia de seguridad de los datos generados y de mantenerlos. En vez de estar repartidos en equipos individuales, los recursos pueden encontrarse en servidores dedicados y especializados para facilitar el acceso. La mayoría de los sistemas cliente/servidor también incluyen recursos para mejorar la red al agregar servicios que extienden la utilidad de la misma. La distribución de las funciones en las redes cliente/servidor ofrece grandes ventajas, pero también lleva aparejado algunos costos. Aunque la agregación de recursos en los sistemas de servidor trae mayor seguridad, acceso más sencillo y control coordinado, el servidor introduce un punto único de falla a la red. Sin el servidor operacional, la red no puede funcionar en absoluto. Los servidores requieren de personal entrenado y capacitado para su administración y mantenimiento. Esto aumenta los costos de hacer funcionar la red. Los sistemas de servidor también necesitan hardware adicional y especializado que hace que el costo aumente.

2.6.23 Control de enlace lógico (LLC)

Dado que la subcapa MAC es una capa que varía de acuerdo al tipo tecnología de acceso que se esté utilizando (802.3, 802.4, 802.11, etc.), y dado que existen diferentes pilas de protocolos de capa 3 y superiores (TCP/IP, IPX/SPX, AppleTalk, etc.), debe existir un punto en común para que se puedan comunicar. La IEEE creó la subcapa de control enlace lógico para permitir que la capa de enlace de datos sea independiente de las capas de red y física. Esta capa proporciona una interfase estándar hacia los protocolos de capa de red que están sobre ella, mientras que se comunica de forma efectiva con las diversas tecnologías que están por debajo (las diferentes subcapas MAC).

2.6.24 Control de acceso al medio (MAC)

La subcapa MAC es una capa que depende del medio físico que se utilizará para realizar la comunicación. Existen diversos estándares normalizados por la IEEE. La subcapa MAC es la encargada de ordenar la forma en que los hosts accederán al medio para poder transferir información. Como el medio físico es compartido por todos los hosts, se debe definir algún sistema de control para asegurarse que dos estaciones no transmitan simultáneamente, o, en caso de que esto suceda, sea detectado y se retransmitan los datos alterados.

Existen dos tipos de protocolos Control de Acceso al Medio:

- No determinísticos: Acceso de tipo "Primero en Llegar, Primero en Transmitir" (FCFS o First Come, First Served)
- Determinísticos: Las estaciones se turnan para transmitir.

Un ejemplo de protocolo no determinístico es CSMA/CD (Carrier Sense Multiple Access with Collision Detection o acceso múltiple con detección de portadora y detección de colisiones), utilizado como método de acceso en el estándar 802.3. En CSMA/CD, cuando una estación quiere transmitir, escucha en el medio. Si el medio está ocupado, la estación espera hasta que se desocupa; sino, transmite de inmediato. Si dos o más estaciones comienzan a transmitir simultáneamente por un medio desocupado, las tramas se superponen en el medio y la señal resultante se altera, esto se conoce como colisión. Todas las estaciones involucradas en la colisión abortan su transmisión, esperan un tiempo aleatorio y repiten de nuevo todo el proceso.

Por otro lado, Token Ring y FDDI, son ejemplos de protocolos determinísticos. En una red Token Ring, los hosts se organizan en forma de anillo y una trama especial llamada "token" viaja de estación a estación. Sólo la estación que tiene en su posesión el token es la estación que puede transmitir. Como sólo existe un token, sólo una estación puede transmitir a la vez y de esta forma se evitan las colisiones.

2.6.25 Direcciones MAC

Para posibilitar la correcta distribución de tramas en las redes LAN, debe existir un sistema que permita identificar a cada estación. Este sistema de identificación se conoce como "direccionamiento MAC" y la forma de identificar cada estación es asignarle una dirección, conocida como "dirección MAC". El formato de estas direcciones se define en la capa de enlace de datos, más precisamente en la subcapa MAC. Las direcciones MAC tienen 48 bits de largo y se expresan como doce dígitos hexadecimales . Los primeros 6 dígitos hexadecimales se conocen como OUI (Organizational Unique Identifier - Identificador Único de Organización) e identifican al fabricante de la interfaz. La IEEE se encarga de administrar la asignación de OUI entre los fabricantes. Los restantes 6 dígitos son asignados por el fabricante, cuidando que no se repitan.

Existen dos bits que definen el “tipo” de la dirección:

- El bit 47 es conocido como Individual/Global (I/G): si se encuentra en 1 significa que la trama es un broadcast, si está en 0 la trama es un unicast.
- El bit 46 es conocido como Universal/Local (U/L): si se encuentra en 1 significa que la dirección se encuentra administrada localmente, por ejemplo, si la dirección MAC se encuentra configurada por software sobreescribiendo la dirección grabada en la NIC.

Las direcciones MAC se encuentran grabadas en las interfaces de red y no pueden ser modificadas, por este motivo, también se las conoce como "direcciones físicas". Cuando una estación quiere enviar datos hacia otra estación, debe incluir la dirección de destino en el encabezado de la trama. Todas las estaciones de la red LAN recibirán esta trama, pero sólo la estación que reconoce la dirección de destino como propia será la que procese la trama. Una estación de trabajo podría configurar su NIC para copiar localmente todas las tramas que son recibidas. Esta técnica es conocida como “modo promiscuo” y puede utilizarse para leer todo el tráfico de una red. Más adelante veremos los problemas de seguridad pueden surgir en caso que algún usuario malicioso utilice esta técnica.

Desactivación de filtro MAC: Una de las técnicas más utilizadas por la mayoría de los *sniffers* de redes Ethernet se basa en la posibilidad de configurar la interfaz de red para que desactive su filtro MAC (poniendo la tarjeta de red en modo promiscuo).

Las redes basadas en dispositivos Ethernet fueron concebidas en torno a una idea principal: todas las máquinas de una misma red local comparten el mismo medio, de manera que todos los equipos son capaces de ver el tráfico de la red de forma global.

Cuando se envían datos es necesario especificar claramente a quién van dirigidos, indicando la dirección MAC. De los 48 bits que componen la dirección MAC, los 24 primeros bits identifican al fabricante del hardware, y los 24 bits restantes corresponden al número de serie asignado por el fabricante. Esto garantiza que dos tarjetas no puedan tener la misma dirección MAC.

Para evitar que cualquier máquina se pueda apropiar de información fraudulenta, las tarjetas Ethernet incorporan un filtro que ignora todo el tráfico que no les pertenece, descartando aquellos paquetes con una dirección MAC que no coincide con la suya. La desactivación de este filtro se conoce con el nombre de modo promiscuo.

Con el uso adecuado de expresiones regulares y otros filtros de texto, se podrá visualizar o almacenar únicamente la información que más interese; en especial, aquella información sensible, como nombres de usuario y contraseñas.

El entorno en el que suele ser más efectivo este tipo de escuchas son las redes de área local configuradas con una topología en bus. En este tipo de redes, todos los equipos están conectado a un mismo cable. Esto implica que todo el tráfico transmitido y recibido por los equipos de la red pasa por este medio común.

Una solución para evitar esta técnica consiste en la segmentación de la red y de los equipos mediante el uso de conmutadores (switches). Al segmentar la red y los equipos, el único tráfico que tendrían que ver las máquinas sería el que les pertenece, puesto que el conmutador se encarga de encaminar hacia el equipo únicamente aquellos paquetes destinados a su dirección MAC. Aun así, existen técnicas para poder continuar realizando *sniffing* aunque se haya segmentado la red mediante switches. Una de estas técnicas es la *suplantación de ARP*.

2.7 ETHERNET

El primer estándar Ethernet fue publicado en la década del 80 por Digital, Intel y Xerox (DIX), evolucionando hasta convertirse en la actualidad en la tecnología LAN de mayor difusión. Como

referencia pensemos que la mayoría del tráfico de Internet comienza y termina en una red Ethernet. La versión original brindaba un ancho de banda de 10 Mbps sobre cable coaxil grueso (Thick Ethernet, 10BASE5) y permitía comunicar estaciones hasta una distancia de 500 mts. Utilizaba el protocolo CSMA/CD para ordenar el acceso al medio y resolver las colisiones.

Ethernet se fue adaptando de acuerdo a las nuevas necesidades y tecnologías. Así es como hoy podemos contar con redes ethernet de hasta 10Gbps de ancho de banda, transmitiendo sobre distintos tipos de cobre y fibra óptica.

Tipo	Medio	Ancho de Banda máximo	Longitud de de segmento máxima	Topología Física	Topología Lógica
10BASE2	Coaxial fino	10 Mbps	200 m	Bus	Bus
10BASE5	Coaxial grueso	10 Mbps	500 m	Bus	Bus
10BASE-T	UTP CAT 5	10 Mbps	100 m	Estrella E. Extendida	Bus
10BASE-FL	Fibra óptica multimodo	10 Mbps	2000 m	Estrella	Bus
100BASE-TX	UTP CAT 5	100 Mbps	100 m	Estrella	Bus
100BASE-FX	Fibra óptica multimodo	100 Mbps	2000 m	Estrella	Bus
1000BASE-T	UTP CAT 5	1000 Mbps	100 m	Estrella	Bus
1000BASELX	Fibra óptica Onda Larga	1000 Mbps	550 m	Estrella	Bus
1000BASESX	Fibra óptica Onda Corta	1000 Mbps	220 m	Estrella	Bus
1000BASECX	Coaxil de 150 ohms	1000 Mbps	25 m	Estrella	Bus

En la tabla puede observar un resumen de las características principales de las diferentes versiones.

2.7.1 Colisiones

En las redes ethernet todas las estaciones comparten el mismo medio para la transferencia de datos, es decir que comparten el mismo cable físico. Por este motivo, si dos estaciones comienzan a transmitir de forma simultánea, las señales eléctricas que se propagan por el cable colisionarán, produciéndose una pérdida de la información en tránsito .

El área de la red donde las transmisiones pueden colisionar, se denomina "dominio de colisión". Un dominio de colisión incluye todos los medios y dispositivos que conforman el área (estaciones de trabajo, repetidores, hubs, transceptores, medios físicos, etc.).

2.7.2 CSMA/CD

El método de acceso al medio de las redes Ethernet se denomina CSMA/CD por sus siglas en inglés (*Carrier Sense, Multiple Access with Collission Detection* - Acceso Múltiple con Detección de portadora y Detección de Colisiones).

Esté método define la forma en que las estaciones deben transmitir los datos por el medio físico

compartido. Cuando una estación quiere transmitir una trama, lo primero que realiza es un sensado del medio para asegurarse que no exista otra estación transmitiendo. Si el medio está ocupado, espera un tiempo y vuelve a sensarlo. Si el medio está libre, comienza a transmitir y simultáneamente continúa escuchando el medio para asegurarse que su transmisión no colisione con la transmisión de otra estación. Si finaliza la transmisión sin detectar colisión, significa que la trama se ha enviado de forma exitosa. Si durante la transmisión detectó una colisión, envía una señal de "jamming" para asegurarse que todas las demás estaciones detecten la colisión y descarten la trama que estaban recibiendo. Una vez enviada la señal de jamming, la estación deja de transmitir y elige en forma aleatoria el intervalo de tiempo que deberá esperar antes de intentar la retransmisión.

Si en la retransmisión vuelve a ocurrir una colisión se repite el proceso; pero antes, se incrementa la cantidad de posibles intervalos de tiempo entre los que la estación tendrá la posibilidad de elegir, de esta manera las posibilidades que tendrán dos estaciones de coincidir en el mismo intervalo se reducen. Este ciclo se repite 15 veces, si en la 15° retransmisión ocurre una colisión, se descarta la trama y se reportan problemas en el acceso a la red.

Se ha visto que, aun cuando CSMA reduce la posibilidad de colisiones, éstas todavía se producen. Dos o más estaciones transmitiendo tramas que colisionan originan un desperdicio de la capacidad (ancho de banda) disponible, pues la información en el medio físico no es válida durante todo el tiempo que dura la transmisión de dichas tramas.

El inconveniente en CSMA es que cuando se produce una colisión entre tramas, el medio queda ocupado durante todo el tiempo que dura la transmisión de la trama. Parece obvio que sería adecuado cortar lo antes posible la transmisión con el fin de dejar libre el canal lo antes posible para iniciar un nuevo intento.

Dotando a las estaciones de la capacidad de detectar en tiempo real que sus transmisiones se superponen (colisionan) con otras, aquellas podrían interrumpir su transmisión cuando eso sucediera, ahorrando tiempo de “mal uso” del medio. El mecanismo de detección de colisiones (CD), por tanto, reduce la duración de las colisiones en caso de que éstas se produzcan.

La realización del mecanismo CD depende de las características del medio físico de transmisión, de la técnica de codificación/modulación empleada e incluso de la topología de la red y de las variaciones en los niveles de señal en cada punto de la red de las transmisiones procedentes de cualquier estación. La detección de colisiones es, por tanto, una tarea de la capa física aunque ésta no toma decisiones y simplemente notifica de la ocurrencia de colisión a la subcapa MAC, que es la que ejecuta el algoritmo de acceso CSMA/CD.

En algunos contextos, el mecanismo CD no está exento de problemas; por ejemplo, en las redes vía radio la atenuación de las señales es muy grande (como mínimo, aumenta con el cuadrado de la distancia), por lo que, a veces, puede ser muy difícil detectar que una transmisión con un nivel de señal fuerte se superpone con otra cuyo nivel es varios ordenes de magnitud más débil. (Este es el llamado *captura* o *enmascaramiento*.)

2.7.3 Ethernet versus 802.x

En Febrero de 1980, en el seno del IEEE (Institute of Electrical and Electronic Engineers), se constituye el comité 802, al mando de Marius Graube (de Tektronic), con el fin de promover el desarrollo de estándares para redes de área local. Así, la serie de estándares IEEE 802.x (donde x es un número de 1 en adelante) ha venido definiendo los niveles arquitectónicos inferiores (capa física y de enlace de datos según el modelo OSI) para redes locales. En este ámbito, la organización ISO (International Standards Organization) también emite sus estándares, totalmente equivalentes a los anteriores, bajo la denominación ISO 8802-x.

La lista de estándares IEEE 802 ha ido creciendo con el tiempo, tanto por la incorporación de nuevos estándares como por la revisión/ampliación de los ya existentes (que se representan mediante IEEE 802.xy, donde x es el número que denota el estándar e y es una letra, de la “a” en adelante, que denota la ampliación/revisión llevada a cabo). Los principales estándares IEEE de la serie 802 son los

siguientes:

- ***802.1***: Describe el marco general de la serie de estándares, así como aspectos de gestión de red e interconexión entre redes a nivel MAC.
- ***802.2***: Describe el LLC (Logical Link Control), subcapa superior de la capa de enlace de datos OSI, común a todas las redes locales.
- ***802.3***: Describe una familia de redes locales basadas en el protocolo de acceso aleatorio de tipo CSMA/CD. Inicialmente describía una red local con topología en bus, de cable coaxial, y velocidad de 10 Mbit/s (la conocida Ethernet, propuesta por Xerox, Digital e Intel en la década de 1970); las numerosas revisiones posteriores introducen topologías en estrella, de cable de pares trenzados o fibra óptica, y velocidades de 100 Mbit/s y 1 Gbit/s.
- ***802.4***: Describe Token Bus, una red con topología en bus y protocolo de acceso basado en pase de testigo (a partir de una propuesta de red de General Motors para entornos de producción); actualmente en desuso.
- ***802.5***: Describe Token Ring, una red con topología en anillo, velocidades de 4 y 16 Mbit/s y protocolo de acceso basado en pase de testigo (a partir de una propuesta de IBM hacia 1980); si bien a finales del siglo pasado llegó a tener una implantación del orden del 10-15% de las instalaciones de redes locales, actualmente está en desuso.
- **802.6**: Describe DQDB (Dual Queue Dual Bus), una red de área metropolitana con topología de doble bus, velocidades de decenas de Mbits/s y sofisticado protocolo de acceso basado en una cola distribuida; si bien en la década de 1990 tuvo cierta implantación, su futuro es incierto.
- **802.7**: Describe recomendaciones para la realización de redes locales en medios de transmisión de banda ancha (broadband).
- **802.8**: Describe recomendaciones para la realización de redes locales en medios de fibra óptica.
- **802.9**: Describe recomendaciones para la integración de voz y datos en redes LAN.
- **802.10**: Describe procedimientos de seguridad (cifrado en niveles arquitectónicos inferiores) para redes locales.
- **802.11**: Describe a las WLAN (Wireless LAN), redes locales sin hilos basadas en la transmisión por microondas o infrarrojos y protocolo de acceso aleatorio.
- **802.12** Describe la red 100 VG-AnyLAN, una red con topología en árbol, velocidad de 100 Mbit/s y protocolo de acceso por demanda (propuesta por Hewlett-Packard y otros); actualmente en desuso.

El estándar IEEE 802.2 (LLC): El estándar IEEE 802.2 (o ISO 8802-2) describe la subcapa superior de la capa de enlace de datos, siendo sus características principales:

- Utilizando los servicios ofrecidos por la subcapa MAC (Medium Access Control), proporciona servicios a la capa de red.
- Proporciona capacidad de direccionamiento interno (a nivel de sistema) mediante los L-SAP y control de errores y de flujo (opcionalmente).
- Su protocolo interno (o de subcapa) está basado en la familia de protocolos de enlace HDLC.
- Independiza las capas superiores de las particularidades de cada LAN.

El estándar IEEE 802.3 (Ethernet): Los antecedentes de este estándar se sitúan hacia el año 1974

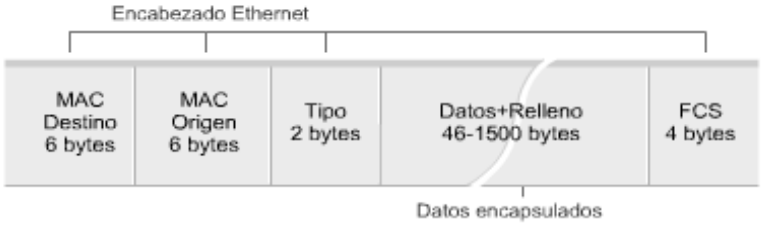
en el centro de investigaciones de Xerox Corporation en Palo Alto (California, USA). Allí, los ingenieros David R. Boggs y Robert M. Metcalfe, entre otros, diseñaron una red basada en el protocolo CSMA/CD, operando a 2,94 Mbit/s, que conectaba 100 estaciones de trabajo a lo largo de un bus de 1 km de longitud. Poco después, la alianza entre las compañías Digital, Intel y Xerox propone una norma industrial para conectividad local, a la que llamaron Ethernet, operando a 10 Mbit/s.

La norma IEEE 802.3 difiere ligeramente de la norma de facto Ethernet y, además, describe a toda una familia de redes basadas en el protocolo CSMA/CD. La especificación original de Ethernet, definía las capas física y de enlace de datos del modelo OSI. Como esta especificación no era un estándar abierto, la organización IEEE definió un estándar llamado IEEE 802.3.

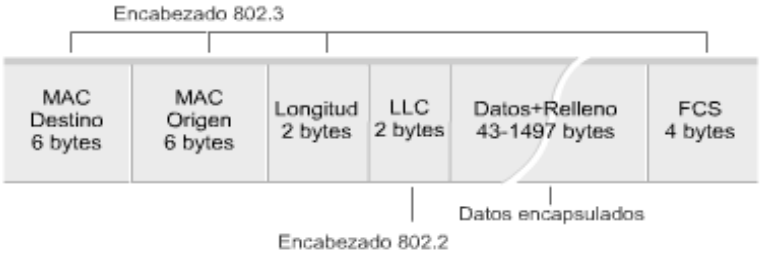
Este estándar no es compatible con la especificación de Ethernet, porque no define completamente la capa de enlace de datos, sino que la divide en dos subcapas, como ya se mencionó, las subcapas MAC y LLC. El estándar IEEE 802.3 cubre la capa física y la subcapa MAC, mientras que otro estándar, el IEEE 802.2, define la subcapa LLC.

Hoy en día, el término Ethernet a menudo se usa para referirse a todas las LAN de acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD). Es muy común que en una misma red se utilicen de forma simultánea las dos especificaciones.

Formato de trama Ethernet



Formato de trama IEEE



En el gráfico se pueden observar las diferencias en el formato de trama que utilizan. En la trama IEEE se detalla el encabezado propio de 802.3 más el encabezado que corresponde a la subcapa LLC - 802.2. Las tramas Ethernet incluyen un campo "tipo" donde se especifica el tipo de protocolo que transporta encapsulado. Cada protocolo tiene asignado un número, por ejemplo IP tiene asignado el número 0x0800. En las tramas IEEE 802.3, esta identificación no es necesaria porque siempre transportan el mismo protocolo, el IEEE 802.2, y éste es el encargado de identificar el protocolo encapsulado (mediante campos del encabezado 802.2). Las tramas IEEE incluyen un campo de longitud (Length) que contiene el tamaño de los datos encapsulados (802.2 más datos).

2.7.4 Fragmentación en Redes Ethernet

La MTU (*Maxim Transfer Unit*) por defecto de un datagrama IP para una red de tipo Ethernet es de 1500 bytes. Así pues, si un datagrama IP es mayor a este tamaño y necesita circular por este tipo de red, será necesario fragmentarlo por medio del encaminador que dirige la red. Los fragmentos pueden

incluso fragmentarse m ás si pasan por una red con una MTU más pequeña que su tamaño.

Para que el equipo de destino pueda reconstruir los fragmentos, estos deben contener la siguiente información:

- Cada fragmento tiene que estar asociado a otro utilizando un identificador de fragmento común.
- Este se clonará desde un campo de la cabecera IP, conocido como identificador IP (también llamado ID de fragmento).
- Información sobre su posición en el paquete inicial (paquete no fragmentado).
- Información sobre la longitud de los datos transportados al fragmento.
- Cada fragmento tiene que saber si existen más fragmentos a continuación. Esto se indica en la cabecera, dejando o no activado el indicador de más fragmentos (more fragments, MF) del datagrama IP.

Toda esta información irá en la cabecera IP, colocada en el datagrama IP. Esto afectará a todo el tráfico TCP/IP puesto que IP es el protocolo responsable de la entrega de los paquetes.

2.7.5 Otras tecnologías LAN

La tecnología LAN más utilizada es Ethernet, pero existen otras tecnologías LAN con menor difusión como Token Ring y FDDI. Veamos algunos detalles de estas tecnologías:

Token Ring: Esta tecnología fue creada por IBM en los años setenta y luego fue estandarizada por la IEEE bajo el nombre de 802.5. Define una red donde todos los hosts conforman un anillo. El método de acceso al medio se denomina "token passing", porque se utiliza una trama de datos especial, llamada token, para determinar qué estación transmite. Como sólo existe una trama de token, sólo una estación podrá transmitir simultáneamente y no se producirán colisiones . El medio físico es par trenzado y puede trabajar a 4 Mbps o a 16 Mbps. En se pueden observar los formatos de una trama de token y una trama de datos.

FDDI: Esta tecnología define un anillo doble de fibra óptica y un ancho de banda de 100Mbps. El método de acceso al medio es similar a Token Ring, utiliza un token para definir qué estación se encuentra habilitada para transmitir. Es una red muy robusta dado el tipo de medio empleado (fibra óptica) y porque contempla recuperación ante fallas en el enlace físico. Si ocurre una falla en un anillo, se utiliza el segundo. En se pueden observar los formatos de una trama de token y una trama de datos. Ambas tecnologías, así como Ethernet y sus derivados, son tecnologías de difusión, esto significa que cuando una estación transmite una trama, esta trama es recibida por todas las demás estaciones. Cada estación que recibe la trama, lee el campo de dirección destino, si no corresponde a su dirección MAC, entonces descarta la trama, pero si se identifica como el destino, entonces termina de recibir la trama y procede a interpretarla.

2.8 FRAME RELAY

Frame Relay es una propuesta de ANSI de 1990, planteada como una evolución del servicio de X.25, que incorpora las mejoras tecnológicas disponibles, para sustituir a las tecnologías de ese momento. Frame Relay pretende sintetizar una tecnología articulada sobre mecanismos simples. Por este motivo, Frame Relay potencia los aspectos destinados a alcanzar esta simplicidad, entre los cuales destacan la desaparición de los elementos de gestión de la transmisión de los datos, la señalización fuera de banda y la supresión de los controles de error en los nodos intermedios.

De esta forma, Frame Relay se perfila como una tecnología que con una menor potencia en los equipos consigue mejorar la velocidad de transmisión de datos y el funcionamiento general de la red al simplificar los aspectos de gestión.

Entre las motivaciones que llevaron al desarrollo de esta tecnología, pueden distinguirse las causas funcionales y a las de implementación.

Frame Relay es una tecnología de red cuya simplicidad afecta a dos aspectos de control fundamentales, que en otras redes como X.25 son muy importantes para su correcto funcionamiento: En primer lugar, no hay controles de flujo, por lo que si se produce congestión en la red, el tráfico entrante puede perderse por simple desbordamiento de colas. En segundo lugar, no hay control de errores en los nodos de la red, gracias a que el medio físico proporciona una probabilidad de error de símbolo baja.

El servicio ofrecido es orientado a conexión. Durante la fase de conexión, se establece la ruta del circuito virtual y se señaliza a la red con el fin de garantizar parámetros de calidad al usuario (caudal y retardo). La conmutación se caracteriza por operar en modo conmutación rápida de mensajes. Este procedimiento trata de encaminar la información tan pronto la trama de datos entra al conmutador.

Frame Relay no prevé mecanismos de prioridad para los paquetes de información, de tal modo que todos ellos reciben el mismo trato por parte de la red. Sin embargo, esta afirmación deberá ser matizada más adelante puesto que aunque efectivamente la red no proporciona herramientas explícitas de prioridad, sí es cierto que existe una forma práctica que permite definir dos niveles de calidad, basados en el campo DE de la trama.

2.9 PROTOCOLO IP

El Protocolo Internet (IP) es la implementación más utilizada de los protocolos de capa de red. IP es el protocolo de red que usa Internet. En esta capa, los datos se encapsulan en paquetes (también denominados datagramas). El protocolo IP define el formato del encabezado del paquete, que incluye información de direccionamiento y otra información de control, pero no se ocupa de los datos en sí, es decir, acepta cualquier información que recibe desde las capas superiores.

2.9.1 Fragmentación IP

El protocolo IP es el encargado de seleccionar la trayectoria que deben seguir los datagramas IP. No es un protocolo fiable ni orientado a conexión, es decir, no garantiza el control de flujo, la recuperación de errores ni que los datos lleguen a su destino.

A la hora de pasar a la capa inferior, los datagramas IP se encapsulan en tramas que, dependiendo de la red física utilizada, tienen una longitud determinada. Cuando los datagramas IP viajan de unos equipos a otros, pueden pasar por distintos tipos de redes. El tamaño exacto de estos paquetes, denominado MTU (*Maxim Transfer Unit.*), puede variar de una red a otra dependiendo del medio físico empleado para su transmisión.

Así, el protocolo IP debe tener en cuenta que ningún dispositivo puede transmitir paquetes de una longitud superior al MTU establecido por la red por la que hay que pasar. A causa de este problema, es necesaria la reconversión de datagramas IP al formato adecuado.

La fragmentación divide los datagramas IP en fragmentos de menor longitud y se realiza en el nivel inferior de la arquitectura para que sea posible recomponer los datagramas IP de forma transparente en el resto de niveles. El reensamblado realiza la operación contraria.

El proceso de fragmentación y reensamblado se irá repitiendo a medida que los datagramas vayan viajando por diferentes redes.

Aunque la fragmentación es, por lo general, una consecuencia natural del tráfico que viaja a través de

redes con MTU de distintos tamaños, es posible que un atacante pueda realizar un mal uso de esta propiedad del protocolo IP para provocar ataques de denegación de servicio (a causa de una mala implementación de la pila TCP/IP), así como para esconder y facilitar la fase de recogida de información (búsqueda de huellas identificativas, exploración de puertos, ...) o incluso para hacer pasar desapercibidos e introducir en la red paquetes para la explotación de servicios. Esto último es posible porque muchos de los mecanismos de prevención y de detección no implementan el reensamblado de paquetes, y por ello no detectarán ni prevendrán este tipo de actividad a causa del enmascaramiento que la fragmentación les ofrece.

Así pues, es importante comprender cómo funciona esta faceta del protocolo IP para entender este mal uso del tráfico fragmentado que podría realizar un posible atacante para conseguir su objetivo.

2.9.2 Fragmentación para enmascaramiento de datagramas IP

Como ya hemos introducido al principio de esta sección, la fragmentación IP puede plantear una serie de problemáticas relacionadas con la seguridad de nuestra red. Una de las problemáticas más destacadas es la utilización de fragmentación IP malintencionada para burlar las técnicas básicas de inspección de datagramas IP.

En este caso, un atacante tratará de provocar intencionadamente una fragmentación en los datagramas que envía a nuestra red con el objetivo de que pasen desapercibidos por diferentes dispositivos de prevención y de detección de ataques que no tienen implementado el proceso de fragmentación y reensamblado de datagramas IP.

En el caso de los dispositivos de prevención más básicos (como, por ejemplo, encaminadores con filtrado de paquetes), las decisiones para bloquear paquetes se basan generalmente en la información de cabecera de los paquetes (como, por ejemplo, puertos TCP o UDP de destino, banderas de TCP). Esto significa que los paquetes TCP y UDP fragmentados son susceptibles de burlar aquellos mecanismos de prevención que no implementen el proceso de reensamblado para poder tener una visión global del paquete que hay que bloquear.

Por otro lado, en el caso de dispositivos de prevención más avanzados (como, por ejemplo, pasarelas a nivel de aplicación), así como en la mayor parte de los mecanismos de detección, las decisiones para detectar paquetes potencialmente peligrosos acostumbran a basarse nuevamente en la inspección de la cabecera del datagrama IP, así como en la parte de datos del paquete. Esto significa que la fragmentación se puede utilizar nuevamente para burlar este proceso de detección y conseguir que estos paquetes entren o salgan de la red de forma desapercibida.

Con el objetivo de descubrir la MTU de la red e intentar asi realizar fragmentación, el atacante puede utilizar el indicador de no fragmentación del datagrama IP. Cuando el indicador de no fragmentación está activado, como indica su nombre, no se realizará ninguna fragmentación en el datagrama. Por lo tanto, si un datagrama con este indicador cruza una red en la que se exija la fragmentación, el encaminador lo descubrirá, descartará el datagrama y devolverá el mensaje de error al equipo emisor. Este mensaje de error ICMP contiene la MTU de la red que requiere la fragmentación. De esta forma, el atacante solo deberá construir datagramas con diferentes longitudes, con el indicador de fragmentación establecido, a la espera de recibir estos mensajes de error.

Para solucionar el uso de la fragmentación fraudulenta y garantizar una correcta inspección de paquetes, es necesaria la implementación del proceso de fragmentación y el reensamblado de datagramas en dispositivos de prevención y detección. Esta solución puede suponer un coste adicional, ya que significa tener que examinar y almacenar cada fragmento. Aunque puede resultar muy costoso en cuanto a recursos (tiempo, proceso y memoria), será la única forma de asegurar que la inspección del paquete se ha realizado de forma correcta.

2.9.3 ¿Orientado o no orientado a la conexión?

Los sistemas orientados a conexión (como el sistema telefónico actual), establecen una conexión entre emisor y receptor antes de que se transfieran los datos entre ambos. Esa conexión que se establece mantiene activa durante toda la transferencia de datos y hasta que una de las partes decida finalizarla.

La mayoría de los servicios de red usan un sistema de entrega no orientado a conexión. Estos servicios no establecen una conexión entre el origen y el destino y la mantienen durante la transferencia, en su lugar, toman una a una cada unidad de datos a transferir (paquetes de datos, o simplemente paquetes) y determinan en forma separada como enviarlos a través de la red. Así, los paquetes pueden tomar distintas rutas en su camino hacia el destino . Una analogía para un sistema de entrega no orientado a conexión es el sistema postal. No se hace contacto con el destinatario antes de que la carta se envíe, la misma se encamina hacia su destino y el destinatario se entera de su existencia cuando la recibe.

2.9.4 Direccionamiento de capa de red

El direccionamiento IP representa la dirección lógica de un host y se utiliza para identificarlo. Cada dirección IP está formada por 32 bits, o cuatro bytes, pero normalmente se expresan en notación decimal punteada, la cual muestra un número decimal con cada byte separado por un punto, por ejemplo 192.132.234.102. Cada byte es nombrado con frecuencia como un octeto, así una dirección IP consiste de cuatro octetos, que pueden tomar valores entre 0 y 255. Las direcciones IP se pueden asignar a cada host en forma manual, por el administrador de la red, o automática por el sistema.

Las direcciones IP se componen principalmente por dos partes:

- Una porción de red: Identifica al grupo de hosts que comparten la misma red.
- Una porción de host: Identifica al host dentro de su grupo o red.

Los dispositivos en la misma red lógica deben tener la misma dirección de red, pero cada uno debe tener una dirección de host diferente . Esta agrupación de direcciones en grupos de hosts o redes hace que el direccionamiento de red tenga una estructura jerárquica, a diferencia del direccionamiento de capa 2 cuya estructura es plana.

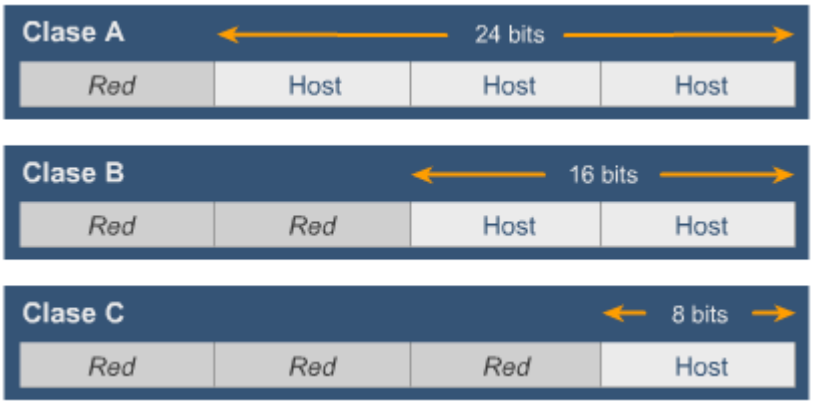
Una analogía al sistema de direccionamiento pueden ser los números telefónicos, donde una parte (el prefijo) identifica el país o la región y otra parte identifica el número particular. El prefijo es idéntico para todos los números particulares del mismo país o región, pero cada teléfono particular tiene un número único asociado.

2.9.5 Clases

Como se ha visto, las direcciones de red se dividen en una porción asignada a la red y otra al host. Con el fin de facilitar la administración y optimizar el uso de direcciones, los diseñadores del direccionamiento determinaron la existencia de cinco clases de direcciones IP.

Clase A: La dirección Clase A se diseñó para admitir redes de tamaño extremadamente grande, de más de 16 millones de direcciones de host disponibles. Las direcciones IP Clase A utilizan sólo el primer octeto para indicar la dirección de la red. Los tres octetos restantes son para las direcciones host. Utiliza el primer octeto para direccionar redes y los tres restantes para direccionar los hosts dentro de la red. El primer bit del primer octeto siempre es 0, entonces las direcciones de red de clase

A tienen un rango de 0 a 127, pero las direcciones 0 y 127 están reservadas para fines especiales. Así, podemos tener hasta 126 redes clase A y en cada una de estas redes más de 16 millones de hosts. La red 127.0.0.0 se reserva para las pruebas de loopback. Los Routers o las máquinas locales pueden utilizar esta dirección para enviar paquetes nuevamente hacia ellos mismos. Por lo tanto, no se puede asignar este número a una red.



Clase B: La dirección Clase B se diseñó para cumplir las necesidades de redes de tamaño moderado a grande. Una dirección IP Clase B utiliza los primeros dos de los cuatro octetos para indicar la dirección de la red. Los dos octetos restantes especifican las direcciones del host. Emplea dos octetos para la porción de red y los otros dos para la porción del host. Los primeros dos bits de la dirección de red han sido ajustados a 1 y 0, de esta manera la dirección de red tiene un rango desde 128 a 191. Con este formato, cada red podrá tener más de 65 mil hosts.

Clase C: Utiliza tres octetos para la porción de red y los hosts de la red. Los tres primeros bits son ajustados a 1, 1 y 0 respectivamente. Esto significa que la dirección de red para una red de clase C varía desde 192 a 223. A cada una de estas redes se les pueden asignar hasta 254 hosts.

El espacio de direccionamiento Clase C es el que se utiliza más frecuentemente en las clases de direcciones originales. Este espacio de direccionamiento tiene el propósito de admitir redes pequeñas con un máximo de 254 hosts. Una dirección Clase C comienza con el binario 110. Por lo tanto, el menor número que puede representarsees 11000000, 192 decimal. El número más alto que puede representarse es 11011111, 223 decimal. Si una dirección contiene un número entre 192 y 223 en el primer octeto, es una dirección de Clase C.

Clase D y E: Estas clases de dirección están reservadas para multicast (envío de información desde un origen hacia varios destinos) y fines investigativos. No son utilizadas comercialmente para la asignación de direcciones a los hosts.

La dirección Clase D se creó para permitir multicast en una dirección IP. Una dirección multicast es una dirección exclusiva de red que dirige los paquetes con esa dirección destino hacia grupos predefinidos de direcciones IP. Por lo tanto, una sola estación puede transmitir de forma simultánea una sola corriente de datos a múltiples receptores. El espacio de direccionamiento Clase D, en forma similar a otros espacios de direccionamiento, se encuentra limitado matemáticamente. Los primeros cuatro bits de una dirección Clase D deben ser 1110. Por lo tanto, el primer rango de octeto para las direcciones Clase D es 11100000 a 11101111, o 224 a 239. Una dirección IP que comienza con un valor entre 224 y 239 en el primer octeto es una dirección Clase D. Se ha definido una dirección Clase E. Sin embargo, la Fuerza de tareas de ingeniería de Internet (IETF) ha reservado estas direcciones para su propia investigación. Por lo tanto, no se han emitido direcciones Clase E para ser utilizadas en Internet. Los primeros cuatro bits de una dirección Clase E siempre son 1s. Por lo tanto, el rango del primer octeto para las direcciones Clase E es 11110000 a 11111111, o 240 a 255.

Clase	intervalo de direcciones internas RFC 1918
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

2.9.6 Direcciones reservadas y privadas

En una dirección IP, nunca se asigna un campo de hosts igual a 0 a un host individual. En vez de esto, una dirección IP con un campo de hosts de 0 se utiliza para referirse a la red en sí misma. Por ejemplo, 11.0.0.0.

El direccionamiento IP incluye, además, una dirección de difusión o broadcast que se refiere a todos los hosts de la red. Por regla, una dirección de difusión tiene todos los bits del campo de hosts asignados como 1 (recordemos que el equivalente en decimal, de 8 bits 1 es 255). Por ejemplo, la dirección 11.255.255.255, permitiría alcanzar todos los hosts de la red 11.0.0.0. La dirección IP 255.255.255.255, se denomina comúnmente broadcast de red local, y la utilizan los procesos para alcanzar todos los hosts de la red local. Los routers normalmente no reenviarán estos paquetes.

La dirección de red 127.0.0.0, tampoco se puede utilizar para direccionamiento, porque se reserva para loopback; y está diseñada para utilizarse en las pruebas de funcionamiento del TCP/IP y para la comunicación de los procesos internos de la máquina local. Cuando algún programa utiliza la dirección de loopback como destino, el software de protocolo regresa los datos sin generar tráfico a través de la red.

Por otro lado, encontramos que hay ciertas direcciones en cada clase de dirección IP que no están asignadas. Estas direcciones se denominan direcciones privadas. Comúnmente se utilizan para direccionamiento en redes que no se conectan a Internet o en una red en la que no hay suficientes direcciones públicas disponibles. Debemos tener en cuenta que si deseamos conectar nuestra red con Internet, estas direcciones deben ser traducidas a direcciones públicas, porque cualquier tráfico que posea una dirección destino dentro de uno de los intervalos de direcciones privadas NO se enrutará a través de Internet .

2.9.7 División en Subredes

A veces resulta muy conveniente por razones de flexibilidad, costos y administración dividir las redes IP, especialmente las más grandes, en redes más pequeñas. Estas divisiones más pequeñas se denominan subredes.

Las subredes se forman al tomar bits prestados de la porción de hosts de la dirección. Esto tiene el efecto de aumentar el número de redes disponibles, pero reduce el número de anfitriones que pueden direccionarse en cada red. Cuando utilizamos direccionamiento con subredes, debemos tener en cuenta que estamos definiendo un campo adicional en la dirección IP (formado por los bits que pedimos prestados), además de los campos de red y host.

La cantidad mínima de bits que se puede pedir prestada para direccionar subredes es 2. Si pidiera prestado sólo 1 bit para crear una subred, sólo dispondría de los bits 0 y 1 para la primer y segunda subred, pero dijimos que el 0 se utiliza para referenciar a la subred y el 1 para referenciar a todas las subredes de la red. La cantidad máxima de bits que se puede pedir prestada será aquella que resulte, luego de reservar 2 bits para el campo de host.

La división en subredes es otro método para administrar las direcciones IP. Este método, que consiste en dividir las clases de direcciones de red completas en partes de menor tamaño, ha evitado el

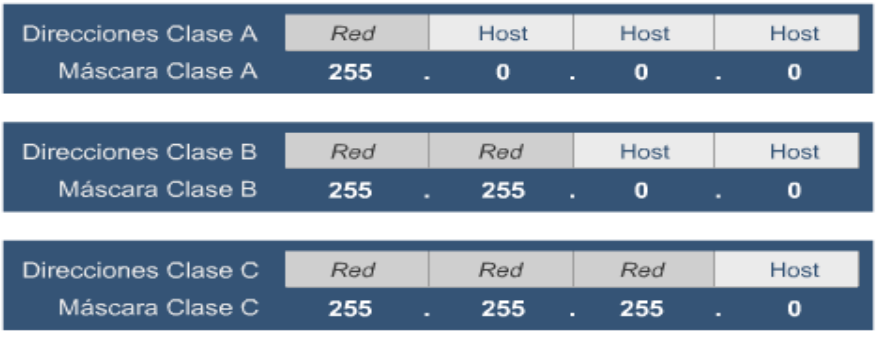
completo agotamiento de las direcciones IP. Resulta imposible hablar sobre el TCP/IP sin mencionar la división en subredes. Como administrador de sistemas, es importante comprender que la división en subredes constituye un medio para dividir e identificar las redes individuales en toda la LAN. No siempre es necesario subdividir una red pequeña. Sin embargo, en el caso de redes grandes a muy grandes, la división en subredes es necesario. Dividir una red en subredes significa utilizar una máscara de subred para dividir la red y convertir una gran red en segmentos más pequeños, más eficientes y administrables o subredes.

El administrador del sistema debe resolver estos problemas al agregar y expandir la red. Es importante saber cuántas subredes o redes son necesarias y cuántos hosts se requerirán en cada red. Con la división en subredes, la red no está limitada a las máscaras de red por defecto Clase A, B o C y se da una mayor flexibilidad en el diseño de la red. Las direcciones de subredes incluyen la porción de red más el campo de subred y el campo de host. El campo de subred y el campo de host se crean a partir de la porción de host original de la red entera. La capacidad para decidir cómo se divide la porción de host original en los nuevos campos de subred y de host ofrece flexibilidad en el direccionamiento al administrador de red. Para crear una dirección de subred, un administrador de red pide prestados bits del campo de host y los designa como campo de subred. El número mínimo de bits que se puede pedir es dos. Al crear una subred, donde se solicita un sólo bit, el número de la red suele ser red .0. El número de broadcast entonces sería la red .255. El número máximo de bits que se puede pedir prestado puede ser cualquier número que deje por lo menos 2 bits restantes para el número de host.

Notación decimal para el primer octeto de host	Número de subredes	Número de Hosts de clase A por subred	Número de Hosts de clase B por subred	Número de Hosts de clase C por subred
.192	2	4,194,302	16,382	62
.224	6	2,097,150	8,190	30
.240	14	1,048,574	4,094	14
.248	30	524,286	2,046	6
.252	62	262,142	1,022	2
.254	126	131,070	510	-
.255	254	65,534	254	-

2.9.8 Máscara de subred

Una máscara de subred tiene una longitud de 32 bits, dividida en 4 octetos, al igual que la dirección IP. Se utiliza para determinar qué parte de la dirección IP corresponde al campo de red y qué parte corresponde al campo de host



Una máscara de subred tiene una longitud de 32 bits, dividida en 4 octetos, al igual que la dirección IP. Se utiliza para determinar qué parte de la dirección IP corresponde al campo de red y qué parte

corresponde al campo de host.

La subred se interpreta mediante la máscara de red o subred. Si el bit de la máscara de red es 1, ese bit equivalente en la dirección IP se interpreta como un bit de red. Si el bit de la mascara es 0, al bit equivalente de la dirección IP se le considera parte de la dirección de host. De esta forma, un método para determinar la máscara de subred para una dirección IP particular, podría ser el siguiente:

1. Expresar la dirección IP en forma binaria.
2. Cambiar la porción de red y subred de la dirección por todos unos.
3. Cambiar la porción del host de la dirección por todos ceros.
4. Convertir la expresión en números binarios nuevamente a la notación decimal punteada.

2.9.9 Problemas en la resolución de direcciones

Uno de los principales problemas del networking es cómo comunicarse con los otros dispositivos de la red. En la comunicación TCP/IP, el datagrama de una red de área local debe contener tanto una dirección MAC destino como una dirección IP destino. Estas direcciones deben ser correctas y concordar con las direcciones IP y MAC destino del dispositivo host. Si no concuerdan, el host destino descartará el datagrama. La comunicación dentro de un segmento de LAN requiere de dos direcciones. Debe haber una forma de mapear las direcciones IP a MAC de forma automática. Se necesitaría demasiado tiempo si el usuario creara los mapas de forma manual. El conjunto TCP/IP cuenta con un protocolo, llamado Protocolo de resolución de direcciones (ARP), que puede obtener las direcciones MAC, de forma automática, para la transmisión local. Pueden surgir diferentes problemas cuando se manda información fuera de la LAN.

Las comunicaciones entre dos segmentos de LAN tienen una tarea extra. Tanto las direcciones IP como las MAC son necesarias para el dispositivo de enrutamiento intermedio y el host destino. TCP/IP tiene una variante en ARP llamada ARP proxy que proporciona la dirección MAC de un dispositivo intermedio para realizar la transmisión a otro segmento de la red fuera de la LAN.

2.9.10 Formato y descripción del datagrama

Dentro del datagrama, algunos de los campos más importantes son:

- VERS: Indica la versión del protocolo IP que se utilizó para crear el datagrama, permite diferenciar los formatos de encabezado.
- HLEN: Indica la longitud del encabezado medido en palabras de 32 bits (por Ej. Un encabezado de 20 octetos tendrá un HLEN = 5)
- Service Type: Indica la prioridad que le ha sido asignado al datagrama por un protocolo de capa superior, de acuerdo al tipo de servicio. IPv4 posee 8 niveles de servicio, de 0 (prioridad normal) a 7 (control de red).
- Total Lenght: Proporciona la longitud del paquete medido en octetos (bytes), incluyendo los bytes del encabezado y los datos. Se puede calcular la longitud de los datos, restando a la longitud total la longitud de la cabecera.
- Identification: Contiene un entero único que permite identificar el paquete.
- Flags: Controlan la fragmentación. El primer bit indica si se puede fragmentar. El último bit indica si hay más fragmentos.
- Fragment Offset: Especifica el desplazamiento en el paquete original de los datos que se están acarreando en el fragmento, medido en bytes, comenzando en 0.

- Time to live: Mantiene un contador que decrece hasta cero, momento en el cual el dispositivo donde se encuentra lo descarta (comúnmente un ruteador). Permite evitar los loops.
- Protocolo: Especifica qué protocolo de alto nivel se utilizó para crear el mensaje que se está transportando en el campo Datos. Por ejemplo TCP.
- Header checksum: Asegura la integridad de los valores del encabezado.
- Source IP Address (Destination IP Address): Contiene las direcciones IP del emisor y del receptor del paquete. Estos campos se mantienen fijos en la ruta desde el origen al destino.
- IP Options: Campo de longitud variable. Las opciones pueden incluir pruebas de red o depuración.
- Padding: Depende del campo Opciones. Se agregan ceros adicionales para garantizar que la longitud del encabezado IP sea un múltiplo de 32 bits.
- Data: Contiene la información de capa superior.

2.9.11 Asignación de direcciones IP

Las direcciones IP identifican a los hosts en una red IP. Por este motivo, todos los hosts que necesiten acceder y ser accedidos en una red necesitan de una dirección IP. La asignación de las direcciones IP a los hosts puede ser establecida básicamente de dos maneras:

- De forma manual, cuando la asigna el usuario o el administrador de la red
- De forma automática, a través de algún protocolo de configuración automática de hosts

La asignación manual de direcciones IP permite implementar redes pequeñas sin la necesidad de utilizar un servidor de asignación de direcciones IP, pero se debe tener la precaución de mantener una documentación detallada y una administración de red consistente con el fin de no utilizar números IP repetidos, ni realizar asignaciones inconsistentes.

Por otro lado, la utilización de un sistema automático de asignación de direcciones IP hace que una red sea más fácilmente administrable por lo que resulta el método más apropiado para redes medianas a grandes. Existen varios protocolos de asignación de direcciones IP:

- RARP: El protocolo de resolución de dirección inversa (RARP) relaciona las direcciones físicas de las NIC (direcciones MAC) con las direcciones IP. Esta relación de MAC a IP está almacenada en un servidor que se encarga de contestar las solicitudes RARP a las estaciones que desconocen su IP.
- BOOTP: El protocolo BOOTstrap trabaja de una forma muy similar al RARP, utiliza un servidor y relaciona de forma estática las MAC a los IP. A diferencia del anterior que sólo le asignaba una dirección IP al cliente, BOOTP permite asignarle no sólo una dirección IP, sino también la dirección IP del gateway y del servidor.
- DHCP: El protocolo de configuración dinámica del host (DHCP) se ha propuesto como sucesor del BOOTP. A diferencia del BOOTP, DHCP permite que un host obtenga una dirección IP de forma rápida y dinámica. Con DHCP, se puede obtener la configuración completa del computador en un solo mensaje (por ejemplo, junto con la dirección IP, el servidor también puede enviar la máscara de subred).

2.9.12 IPv4 en comparación con IPv6

Cuando se adoptó TCP/IP en los años 80, dependía de un esquema de direccionamiento de dos niveles. En ese entonces, esto ofrecía una escalabilidad adecuada. Desafortunadamente, los

diseñadores de TCP/IP no pudieron predecir que, con el tiempo, su protocolo sostendría una red global de información, comercio y entretenimiento. Hace más de viente años, la Versión 4 del IP (IPv4) ofrecía una estrategia de direccionamiento que, aunque resultó escalable durante algún tiempo, produjo una asignación poco eficiente de las direcciones. Las direcciones Clase A y B forman un 75 por ciento del espacio de direccionamiento IPv4, sin embargo, se pueden asignar menos de 17 000 organizaciones a un número de red Clase A o B. Las direcciones de red Clase C son mucho más numerosas que las direcciones Clase A y B aunque ellas representan sólo el 12,5 por ciento de los cuatro mil millones de direcciones IP posibles.

Lamentablemente, las direcciones Clase C están limitadas a 254 hosts utilizables. Esto no satisface las necesidades de organizaciones más importantes que no pueden adquirir una dirección Clase A o B. Aún si hubiera más direcciones Clase A, B y C, muchas direcciones de red harían que los Routers se detengan debido a la carga del enorme tamaño de las tablas de enrutamiento, necesarias para guardar las rutas de acceso a cada una de las redes. Ya en 1992, la Fuerza de tareas de ingeniería de Internet (IETF) identificó las dos dificultades siguientes:

- Agotamiento de las restantes direcciones de red IPv4 no asignadas. En ese entonces, el espacio de Clase B estaba a punto de agotarse.
- Se produjo un gran y rápido aumento en el tamaño de las tablas de enrutamiento de Internet a medida que las redes Clase C se conectaban en línea. La inundación resultante de nueva información en la red amenazaba la capacidad de los Routers de Internet para ejercer una efectiva administración.

Durante las últimas dos décadas, se desarrollaron numerosas extensiones al IPv4. Estas extensiones se diseñaron específicamente para mejorar la eficiencia con la cual es posible utilizar un espacio de direccionamiento de 32 bits. Dos de las más importantes son las máscaras de subred y el enrutamiento entre dominios sin clase (CIDR).

Mientras tanto, se ha definido y desarrollado una versión más extensible y escalable del IP, la Versión 6 del IP (IPv6). IPv6 utiliza 128 bits en lugar de los 32 bits que en la actualidad utiliza el IPv4. IPv6 utiliza números hexadecimales para representar los 128 bits. IPv6 proporciona 640 sextillones de direcciones. Esta versión del IP porporciona un número de direcciones suficientes para futuras necesidades de comunicación.

Después de diez años de planificación y desarrollo, el IPv6 lentamente comienza a implementarse en redes selectas. Con el tiempo, el IPv6 podrá reemplazar el IPv4 como el protocolo de Internet dominante.

2.9.13 Anatomía de un paquete IP

Los paquetes IP constan de los datos de las capas superiores más el encabezado IP. El encabezado IP está formado por lo siguiente:

- ***Versión***: Especifica el formato del encabezado de IP. Este campo de cuatro bits contiene el número 4 si el encabezado es IPv4 o el número 6 si el encabezado es IPV6. Sin embargo este campo no se usa para distinguir entre ambas versiones, para esto se usa el campo de tipo que se encuentra en el encabezado de la trama de capa 2.
- ***Longitud del encabezado IP (HLEN)***: Indica la longitud del encabezado del datagrama en palabras de 32 bits. Este número representa la longitud total de toda la información del encabezado, e incluye los dos campos de encabezados de longitud variable.
- ***Tipo de servicio (TOS)***: Especifica el nivel de importancia que le ha sido asignado por un protocolo de capa superior en particular, 8 bits.
- ***Longitud total***: Especifica la longitud total de todo el paquete en bytes, incluyendo los datos y

el encabezado, 16 bits. Para calcular la longitud de la carga de datos reste HLEN a la longitud total.

- ***Identificación***: Contiene un número entero que identifica el datagrama actual, 16 bits. Este es el número de secuencia.
- ***Señaladores***: Un campo de tres bits en el que los dos bits de menor peso controlan la fragmentación. Un bit especifica si el paquete puede fragmentarse, y el otro especifica si el paquete es el último fragmento en una serie de paquetes fragmentados.
- ***Desplazamiento de fragmentos***: usado para ensamblar los fragmentos de datagramas, 13 bits. Este campo permite que el campo anterior termine en un límite de 16 bits.
- ***Tiempo de existencia (TTL)***: campo que especifica el número de saltos que un paquete puede recorrer. Este número disminuye por uno cuando el paquete pasa por un Router. Cuando el contador llega a cero el paquete se elimina. Esto evita que los paquetes entren en un loop (bucle) interminable.
- ***Protocolo***: indica cuál es el protocolo de capa superior, por ejemplo, TCP o UDP, que recibe el paquete entrante luego de que se ha completado el procesamiento IP, ocho bits.
- ***Checksum del encabezado***: ayuda a garantizar la integridad del encabezado IP, 16 bits.
- ***Dirección de origen***: especifica la dirección IP del nodo emisor, 32 bits.
- ***Dirección de destino***: especifica la dirección IP del nodo receptor, 32 bits.
- ***Opciones***: permite que IP admita varias opciones, como seguridad, longitud variable.
- ***Relleno***: se agregan ceros adicionales a este campo para garantizar que el encabezado IP siempre sea un múltiplo de 32 bits
- ***Datos***: contiene información de capa superior, longitud variable hasta un de máximo 64 Kb.

2.9.14 Protocolos de enrutamiento IP

La función de enrutamiento es una función de la Capa 3 del modelo OSI. El enrutamiento es un esquema de organización jerárquico que permite que se agrupen direcciones individuales. Estas direcciones individuales son tratadas como unidades únicas hasta que se necesita la dirección destino para la entrega final de los datos. El enrutamiento es el proceso de hallar la ruta más eficiente desde un dispositivo a otro. El dispositivo primario que realiza el proceso de enrutamiento es el Router.

Las siguientes son las dos funciones principales de un Router:

- Los Routers deben mantener tablas de enrutamiento y asegurarse de que otros Routers conozcan las modificaciones a la topología de la red. Esta función se lleva a cabo utilizando un protocolo de enrutamiento para comunicar la información de la red a otros Routers.
- Cuando los paquetes llegan a una interfaz, el Router debe utilizar la tabla de enrutamiento para establecer el destino. El Router envía los paquetes a la interfaz apropiada, agrega la información de entramado necesaria para esa interfaz, y luego transmite la trama.

Un Router es un dispositivo de la capa de red que usa una o más métricas de enrutamiento para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red. Las métricas de enrutamiento son valores que se utilizan para determinar las ventajas de una ruta sobre otra. Los protocolos de enrutamiento utilizan varias combinaciones de métricas para determinar la mejor ruta para los datos. Los Routers interconectan segmentos de red o redes enteras. Pasan tramas de datos entre redes basándose en la información de Capa 3. Los Routers toman decisiones lógicas con respecto a cuál es la mejor ruta para la entrega de datos. Luego dirigen los paquetes al puerto de

salida adecuado para que sean encapsulado para la transmisión. Los pasos del proceso de encapsulamiento y desencapsulamiento ocurren cada vez que un paquete atraviesa un router. El router debe desencapsular la trama de capa 2 y examinar la dirección de capa 3. El proceso completo del envío de datos de un dispositivo a otro comprende encapsulamiento y desencapsulamiento de las siete capas OSI. Este proceso divide el flujo de datos en segmentos, agrega los encabezados apropiados e información final y luego transmite los datos. El proceso de desencapsulamiento es el proceso inverso: quita los encabezados e información final, y luego combina los datos en un flujo continuo.

La determinación de la ruta ocurre a nivel de la capa de red. La determinación de la ruta permite que un Router compare la dirección destino con las rutas disponibles en la tabla de enrutamiento, y seleccione la mejor ruta. Los Routers conocen las rutas disponibles por medio del enrutamiento estático o dinámico. Las rutas configuradas de forma manual por el administrador de la red son las rutas estáticas. Las rutas aprendidas por medio de otros Routers usando un protocolo de enrutamiento son las rutas dinámicas. El Router utiliza la determinación de la ruta para decidir por cuál puerto debe enviar un paquete en su trayecto al destino. Este proceso se conoce como enrutamiento del paquete. Cada Router que un paquete encuentra a lo largo del trayecto se conoce como salto. El número de saltos es la distancia cubierta. La determinación de la ruta puede compararse a una persona que conduce un automóvil desde un lugar de la ciudad a otro. El conductor tiene un mapa que muestra las calles que puede tomar para llegar a su destino, así como el Router posee una tabla de enrutamiento. El conductor viaja desde una intersección a otra al igual que un paquete va de un Router a otro en cada salto. En cualquier intersección el conductor determinar su ruta al ir hacia la izquierda, la derecha, o avanzar derecho. Del mismo modo, un Router decide por cuál puerto de salida debe enviarse un paquete.

Las decisiones del conductor se ven influenciadas por múltiples factores como el tráfico en la calle, el límite de velocidad, el número de carriles, si hay peaje o no, y si esa ruta se encuentra cerrada o no con frecuencia. A veces es más rápido tomar un recorrido más largo por una calle más angosta y menos transitada que ir por una autopista con mucho tránsito. De la misma forma, los Routers pueden tomar decisiones basándose en la carga, el ancho de banda, el retardo, el costo y la confiabilidad en los enlaces de red. Se utiliza el siguiente proceso durante la determinación de la ruta para cada paquete que se enruta:

- El router compara la dirección IP del paquete recibido contra las tablas que tiene.
- Se obtiene la dirección destino del paquete .
- Se aplica la máscara de la primera entrada en la tabla de enrutamiento a la dirección destino.
- Se compara el destino enmascarado y la entrada de la tabla de enrutamiento.
- Si hay concordancia, el paquete se envía al puerto que está asociado con la entrada de la tabla.
- Si no hay concordancia, se compara con la siguiente entrada de la tabla.
- Si el paquete no concuerda con ninguno de las entradas de la tabla, el Router verifica si se envió una ruta por defecto.
- Si se envió una ruta por defecto, el paquete se envía al puerto asociado. Una ruta por defecto es aquella que está configurada por el administrador de la red como la ruta que debe usarse si no existe concordancia con las entradas de la tabla de enrutamiento.
- El paquete se elimina si no hay una ruta por defecto. Por lo general se envía un mensaje al dispositivo emisor que indica que no se alcanzó el destino.

2.9.15 El enrutamiento en comparación con la conmutación

A menudo, se compara el enrutamiento con la conmutación. Un observador inexperto puede pensar

que el enrutamiento y la conmutación cumplen la misma función. La diferencia básica es que la conmutación tiene lugar en la Capa 2, o sea, la capa de enlace de los datos, en el modelo OSI y el enrutamiento en la Capa 3. Esta diferencia significa que el enrutamiento y la conmutación usan información diferente en el proceso de desplazar los datos desde el origen al destino.

La relación entre la conmutación y el enrutamiento es comparable con la relación entre las comunicaciones telefónicas locales y de larga distancia. Cuando se realiza una comunicación telefónica a un número dentro de un mismo código de área, un Switch local administra la llamada. Sin embargo, el Switch local sólo puede llevar registro de sus propios números locales. El Switch local no puede administrar todos los números telefónicos del mundo. Cuando el Switch recibe un pedido de llamada fuera de su código de área, transfiere la llamada a un Switch de nivel superior que reconoce los códigos de área. El Switch de nivel superior entonces transfiere la llamada de modo que finalmente llegue al Switch local del código de área marcado. El Router tiene una función parecida a la del Switch de nivel superior en el ejemplo del teléfono. La figura muestra las tablas ARP de las direcciones MAC de Capa 2 y las tablas de enrutamiento de las direcciones IP de Capa 3. Cada interfaz de computador y de Router mantiene una tabla ARP para comunicaciones de Capa 2. La tabla ARP funciona sólo para el dominio de broadcast al cual está conectada.. El Router también mantiene una tabla de enrutamiento que le permite enrutar los datos fuera del dominio de broadcast. Cada componente de la tabla ARP contiene un par de direcciones IP-MAC (en el gráfico las direcciones MAC están representadas por la sigla MAC, debido a que las direcciones verdaderas son demasiado largas y no caben en el gráfico). Las tablas de enrutamiento también registran cómo se informó la ruta (en este caso ya sea directamente conectada [C] o informada por RIP [R]), la dirección IP de red de las redes alcanzables, el número de saltos o distancia hasta dichas redes, y la interfaz por la que los datos deben enviarse para llegar a la red de destino.

2.9.16 Enrutado en comparación con enrutamiento

Los protocolos usados en la capa de red que transfieren datos de un Host a otro a través de un Router se denominan protocolos enrutados o enrutables. Los protocolos enrutados transportan datos a través de la red. Los protocolos de enrutamiento permiten que los Routers elijan la mejor ruta posible para los datos desde el origen hasta el destino.

Las funciones de un protocolo enrutado incluyen lo siguiente:

- Incluir cualquier conjunto de protocolos de red que ofrece información suficiente en su dirección de capa para permitir que un Router lo envíe al dispositivo siguiente y finalmente a su destino.
- Definir el formato y uso de los campos dentro de un paquete. El Protocolo Internet (IP) y el intercambio de paquetes de internetworking (IPX) de Novell son ejemplos de protocolos enrutados. Otros ejemplos son DECnet, AppleTalk, Banyan VINES y Xerox Network Systems (XNS).

Los Routers utilizan los protocolos de enrutamiento para intercambiar las tablas de enrutamiento y compartir la información de enrutamiento. En otras palabras, los protocolos de enrutamiento permiten enrutar protocolos enrutados.

Las funciones de un protocolo de enrutamiento incluyen lo siguiente:

- Ofrecer procesos para compartir la información de ruta
- Permitir que los Routers se comuniquen con otros Routers para actualizar y mantener las tablas de enrutamiento. Los ejemplos de protocolos de enrutamiento que admiten el protocolo enrutado IP incluyen el Protocolo de información de enrutamiento (RIP) y el Protocolo de enrutamiento de Gateway interior (IGRP), el Protocolo primero de la ruta libre más corta (OSPF), el Protocolo de Gateway fronterizo (BGP), el IGRP mejorado (EIGRP).

2.9.17 Protocolos enrutables y enrutados

Un protocolo es un conjunto de reglas que determina cómo se comunican los computadores entre sí a través de las redes. Los computadores se comunican intercambiando mensajes de datos. Para aceptar y actuar sobre estos mensajes, los computadores deben contar con definiciones de cómo interpretar el mensaje. Los ejemplos de mensajes incluyen aquellos que establecen una conexión a una máquina remota, mensajes de correo electrónico y archivos que se transmiten en la red. Un protocolo describe lo siguiente:

- El formato al cual el mensaje se debe conformar
- La manera en que los computadores intercambian un mensaje dentro del contexto de una actividad en particular

Un protocolo enrutado permite que un Router envíe datos entre nodos de diferentes redes. Para que un protocolo sea enrutable, debe admitir la capacidad de asignar a cada dispositivo individual un número de red y uno de Host. Algunos protocolos como los IPX, requieren sólo de un número de red porque estos protocolos utilizan la dirección MAC del Host como número de Host. Otros protocolos, como el IP, requieren una dirección completa que especifique la porción de red y la porción de Host. Estos protocolos también necesitan una máscara de red para diferenciar estos dos números. La dirección de red se obtiene al realizar la operación "AND" con la dirección y la máscara de red. La razón por la que se utiliza una máscara de red es para permitir que grupos de direcciones IP secuenciales sean considerados como una sola unidad. Si no se pudiera agrupar, cada Host tendría que mapearse de forma individual para realizar el enrutamiento.

El Protocolo Internet (IP) es la implementación más popular de un esquema de direccionamiento de red jerárquico. IP es un protocolo de entrega no orientado a la conexión, poco confiable y de máximo esfuerzo. El término no orientado a la conexión significa que no se establece ningún circuito de conexión dedicado antes de la transmisión, como sí lo hay cuando se establece una comunicación telefónica. IP determina la ruta más eficiente para los datos basándose en el protocolo de enrutamiento. Los términos poco confiables y de máximo esfuerzo no implican que el sistema no sea confiable y que no funcione bien; más bien significan que IP no verifica que los datos lleguen a su destino. La verificación de la entrega no siempre se lleva a cabo. A medida que la información fluye hacia abajo por las capas del modelo OSI, los datos se procesan en cada capa. En la capa de red, los datos se encapsulan en paquetes, también denominados datagramas. IP determina los contenidos de cada encabezado de paquete IP, lo cual incluye el direccionamiento y otra información de control, pero no se preocupa por la información en sí. IP acepta todos los datos que recibe de las capas superiores.

2.10 PROTOCOLO ARP

Uno de los principales problemas del networking es cómo comunicarse con los otros dispositivos de la red. En la comunicación TCP/IP, el datagrama de una red de área local debe contener tanto una dirección MAC destino como una dirección IP destino. Estas direcciones deben ser correctas y concordar con las direcciones IP y MAC destino del dispositivo host. Si no concuerdan, el host destino descartará el datagrama. La comunicación dentro de un segmento de LAN requiere de dos direcciones. Debe haber una forma de mapear las direcciones IP a MAC de forma automática. Se necesitaría demasiado tiempo si el usuario creara los mapas de forma manual. El cojunto TCP/IP cuenta con un protocolo, llamado Protocolo de resolución de direcciones (ARP), que puede obtener las direcciones MAC, de forma automática, para la transmisión local. Pueden surgir diferentes problemas cuando se manda información fuera de la LAN.

Para que TCP/IP pueda realizar la entrega de un paquete a un host, no es suficiente con conocer su dirección IP, además debe conocer la dirección física. De esta manera, la dirección MAC cumple la

función de identificar el destinatario próximo directo en el camino hacia el destinatario final, identificado por la dirección IP (que podría ser el mismo).

La función del protocolo de resolución de direcciones (Address Resolution Protocol - ARP) es garantizar que un host encuentre la dirección física de otro host ubicado en la misma red, conociendo su dirección IP . Para lograr su objetivo, el protocolo ARP utiliza dos tipos de tramas :

- *Una trama de petición ARP*. Esta trama permite solicitar la dirección MAC de un dispositivo, identificado por su dirección IP. Para asegurarse que todos los dispositivos de la red local procesen la petición ARP, el origen coloca como dirección física de destino la dirección de broadcast MAC (formada por F hexadecimales en todas las posiciones, es decir, FF-FF-FF-FF-FF-FF).
- *Una trama de respuesta ARP*. Esta trama es la respuesta a una petición ARP, y se utiliza para informar la dirección MAC solicitada. Se envía sólo al host que originó la petición ARP.

Por motivos de optimización, los hosts mantienen una tabla ARP local . Las tablas ARP son registros guardados en la memoria caché de cada host que contienen las asociaciones de direcciones MAC a direcciones IP, que el dispositivo aprende a través de las solicitudes ARP realizadas. Estos registros se mantienen en cada host por un período de tiempo determinado y luego se borran.

Las comunicaciones entre dos segmentos de LAN tienen una tarea extra. Tanto las direcciones IP como las MAC son necesarias para el dispositivo de enrutamiento intermedio y el host destino. TCP/IP tiene una variante en ARP llamada ARP proxy que proporciona la dirección MAC de un dispositivo intermedio para realizar la transmisión a otro segmento de la red fuera de la LAN.

2.10.1 Problemas con el envío de datos a nodos de diferentes

Como se ha visto anteriormente, las tramas de solicitudes ARP se envían con dirección MAC de destino Broadcast. Cuando una máquina envía una trama con dirección de destino broadcast, esa trama es procesada por todos los hosts de su red física.

Los routers no reenvían los paquetes broadcast por lo que una solicitud ARP no podría reenviarse de una red a otra. Para comunicarse entonces dos host de diferentes redes, existen dos alternativas:

- Configurar el router que conecta las redes con Proxy ARP
- Utilizar un gateway por defecto para el envío de los paquetes a redes diferentes

2.10.2 Gateway por defecto y ARP Proxy

Para que un host pueda enviar datos a otro host ubicado en una red o subred diferente, se le debe configurar un Gateway por defecto o el Router que conecta las dos redes debe estar configurado para operar como Proxy ARP.

Proxy ARP consiste en una variación del protocolo ARP. En esta variación, un Router analiza las solicitudes ARP y responde aquellas que consultan por direcciones MAC de hosts cuyas direcciones IP no pertenecen a la red local. El Router coloca en la respuesta ARP la dirección MAC de la interfaz por la cual recibió la solicitud .

El segundo método consiste en configurar el Gateway por defecto en los hosts de la red. El Gateway por defecto es un Router, y se identifica a través de su dirección IP, específicamente, la dirección IP de la interfaz que está conectada a la misma red. De esta forma, el host origen compara la dirección IP destino del paquete con la propia para determinar si las dos direcciones IP pertenecen a la misma red, si no es así, el host origen envía los datos al Router que actúa como Gateway. El Router recibe la trama, analiza la dirección IP destino del paquete, y encamina el paquete por la mejor ruta . En la

animación se puede observar como las direcciones MAC cambian conforme la trama avanza hacia diferentes redes, por otro lado, las direcciones IP se mantienen como en el origen.

El host origen obtiene la dirección MAC de la interfaz directamente conectada a su misma red, a través de una consulta ARP, con dirección IP del Gateway por defecto. Si el host no tiene configurado un Gateway por defecto o el Router no está trabajando como Proxy ARP, el tráfico generado en una red no podrá pasar a otra subred.

2.10.3 Formato ARP

Una trama Ethernet está compuesta por los siguientes campos:

- **Hardware Type:** Indica la tecnología de acceso al medio físico, normalmente Ethernet.
- **Protocol Type**: Indica el protocolo de capa 3, normalmente IP.
- **Operation:** Indica el tipo de trama ARP, solicitud o respuesta.
- **Hardware Size**: Indica la longitud del tipo de trama señalado en el campo Hardware Type, para el caso de Ethernet es de 6 bytes o 48 bits.
- **Protocol Size**: Indica la longitud del tipo de protocolo de capa 3 señalado en el campo Protocol Type, para el caso de IP es de 4 bytes o 32 bits.
- **Sender Hardware Address**: Indica la dirección origen de la tecnología de acceso al medio.
- **Sender Protocol Address**: Indica la dirección origen del protocolo de capa 3.
- **Target Hardware Address**: Indica la dirección destino de la tecnología de acceso al medio. Si es una solicitud ARP, se desconoce este campo.
- **Target Protocol Address**: Indica la dirección destino del protocolo de capa 3.

2.10.4 Suplantación de ARP

El protocolo ARP es el encargado de traducir direcciones IP de 32 bits, a las correspondientes direcciones hardware, generalmente de 48 bits en dispositivos Ethernet. Cuando un ordenador necesita resolver una dirección IP en una dirección MAC, lo que hace es efectuar una petición ARP (*arp-request*) a la dirección de difusión de dicho segmento de red, FF:FF:FF:FF:FF:FF, solicitando que el equipo que tiene esta IP responda con su dirección MAC. Con el objetivo de reducir el tráfico en la red, cada respuesta de ARP (*arp-reply*) que llega a la tarjeta de red es almacenada en una tabla cache, aunque la máquina no haya realizado la correspondiente petición. Así pues, toda respuesta de ARP que llega a la máquina es almacenada en la tabla de ARP de esta máquina. Este factor es el que se utilizará para realizar el ataque de suplantación de ARP. Este engaño se conoce con el nombre de "***envenenamiento de ARP***" (*ARP poisoning*). El objetivo de un ataque de suplantación de ARP es poder capturar tráfico ajeno sin necesidad de poner en modo promiscuo la interfaz de red. Envenenando la tabla de ARP de los equipos involucrados en la comunicación que se quiere capturar se puede conseguir que el conmutador les haga llegar los paquetes. Si el engaño es posible, cuando las dos máquinas empiecen la comunicación enviarán sus paquetes hacia la máquina donde está el *sniffer*. Éste, para no descubrir el engaño, se encargará de encaminar el tráfico que ha interceptado.

2.10.5 RARP

El Protocolo de resolución inversa de direcciones (RARP) asocia las direcciones MAC conocidas a direcciones IP. Esta asociación permite que los dispositivos de red encapsulen los datos antes de

enviarlos a la red. Es posible que un dispositivo de red, como por ejemplo una estación de trabajo sin disco, conozca su dirección MAC pero no su dirección IP. RARP permite que el dispositivo realice una petición para conocer su dirección IP. Los dispositivos que usan RARP requieren que haya un servidor RARP en la red para responder a las peticiones RARP. Considere el caso en que un dispositivo origen desee enviar datos al dispositivo madre. En este ejemplo, el dispositivo fuente conoce su propia dirección MAC pero es incapaz de ubicar su propia dirección IP en la tabla ARP. El dispositivio origen debe incluir tanto su dirección MAC como su dirección IP para que el dispositivo destino retire los datos, los pase a las capas superiores del modelo OSI y responda al dispositivo transmisor. De esta manera, el origen inicia un proceso denominado petición RARP. Esta petición ayuda al dispositivo origen a detectar su propia dirección IP. Las peticiones RARP se envían en broadcast a la LAN y el servidor RARP que por lo general es un Router responde. RARP utiliza el mismo formato de paquete que ARP. Sin embargo, en una petición RARP, los encabezados MAC y el "código de operación" son diferentes a los de una petición ARP. El formato de paquete RARP contiene lugares para las direcciones MAC tanto de los dispositivos de origen como de los de destino. El campo de dirección IP origen está vacío. El broadcast se dirige a todos los dispositivos de la red. Por lo tanto, la dirección MAC destino deberá ser: FF:FF:FF:FF:FF:FF. Las estaciones de trabajo que admiten RARP tienen códigos en ROM que los dirige a iniciar el proceso de RARP.

2.10.6 BOOTP

El protocolo bootstrap (BOOTP) opera en un entorno cliente-servidor y sólo requiere el intercambio de un solo paquete para obtener la información IP. Sin embargo, a diferencia del RARP, los paquetes de BOOTP pueden incluir la dirección IP, así como la dirección de un Router, la dirección de un servidor y la información específica del fabricante.

Un problema del BOOTP es que no se diseñó para proporcionar la asignación dinámica de las direcciones. Con el BOOTP, un administrador de redes crea un archivo de configuración que especifica los parámetros de cada dispositivo. El administrador debe agregar hosts y mantener la base de datos del BOOTP. Aunque las direcciones se asignan de forma dinámica, todavía existe una relación exacta entre el número de direcciones IP y el número de hosts. Esto significa que para cada host de la red, debe haber un perfil BOOTP con una asignación de dirección IP en él. Dos perfiles nunca pueden tener la misma dirección IP. Es posible que estos perfiles se utilicen al mismo tiempo y esto quiere decir que dos hosts tendrían la misma dirección IP.

Un dispositivo utiliza el BOOTP para obtener una dirección IP cuando se inicializa. El BOOTP utiliza UDP para transportar los mensajes. El mensaje UDP se encapsula en un paquete IP. Un computador utiliza el BOOTP para enviar un paquete IP de broadcast a la dirección IP destino de todos unos, o sea, 255.255.255.255 en anotación decimal punteada. El servidor del BOOTP recibe el broadcast y responde en forma de broadcast. El cliente recibe una trama y verifica la dirección MAC. Si el cliente encuentra su propia dirección MAC en el campo de dirección destino y un broadcast en el campo IP destino, toma la dirección IP y la guarda junto con la otra información proporcionada por el mensaje BOOTP de respuesta.

2.10.7 ICMP

IP utiliza un método de entrega de paquetes no confiable conocido como mecanismo de entrega con el mejor esfuerzo. Esto significa que IP no incluye procesos para asegurar que los datos enviados sean entregados al destino en los casos que ocurran problemas en la red, los paquetes que se pierden, simplemente se pierden.

Si un dispositivo intermedio como un router falla, o si el dispositivo destino está desconectado de la red, los paquetes de datos no se podrán entregar y el protocolo IP no tiene implementado ningún mecanismo que le permita notificar al origen que la transmisión ha fallado.

El protocolo de mensajes de control de Internet (ICMP) es el componente de la pila de protocolos

TCP/IP que se ocupa de estas limitaciones de IP. Es importante tener en cuenta que ICMP no hace que el protocolo IP sea confiable, la confiabilidad debe ser provista por las capas superiores en el caso que sean necesarias.

ICMP se ocupa básicamente de informar errores y sucesos para IP. Cuando ocurre un error en la entrega de un datagrama, ICMP es usado para reportar ese error al origen del datagrama. Por ejemplo, si la estación 1 de la figura envía un datagrama a la estación 2 pero la interfaz Ethernet del router B no está disponible, el router utiliza ICMP para enviarle un mensaje a la estación 1 (y sólo a la estación 1) indicando que el datagrama no puede ser entregado. Note que ICMP no soluciona los errores encontrados, simplemente los informa.

2.10.8 Tipos de mensaje ICMP

Como cualquier tipo de paquetes, los mensajes ICMP tiene formatos especiales. Cada mensaje ICMP tiene características propias pero comparten tres campos similares :

- Tipo: Identifica el tipo de mensaje ICMP que es enviado
- Código: Incluye información específica de cada tipo de mensaje
- Checksum: Verifica la integridad de los datos

Los mensajes ICMP se encapsulan y se envían en paquetes IP por lo que pueden perderse o descartarse. No obstante ante la pérdida o error de un paquete IP que contenga un mensaje ICMP no se generan más mensajes de error ICMP.

Cuando los mensajes ICMP reportan errores siempre incluyen el encabezado y los primeros 64 bits de datos del datagrama que causó el problema. Esto le permite al receptor determinar de una manera precisa qué protocolo y programa de aplicación es el responsable del datagrama.

2.10.9 Identificación de respuestas ICMP

Aunque el objetivo original del protocolo ICMP es el de notificar errores y condiciones inusuales (que requieren una especial atención respecto al protocolo IP), es posible poder realizar un uso indebido de este protocolo para obtener huellas identificativas de un sistema remoto.

Comentaremos a continuación algunos ejemplos de cómo obtener estas huellas a partir de las distintas respuestas ofrecidas mediante el tráfico ICMP:

- **ICMP echo**. Como hemos visto anteriormente, el uso de tráfico ICMP de tipo *echo* permite la exploración de sistemas activos. Así, con esta exploración se pretende identificar los equipos existentes dentro de la red que se quiere explorar, normalmente accesibles desde internet. El campo TTL, utilizado en este intercambio de paquetes echode ICMP, suele ser inicializado de forma distinta según el sistema operativo que haya detrás del equipo.

  Por otra parte, cuando se envía un paquete ICMP *echo-request* hacia la dirección de difusión (broadcast), se consigue que con un único paquete enviado todos los equipos respondan con un paquete ICMP de tipo *echo-reply*.

  Esta característica no es propia de todos los sistemas operativos. Así, por ejemplo, puede estar presente en algunas variantes de sistemas operativos Unix, mientras que los sistemas operativos de Microsoft no responden a este tipo de paquetes.

  Estas dos informaciones, el número de TTL inicial y la respuesta a un ping enviado por difusión, podría ser de utilizado como una primera huella identificativa de los sistemas de la red.

- **ICMP timestamp**. Mediante la transmisión de un paquete ICMP de tipo *timestamp-request*, si

un sistema está activo, se recibirá un paquete de tipo *timestamp-reply*, indicando si es posible conocer la referencia de tiempo en el sistema de destino.

La decisión de responder o no a estos paquetes depende de la implementación. Algunos sistemas operativos Windows si responden, mientras que otros no lo hacen. No obstante, la mayoría de los sistemas operativos Unix si que suelen implementarlo.

- **ICMP information**. La finalidad de los paquetes ICMP de tipo *information-request* y su respuesta asociada, *information-reply*, consiste en permitir que ciertos equipos que no disponen de disco puedan extraer su propia configuración, autoconfigurarse en el momento de inicio, obtener su dirección IP, etc.

  Aunque las recomendaciones de seguridad indican que los sistemas operativos no deberían generar este tipo de paquetes ni responder a ellos, la realidad de las implementaciones existentes es otra.

  La respuesta, en lugar de indicar la dirección IP de la red en el campo de origen, indica la dirección IP del equipo. Algunos sistemas operativos responderán únicamente cuando la dirección IP de destino del paquete tenga el valor de una dirección IP de confianza. Otros sistemas, así como muchos dispositivos de red, implementan distintos métodos de respuesta ante este tipo de paquetes. Todas estas diferencias se pueden utilizar en el momento de confeccionar la huella identificativa.

2.11 PROTOCOLO TCP

Como se mencionó anteriormente, el protocolo IP es un protocolo de "mejor esfuerzo", esto significa, que no provee confiabilidad en las transmisiones, si se pierde un paquete en tránsito, por un error en la transmisión o por un desbordamiento de buffer de algún dispositivo u otro motivo, IP no realizará ninguna tarea para recuperar el paquete o retransmitirlo. Para garantizar confiabilidad en la comunicación, se diseñó el Protocolo TCP.

El Protocolo de Control de Transmisión (Transmission Control Protocol - TCP) es uno de los protocolos de capa de transporte (capa 4) de la familia de protocolos TCP/IP . Es orientado a la conexión y provee transmisión de datos confiable full-duplex. TCP es responsable de dividir los mensajes en segmentos, reensamblarlos en el destino y retransmitir aquellos que no fueron recibidos.

El objetivo de TCP es proveer circuitos virtuales confiables entre los extremos de la comunicación. Para brindar estos servicios utiliza diferentes técnicas que estudiaremos a continuación.

TCP es un protocolo orientado a la conexión. Los protocolos orientados a la conexión, deben realizar una conexión entre el emisor y el receptor antes de transmitir información. Un extremo debe iniciar la conexión (generalmente el cliente), y el otro extremo debe aceptarla (generalmente el servidor).

La conexión se divide en tres fases:

1. Establecimiento de la conexión
2. Transferencia de datos
3. Finalización de la conexión

Algunos protocolos que utilizan TCP para garantizar una comunicación confiable entre las entidades cliente y el servidor son los siguientes:

- ***Telnet***
- ***FTP***
- ***HTTP***

2.11.1 Identificación de mecanismos de Control TCP

La huella identificativa que un atacante querría obtener de los sistemas de una red hace referencia a toda aquella información de la implementación de pila TCP/IP de los mismos. En primer lugar, esta información le permitirá descubrir de forma muy fiable el sistema operativo que se ejecuta en la máquina analizada. Por otro lado, estos datos, junto con la versión del servicio y del servidor obtenidos anteriormente, facilitarán al atacante la búsqueda de herramientas necesarias para realizar, por ejemplo, una explotación de un servicio contra algunos de estos sistemas.

La mayor parte de las técnicas para obtener esta huella identificativa se basan en la información de la pila TCP/IP que puede obtenerse a partir de los mecanismos de control del intercambio de tres pasos propio del protocolo TCP/IP.

El protocolo TCP es un protocolo de la capa de transporte que asegura que los datos sean enviados correctamente. Esto significa que se garantiza que la información recibida se corresponda con la información enviada y que los paquetes sean ensamblados en el mismo orden en que fueron enviados.

Generalmente, las características de implementación de los mecanismos de control incorporados en el diseño de TCP en pila TCP/IP de un sistema operativo se basa en la interpretación que los desarrolladores realizan de los RFC. La interpretación de los RFC (y por lo tanto, las características propias de implementación) puede ser muy distinta en cada sistema operativo (incluso en diferentes versiones de un mismo sistema operativo). Así pues, la probabilidad de acierto del sistema operativo remoto mediante esta información es muy elevada.

2.11.2 Saludo de tres vías

Para establecer las conexiones, TCP utiliza una técnica llamada "saludo de tres vías" (three way handshake). El saludo de tres vías consiste en tres segmentos TCP que se envían entre el emisor y el receptor. Una vez que se realizó el acuerdo de tres vías, se finaliza la fase de establecimiento de la conexión y se procede a transmitir datos (Fase 2).

El saludo de tres vías se puede describir con los siguientes pasos :

1. El Cliente envía un segmento con el bit de control SYN=1 y un número de secuencia elegido al azar.
2. El Servidor responde con un segmento con los bits de control SYN=1 y ACK=1. En este segmento, el Número de Secuencia es elegido al azar, y el Número de Acuse de Recibo debe ser igual al Número de Secuencia del Cliente + 1.
3. El cliente realiza el acuse de recibo de la respuesta enviando un segmento con el bit de control ACK=1, indicando su Número de Secuencia, y el Número de Acuse de Recibo debe ser igual al Número de Secuencia del Servidor + 1.

Los restantes bits de control que no se mencionaron en la descripción tienen un valor = 0 (no se encuentran activados). Una vez que la conexión se encuentra establecida el número de secuencia contabiliza la cantidad de bytes que se transmiten.

2.11.3 Formato del segmento TCP

Se puede observar el formato de un segmento TCP. El detalle de los campos es el siguiente:

- Puerto Origen: Número de puerto origen.
- Puerto Destino: Número de puerto destino.

- Número de secuencia: utilizado para ordenar los segmentos recibidos.
- Número de acuse de recibo: utilizado para confirmar la recepción de un Número de Secuencia.
- HLEN: Cantidad de bloques de 32 bits del encabezado.
- Reservado: No utilizado.
- Bits de Código: Banderas (flags) para indicar el tipo de segmento (ver detalle más abajo).
- Ventana: Cantidad de octetos que el emisor está preparado para recibir simultáneamente.
- Suma de Comprobación: Checksum calculado considerando el encabezado TCP, los datos y un pseudoencabezado IP que genera para asegurar principalmente el destino y tipo de protocolo correcto.
- Marcador Urgente: Indica la posición final de los datos que deben ser procesados sin respetar la secuencia en el flujo.
- Opciones: Diferentes opcionales, como por ejemplo, el tamaño máximo de segmento TCP.
- Datos: Datos recibidos del protocolo de la capa superior.

Los bits de código son un componente esencial del segmento TCP, dado que definen el tipo de segmento. Comprenden 6 bits, cada bit corresponde a una bandera:

- U (URG): Indica que el campo Marcador Urgente es válido.
- A (ACK): Indica que el número de acuse de recibo almacenado en el campo Acuse de Recibo es válido.
- P (PSH): Función PUSH, para indicar al TCP que entregue los datos de este mensaje de inmediato al proceso de la capa superior.
- R (RST): Indica al TCP que debe restablecer el circuito virtual, a causa de un error no recuperable.
- S (SYN): Indica la apertura de una conexión de circuito virtual, y un pedido de sincronía entre el número de secuencia enviado y el número de acuse esperado.
- F (FIN): Indica al TCP que debe finalizar la conexión, probablemente porque la aplicación no tiene más datos para enviar.

2.11.4 Puertos

Entre dos estaciones de trabajo puede existir más de una conexión TCP. Supongamos que desde nuestra estación de trabajo accedemos a un servidor web para visualizar una página y, simultáneamente transferimos un archivo hacia el mismo servidor. Para cada una de estas tareas, se establece una conexión TCP diferente. Para indicarle al servidor que solicitamos una conexión para transferir un archivo, o para visualizar una página, se utilizan los Puertos.

Los puertos (ports) tienen como objetivo identificar las diferentes aplicaciones. El puerto es un número (entre 1 y 65535) que identifica la aplicación que está transfiriendo información . Para cada segmento TCP que se envía, se especifica un puerto origen (aplicación transmisora) y un puerto destino (aplicación receptora) .

Los números de puerto se pueden dividir en los siguientes intervalos:

- Puertos inferiores a 255: asignados a aplicaciones públicas, llamados puertos "bien conocidos" (well known)

- Puertos entre 255 y 1023: asignados a empresas para aplicaciones comercializables.
- Puertos superiores a 1023: no están regulados.

Cuando un cliente quiere conectarse a un servidor envía un segmento indicando, el puerto destino (generalmente un puerto bien conocido) asociado a la aplicación requerida y el puerto origen, generalmente asociado a un número mayor a 1023.

2.11.5 Exploración de puertos TCP

Aparte de ser de utilidad para obtener la huella identificativa de un sistema conectado a la red, la exploración de puertos TCP se puede utilizar para descubrir si dicho sistema ofrece o no un determinado servicio.

Existe un grande número de técnicas para realizar esta exploración de puertos TCP. Entre las más conocidas, podemos destacar las siguientes:

- **TCP connect scan**. Mediante el establecimiento de una conexión TCP completa (completando los tres pasos del establecimiento de la conexión) la exploración puede ir analizando todos los puertos posibles. Si la conexión se realiza correctamente, se anotará el puerto como abierto (realizando una suposición de su servicio asociado según el número de puerto).
- **TCP SYN scan**. Enviando únicamente paquetes de inicio de conexión (SYN) por cada uno de los puertos que se quieren analizar se puede determinar si estos están abiertos o no. Recibir como respuesta un paquete *RST-ACK* significa que no existe ningún servicio que escuche por este puerto.

  Por el contrario, si se recibe un paquete *SYN-ACK*, podemos afirmar la existencia de un servicio asociado a dicho puerto TCP. En este caso, se enviará un paquete *RST-ACK* para no establecer conexión y no ser registrados por el sistema objetivo, a diferencia del caso anterior (TCP connect scan).
- **TCP FIN scan**. Al enviar un paquete *FIN* a un puerto, deberíamos recibir un paquete de reset (RST) si dicho puerto está cerrado. Esta técnica se aplica principalmente sobre implementaciones de pilas TCP/IP de sistemas Unix.
- **TCP Xmas Tree scan**. Esta técnica es muy similar a la anterior, y también se obtiene como resultado un paquete de reset si el puerto está cerrado. En este caso se envían paquetes *FIN*, *URG* y *PUSH*.
- **TCP Null scan**. En el caso de poner a cero todos los indicadores de la cabecera TCP, la exploración debería recibir como resultado un paquete de reset en los puertos no activos.

La mayor parte de aplicaciones para realizar exploración de puertos TCP suelen ser ruidosas, es decir, no intentan esconder lo que se está analizando en la red. Esto suele ser así porque se presume que o bien nadie está revisando la actividad de exploración o que, utilizando un equipo comprometido, nadie podrá descubrir el equipo desde el que realmente se realiza la exploración de puertos.

2.11.6 Control de errores

El protocolo TCP provee control de flujo y recuperación ante errores, es decir que si falla la transmisión, recepción o tránsito de un segmento, el protocolo detecta el error y retransmite los datos necesarios. Por este motivo, se declara al protocolo TCP como "confiable".

Al proveer recuperación ante fallas, los protocolos superiores que se apoyan en TCP pueden omitir este control, dado que tienen la certeza que todos los datos que pasen a TCP, serán transmitidos y

recibidos en forma ordenada y sin pérdidas.

El método de corrección de errores que implementa TCP se basa en la retransmisión de los segmentos dañados o perdidos, para realizar esta tarea debe controlar los números de secuencia y acuses de recibo. En la fase de transferencia de datos, cada segmento que se envía viaja con un número de secuencia, que corresponde a la porción del mensaje que se está transfiriendo .

Cuando se envía el acuse de recibo, se referencia el número de secuencia que se está esperando recibir, es decir, se informa al otro extremo los segmentos que se han recibido correctamente y desde qué punto del mensaje tiene que continuar la transmisión. A esto se le llama acuse de recibo de expectativa, porque se informa lo que se está esperando recibir .

Si se pierde un mensaje en tránsito, o es descartado por el receptor por un error de transmisión, el receptor no envía el acuse de recibo correspondiente. Pasado cierto tiempo en que el emisor no recibe el acuse, procede a reenviar segmentos a partir del último byte para el cual ha recibido un acuse de recibo . Si por algún motivo se pierde el acuse de recibo, el emisor considerará que el segmento no ha llegado al destino y también lo retransmitirá .

2.11.7 Control de flujo

Hasta ahora, en los ejemplos expuestos, el emisor transmite un segmento y espera recibir el acuse de recibo para continuar transmitiendo. En la realidad, esto no se cumple, porque el protocolo tendría bajo rendimiento. Para mejorar la eficiencia, TCP acepta la transmisión de varios segmentos sin esperar un acuse de recibo. El control de la cantidad de datos que se transmiten simultáneamente se denomina control de flujo y la cantidad de datos que se pueden transmitir simultáneamente sin recibir el acuse de recibo correspondiente se llama ventana (window).

En TCP, el tamaño de la ventana puede variar a lo largo de una conexión. El emisor y receptor se comunican el tamaño de su ventana utilizando el campo ventana del encabezado TCP, de esta manera se puede maximizar la utilización del vínculo, pero sin llegar a saturarlo . En caso que la cantidad de datos supere la capacidad del vínculo o del receptor, el receptor acuerda con el emisor un tamaño menor de ventana. Esta técnica se denomina "Ventana Deslizante".

2.11.8 Liberación de la conexión

Una vez que se han transmitido los datos, comienza la liberación de la conexión (Fase 3). En TCP la liberación de la conexión puede realizarse en forma independiente en cada uno de los extremos.

Para finalizar la conexión, se utilizan segmentos con el bit de control FIN = 1 . Cada segmento FIN debe ser reconocido con un acuse de recibo. Si los dos extremos finalizan la conexión al mismo tiempo, puede suceder que en el mismo acuse de recibo se transmita el FIN .

2.11.9 Sockets

Los sockets son interfaces utilizadas por los sistemas operativos para brindar acceso a los protocolos de comunicaciones. Consideremos la siguiente terminología:

- Un socket es un tipo de "archivo" especial, el cual es usado por los procesos del sistema para solicitar servicios de red al sistema operativo
- Una dirección de socket está compuesta por tres componentes: <protocolo, dirección local, proceso local>, por ejemplo, en TCP/IP, <tcp, 193.44.234.3, 12345>
- Una conversación es el enlace de comunicación entre dos procesos

- Una asociación está formada por 5 componentes que especifican completamente los dos procesos que comprenden una conexión: <protocolo, dirección local, proceso local, dirección remota, proceso remoto>. Por ejemplo, en TCP/IP, una asociación podría ser: <tcp, 193.44.234.3, 1500, 193.44.234.5, 21>
- Para especificar cada extremo de la conexión se utiliza el término Media asociación que puede ser: <protocolo, dirección local, proceso local> o bien <protocolo, dirección remota, proceso remoto>.
- A las medias asociaciones, también se las llama socket, o direcciones de transporte.

En definitiva, un socket es un extremo de una comunicación que puede ser llamado y direccionado a una red. Dos procesos se comunican a través de sockets TCP. Los sockets le proveen a los procesos una conexión full-duplex hacia otro proceso . En una conexión TCP, cada extremo de la conexión puede ser identificado por la dirección de socket <TCP, dirección IP, número de puerto>. La conexión puede ser identificada unívocamente por la asociación <TCP, dirección IP local, puerto local, dirección IP remota, puerto remoto>. De esta forma, los servidores pueden establecer múltiples conexiones con un mismo puerto origen, dado que cada conexión tendrá una dirección de asociación diferente.

2.12 PROTOCOLO UDP

El Protocolo de datagramas de usuario (UDP) es el protocolo de transporte no orientado a la conexión de la pila de protocolos TCP/IP . UDP es un protocolo simple que intercambia datagramas sin implementar técnicas de acuse de recibo para garantizar la entrega o tecnicas de ventanas para el control de flujo. Por este motivo, el procesamiento de errores y retransmisiones, debe ser manejado por los protocolos de capas superiores.

UDP está diseñado para ser utilizado por aplicaciones que no requieran la confiabilidad de TCP.

Como se vio anteriormente, UDP está diseñado para el transporte de datos de manera no confiable entre hosts

Características:

- No orientado a la conexión
- No aporta confiabilidad
- Transmite mensajes (llamados datagramas de usuario)
- No reensambla los mensajes entrantes
- Ni implementa acuses de recibo
- No proporciona control de flujo
- Los datagramas tienen un tamaño limitado
- Permite transmitir tanto broadcast como multicast

Algunos de los protocolos más comunes que utilizan UDP son:

- SNMP
- DNS
- TFTP

2.12.1 Formato de UDP

El formato del segmento UDP muestra los campos son los siguientes:

- Puerto origen: Indica el puerto UDP del host origen
- Puerto destino: Indica el puerto UDP del host destino
- Longitud del mensaje: Indica el número de bytes incluyendo el encabezado y los datos
- Checksum: Suma de comprobación para verificar la integridad del los datos, el encabezado UDP y un pseudoencabezado IP que genera para asegurar principalmente el destino y tipo de protocolo correcto.
- Datos: Contiene los datos de las capas superiores.

2.12.2 Exploración de puertos UDP

Mediante la exploración de puertos UDP es posible determinar si un sistema está o no disponible, así como encontrar los servicios asociados a los puertos UDP que encontramos abiertos.

Para realizar esta exploración se envían datagramas UDP sin ninguna información al campo de datos. En el caso de que el puerto esté cerrado, se recibirá un mensaje ICMP de puerto no alcanzable (port unreachable). Si el puerto está abierto, no se recibirá ninguna respuesta.

Dado que UDP es un protocolo no orientado a conexión, la fiabilidad de este método depende de numerosos factores (más todavía en Internet), como son la utilización de la red y sus recursos, la carga existente, la existencia de filtros de paquetes en sistemas finales o en sistemas cortafuegos, etc. Asimismo, y a diferencia de las exploraciones TCP, se trata de un proceso mucho más lento, puesto que la recepción de los paquetes enviados se consigue mediante el vencimiento de temporizadores (timeouts).

En el caso de detectar un elevado número de puertos UDP abiertos, el atacante podría concluir que existe un sistema cortafuegos entre su equipo y el objetivo. Para confirmar esta última posibilidad, se puede enviar un datagrama UDP al puerto cero. Esto tendría que generar una respuesta ICMP de puerto no alcanzable. No recibir esta respuesta significa que existe un dispositivo que filtra el tráfico.

La aplicación por excelencia para realizar exploración de puertos es **Nmap** (*Network Mapper*). Esta herramienta implementa la gran mayoría de técnicas conocidas para exploración de puertos y permite descubrir información de los servicios y sistemas encontrados. Nmap también implementa un gran número de técnicas de reconocimiento de huellas identificativas, como las que hemos visto anteriormente. **Nmap**, junto con **Nessus**, son dos de las herramientas más frecuentemente utilizadas tanto por administradores de redes como por posibles atacantes, puesto que ofrecen la mayor parte de los datos necesarios para estudiar el comportamiento de un sistema o red que se quiere atacar.

2.13 VLANs

Una Red de Área Local Virtual (VLAN) es una agrupación lógica de dispositivos o estaciones, independientemente de su ubicación física. No necesariamente estos dispositivos o estaciones estarán conectados al mismo switch, ni todos los enlaces de un switch formarán parte de esta agrupación.

Anteriormente vimos que los switches conforman un sólo dominio de broadcast entre todos sus puertos. Esto no se cumple cuando tenemos VLANs: cada VLAN es un dominio de broadcast diferente. Los dispositivos o usuarios de una VLAN se pueden agrupar por funciones, departamentos, aplicaciones, etc., sin importar la ubicación física de su segmento.

La configuración de las VLANs se realiza en los switches en forma estática o dinámica, en el primer caso el administrador define los puertos de cada switch que pertenecerán a cada VLAN, en el segundo caso los puertos se asignan automáticamente a las VLANs conforme a la dirección MAC o IP de cada estación. Sin embargo las VLANs no necesariamente se encuentran en un sólo switch, sino que se pueden crear VLANs distribuidas a lo largo de varios switches. Esto se logra interconectando los switches mediante enlaces VLAN Trunking, estos enlaces transportan la información de todas las VLANs entre los distintos switches.

Cuando se utilizan VLANs distribuidas, los enlaces de trunk deben transportar las tramas de todas las VLANs para luego ser distribuidas en los puertos que correspondan de cada switch. Cada trama debe llevar una identificación de la VLAN a la que corresponde. A esto se le llama "etiquetado de trama". Existen dos protocolos difundidos para realizar el etiquetado de tramas: ISL (Inter Switch Link) protocolo propietario de Cisco, y 802.1q, que es un estándar abierto definido por la IEEE. Como cada VLAN implica un direccionamiento de red diferente, la comunicación entre VLANs se debe llevar a cabo a través de dispositivos de capa 3 (Routers).

2.14 REDES INALÁMBRICAS (WLAN)

En términos sencillos, una red de área local inalámbrica (WLAN) hace exactamente lo que el nombre implica. Proporciona todas las funciones y beneficios de las tecnologías LAN tradicionales, como Ethernet y Token Ring, pero sin las limitaciones impuestas por los alambres o cables. De esta forma, las WLANs redefinen la forma en la cual la industria contempla las LANs. Conectividad ya no significa conexión física. Las áreas locales ya no se miden en pies ni en metros, sino en millas o kilómetros. Una infraestructura no necesita estar enterrada u oculta detrás de los muros, sino que puede desplazarse y cambiar según las necesidades de una organización.

Una WLAN, al igual que una LAN, requiere un medio físico a través del cual pasan las señales de transmisión. En lugar de utilizar par trenzado o cable de fibra óptica, las WLANs utilizan luz infrarroja (IR) o frecuencias de radio (RFs). El uso de la RF es mucho más popular debido a su mayor alcance, mayor ancho de banda y más amplia cobertura. Las WLANs utilizan las bandas de frecuencia de 2,4 gigahertz (GHz) y de 5 GHz. Estas porciones del espectro de RF están reservadas en la mayor parte del mundo para dispositivos sin licencia. El networking inalámbrico proporciona la libertad y la flexibilidad para operar dentro de edificios y entre edificios.

Los sistemas inalámbricos no carecen completamente de cables. Los dispositivos inalámbricos son sólo una parte de la LAN cableada tradicional. Estos sistemas inalámbricos, diseñados y construidos utilizando microprocesadores y circuitos digitales estándar, se conectan a sistemas LAN cableados tradicionales. Además, los dispositivos inalámbricos deben recibir alimentación que les proporcionen energía para codificar, decodificar, comprimir, descomprimir, transmitir y recibir señales inalámbricas. Los dispositivos WLAN de primera generación, con sus bajas velocidades y falta de estándares, no fueron populares. Los sistemas estandarizados modernos pueden ahora transferir datos a velocidades aceptables. El comité IEEE 802.11 y la Alianza Wi-Fi han trabajado diligentemente para hacer al equipo inalámbrico estandarizado e interoperable. La tecnología inalámbrica soportará ahora las tasas de datos y la interoperabilidad necesarias para la operación de la LAN. Además, el costo de los nuevos dispositivos inalámbricos ha disminuido mucho. Las WLANs son ahora una opción económicamente factible para la conectividad LAN. En la mayoría de los países estos dispositivos no requieren licencia gubernamental.

2.14.1 Beneficios

Las LANs Ethernet cableadas actuales operan a velocidades de alrededor de 100 Mbps en la capa de acceso, 1 Gbps en la capa de distribución, y hasta 10 Gbps a nivel de la capa principal. La mayoría de las WLANs operan a una velocidad de 11 Mbps a 54 Mbps en la capa de acceso y no tienen como

objetivo operar en la capa de distribución o en la capa principal. El costo de implementar WLANs compite con el de las LANs cableadas. Por lo tanto, ¿por qué instalar un sistema que se encuentra en el extremo más bajo de las capacidades de ancho de banda actuales? Una razón es que en muchos entornos LAN pequeños, las velocidades más lentas son adecuadas para soportar las necesidades de las aplicaciones y del usuario. Con muchas oficinas conectadas ahora a la Internet por medio de servicios de banda ancha como DSL o cable, las WLANs pueden manejar las demandas de ancho de banda. Otra razón es que las WLANs permiten a los usuarios movilizarse dentro de un área definida con libertad y aún así permanecer conectados. Durante las reconfiguraciones de oficina, las WLANs no requieren un recableado ni sus costos asociados.

Las WLANs presentan numerosos beneficios para las oficinas hogareñas, los negocios pequeños, los negocios medianos, las redes de campus y las corporaciones más grandes. Los entornos que es probable que se beneficien de una WLAN tienen las siguientes características:

- Requieren las velocidades de una LAN Ethernet estándar
- Se benefician de los usuarios móviles
- Reconfiguran la disposición física de la oficina a menudo
- Se expanden rápidamente
- Utilizan una conexión a Internet de banda ancha
- Enfrentan dificultades significativas al instalar LANs cableadas
- Necesitan conexiones entre dos o más LANs en un área metropolitana
- Requieren oficinas y LANs temporales

Las WLANs no eliminan la necesidad de la existencia de los Proveedores de Servicios de Internet (ISPs). La conectividad a Internet aún requiere de acuerdos de servicios con portadoras de intercambio locales o ISPs para un acceso a la Internet. Existe una tendencia actual para que los ISPs proporcionen un servicio de Internet inalámbrico. Estos ISPs se denominan Proveedores de Servicios de Internet Inalámbricos (WISPs). Además, las WLANs no reemplazan la necesidad de los routers, switches y servidores cableados tradicionales de una LAN típica.

Incluso aunque las WLANs han sido diseñadas principalmente como dispositivos LAN, pueden utilizarse para proporcionar una conectividad de sitio a sitio a distancias de hasta 40 km (25 millas). El uso de dispositivos de WLAN es mucho más eficaz en costos que el uso del ancho de banda WAN o la instalación o arrendamiento de largas trayectorias de fibra. Por ejemplo, para instalar una WLAN entre dos edificios se incurrirá en un costo único de varios miles de dólares estadounidenses. Un enlace E1 dedicado, que sólo proporciona una fracción del ancho de banda de una WLAN, fácilmente costará cientos de dólares estadounidenses por mes o más. Instalar fibra a través de una distancia de más de 1,6 km (1 milla) es difícil y costaría mucho más que una solución inalámbrica.

Las primeras tecnologías LAN inalámbricas definidas mediante el estándar 802.11 eran ofertas propietarias de baja velocidad de 1 a 2 Mbps. A pesar de estos inconvenientes, la libertad y flexibilidad de las tecnologías inalámbricas permitieron a estos primeros productos encontrar su lugar en los mercados tecnológicos. Los trabajadores móviles utilizaban dispositivos portátiles para la administración de inventarios y la recolección de datos en ventas al por menor y almacenamiento. Posteriormente, los hospitales aplicaron la tecnología inalámbrica para reunir y entregar información acerca de los pacientes. A medida que las computadoras se abrían paso hacia las aulas, las escuelas y universidades comenzaron a instalar redes inalámbricas para evitar costos de cableado, a la vez que habilitaban un acceso compartido a la Internet. Al darse cuenta de la necesidad de un estándar similar a Ethernet, los fabricantes de tecnologías inalámbricas se aliaron en 1991 y formaron la Alianza de Compatibilidad de Ethernet Inalámbrica (WECA). La WECA propuso y construyó un estándar basado en tecnologías contribuyentes. WECA cambió posteriormente su nombre a Wi-Fi. En junio de 1997 IEEE lanzó el estándar 802.11 para el networking de área local inalámbrico. Así como el estándar de Ethernet 802.3 permite la transmisión de datos a través de par trenzado y cable

coaxial, el estándar de WLAN 802.11 permite la transmisión a través de medios diferentes. Los medios especificados incluyen los siguientes:

- Luz infrarroja (IR)
- Tres tipos de transmisión de radio dentro de las bandas de frecuencia de 2,4 GHz no licenciadas:
    - Espectro expandido de saltos de frecuencia (FHSS)
    - Espectro expandido de secuencia directa (DSSS) 802.11b
    - Multiplexado por división de frecuencia ortogonal (OFDM) 802.11g
- Un tipo de transmisión de radio dentro de las bandas de frecuencia de 5 GHz no licenciadas:
    - Multiplexado por división de frecuencia ortogonal (OFDM) 802.11a

2.14.2 Consideraciones

En las LANs inalámbricas, una dirección MAC equivale a una ubicación física. Esto se da por supuesto implícitamente en el diseño de LANs cableadas. En IEEE 802.11 una estación tiene una MAC asociada, pero no es, en general, una ubicación física fija . Las capas físicas utilizadas en IEEE 802.11 son fundamentalmente diferentes de aquéllas utilizadas en medios alámbricos. Lo siguiente es cierto respecto a los protocolos de capa física de IEEE 802.11:

- Utilizan un medio que no tiene fronteras absolutas ni fácilmente observables
- No están protegidos de señales externas
- Se comunican a través de un medio que es significativamente menos confiable que los medios cableados
- Tienen topologías dinámicas
- Les falta una conectividad completa. Normalmente, se supone que cada estación puede escuchar a cada una de las otras estaciones. Esta suposición es inválida en el caso de las WLANs. Bajo ciertas circunstancias, algunas estaciones pueden estar "ocultas" entre sí.

A causa de las limitaciones de la capa física inalámbrica, las WLANs que necesitan cubrir distancias geográficas razonables deben construirse a partir de bloques de construcción de una cobertura básica.

Uno de los requisitos de IEEE 802.11 es manipular estaciones tanto móviles como portátiles. Una estación portátil se desplaza de ubicación a ubicación, pero sólo se utiliza mientras se encuentra en una ubicación fija. Las estaciones móviles en realidad acceden a la LAN mientras se encuentran en movimiento. Otro aspecto de las estaciones móviles es que a menudo reciben alimentación proveniente de baterías. De ahí que la administración de energía sea una consideración importante. Por ejemplo, no puede presuponerse que el receptor de una estación siempre estará encendido.

Las WLANs son sólo uno de los usos del espectro de frecuencia de radio (RF).

La definición de radio de la Administración de Servicios Generales de EE.UU. es la siguiente:

1. Telecomunicación por medio de modulación e irradiación de ondas electromagnéticas
2. Un transmisor, receptor o transceptor utilizado para la comunicación a través de ondas electromagnéticas
3. Un término general aplicado al uso de ondas de radio

Las tecnologías inalámbricas se componen de muchos parámetros variables. Algunas tecnologías proporcionan comunicaciones en un solo sentido mientras que otras proporcionan comunicaciones simultáneas en dos sentidos. Algunas operan a niveles de baja energía, mientras que otros operan a niveles de energía altos. Algunos son digitales y otros son analógicos. Algunos operan a distancias cortas de 30,5 m (100 pies) o menos, y otros operan a mayores distancias, incluso a través de continentes. El costo de las diversas tecnologías inalámbricas puede variar de varios dólares estadounidenses a billones de dólares estadounidenses. Las tecnologías inalámbricas, han estado en circulación durante muchos años. La televisión, la radio AM/FM, la televisión satelital, los teléfonos celulares, los dispositivos de control remoto, el radar, los sistemas de alarmas, las radios climáticas, las CBs, y los teléfonos inalámbricos están integrados a la vida cotidiana. Las tecnologías beneficiosas que dependen de la tecnología inalámbrica incluyen sistemas de radares climáticos, rayos x, Imágenes de Resonancia Magnética (MRIs), hornos a microondas, y Satélites de Posicionamiento Global (GPSs). La tecnología inalámbrica rodea a la humanidad diariamente, en los negocios y en la vida personal.

Los cuatro requisitos principales para una solución WLAN son los siguientes:

1. **Alta disponibilidad** — La alta disponibilidad se logra mediante la redundancia del sistema y un diseño de área de cobertura apropiado. La redundancia del sistema incluye APs redundantes en frecuencias separadas. Un diseño de área de cobertura apropiado incluye cuentas para roaming, negociación de velocidad automática cuando se debilita la señal, una selección apropiada de la antena, y el posible uso de repetidores para extender la cobertura a áreas donde un AP no podría utilizarse de otro modo.
2. **Escalabilidad** — se logra soportando múltiples APs por área de cobertura, que utilizan múltiples frecuencias. Los APs también pueden llevar a cabo el equilibrio de la carga, si así se lo desea.
3. **Capacidad administrativa** — Las herramientas de diagnóstico representan una gran porción de la administración dentro de las WLANs. Los clientes deberán poder administrar dispositivos WLAN a través de APIs estándar de la industria, incluyendo SNMP y Web, o a través de aplicaciones de administración empresarial importantes, como CiscoWorks 2000, Cisco Stack Manager, y Cisco Resource Monitor.
4. **Arquitectura abierta** — La apertura se logra mediante la adhesión a estándares tales como 802.11a y 802.11b, la participación en asociaciones de interoperabilidad como la Alianza Wi-Fi, y de certificación, como la certificación FCC de EE.UU.

Otros requisitos están evolucionando a medida que las tecnologías WLAN obtienen popularidad:

- **Seguridad** — Es esencial para encriptar los paquetes de datos transmitidos por vía aérea. Para instalaciones más grandes, se requieren también una autenticación centralizada del usuario y una administración centralizada de claves de cifrado.
- **Costo** — Los clientes esperan reducciones continuas en el precio de un 15 a un 30 por ciento cada año, e incrementos en desempeño y seguridad. Los clientes están preocupados no sólo por el precio de adquisición sino por el costo total propietario (TCO), incluyendo los costos de instalación.

La mayoría de los fabricantes desean que sus clientes utilicen sus APs y NICs de manera exclusiva. Ofrecen cierto grado de capacidad reducida si existe la necesidad de combinar y hacer coincidir diferentes marcas de APs y NICs. En la mayoría de los casos los problemas son mayormente cosméticos pero pueden resultar en un incremento de llamadas al escritorio de ayuda. Hasta el lanzamiento de la siguiente generación, el administrador del sistema tiene que tomar una difícil decisión, utilizar un sistema de un único fabricante, con todos los NICs y APs provenientes de ese fabricante, o arreglárselas sin las herramientas de administración avanzadas que proporcionan las soluciones de un único fabricante.

2.14.3 Instalación de los medios

Es importante calcular todos los costos involucrados al diseñar redes. El impacto del diseño y la construcción del edificio deben considerarse al instalar medios LAN. Algunos factores importantes a considerar incluyen la calefacción, ventilación y acondicionamiento de aire (HVAC), el agua, los desagües cloacales, la iluminación y los sistemas eléctricos existentes. Los materiales estructurales como el yeso, el cemento armado, la madera y el acero, así como los códigos de incendios, deben considerarse también. Muchas paredes representan un papel estructural y de contención de incendios, y no pueden perforarse sin seguir pasos especiales para restaurar su integridad.

Las LANs se convertirán rápidamente en una combinación de sistemas cableados e inalámbricos, dependiendo de las necesidades de la red y de las restricciones de diseño. En redes empresariales más grandes, las capas principal y de distribución continuarán siendo sistemas de backbone cableados, conectados en general por medio de fibra óptica y cables UTP. La capa más cercana al usuario final, la capa de acceso, será la más afectada por la implementación de la tecnología inalámbrica.

Enlaces inalámbricos de edificio a edificio: Las conexiones de edificio a edificio se llevan a cabo en general utilizando fibra óptica, a causa de las altas velocidades disponibles y para evitar medidas de protección de conexión a tierra que se requieren en los medios de cobre. Instalar cable de fibra óptica entre edificios es muy costoso y consume mucho tiempo. Incluso cortas distancias son difíciles de cubrir debido a utilidades subterráneas existentes, cemento armado y otros obstáculos estructurales. Una instalación aérea sujeta con cuerdas es una opción de instalación alternativa. Las WLANs se han convertido actualmente en una opción popular puesto que la instalación se limita a construir antenas montadas. ¿Qué sucedería si utilizáramos conexiones de edificio a edificio allí donde las distancias excedieran los límites de una propiedad o las limitaciones de cableado? La mayoría de los negocios utilizan una conectividad WAN entre sitios metropolitanos distantes. Algunos negocios utilizan microondas entre sitios distantes. En el caso de los bridges LAN inalámbricos, los edificios que se encuentran a hasta 32 km (20 millas) de distancia pueden conectarse a velocidades de hasta 11 Mbps.

En general, cuanto mayor es la distancia entre edificios, más alto es el costo de la instalación LAN inalámbrica. Las antenas estándar rubber ducky no serán adecuadas. Se requieren torres y antenas de elevada ganancia. Las torres pueden resultar costosas, dependiendo de la altura y los requisitos de la construcción. El costo inicial puede recuperarse dentro del primer año. Se generan ganancias provenientes de un incremento en la productividad utilizando más elevado ancho de banda y tarifas de líneas arrendadas mensuales discontinuas.

Los bridges inalámbricos Cisco ofrecen muchas ventajas sobre conexiones alternativas más costosas. Por ejemplo, una línea T-I cuesta en general aproximadamente 400 a 1000 dólares estadounidenses por mes. Para un sitio con cuatro edificios, eso significaría alrededor de 15.000 a 36.000 dólares estadounidenses al año. Con un sistema inalámbrico, la recuperación de los costos de hardware podría tener lugar realmente en menos de un año.

Si una línea T-I no está disponible o los edificios están ubicados en la misma propiedad, podría colocarse un cable subterráneo. No obstante, la introducción en la tierra puede costar más de 100 dólares estadounidenses por cada 0,3 m (1 pie), dependiendo de la tarea. Para conectar tres edificios ubicados a 305 m (1000 pies) separados entre sí, el costo podría exceder los 200.000 dólares estadounidenses.

Las microondas son una solución posible. En el caso de las microondas se requiere usualmente un permiso del gobierno. En Estados Unidos, éste se obtiene de la Comisión Federal de Comunicaciones (FCC). Este permiso sirve como proceso de registro que permite al dueño del permiso tomar acciones legales contra aquéllos que interfieran. El costo del equipamiento es en general de más de 10.000 dólares estadounidenses por sitio, lo cual no incluye el costo de los elementos de instalación. El desempeño puede verse severamente degradado en el caso de niebla espesa, lluvia o nieve. Las

microondas también tienden a ser punto a punto. Las conexiones multipunto usualmente no son posibles.

Independientemente de si son cableadas o inalámbricas, las redes modernas deben poder manipular un ancho de banda más elevado, más aplicaciones y una mayor movilidad. Se requieren combinaciones de tecnologías cableadas e inalámbricas para proporcionar las soluciones. El diseñador de redes es responsable de proporcionar el diseño más eficaz en materia de costos y la solución que cumpla con o exceda las necesidades de la organización.

El diseño, la preparación y el sondeo del sitio se tratarán en detalle posteriormente en el curso. Debe completarse un sondeo del sitio antes de tomar las decisiones de implementación. Por ejemplo, los planes iniciales pueden incluir una solución inalámbrica, pero el sondeo del sitio podría indicar que la tecnología inalámbrica sería ineficaz. Inversamente, una solución cableada puede planificarse inicialmente y el sondeo final puede probar que la solución inalámbrica resultaba una mejor opción.

2.14.4 Confiabilidad y conectividad

Las LANs inalámbricas incluyen mecanismos para mejorar la confiabilidad de las transmisiones de paquetes, para que al menos tengan el mismo nivel que la Ethernet cableada. El uso de protocolos TCP/IP ayudará a proteger la red contra cualquier pérdida o corrupción de datos en el aire. La mayoría de los sistemas de WLAN utilizan una tecnología de espectro expandido o multiplexado por división de frecuencia ortogonal (OFDM). Los dos tipos de radio de espectro expandido son secuencia directa (DSSS) y salto de frecuencia (FHSS).

Se basan en la idea de que una señal que se expande ampliamente o que se mueve rápidamente de canal a canal será difícil de detectar y de interferir con ella. DSSS genera un patrón de bits redundante denominado chip o código de chipping, para cada bit a transmitir. FHSS utiliza una portadora de banda angosta que cambia la frecuencia en un patrón conocido tanto por el transmisor como por el receptor. Si todo se mantiene apropiadamente sincronizado, esto crea un único canal lógico, incluso aunque la frecuencia cambie constantemente. Las primeras implementaciones de 802.11 utilizaban FHSS, no obstante 802.11b estandarizó DSSS.

Actualmente los estándares 802.11a y 802.11g, que operan en hasta 54 Mbps, utilizan OFDM en lugar de DSSS. OFDM limita la diafonía o la interferencia de los canales de transmisión. OFDM se utiliza en servicios de emisión de audio digital europeos. En comparación con DSSS, OFDM permite más velocidad. OFDM no pierde distancia. De hecho, facilita la capacidad para lograr distancias más largas. OFDM sí requiere más potencia de procesamiento en la radio.

Además de cuidar de que coincidan las tecnologías de transmisión, los administradores de redes inalámbricas deben tener en cuenta que los problemas de conexión también pueden existir en entornos cambiantes donde hay obstáculos que pueden bloquear, reflejar o dificultar el paso de las señales. La elección y ubicación del montaje de la antena debe considerarse cuidadosamente al diseñar WLANs para evitar una futura interferencia. La conexión usualmente no se perderá incluso aunque el ancho de banda disponible caiga hasta niveles muy bajos. La falta de un ancho de banda garantizado es de particular interés para muchas compañías.

2.14.5 Componentes

Estaciones: Las estaciones de trabajo deben poseer un adaptador inalámbrico para poder conectarse a una red IEEE 802.11. En general, los adaptadores clientes ya vienen incorporados en la mayoría de las notebooks actuales, e inclusive en algunas PDAs y celulares. A las PCs de escritorio se les puede agregar un adaptador mediante una ranura de expansión (PCI, USB, etc.). Al momento de seleccionar el adaptador, debe verificar que sea compatible con la tecnología utilizada en la red. Existen diferentes substandards de la norma IEEE 802.11, y algunos de ellos no son compatibles entre sí.

Access Points (AP) Los Access Points cumplen un rol de concentradores en las redes inalámbricas. Este dispositivo gobierna las comunicaciones entre las estaciones. Su función es similar a la de un hub dentro de una red cableada. Un Access Point contiene un transceptor de radio. Puede actuar como punto central de una red inalámbrica autónoma o como punto de conexión entre redes inalámbricas y cableadas. En grandes instalaciones, la funcionalidad de roaming proporcionada por múltiples APs permite a los usuarios inalámbricos desplazarse libremente a través de la facilidad, a la vez que se mantiene un acceso sin interrupciones a la red.

Los APs vienen con funciones de tecnología, seguridad y administración variadas. Algunos APs son de banda dual y soportan tecnologías tanto de 2,4 GHz como de 5 GHz, mientras que otros sólo soportan una única banda. Algunos Access Point tienen firmware actualizable.

Estaciones inalámbricas (STA): Son dispositivos de usuario que cuentan con adaptadores que realizan las funciones de las tarjetas de red Ethernet, adaptando las tramas Ethernet que genera el dispositivo, a las tramas del estándar inalámbrico y viceversa, posibilitando la transmisión transparente de la información. Estos adaptadores pueden estar integrados en el propio dispositivo o, en caso contrario, tratarse de una tarjeta externa.

Bridges: Los bridges inalámbricos se usan generalmente para interconectar dos o más redes LAN cableadas. Los bridges se conectan entre ellos. Algunos bridges no permiten la conexión de estaciones de trabajo (sólo permiten conectarse con otro bridge). Se pueden utilizar para conectar dos edificios, quizás se requiera el uso de antenas externas para expandir la cobertura del enlace inalámbrico. Como el enlace se realiza en la capa de enlace de datos (Capa 2), es totalmente transparente para las estaciones de trabajo que se encuentran en las redes cableadas. Ambas redes forman parte del mismo segmento de capa 2.

Routers Los routers son dispositivos que implementan las funciones tradicionales de los routers, con las de un Access Point. En general incluyen una o más interfaces cableadas y una interface inalámbrica a través de un Access Point. Se utilizan mayormente para que un grupo de estaciones cableadas e inalámbricas se conecten a Internet.

Los routers más comunes incluyen una interface ethernet conectada mediante un puente a una interface inalámbrica, similar a cualquier Access Point. Estas dos interfaces conforman un segmento de capa 2, es decir, una red IP. Además cuentan con una segunda interface ethernet que se encuentra en otro segmento de capa 2. En general, esta interface se utiliza para conectar el vínculo a Internet.

Antenas Todos los dispositivos o adaptadores inalámbricos cuentan con antenas para la transmisión y recepción de los datos. En algunos casos, estas antenas se encuentran embebidas en el dispositivo, mientras que en otros casos son visibles y/o extraíbles. Estas antenas son conocidas como “Rubber duck” y ofrecen una cobertura limitada de la señal.

Una variedad de antenas opcionales de 2,4 GHz están disponibles para APs y bridges, que pueden utilizarse para reemplazar la antena estándar rubber ducky. Las antenas deberán escogerse cuidadosamente para asegurar la obtención de un rango y cobertura óptimos.

Cada antena tiene diferentes capacidades de ganancia y rango, amplitudes de rayo, cobertura y factores de forma. El acoplamiento de la antena correcta con el AP correcto permite una cobertura eficiente en cualquier instalación, así como una mejor confiabilidad a velocidades de datos más altas. Una cobertura detallada de las antenas se proporcionará posteriormente en el curso.

Los posibles modos de funcionamiento de los dispositivos de una red WLAN son los siguientes:

- ***Modo ad-hoc***: Permite la interconexión entre dispositivos de usuario sin necesidad de un

punto de acceso; cada estación inalámbrica se comunica directamente con las otras estaciones de la red.

- ***Modo infraestructura***: permite la conexión de las estaciones inalámbricas o dispositivos de usuario a un punto de acceso que es quién gestiona las conexiones. Las estaciones inalámbricas envían los paquetes al punto de acceso.

La mayor parte de las estaciones inalámbricas pueden funcionar en estos dos modos. Adicionalmente existen otros modos de funcionamiento no tan usuales en las estaciones inalámbricas que se describen a continuación:

- ***Modo master***: permite a la estación inalámbrica actuar como un punto de acceso para dar servicio y gestionar las conexiones de otros dispositivos.
- ***Modo monitor***: permite capturar paquetes sin asociarse a un punto de acceso inalámbrico de una red WLAN en modo infraestructura o sin asociarse a una red ad-hoc, es decir, permite monitorizar la red sin transmitir tráfico a la misma (forma pasiva).
- ***Modo promiscuo***: también permite capturar los paquetes de la red, pero en este caso es necesario estar asociado a la misma.

El modo monitor y el modo promiscuo son dos modos utilizados en ataques en redes WLAN

2.14.6 Arquitectura lógica

Conjunto de servicios básicos (BSS): El conjunto de servicios básicos (BSS) es el bloque constructor básico de una LAN IEEE 802.11. El BSS abarca una única área RF (un canal), o celda, según lo indica el círculo. A medida que una estación se aleja del AP, su velocidad de datos disminuirá. Cuando sale de su BSS, ya no puede comunicarse con otros miembros del mismo. Un BSS utiliza el modo de infraestructura, un modo que necesita un AP. Todas las estaciones se comunican por medio del AP, y no directamente. Un BSS tiene una única ID de conjunto de servicios (SSID).

BSS independiente (IBSS) El conjunto de servicios básicos independiente (IBSS) es el tipo más básico de LAN IEEE 802.11. Una LAN IEEE 802.11 mínima consiste sólo en dos estaciones. En este modo de operación, las estaciones IEEE 802.11 se comunican directamente. Puesto que este tipo de LAN IEEE 802.11 se forma a menudo sin pre-planificar, solamente mientras es necesaria una WLAN, a menudo se denomina red ad-hoc. Puesto que un IBSS consiste en estaciones conectadas directamente, también se denomina red peer-to-peer. Existe, por definición, sólo un BSS y no hay un Sistema de Distribución. Un IBSS puede tener una cantidad arbitraria de miembros. Para comunicarse fuera del IBSS, una de las estaciones debería actuar como gateway o router.

Sistema de distribución (DS) Las limitaciones de la capa física determinan las distancias de estación a estación que pueden soportarse. En el caso de algunas redes esta distancia es suficiente. En el caso de otras, se requiere un incremento en la cobertura. En lugar de existir independientemente, un BSS también puede formar un conjunto de servicios extendido (ESS). Un ESS se construye a partir de múltiples BSSs, que se conectan a través de APs. Los APs se conectan a través de un DS común. El DS puede ser cableado o inalámbrico, LAN o WAN. Cuando el DS es inalámbrico, se le llama WDS (Wireless Distribution System). El DS permite que existan dispositivos móviles proporcionando los servicios necesarios para manipular el mapeo de una dirección en movimiento y la integración transparente de múltiples BSSs. Los datos se desplazan entre un BSS y otro BSS a través del DS.

Conjunto de servicios extendido (ESS) Un conjunto de servicios extendido (ESS) se define como dos o más BSSs conectados por medio de un DS común. Esto permite la creación de una red inalámbrica de tamaño y complejidad arbitrarios. Al igual que sucede con un BSS, todos los paquetes de un ESS deben atravesar uno de los APs. Un concepto clave es que la red ESS se comporta de la misma manera que una red IBSS o que una única red BSS, es totalmente transparente para las estaciones. Las estaciones que se encuentran dentro de un ESS pueden comunicarse entre diferentes BSSs, y las estaciones móviles pueden desplazarse de un BSS a otro (dentro del mismo ESS), sin que esto afecte su conectividad.

Roaming: es el proceso o capacidad de un cliente inalámbrico de desplazarse de una celda, o BSS, a otra, sin perder conectividad con la red. Los access points se entregan el cliente entre sí y son invisibles al mismo. El estándar IEEE 802.11 no define cómo debería llevarse a cabo el roaming, pero sí define los bloques de construcción básicos, que incluyen la búsqueda activa y pasiva y un proceso de re-asociación. La re-asociación con el AP debe tener lugar cuando una estación hace roaming de un AP a otro.

2.14.7 Implicancias

Un desafío importante de las WLANs es la interferencia de las señales de radio. En diseños de área metropolitana de edificio a edificio, es posible tener interferencia de terceros, otras compañías que utilizan tecnología inalámbrica. En esta situación, los administradores de la red deben asegurarse de utilizar diferentes canales. La interferencia no puede detectarse hasta que el enlace no se implemente realmente. Puesto que los estándares 802.11 utilizan un espectro sin licencia, la mejor forma de evitar la interferencia es cambiar de canales. Muchos otros dispositivos, como los teléfonos portátiles, los hornos a microondas, los parlantes inalámbricos y los dispositivos de seguridad, utilizan también estas frecuencias. La cantidad de interferencia mutua que será experimentada por estos dispositivos de networking y otros planificados no está clara. La interferencia entre parlantes inalámbricos y otros dispositivos es común hoy en día. A medida que esta banda sin licencia se va poblando, es probable que aparezcan otros tipos de interferencia. Los objetos físicos y las estructuras de los edificios también crean diversos niveles de interferencia.

2.14.8 IEEE y 802.11

En el área de networking, el IEEE ha producido muchos estándares ampliamente utilizados como el grupo 802.x de estándares de red de área local (LAN) y los estándares de red de área metropolitana (MAN).

El Comité de Normalización LAN/MAN (LMSC) de IEEE 802 desarrolla estándares de red de área local (LAN) y de red de área metropolitana (MAN), principalmente para las dos capas inferiores del modelo de referencia de Interconexión de Sistemas Abiertos (OSI). LMSC, o IEEE Project 802, se coordina con otros estándares nacionales e internacionales. Algunos estándares que comenzaron aquí están publicados por el ISO como estándares internacionales.

El control de acceso al medio (MAC) y las capas físicas (PHY) están organizados en un conjunto separado de estándares desde el control de enlace lógico (LLC). Esto se debe a la interdependencia entre el control de acceso al medio, el medio y la topología de cada estándar. Al mismo tiempo, un único proceso LLC puede soportar las funciones lógicas para todos los protocolos MAC y PHY subyacentes.

El término 802.11 se refiere realmente a una familia de protocolos, incluyendo la especificación original, 802.11, 802.11b, 802.11a, 802.11g y otros. El 802.11 es un estándar inalámbrico que especifica conectividad para estaciones fijas, portátiles y móviles dentro de un área local. El propósito del estándar es proporcionar una conectividad inalámbrica para automatizar la maquinaria y el

equipamiento o las estaciones que requieren una rápida implementación. Éstos pueden ser portátiles, handheld o montados en vehículos en movimiento dentro de un área local.

El estándar 802.11 se denomina oficialmente Estándar IEEE para especificaciones MAC y PHY de WLAN. Define los protocolos por aire necesarios para soportar un networking inalámbrico en un área local. El servicio principal del estándar 802.11 es entregar Unidades MAC de Servicio de Datos (MSDUs) entre dispositivos peer LLC en la capa de enlace de datos. En general, una placa de radio, o NIC, y uno o más access points proporcionan las funciones del estándar 802.11.

Las características de MAC y PHY para las redes de área local inalámbricas (WLANs) están especificadas en 802.11, 802.11b, 802.11a, y 802.11g, entre otros estándares. La capa MAC de este estándar está diseñada para soportar unidades de capa física adicionales a medida que se adoptan, dependiendo de la capacidad del espectro y de las nuevas técnicas de modulación.

Número	Mensaje
802.11a	54 mbps WLAN en la banda 5GHz
802.11b	11 mbps WLAN en la banda 2.4GHz
802.11c	Cruces sin cables
802.11d	"Modo Mundial". Adaptación a los requerimientos regionales
802.11e	Qos y extenciones que fluyen a travez de 802.11a/g/h
802.11f	Transito para 802.11a/g/h (Protocolo de acceso a interno IAPP)
802.11g	54 mbps WLAN en la banda 2.4GHz
802.11h	802.11a con DFS Y TCP, "na Europa"
802.11i	Autenticacion y Encriptado (AES 802.1x)
802.11j	802.11a con canales adicionales por encima de 4.9GHz "na Japon"
802.11k	Intercambio de información de capacidad entre clientes y puntos de acceso
802.11l	no se usa debido al peligro de la confución típografica
802.11m	"Mantenimiento", publicación de acualizaciones estándar
802.11n	Nueva generación de WLAN de redes de al menos 100Mbps

Las redes inalámbricas tienen características fundamentales que las hacen significativamente diferentes a las LANs cableadas tradicionales. Algunos países imponen requisitos específicos para el equipamiento de radio además de aquéllos especificados en el estándar 802.11.

En las LANs inalámbricas, una dirección MAC equivale a una ubicación física. Esto se da por supuesto implícitamente en el diseño de LANs cableadas. En IEEE 802.11, la unidad direccionable es una estación (STA). La STA es el destino de un mensaje, pero no es, en general, una ubicación física fija.

Las capas físicas utilizadas en IEEE 802.11 son fundamentalmente diferentes de aquéllas utilizadas en medios alámbricos. Lo siguiente es cierto respecto a los protocolos PHY IEEE 802.11:

- Utilizan un medio que no tiene fronteras absolutas ni fácilmente observables, fuera de las cuales las estaciones no podrán enviar ni recibir frames de red.
- No están protegidos de señales externas.
- Se comunican a través de un medio que es significativamente menos confiable que los medios cableados.
- Tienen topologías dinámicas.
- Les falta una conectividad completa. Normalmente, se supone que cada STA puede escuchar a cada una de las otras STAs. Esta suposición es inválida en el caso de las WLANs. Las STAs

pueden estar "ocultas" entre sí.

- Tienen propiedades de propagación variables en el tiempo y asimétricas.

A causa de las limitaciones de los rangos PHY inalámbricos, las WLANs que necesitan cubrir distancias geográficas razonables deben construirse a partir de bloques de construcción de una cobertura básica.

Uno de los requisitos de IEEE 802.11 es manipular estaciones tanto móviles como portátiles. Una estación portátil se desplaza de ubicación a ubicación, pero sólo se utiliza mientras se encuentra en una ubicación fija. Las estaciones móviles en realidad acceden a la LAN mientras se encuentran en movimiento. No es suficiente para manipular sólo estaciones portátiles, puesto que los efectos de propagación desdibujan la distinción entre estaciones portátiles y móviles. Las estaciones fijas a menudo parecen ser móviles, debido a estos efectos de propagación.

Otro aspecto de las estaciones móviles es que a menudo reciben alimentación proveniente de baterías. De ahí que la administración de energía sea una consideración importante. Por ejemplo, no puede presuponerse que el receptor de una estación siempre estará encendido.

Se requiere IEEE 802.11 para aparecer en capas superiores, como LLC, como LAN IEEE 802. La red IEEE 802.11 debe manipular la movilidad de la estación dentro de la subcapa MAC.

IEEE 802.11: El término 802.11 se refiere realmente a una familia de protocolos, incluyendo la especificación original, 802.11, 802.11b, 802.11a, 802.11g y otros. El 802.11 es un estándar inalámbrico que especifica conectividad para estaciones fijas, portátiles y móviles dentro de un área local. El propósito del estándar es proporcionar una conectividad inalámbrica para automatizar la maquinaria y el equipamiento o las estaciones que requieren una rápida implementación. Éstos pueden ser portátiles, handheld o montados en vehículos en movimiento dentro de un área local. El estándar 802.11 se denomina oficialmente Estándar IEEE para especificaciones MAC (Capa de enlace de datos – Control de Acceso al Medio) y PHY (Capa Física) de WLAN. Define los protocolos por aire necesarios para soportar un networking inalámbrico en un área local. El servicio principal del estándar 802.11 es entregar tramas entre dispositivos pares que utilizan LLC en la capa de enlace de datos. En general, una placa de radio, o NIC, y uno o más access points proporcionan las funciones del estándar 802.11.

IEEE 802.11b: La norma IEEE 802.11b, quizás la mas difundida de todas, trabaja en un rango de frecuencias que van desde 2401MHz a 2495MHz. Presenta una división de este espectro en hasta 14 canales. Cada canal tiene un ancho de 22MHz.

La norma IEEE 802.11b especifica 4 anchos de banda del medio físico: 1 Mbps, 2Mbps, 5.5Mbps y 11Mbps. Una estación comenzará utilizando el mayor ancho de banda para ir decrementando dependiendo de la calidad y potencia de la señal que recibe. IEEE 802.11b transmite mediante una técnica llamada DSSS (Espectro Expandido de Secuencia Directa) y utiliza tres tipos diferentes de modulación, dependiendo de la velocidad de datos usada:

- Modulación por Desplazamiento de Fase Bivalente (BPSK): se utiliza para transmitir datos a 1 Mbps.
- Modulación por Desplazamiento de Fase en Cuadratura (QPSK): se utiliza para transmitir datos a 2 Mbps.
- Modulación de Código Complementario (CCK): CCK utiliza un conjunto complejo de funciones conocidas como códigos complementarios para enviar más datos. CCK es utilizado para transmitir datos a 5.5 Mbps y a 11 Mbps.

La distribución del ancho de banda se puede pensar como anillos concéntricos cuyo centro es el access point. En la medida que una estación se aleja del centro, se conectará a un ancho de banda menor.

IEEE.11a: La norma IEEE 802.11a fue la primer norma de alta velocidad, ofreciendo un ancho de banda de 54Mbps. Esta norma trabaja en el rango de frecuencias de 5GHz. Se decidió cambiar de frecuencia para lograr un mayor ancho de banda y para evitar interferencias con las redes IEEE 802.11b existentes. Como gran desventaja, al usar una frecuencia superior, las redes 802.11a tienen una cobertura menor, debido a que la señal sufre una mayor atenuación al traspasar paredes u obstáculos sólidos. Como trabajan en frecuencias diferentes, un dispositivo 802.11a no será compatible con un dispositivo 802.11b.

IEEE.11g: La especificación de la norma IEEE 802.11g opera en el rango de frecuencias de 2.4GHz, y ofrece un ancho de banda de 54Mbps. Opera en la misma frecuencia que la norma 802.11b, y se dedicó gran trabajo para hacerla compatible, permitiendo que coexista equipamiento b y g en la misma red. Sin embargo, la existencia de equipamiento b en una red g, reducirá su performance. Cabe recordar que en esta misma frecuencia podemos encontrarnos con interferencias de otro equipamiento inalámbrico, como teléfonos, micrófonos, etc. Similar a lo que ocurre en las normas vistas anteriormente, la provisión del ancho de banda va decreciendo conforme a la calidad y potencia de señal recibida por el cliente, con 54Mbps en el mejor de los casos, y disminuyendo a 48, 36, 24, 18, 12, 9, y 6, con el agregado de 11, 5.5, 2 y 1Mbps que aporta la norma 802.11b.

IEEE.11n: Es una propuesta de modificación al estándar IEEE 802.11-2007 para mejorar significativamente el desempeño de la red más allá de los estándares anteriores, tales como 802.11b y 802.11g, con un incremento significativo en la velocidad máxima de transmisión de 54 Mbps a un máximo de 600 Mbps. Actualmente la capa física soporta una velocidad de 300Mbps, con el uso de dos flujos espaciales en un canal de 40 MHz. Dependiendo del entorno, esto puede transformarse a un desempeño visto por el usuario de 100Mbps.

El estándar 802.11n fue ratificado por la organización IEEE el 11 de septiembre de 2009.

IEEE 802.11n está construido basándose en estándares previos de la familia 802.11, agregando multiple-input multiple-output (MIMO) y unión de interfaces de red (Channel Bonding), además de agregar tramas a la capa MAC.

MIMO usa múltiples antenas transmisoras y receptoras para mejorar el desempeño del sistema. MIMO es una tecnología que usa múltiples antenas para manejar más información (cuidando la coherencia) que utilizando una sóla antena. Dos beneficios importantes que provee a 802.11n son la diversidad de antenas y el multiplexado espacial.

La tecnología MIMO depende de señales multiruta. Las señales multiruta son señales reflejadas que llegan al receptor un tiempo después de que la señal de línea de visión (line of sight, LOS) ha sido recibida. En una red no basada en MIMO, como son las redes 802.11a/b/g, las señales multiruta son percibidas como interferencia que degradan la habilidad del receptor de recobrar el mensaje en la señal. MIMO utiliza la diversidad de las señales multirutas para incrementar la habilidad de un receptor de recobrar los mensajes de la señal.

Otra habilidad que provee MIMO es el Multiplexado de División Espacial (SDM). SDM multiplexa espacialmente múltiples flujos de datos independientes, transferidos simultáneamente con un canal espectral de ancho de banda. SDM puede incrementar significativamente el desempeño de la transmisión conforme el número de flujos espaciales es incrementado. Cada flujo espacial requiere una antena discreta tanto en el transmisor como el receptor. Además, la tecnología MIMO requiere una cadena de radio frecuencia separada y un convertir de análogo a digital para cada antena MIMO lo cual incrementa el costo de implantación comparado con sistemas sin MIMO.

Channel Bonding, también conocido como 40Mhz o unión de interfaces de red, es la segunda tecnología incorporada al estándar 802.11n la cual puede utilizar dos canales separados, que no se solapen, para transmitir datos simultáneamente. La unión de interfaces de red incrementa la cantidad de datos que pueden ser transmitidos. Se utilizan dos bandas adyacentes de 20Mhz cada una, por eso el nombre de 40Mhz. Esto permite doblar la velocidad de la capa física disponible en un solo canal de 20Mhz. (Aunque el desempeño del lado del usuario no será doblado.)

Utilizar conjuntamente una arquitectura MIMO con canales de mayor ancho de banda ofrece la oportunidad de crear sistemas muy poderosos y rentables para incrementar la velocidad de transmisión de la capa física.

2.14.9 Método de acceso al medio CSMA/CA

En las redes inalámbricas se define un método de acceso al medio llamado CSMA/CA (Carrier Sense, Multiple Access with Collission Avoidance) diferente que para las redes ethernet cableadas. En las redes tradicionales se utiliza el método CSMA/CD. Todas las técnicas CSMA parten de la existencia de un medio común de transmisión que debe ser compartido por todas las estaciones interesadas en transmitir. Si en un determinado momento, más de una estación transmite simultáneamente, existirá una colisión y los datos transmitidos se perderán.

CSMA/CD: Repasemos primero el funcionamiento del control de acceso al medio en las redes tradicionales. Cuando una estación quiere transmitir, primero realiza un censado del medio para asegurarse que se encuentre libre. Si el medio esta ocupado, espera un tiempo y vuelve a intentar. Si el medio está libre, la estación comienza su transmisión. Mientras está transmitiendo, continúa escuchando el medio para verificar que la información transmitida no ha colisionado con otra. Si finaliza su transmisión sin detectar una colisión, entonces se toma la transmisión como exitosa. En caso que se detecte una colisión, se procede a esperar un tiempo aleatorio y volver a intentar la transmisión.

CSMA/CA: Debido a las particularidades que tiene el aire para la dispersión de la señal, donde la transmisión puede se diseminará ocupando todo el medio, no se puede implementar la detección de colisiones. Las colisiones deben ser eliminadas. Para lograr esto, el control de acceso al medio en las redes 802.11 es CSMA/CA, donde se implementa una técnica para evitar que las estaciones colisionen entre sí. La modificación implementada por CSMA/CA es sencilla, se agregan avisos y confirmaciones de transmisión:

- Antes de transmitir, un nodo debe enviar un “Pedido de Transmisión” RTS (Request To Send), donde especifica el origen y destino.
- Cuando el destino recibe el RTS, puede confirmar mediante un “Preparado para transmitir” CTS (Clear To Send) o rechazar la transmisión con un mensaje de “Ocupado” RxBUSY.
- Si el transmisor recibe un RxBUSY aborta la transmisión. Si recibe un CTS, comienza a transmitir.
- Una vez que finalizó la transmisión, el receptor debe enviar una confirmación de recepción. Si fue correcta, envía un Acuse positivo ACK (Acknowledgement) y finaliza el proceso. Si fue errónea, envía un Acuse negativo NACK (Not Acknowledgement) y el emisor intentará retransmitir la trama.

La performance real que se puede obtener en una red inalámbrica se encuentra muy por debajo del ancho de banda que provee el enlace físico. Diferentes factores afectan a la performance, algunos de ellos podemos mejorarlos y otros son intrínsecos de la tecnología utilizada.

Para conocer las limitaciones de la performance, debemos partir del análisis del Método de Acceso al Medio que se utiliza (CSMA/CA). Este método impide que dos o más estaciones transmitan simultáneamente (porque llevaría a una colisión), mediante la reserva del medio previo a la transmisión (RTS). Esto significa que si una estación quiere transmitir 1 trama de datos, antes de lograr su transmisión efectiva, debe enviar un RTS y esperar a recibir un CTS. Y una vez transmitido, quedará a la espera de la confirmación ACK enviada por el destinatario. Todo este proceso lleva a que la performance máxima que se puede lograr en una red 802.11 no será superior al 50% del ancho de banda del medio. Esto quiere decir que para una red 802.11g, donde el ancho de banda del medio es de 54Mbps, nunca tendremos tasas de transferencia superiores a 27Mbps. Otro factor que afecta de manera directa al ancho de banda es la cantidad de estaciones que existen en el BSS. Cuanto mayor sea el número de estaciones intentando transmitir, menor será la porción de ancho de banda para cada una.

Otra consideración a tener en cuenta es la existencia de repetidores. Cuando un AP no nos alcanza para cubrir el radio necesario, y no tenemos alcance a través de la infraestructura cableada, podemos utilizar repetidores inalámbricos, formando una topología.

Cuando existen dispositivos de diferente ancho de banda dentro de una red, como por ejemplo dispositivos 802.11b y G asociados al mismo AP, existe una modificación en el método de transmisión. Como se vio anteriormente, el ancho de banda máximo alcanzable en una red 802.11g será de 27Mbps. Sin embargo, cuando existen dispositivos 802.11b, el AP debe asignar un tiempo para darles la posibilidad de transmitir y que no queden en una espera infinita de liberación del canal. Para asignar este tiempo se agregan mecanismos de protección en la transmisión de los RTS y CTS y se modifican algunos temporizadores de transmisión. Tomando estas modificaciones, cuando un AP 802.11g tiene habilitada la compatibilidad con 802.11b, tendrá una performance máxima de 18Mbps. Y esto suponiendo que no existen clientes 802.11b transmitiendo, sólo por el hecho de ofrecer la compatibilidad es que la performance sufre este impacto. Si agregamos dispositivos 802.11b, estos dispositivos tienen una performance máxima de 6Mbps, mientras que un 802.11g tendrá 18Mbps. Lo que significa que un 802.11B tardará tres veces más en transmitir que un 802.11G.

Cuando tenemos que cubrir grandes espacios con conectividad inalámbrica, debemos realizar una planificación en la asignación de canales y la ubicación de los APs, para aprovechar de la mejor manera el ancho de banda disponible. Recordemos que en una red 802.11a existen 8 canales sin solapamiento, mientras que en una red 802.11b/g existen sólo 3. El objetivo de la planificación de APs y canales es evitar que exista un solapamiento entre las señales de dos dispositivos adyacentes. Para esto debemos organizar una estructura de celdas, donde cada celda utiliza un canal y sus celdas adyacentes utilizan canales no solapados.

2.14.10 Servicios MAC

Un aspecto de la definición de estándares para una red inalámbrica interoperable es proporcionar estándares para servicios en las capas MAC y física (PHY). Tres servicios son proporcionados por la subcapa MAC en IEEE 802.11. Estos servicios son los siguientes:

1. Servicio de datos asíncronos
2. Servicios de seguridad
3. Ordenamiento de MSDUs

Servicio de datos asíncronos: Este servicio proporciona a las entidades peer LLC la capacidad para intercambiar unidades de datos de servicios MAC (MSDUs). Para soportar este servicio la MAC local utiliza los servicios de nivel PHY subyacentes para transportar una MSDU a una entidad MAC peer, donde se la entregará a la LLC peer. Ese transporte MSDU asíncrono se lleva a cabo sobre una base de mayor esfuerzo y sin conexión. No existen garantías de que la MSDU se entregará exitosamente.

El transporte broadcast y multicast es parte del servicio de datos asíncrono proporcionado por la MAC. Debido a las características del medio inalámbrico, las MSDUs broadcast y multicast pueden experimentar una más baja calidad de servicio, en comparación a la de las MSDUs unicast. Todas las STAs soportan el servicio de datos asíncrono.

Servicios de seguridad: Los servicios de seguridad de IEEE 802.11 son proporcionados por el servicio de autenticación y el mecanismo de Privacidad Equivalente a la Cableada (WEP). El alcance de los servicios de seguridad proporcionados se limita a un intercambio de datos de estación a estación. El servicio de privacidad ofrecido por la implementación WEP IEEE 802.11 es el cifrado de la MSDU. Para los propósitos de este estándar, WEP se visualiza como servicio de capa lógica ubicado dentro de la subcapa MAC. La implementación real del servicio WEP es transparente para la LLC y para las otras capas que se encuentran por encima de la subcapa MAC. Los servicios de seguridad proporcionados por la WEP en IEEE 802.11 fueron diseñados para soportar los siguientes objetivos de seguridad:

- Confidencialidad
- Integridad de los datos
- Control de acceso

Ordenamiento de MSDUs: Los servicios proporcionados por la subcapa MAC permiten, y pueden requerir, el reordenamiento de las MSDUs. La MAC reordenará intencionalmente las MSDUs, sólo si es necesario para aumentar la probabilidad de una entrega exitosa basada en el modo operativo actual ("administración de energía") de la(s) estación o estaciones receptora(s). El único efecto de este reordenamiento es un cambio en el orden de la entrega de MSDUs broadcast y multicast. Este cambio es relativo a MSDUs dirigidas, o unicast, que se originan desde una única dirección de estación de origen. A las MSDUs unicast se les otorga prioridad sobre las multicast y broadcast.

Todas las estaciones deben construir frames para la transmisión y decodificación de los frames al recibirlos, basándose en un formato de frames estándar. Las unidades de datos del protocolo MAC (MPDUs), o frames, se describen como una secuencia de campos en un orden específico, como lo muestra la actividad que aparece más abajo.

Cada frame consiste en los siguientes componentes básicos:

- Un encabezado MAC, que consiste en información acerca del control de frames, la duración, la dirección y el control de las secuencias
- Un cuerpo de frames de longitud variable, que contiene información específica del tipo de frame. Por ejemplo, en los frames de datos, esto contendría datos de la capa superior
- Una secuencia de verificación de frames (FCS), que contiene una verificación de redundancia cíclica (CRC) IEEE de 32 bits

Los tres tipos principales de frames utilizados en la capa MAC son los siguientes:

1. *Frames de datos*
2. *Frames de control*
3. *Frames de administración*

Los frames de datos se utilizan para la transmisión de datos. Los frames de control, como la Solicitud para Enviar (RTS), Despejado para Enviar (CTS) y Confirmación (ACK), controlan el acceso al medio utilizando frames RTS, CTS y ACK. Los frames de administración, como los frames baliza, se transmiten de la misma manera en que los frames de datos intercambian la información de

administración, pero no se envían a las capas superiores.

Arquitectura MAC: Antes de transmitir un frame, una STA debe obtener acceso al medio utilizando uno de dos métodos

1. El método de acceso fundamental del MAC IEEE 802.11, acceso múltiple con detección de portadora y colisión evitable (CSMA/CA), se denomina Función de Coordinación Distribuida (DCF). La DCF se implementa en todas las STAs, para su uso tanto en configuraciones de red ad hoc como de infraestructura.
2. El MAC IEEE 802.11 MAC también puede incorporar un método de acceso opcional, denominado Función de Coordinación de Punto (PCF), que crea un acceso libre de contención (CF). La PCF sólo puede utilizarse en configuraciones de red de infraestructura.

Coexistencia de DCF y PCF: La DCF y la PCF pueden operar ambas concurrentemente dentro del mismo BSS. Cuando éste es el caso, los dos métodos de acceso se alternan, con un periodo de CF seguido por un periodo de contención. Además, todas las transmisiones bajo la PCF pueden utilizar el Espacio Interframe (IFS), que es más pequeño que el utilizado para los frames transmitidos por medio de la DCF. El uso de IFSs más pequeños implica que el tráfico coordinado por punto tendrá un acceso de prioridad al medio a través de STAs que operan en modo DCF.

La capa MAC es sólo la mitad de la operación total de 802.11. El estándar de capa física (PHY) es la otra mitad. La mayoría de las definiciones de PHY contienen tres entidades funcionales, Diferentes PHYs se definen como parte del estándar IEEE 802.11.

Procedimiento de convergencia de la capa física (PLCP): La función de convergencia de PHY adapta las capacidades del sistema dependiente del medio físico (PMD) para el servicio MAC. PLCP define un método para mapear las unidades de datos de protocolo de subcapa MAC (MPDUs) en un formato de framing apto para su envío y recepción entre dos o más STAs utilizando el sistema PMD asociado. El PHY intercambia unidades de datos de protocolo PHY (PPDUs) que contienen una MPDU, más información adicional acerca de encabezados para los transmisores y receptores de la capa física. El PLCP también entrega frames entrantes desde el medio inalámbrico a la subcapa MAC.

El servicio de PHY es proporcionado a la entidad MAC de la STA a través de un access point de servicio (SAP), denominado SAP PHY.

Sistema dependiente del medio físico (PMD): El sistema PMD define las características y métodos de transmisión y recepción de datos a través de un medio inalámbrico entre dos o más STAs, cada una de ellas utilizando el mismo sistema PHY. También se definen conjuntos de primitivos, para describir la interfaz entre el PLCP y la subcapa PMD. La interfaz se denomina SAP PMD.

La subcapa PMD acepta los primitivos del servicio de la subcapa PLCP y proporciona el medio mediante el cual se transmiten o reciben realmente los datos provenientes del medio. El flujo de datos, la información de temporización y los parámetros de la señal recibidos se entregan a la subcapa PLCP. Una funcionalidad similar se proporciona para la transmisión de datos.

2.14.11 Ondas

El diccionario Webster define una onda como: una "perturbación o variación" que pasa a través de un medio. El medio a través del cual viaja la onda puede experimentar algunas oscilaciones de índole local a medida que la onda pasa, pero las partículas del medio no viajan con la onda. La perturbación puede asumir cualquier cantidad de formas, desde un impulso de amplitud finito hasta una onda sinusoidal infinitamente larga.

Una forma de onda es una representación de cómo la corriente alterna (AC) varía con el tiempo. La

forma de onda AC familiar es la onda sinusoidal, que deriva su nombre del hecho de que la corriente o voltaje varía según la función sinusoidal matemática del tiempo transcurrido. La onda sinusoidal es única por el hecho de que representa energía enteramente concentrada en una única frecuencia. Una señal inalámbrica ideal asume una forma de onda sinusoidal, con una frecuencia usualmente medida en ciclos por segundo o Hertz (Hz). Un millón de ciclos por segundo está representado por un megahertz (MHz). Un billón de ciclos por segundo está representado por un gigahertz (GHz). Una onda sinusoidal tiene varias propiedades básicas:

- Amplitud — La distancia de cero al valor máximo de cada ciclo se denomina amplitud. La amplitud positiva del ciclo y la amplitud negativa del ciclo son las mismas.
- Periodo — El tiempo que le lleva a una onda sinusoidal completar un ciclo se define como periodo de la forma de onda. La distancia que viaja el seno durante este periodo se denomina longitud de onda.
- Longitud de onda — La longitud de onda, indicada por el símbolo griego lambda l, es la distancia a través de la forma de onda desde un punto al mismo punto del siguiente ciclo.
- Frecuencia — La cantidad de repeticiones o ciclos por unidad de tiempo es la frecuencia, expresada en general en ciclos por segundo, o Hz.

2.14.12 Watts

Para comprender qué es un watt, se debe considerar primero la energía. Una definición de energía es la capacidad para producir trabajo. Existen muchas formas de energía, incluyendo energía eléctrica, energía química, energía térmica, energía potencial gravitatoria, energía cinética y energía acústica. La unidad métrica de la energía es el Joule. La energía puede considerarse una cantidad.

Un watt es la unidad básica de potencia, y la potencia está relacionada con la energía. No obstante, potencia es un índice, y energía una cantidad. La fórmula para la potencia es

P = DE / Dt

- DE es la cantidad de energía transferida.
- Dt es el intervalo temporal durante el cual se transfiere la energía.

Si un Joule de energía se transfiere en un segundo, esto representa un watt (W) de potencia. Un watt se define como un ampère (A) de corriente por un volt (V).

El FCC de EE.UU. permite que se emita un máximo de cuatro watts de energía en las transmisiones WLAN en la banda no licenciada de 2,4 GHz. En las WLANs, los niveles de energía son tan bajos como un miliwatt (mW), o una milésima (1/1000) de watt, que pueden utilizarse en un área pequeña. Los niveles de energía en un único segmento de WLAN son raramente más elevados que 100 mW, lo suficiente para comunicarse a una distancia de hasta tres cuartos de un kilómetro o media milla bajo condiciones óptimas. Los access points en general tienen la capacidad para radiar desde 30 a 100 mW, dependiendo del fabricante. Las aplicaciones para exteriores de edificio a edificio son las únicas que utilizan niveles de potencia por encima de los 100 mW.

2.14.13 Decibeles

El decibel (dB) es una unidad que se utiliza para medir la potencia eléctrica. Un dB es un décimo de un Bel, que es una unidad de sonido más grande así denominada en homenaje a Alexander Graham Bell. El dB se mide en una escala logarítmica base 10.

La base se incrementa en diez veces diez por cada diez dB medidos. Esta escala permite a las

personas trabajar más fácilmente con grandes números. Una escala similar (la escala de Richter) se utiliza para medir terremotos. Por ejemplo, un terremoto de magnitud 6.3 es diez veces más fuerte que un terremoto de 5.3.

Puesto que dB no tiene ninguna referencia definida en particular, el dBx, donde la x representa un valor específico, se utiliza a menudo en lugar del dB. Por ejemplo, el dBm hace referencia al miliwatt. Puesto que el dBm tiene una referencia definida, también puede convertirse a watts, si se lo desea. La ganancia o pérdida de potencia en una señal se determina comparándola con este punto de referencia fijo, el miliwatt. Existen varios términos relacionados con los que uno debería familiarizarse, para diseñar e instalar WLANs apropiadamente:

- **dB miliWatt (dBm)** — Ésta es la unidad de medida del nivel de potencia de una señal. Si una persona recibe una señal de un miliwatt, esto representa una pérdida de cero dBm. No obstante, si una persona recibe una señal de 0,001 miliwatts, entonces tiene lugar una pérdida de 30 dBm. Esta pérdida se representa de la forma -30 dBm. Para reducir la interferencia con otras, los niveles de potencia de una WLAN 802.11b están limitados por los siguientes organismos:
    - 36 dBm de EIRP según el FCC
    - 20 dBm de EIRP según el ETSI
- **dB dipolo (dBd)** — Esto se refiere a la ganancia que tiene una antena, en comparación con la antena dipolo de la misma frecuencia. Una antena dipolo es la antena más pequeña y menos práctica en cuanto a la ganancia que puede obtenerse.
- **dB isotrópico (dBi)** — Esto se refiere a la ganancia que tiene una determinada antena, en comparación con una antena isotrópica, o de origen puntual, teórica. Desafortunadamente, una antena isotrópica no puede existir en el mundo real, pero es útil para calcular áreas de cobertura y debilitamiento teóricas.
    - Una antena dipolo tiene una ganancia de 2,14 dB por encima de la ganancia de una antena isotrópica de 0 dBi. Por ejemplo, una simple antena dipolo tiene una ganancia de 2,14 dBi o 0 dBd.
- Potencia Irradiada Isotrópica Efectiva (EIRP) — La EIRP se define como la potencia efectiva que se halla en el lóbulo principal de la antena transmisora. Es igual a la suma de la ganancia de la antena, en dBi, más el nivel de potencia, en dBm, que entra a la antena.
- Ganancia — Esto se refiere al incremento en la energía que parece agregar una antena a una señal RF. Existen diferentes métodos para medir esto, dependiendo del punto de referencia elegido. Cisco Aironet inalámbrico se estandariza en dBi para especificar mediciones de ganancia. Algunas antenas se clasifican en dBd. Para convertir cualquier número de dBd a dBi, simplemente agregue 2,14 al número de dBd.

2.14.14 Ondas Electromagnéticas

Espectro EM es simplemente un nombre que los científicos han otorgado al conjunto de todos los tipos de radiación, cuando se los trata como grupo. La radiación es energía que viaja en ondas y se dispersa a lo largo de la distancia. La luz visible que proviene de una lámpara que se encuentra en una casa y las ondas de radio que provienen de una estación de radio son dos tipos de ondas electromagnéticas. Otros ejemplos son las microondas, la luz infrarroja, la luz ultravioleta, los rayos X y los rayos gamma.

Todas las ondas EM viajan a la velocidad de la luz en el vacío y tienen una longitud de onda (l) y frecuencia (f), que pueden determinarse utilizando la siguiente ecuación:

c = l x f, donde c = velocidad de la luz (3 x 108 m/s)

Esta fórmula enuncia que la longitud de onda de cualquier onda EM viajando en el vacío, en metros, multiplicada por la frecuencia de la misma onda EM, en Hz, siempre es igual a la velocidad de la luz o 3 x 108 m/s o 186.000 millas por segundo (aproximadamente 300.000 km/s).

Uno de los diagramas más importantes tanto en ciencia como en ingeniería es la gráfica del espectro EM. El diagrama del espectro EM típico resume los alcances de las frecuencias, o bandas que son importantes para comprender muchas cosas en la naturaleza y la tecnología. Las ondas EM pueden clasificarse de acuerdo a su frecuencia en Hz o a su longitud de onda en metros. El espectro EM tiene ocho secciones principales, que se presentan en orden de incremento de la frecuencia y la energía, y disminución de la longitud de onda:

1. **Ondas de potencia** — Ésta es la radiación EM más lenta y por lo tanto también tiene la menor energía y la mayor longitud de onda.
2. **Ondas de radio** — Ésta es la misma clase de energía que emiten las estaciones de radio al aire para que un aparato de radio la capture y la reproduzca. No obstante, otras cosas, como las estrellas y los gases del espacio también emiten ondas de radio. Muchas funciones de comunicación utilizan ondas de radio.
3. **Microondas** — Las microondas cocinan maíz inflado en pocos minutos. En el espacio, los astrónomos utilizan las microondas para aprender acerca de la estructura de las galaxias cercanas.
4. **Luz infrarroja (IR)** — El infrarrojo a menudo se considera igual que el calor, porque hace que sintamos tibia nuestra piel. En el espacio, la luz IR sirve para rastrear el polvo interestelar.
5. **Luz visible** — Éste es el rango visible para el ojo humano. La radiación visible es emitida por todo, desde luciérnagas hasta lámparas y estrellas. También es emitida por partículas en rápido movimiento que golpean a otras partículas.
6. **Luz ultravioleta (UV)** — Es bien conocido que el sol es una fuente de radiación ultravioleta (UV). Son los rayos UV los que hacen que la piel se queme. Las estrellas y otros objetos calientes del espacio emiten radiación UV.
7. **Rayos X** — Un doctor utiliza rayos X para observar los huesos y un dentista los utiliza para observar los dientes. Los gases calientes del universo también emiten rayos X.
8. **Rayos gamma** — Los materiales radioactivos naturales y fabricados por el hombre pueden emitir rayos gamma. Los grandes aceleradores de partículas que los científicos utilizan para ayudarlos a comprender de qué está hecha la materia pueden irradiar en ocasiones rayos gamma. No obstante, el mayor generador de rayos gamma de todos es el universo, que crea radiación gamma de muchas formas.

El espectro RF incluye varias bandas de frecuencia incluyendo las microondas y las Frecuencias Ultra Altas (UHF) y Frecuencias Muy Altas (VHF) de emisión de radio terrestre y televisión. Aquí es también donde operan las WLANs. El espectro RF tiene un rango que va desde los nueve kHz a miles de GHz. Realmente consiste en dos secciones importantes del espectro EM, ondas de radio y microondas. Por razones históricas, mucha gente se refiere a ambas secciones juntas como espectro RF. Las frecuencias RF, que abarcan una porción significativa del espectro de radiación EM, se utilizan mucho para las comunicaciones. La mayoría de los rangos RF son licenciados, aunque unos pocos rangos se utilizan sin licencia.

Cuando dos ondas EM ocupan el mismo espacio, sus efectos se combinan para formar una nueva onda de diferente forma. Por ejemplo, los cambios en la presión del aire ocasionados por dos ondas de sonido se suman. Las fuerzas eléctricas y magnéticas ocasionadas por dos ondas luminosas o dos ondas de radio también se suman.

Jean Baptiste Fourier es responsable de un importante descubrimiento matemático. Descubrió que una suma especial de ondas sinusoidales, de frecuencias relacionadas armónicamente, podían

sumarse para crear cualquier patrón de ondas. Las frecuencias relacionadas armónicamente son frecuencias simples que son múltiplos de cierta frecuencia básica. Ondas complejas pueden construirse en base a ondas simples. Otra forma de enunciar esto es que cualquier onda reiterativa es matemática y físicamente equivalente al resultado de tan sólo sumar el conjunto correcto de ondas sinusoidales. Esta suma se denomina serie de Fourier.

Es cierto que existe una cantidad infinita de diferentes frecuencias de ondas EM. No obstante, hablando en términos prácticos, cualquier creación de ondas EM realmente ocupa más que una cantidad infinitesimal de espacio de frecuencia. Por lo tanto, las bandas de frecuencia tienen una cantidad limitada de frecuencias, o canales de comunicaciones utilizables diferentes. Muchas partes del espectro EM no son utilizables para las comunicaciones y muchas partes del espectro ya son utilizadas extensamente con este propósito. El espectro electromagnético es un recurso finito. Una forma de adjudicar este recurso limitado y compartido es disponer de instituciones internacionales y nacionales que configuren estándares y leyes respecto a cómo puede utilizarse el espectro. En EE.UU., es el FCC el que regula el uso del espectro. En Europa, el Instituto Europeo de Normalización de las Telecomunicaciones (ETSI) regula el uso del espectro.

Las bandas de frecuencia reguladas se denominan espectro licenciado. Ejemplos de éste incluyen la radio de Amplitud Modulada (AM) y Frecuencia Modulada (FM), la radio de radioaficionados o de onda corta, los teléfonos celulares, la televisión por aire, las bandas de aviación y muchos otros. Para poder operar un dispositivo en una banda licenciada, el usuario debe solicitar primero y luego otorgársele la licencia apropiada.

2.14.15 Señales

Un osciloscopio es un dispositivo electrónico importante y sofisticado que se utiliza para estudiar las señales eléctricas. Un osciloscopio puede graficar ondas, impulsos y patrones eléctricos. Consta de un eje x que representa el tiempo y de un eje y que representa el voltaje. Usualmente existen dos entradas de voltaje al eje y, por lo cual dos ondas pueden observarse y medirse al mismo tiempo.

El estudio de cómo las señales varían con el tiempo se denomina análisis del dominio de tiempo. Otra forma de aprender acerca de las señales es analizar las frecuencias que utilizan. Los ingenieros se refieren a este proceso como análisis del dominio de frecuencia. Un dispositivo electrónico denominado analizador de espectro crea gráficas de potencia versus frecuencia.

Para comprender el análisis del dominio de frecuencia en lo que tiene que ver con las WLANs, es útil examinar primero un sistema de radio más familiar, para ser más precisos, las emisoras de radio FM comerciales. En este caso, el término radio se refiere a un dispositivo receptor, que podría estar ubicado en una casa o automóvil.

Cuando se sintoniza una radio FM, se cambia la configuración de la misma, de modo tal que ésta responda a la frecuencia seleccionada. Las diferentes estaciones tienen cada una un centro o frecuencia portadora diferente. Esto es así porque no interfieren entre sí, transmitiendo en las mismas frecuencias. Además, dependiendo de factores tales como la potencia transmisora y la ubicación de una estación, así como cualquier obstáculo potencial, la fortaleza de la señal en el receptor de radio FM puede ser débil o fuerte. Estos mismos factores existen en una WLAN. Por ejemplo, para obtener el mayor beneficio de múltiples APs en la misma ubicación, es importante que no se superpongan sus frecuencias. De otro modo, los APs interferirán entre sí en lugar de multiplicar la cantidad de ancho de banda utilizable por la cantidad de APs.

Un concepto muy importante en los sistemas de comunicaciones, incluyendo las WLANs, es el ruido. La palabra ruido tiene el significado general de sonidos indeseables. No obstante, en el contexto de las telecomunicaciones, el ruido puede definirse mejor como voltajes indeseables provenientes de fuentes naturales y tecnológicas. Puesto que el ruido es sólo otra señal que produce ondas, puede

agregarse a otras señales, como se trató anteriormente. Si la señal afectada representa información en un sistema de comunicaciones, el ruido puede cambiar la información. Es claro que esto no es aceptable.

En lo que respecta a una WLAN, las fuentes de ruido incluyen la electrónica del sistema de la WLAN, más la interferencia de frecuencia de radio (RFI), y la interferencia electromagnética (EMI) que se encuentra en el entorno WLAN. Estudiando el ruido, la gente puede reducir sus efectos en el sistema WLAN.

Una forma de ruido se denomina de Gauss, o ruido blanco. El analizador espectroscópico de ruido blanco es una línea recta a través de todas las frecuencias. En teoría, el ruido de Gauss afecta a todas las diferentes frecuencias de igual forma. En realidad, el ruido blanco no sigue un patrón tan simple. No obstante, éste es aún un concepto muy útil, al estudiar sistemas de comunicaciones. Puesto que el ruido blanco afectaría de igual forma a todas las frecuencias de una señal de radio, existen implicaciones para los circuitos tanto del transmisor como del receptor. Otra forma de ruido se denomina interferencia de banda angosta. El término banda se refiere a una agrupación de frecuencias. Una banda angosta tiene un rango de frecuencias relativamente más pequeño. La radio FM es un ejemplo de interferencia de banda angosta. Aunque el ruido blanco perturbaría de igual forma a todas las estaciones de radio, la interferencia de banda angosta sólo interferiría con algunas estaciones de radio.

Ambas formas de ruido son importantes para comprender las WLANs. Puesto que el ruido blanco degradaría los diversos canales de igual forma, los diversos componentes de FHSS y DSSS se verían igualmente afectados. La interferencia de banda angosta podría perturbar sólo a ciertos canales o a extensos componentes del espectro. Incluso podría ser posible utilizar un canal diferente para evitar la interferencia por completo.

2.14.16 Acceso Múltiple y ancho de banda

Un problema fundamental de las comunicaciones inalámbricas es que la atmósfera es un medio compartido. ¿Cómo hacen dos o más usuarios para acceder al mismo medio sin que surjan colisiones? Una forma de tratar el acceso compartido es hacer que una autoridad oficial como el FCC o el ETSI establezcan el uso de frecuencias fijas. De esta forma, las diversas estaciones que buscan transmitir pueden hacerlo simultáneamente, sin colisiones, mientras utilicen sus frecuencias de portadora asignadas y sigan las reglas de potencia e interferencia. Los receptores deben sintonizar la frecuencia portadora, para obtener broadcasts de una estación específica. Un buen ejemplo de esto es la radio de emisiones comerciales de FM.

Las redes de telefonía celular han utilizado, en diversos momentos, varios métodos diferentes para compartir su medio. Existen tres técnicas principales que se han utilizado para compartir las ondas por aire:

1. **Acceso Múltiple por División de Tiempo (TDMA)** — Cada dispositivo puede utilizar todo el espectro disponible en la célula, pero sólo durante un periodo breve.
2. **Acceso Múltiple por División de Frecuencia (FDMA)** — Cada dispositivo puede utilizar una porción del espectro disponible, durante tanto tiempo como lo necesite el dispositivo, mientras se encuentra en la célula.
3. **Acceso Múltiple por División de Código (CDMA)** — Esta técnica es realmente una combinación de las dos anteriores. Se trata del sistema más avanzado y el que está conduciendo a las tecnologías inalámbricas móviles de Tercera Generación (3G).

2.14.17 Propagación de RF

El estudio de cómo las ondas EM viajan e interactúan con la materia puede volverse extremadamente

complejo. No obstante, existen varias simplificaciones importantes que pueden llevarse a cabo, para estudiar más fácilmente las propiedades de las ondas EM. Históricamente, estas simplificaciones se desarrollaron para las ondas luminosas, pero también se aplican a las ondas de radio, las microondas y todo el espectro EM.

En el vacío, las microondas de 2,4 GHz viajan a la velocidad de la luz. Una vez que se originan, estas microondas continuarán en la dirección en la cual fueron emitidas para siempre, a menos que interactúen con alguna forma de materia. El rayo geométrico se utiliza para significar que las microondas están viajando en espacio libre. Puesto que las WLANs se encuentran usualmente en tierra, dentro de la atmósfera, las microondas viajan por el aire, no en el vacío. No obstante, en la siguiente sección el alumno verá que esto no cambia significativamente su velocidad.

De manera similar a la luz, cuando la RF viaja a través de materia transparente, algunas de las ondas se ven alteradas. Por lo tanto, la velocidad de las microondas de 2,4 GHz y 5 GHz también cambia, a medida que las ondas viajan a través de la materia. No obstante, la cantidad de la alteración depende mucho de la frecuencia de las ondas y de la materia. En las siguientes dos secciones, se estudiarán algunos de los fenómenos que pueden afectar las ondas de radio de una WLAN a medida que viajan a través de la materia.

2.14.18 Refracción

Una superficie se considera lisa si el tamaño de las irregularidades es pequeño, en relación a la longitud de onda. De otro modo, se la considera irregular. Las ondas electromagnéticas se difractan alrededor de objetos interpuestos. Si el objeto es pequeño en relación a la longitud de onda, tiene muy poco efecto. La onda pasará alrededor del objeto sin perturbaciones. No obstante, si el objeto es grande, aparecerá una sombra detrás del mismo y una cantidad de energía significativa se refleja nuevamente hacia el origen. Si el objeto tiene alrededor del mismo tamaño que la longitud de onda, las cosas se complican, y aparecen patrones de difracción interesantes. Las ondas de radio también cambian de dirección al entrar en materiales diferentes. Esto puede ser muy importante al analizar la propagación en la atmósfera. No sólo es muy significativo para las WLANs, sino que se incluye aquí, como parte del trasfondo general para el comportamiento de las ondas electromagnéticas.

2.14.19 Reflexión

La reflexión tiene lugar cuando la luz rebota en la dirección general de la cual provino. Consideremos una superficie metálica lisa como interfaz. A medida que las ondas golpean la superficie, gran parte de su energía rebotará o se reflejará. Pensemos en experiencias comunes, como mirarse al espejo u observar la luz del sol reflejándose desde una superficie metálica o agua. Cuando las ondas viajan de un medio a otro, un determinado porcentaje de la luz se refleja. Esto se denomina reflexión de Fresnel.

Las ondas de radio también se reflejan al entrar en diferentes medios. La ley de reflexión puede describir estas reflexiones. Las ondas de radio pueden rebotar desde diferentes capas de la atmósfera. Las propiedades reflexivas del área donde ha de instalarse la WLAN son extremadamente importantes y pueden determinar si una WLAN funciona o falla. Además, los conectores a ambos extremos de la línea de transmisión que se dirigen a la antena deberán estar apropiadamente diseñados e instalados, para que no tenga lugar ninguna reflexión de las ondas de radio. Si la línea y los conectores no coinciden apropiadamente, parte de la energía puede rebotar como eco y constituir una pérdida de potencia del sistema.

2.14.20 Difracción y dispersión

La dispersión de una onda en torno a un obstáculo se denomina difracción. Esta dispersión se

denomina en ocasiones rodear un obstáculo. No obstante, para evitar una posible confusión con la refracción, que es un proceso enteramente diferente, aquí utilizaremos el término difracción. Las ondas de radio pasan por una difracción a pequeña escala y a gran escala. Un ejemplo de difracción a pequeña escala son las ondas de radio de una WLAN que se dispersa en un ambiente interior. Un ejemplo de difracción a gran escala son las ondas de radio que se dispersan en torno a una montaña, hacia un área inaccesible.

Un efecto diferente tiene lugar cuando la luz golpea pequeñas partículas. Dependiendo de la frecuencia de la luz y del tamaño y la composición de las partículas, es posible un fenómeno denominado dispersión. La dispersión en general resulta en el redireccionamiento de la energía de onda entrante hacia direcciones que no son la dirección deseada.

2.14.21 Multirrutura

Imaginemos un sándwich de varias capas de materiales transparentes. Imaginemos que la capa central, el núcleo, tiene un índice de refracción más alto que el de las dos capas exteriores. Los rayos de luz que viajan en determinados ángulos a través del medio del núcleo se reflejarán desde las interfaces, de acuerdo a la ley de reflexión interna total. Ahora imaginemos una fuente de luz que emita en varios ángulos, y que todos ellos se reflejarían. Esto se denomina distorsión multirruta o interferencia.

En muchas instalaciones comunes de WLAN, las ondas de radio emitidas desde un transmisor viajan a diferentes ángulos. Pueden reflejarse desde diferentes superficies y terminan llegando al receptor en momentos levemente diferentes. Todas las ondas viajan a aproximadamente la velocidad de la luz. No obstante, sólo una pequeña cantidad de diferencia temporal es necesaria, para resultar en una señal de microondas distorsionada. La interferencia multirruta puede dar fuerza a la señal RF, pero ocasionando niveles de calidad de la señal pobres. Éste es un tema importante a considerar al instalar WLANs.

2.14.22 Pérdida de la ruta

Un factor crucial en el éxito o fracaso de un sistema de comunicaciones es cuánta potencia procedente del transmisor llega al receptor. Se tratarán muchas formas diferentes en las cuales las ondas EM pueden verse afectadas, incluyendo reflexión, difracción y dispersión. Estos efectos diferentes pueden combinarse y describirse por medio de lo que se conoce como cálculos de pérdida de ruta. Los cálculos de pérdida de ruta determinan cuánta potencia se pierde a lo largo de la ruta de comunicaciones. La pérdida del espacio libre (FSL) es la atenuación de la señal que resultaría si todas las influencias de absorción, difracción, obstrucción, refracción, dispersión y reflexión se eliminaran lo suficiente como para que no tuvieran ningún efecto en la propagación.

Cada vez que la distancia desde el transmisor al receptor se duplica, el nivel de la señal baja (o se incrementa) en 6 dB. Además, para cada frecuencia, hay una serie de longitudes de onda, donde la energía escapará de la línea de transmisión y entrará al espacio que la rodea. Esto se denomina efecto de lanzamiento. El efecto de lanzamiento tiene lugar en general en múltiplos de media longitud de onda de la señal.

2.14.23 Ethernet y LANs cableadas

Una topología WLAN puede ser una extensión de una LAN escalable existente. Las internetworks mejor construidas y administradas se diseñan en general en capas, siguiendo un modelo jerárquico. Utilizando capas jerárquicas, el usuario puede dividir una red grande en trozos más pequeños, que pueden tratarse cada uno por separado. Para comprender la importancia de la división en capas, consideremos el Modelo de Referencia OSI. El Modelo de Referencia OSI es un modelo en capas

para comprender e implementar comunicaciones en las computadoras. Dividiendo la funcionalidad de la red total en trozos más pequeños, o capas, el modelo OSI simplifica las tareas requeridas para que dos computadoras se comuniquen.

Los modelos jerárquicos para el diseño de internetworks también utilizan capas, para simplificar la tarea requerida para el internetworking. Cada capa puede concentrarse en funciones específicas, permitiendo así al usuario elegir los sistemas y las funciones apropiadas para la capa. Como resultado de ello, un modelo jerárquico simplifica la administración de la internetwork y permite al usuario controlar el crecimiento, sin pasar por alto los requisitos de la red.

Los dispositivos cableados tradicionales que se utilizan incluyen routers, switches, servidores e impresoras. Tecnologías en desarrollo, como voz sobre IP (VoIP), pueden agregar capacidades adicionales para LANs tanto cableadas como Inalámbricas. Finalmente, los dispositivos de seguridad como Firewalls, dispositivos VPN y sistemas de detección de intrusiones se convierten en requisitos para una LAN/WAN segura. Al implementar una solución WLAN deben considerarse todos los dispositivos. Esto se debe a que la WLAN debe interoperar sin fisuras con la red cableada existente.

2.14.24 Modularidad

La capa principal es la internetwork central de toda la empresa y puede incluir backbones de LAN y WAN. La función principal de esta capa es proporcionar una estructura de transporte optimizada y confiable y enviar tráfico a altas velocidades. Además, la capa principal es un backbone de conmutación de alta velocidad. Puesto que el trabajo primordial de un dispositivo de la capa principal de la red es conmutar paquetes, el alumno deberá diseñar la capa principal para que conmute los paquetes tan rápido como sea posible. Por lo tanto, la capa principal de la red no deberá llevar a cabo ninguna manipulación de paquetes. La manipulación de paquetes, como el verificar las listas de acceso o el filtrado, ralentizaría la conmutación.

La modularidad es otro beneficio de utilizar un diseño jerárquico, porque se ven facilitados los cambios en la internetwork. Además, la modularidad en el diseño de redes permite al usuario crear elementos de diseño que pueden replicarse a medida que la red crece. Cuando un elemento del diseño de la red requiere un cambio, el costo y la complejidad de efectuar la actualización se ve restringida a un pequeño subconjunto de la red total. En grandes arquitecturas de red planas o de malla, los cambios tienden a tener un impacto en una gran cantidad de sistemas.

La estructura modular de la red en elementos pequeños y fáciles de comprender también simplifica el aislamiento de fallos. El usuario puede comprender fácilmente los puntos de transición de la red, e identificar así puntos de fallo.

En ocasiones se considera equivocadamente que las capas principal, de distribución y de acceso deben existir cada una como entidad física clara y diferenciada. No obstante, éste no tiene por qué ser el caso. Las capas se definen para ayudar a un diseño exitoso de la red y para representar la funcionalidad que debe existir en una red. Cada capa puede encontrarse en routers o switches diferenciados, puede combinarse en un único dispositivo o puede omitirse totalmente. La forma en la cual se implementan las capas depende de las necesidades de la red que se está diseñando. Nótese que debe mantenerse una jerarquía para que la red funcione de manera óptima.

2.14.25 Categorías de WLAN

Las WLANs son elementos o productos de la capa de acceso. Los productos WLAN se dividen en dos categorías principales:

1. LANs inalámbricas en el interior de un edificio
2. Bridging inalámbrico de edificio a edificio

Las WLANs reemplazan al medio de transmisión de la Capa 1 de una red cableada tradicional, que es usualmente un cable de Categoría 5, por transmisión de radio por el aire. Las WLANs también reemplazan la funcionalidad MAC de Capa 2, con controladores MAC inalámbricos. Los productos MAC pueden enchufarse a una red cableada y funcionar como aditamento de las LANs tradicionales o cableadas. Las WLANs también pueden implementarse como LAN autónoma, cuando un networking cableado no es factible. Las WLANs permiten el uso de computadoras de escritorio, portátiles y dispositivos especiales de un entorno donde la conexión a la red es esencial. Las WLANs se encuentran en general dentro de un edificio, y se las utiliza para distancias de hasta 305 m (1000 pies). Las WLANs utilizadas apropiadamente pueden proporcionar un acceso instantáneo desde cualquier lugar de una instalación. Los usuarios podrán hacer roaming sin perder sus conexiones de red. La WLAN Cisco proporciona una completa flexibilidad.

Los bridges inalámbricos permiten a dos o más redes que están físicamente separadas conectarse en una LAN, sin el tiempo ni los gastos ocasionados por los cables dedicados o por las líneas T1.

2.14.26 Repetidor Inalámbrico

En un entorno donde es necesaria una cobertura extendida, pero el acceso al backbone no es práctico o no está disponible, puede utilizarse un repetidor inalámbrico. Un repetidor inalámbrico es simplemente un access point que no está conectado al backbone cableado. Esta configuración requiere una superposición del 50% del AP en el backbone y en el repetidor inalámbrico.

El usuario puede configurar una cadena de varios access points repetidores. No obstante, el throughput de los dispositivos clientes que se encuentran en el extremo de la cadena de repetidores puede ser muy bajo. Esto se debe a que cada repetidor debe recibir y luego retransmitir cada paquete por el mismo canal. Por cada repetidor agregado a la cadena, el throughput se reduce a la mitad. Se recomienda el uso de no más de dos saltos.

Al configurar los access points repetidores utilice las siguientes directrices:

- Utilice repetidores para servir a dispositivos clientes que no requieren un throughput elevado. Los repetidores extienden el área de cobertura de la WLAN, pero reducen drásticamente el throughput.
- Utilice repetidores cuando los dispositivos clientes que se asocian a los repetidores son clientes Cisco Aironet. Los dispositivos cliente que no son Cisco en ocasiones tienen problemas para comunicarse con los access points repetidores.
- Utilice antenas omnidireccionales, como las que se venden con el access point, para los access points repetidores.

En general, dentro de los edificios la disponibilidad de las conexiones Ethernet está muy generalizada. Los repetidores pueden utilizarse para extender los APs del borde del edificio a las porciones exteriores que rodean al edificio, para un uso temporal. Por ejemplo, un cliente podría utilizar APs en modo repetidor para extender la cobertura en la playa de estacionamiento durante una época pico de ventas de un supermercado. La asociación de clientes se asigna al AP cableado/raíz y no al AP que actúa como repetidor.

2.14.27 Redundancia del sistema y equilibrio de la carga

En una LAN donde es esencial tener comunicaciones, algunos clientes requerirán redundancia. Con los productos de espectro expandido de secuencia directa (DSSS) de un fabricante diferente, ambas unidades AP se configurarían según la misma frecuencia y velocidad de datos. Puesto que estas unidades comparten el tiempo de la frecuencia, sólo una unidad puede hablar a la vez. Si dicha unidad pasa a inactividad por alguna razón, los clientes remotos transferirán la comunicación a la otra unidad activa. Aunque esto sí proporciona redundancia, no proporciona más throughput que el que

proporcionaría un único AP.

En el caso de los sistemas Cisco DS, las unidades se instalan en canales diferentes. Los clientes remotos equilibrarán la carga, cuando ambas unidades estén activas. Si una unidad pasa a inactividad, los clientes remotos transferirán la comunicación a la unidad restante y continuarán trabajando. El equilibrio de la carga puede configurarse basándose en la cantidad de usuarios, la tasa de errores de bit o la fuerza de la señal.

Otra opción, cuando la tolerancia a fallos y la disponibilidad son críticas, es un AP hot-standby. En este caso, no existe un equilibrio de la carga. Para implementaciones críticas para los negocios, un AP Cisco Aironet puede configurarse como hot-standby redundante de otro AP en la misma área de cobertura. El AP hot-standby monitorea continuamente al AP principal del mismo canal, y asume su papel en el raro caso de un fallo del AP principal. El standby estará listo para tomar su lugar, si el AP principal ya no está disponible.

2.14.28 Topologías de campus

El propósito de una WLAN de campus es servir como sistema de acceso que incorpore una movilidad completa. Las WLANs permiten a los usuarios acceder a la información desde lugares no cableados en el exterior, en comedores o espacios informales para el estudio, los bancos del aula e incluso campos de atletismo. No obstante, las WLANs de campus no deberán considerarse como reemplazo de un entorno inalámbrico, sino más bien como forma de agregar más funcionalidad a la red existente.

Una superposición inalámbrica de todo el campus proporciona networking en ubicaciones difíciles de alcanzar o temporales. Éstos son lugares que podrían haber sido ignorados completamente. Los access points Cisco Aironet 1100 y 1200 y los bridges Aironet 350 se integran bien con los switches Cisco Ethernet, que se utilizan en general en un entorno de campus. Uno de los mayores beneficios de una WLAN de campus es su capacidad para que la gente se siente en áreas comunes y trabaje en conjunto, a la vez que obtiene fácilmente un acceso a la red. En el caso de muchas instituciones educativas, donde los recursos son limitados, esto podría significar que existen menos usuarios que compiten por un puñado de computadoras integradas. La tecnología inalámbrica se está convirtiendo rápidamente en una herramienta viable e importante, en una variedad de entornos de negocios y educativos.

2.14.29 Bandas de Frecuencias

Las redes WLAN funcionan en dos bandas de frecuencias: la banda de 2,4GHz y la banda de 5GHz. En ninguna de las dos bandas se requiere licencia para su utilización, pero se encuentran sujetas a la regulación fijada por la Secretaria de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI) en el Cuadro Nacional de Frecuencias (CNAF). Ambas bandas están designadas para aplicaciones ISM (Industry, Science and Medical) ó ICM (Industrial, Científica y Médica). Las redes WLAN basados en los estándares de capa física IEEE802.11b e IEEE802.11g (ver 2.2.5) funcionan en la banda de 2,4GHz, y el estándar IEEE802.11a en la banda de 5GHz. El estándar IEEE802.11n, todavía bajo estudio, funcionará en la banda de 2,4GHz.

La banda de 2,4GHz para uso en redes WLAN consta del siguiente rango de frecuencias: 2,4GHz - 2,4835 GHz, (ver CNAF en el Anexo I). El ancho de banda por canal en la banda de 2,4GHz es de 22MHz y la separación entre canales de 5MHz; por lo tanto hay 13 canales disponibles, 3 de ellos no solapados. El número de canales disponibles es de 13 en Estados Unidos y 11 en Europa

La banda de 5GHz para uso en redes WLAN consta del siguiente rango de frecuencias: 5,150GHz - 5,725GHz. En la banda de 5 GHz el ancho de banda por canal es de 20MHz y existen 12 canales no solapados, 8 para uso en interiores y 4 para exteriores.

2.15 PREGUNTAS Y TIPS

- **¿Qué son las redes de telecomunicaciones?** Son un conjunto de medios técnicos instalados, organizados, operados y administrados con la finalidad de brindar servicios de comunicaciones a distancia.
- **¿Qué factores representan una ventaja de la división en capas del modelo OSI?**

  Reduce la complejidad, acelera la evolución, facilita la enseñanza y el aprendizaje
- **¿Cuál es el orden correcto de las capas del modelo OSI?** aplicación, presentación, sesión, transporte, red, enlace de datos y física
- **¿Cuál es el orden correcto de las PDU en el proceso de encapsulamiento del modelo de referencia OSI?** datos, segmentos, paquetes, tramas, bits
- **¿Cómo se denominan las capas del modelo TCP/IP?** aplicación, transporte, Internet, acceso a red
- **¿Cuales son las características de un hub?** Regenera y retemporiza las señales, Trabaja en la Capa 1 del modelo OSI, Forma un dominio de colisión entre todas las estaciones conectadas
- **¿Cuál es el objetivo de la subcapa de Control de Enlace Lógico (LLC)?** Permitir que la capa de enlace de datos sea independiente de las capas de red y física.
- **¿Cuál es el método de acceso al medio utilizado en las redes Ethernet?** CSMA/CD
- **¿Cuál es un aspecto de seguridad a considerar en las redes de difusión?** Una transmisión es recibida por todas las estaciones (aunque no sean el destino)
- **¿Para qué se utiliza el protocolo ARP?** Para encontrar una dirección MAC a partir de una dirección IP
- **¿Cuál es la principal función de ICMP?** Informar al host origen que existe algún error en la transferencia de los paquetes
- **¿Por qué es necesario TCP en transmisiones confiables?** Porque los protocolos de capas inferiores no son confiables
- **¿Cuáles son las fases de una conexión TCP?** Establecimiento de la conexión, Transferencia de datos, Liberación de la conexión
- **¿Cómo se establecen las conexiones en TCP?** Mediante el acuerdo de tres vías
- **¿Cuales son características de UDP?** No utiliza técnicas de acuse de recibo, No utiliza control de flujo
- **En una red con topología de estrella, ¿qué pasaría si una sola conexión de uno de los host de la red falla?** Sólo el host que tiene la conexión caída no tendrá conexión a la red.
- **¿Qué dispositivo puede ser usado en una red de tipo token ring?** Una Multistation Access Unit (MSAU). Este dispositivo es usado para interconectar múltiples redes token ring, un Hub o Switch es un dispositivo central usado en una topología de estrella al cual cada host está conectado.
- **¿En qué topología de red se requeriría menos cableado?** En la topología bus. Esta topología consiste en un único cable que conecta los nodos de la red
- **¿Qué topología de red es la más sencilla de implementar?** La topología bus.
- **¿Cuál es la máxima velocidad en que opera una red Token Ring?** Inicialmente operaban a 4 Mbps, esto fue incrementado luego a 16 Mbps

- **¿Cuál es la máxima velocidad en que opera una red Ethernet 10Base-T?** 10 Mbps
- **¿Cuál es la máxima velocidad en que opera una red Ethernet 100Base-TX?** 100 Mbps
- **¿Cuál estándar IEEE describe Ethernet?** El estándar 802.3. El estándar 802.4 describe redes Token Bus, el 802.5 describe redes Token Ring y el 802.11 es para WLAN
- **¿Cuál es la máxima velocidad en la que opera FDDI?** 100 Mbps
- **¿Qué método de acceso es usado en redes Wireless?** CSMA/CA
- **El cable *single-mode* o modo simple de fibra óptica es usado en:** Es usado en 10 GBase-ER y 10 GBase-LR. El cable multimodo de fibra óptica es usado en 10 GBase-SR
- **¿Qué tipo de medio es el más susceptible a interferencia electromagnética (EMI)?** El cable UTP. El cable de fibra óptica no es susceptible a EMI
- **¿Cómo se denomina al servicio que permite resolver hostnames con direcciones IP?** El Servicio DNS permite resolver hostnames con direcciones IP
- **¿Qué protocolo permite compartir archivos en entornos Unix/Linux/Windows?** Se denomina SMB. *Server Message Block* o SMB es un Protocolo de red (que pertenece a la capa de aplicación en el modelo OSI) que permite compartir archivos e impresoras (entre otras cosas) entre nodos de una red.
- **¿Qué significan las siglas LDAP y que hace este?** *Lighweight Directory Access Protocol*. Este funciona como base de datos de información concerniente a cuentas de usuarios y recursos de red. También puede ser utilizado para autenticación de usuarios.
- **¿Cuál servicio de red provee direcciones IP?** Dynamic Host Configuration Protocol (DHCP)
- **¿Cuál es la diferencia entre NTP, ntpd, y xntpd?** NTP es el nombre del protocolo. Las implementaciones del protocolo NTP para Unix conteniendo un demonio son llamados ntpd. xntpd es el nombre del paquete que es considerado actualmente la implementación estándar de referencia.
- **Liste las cuatros capas del modelo TCP/IP , luego liste 2 protocolos usados por cada una ellas.**
    - Aplicación: FTP, Telnet, HTTP
    - Transporte: TCP,UDP
    - Internet: IP,ICMP,ARP
    - Network Access: Ethernet, Token Ring, FDDI, serial, X.25, ATM
- **¿En que año se constituyó POP3 como un protocolo estándar del Internet, el TCP y el IP?** POP3 se convirtió en un estándar de Internet en mayo de 1996. TCP/IP son estándares desde septiembre 1 de 1981.
- **¿Para que es utilizado el puerto 110 ?** Este puerto es usado para POP3
- **¿Para que es utilizado el puerto 533?** Este puerto es utilizado para broadcasts de emergencia
- **¿Que son los RFCs?** Los RFCs significan *Request for Comments*. Estos son documentos que contienen estándares TCP/IP con información sobre definiciones de protocolos.
- Liste tres protocolos comunes del Internet y los puertos que generalmente usan. HTTP puerto 80, POP puerto 110, FTP puerto 21
- **¿Cuáles son los tres tipos de topologías lógicas de redes?** Bus, Anillo y estrella.
- **¿Cuáles protocolos pueden ser usados para conectarse al Internet vía modem, cuál es**

mejor y porqué? SLIP y PPP. PPP es mejor porque además de ser más reciente, provee autenticación y puede encapsular múltiples protocolos de red.

- **¿Cuál es el rango de las tres principales clases de direcciones?** 1.0.0.0 / 126.255.255.255 – 128.0.0.0 / 191.255.255.255 – 192.0.0.0 / 225.255.255.255
- **¿Qué hace el Protocolo de Resolución de Direcciones(arpa)?** El protocolo ARP resuelve direcciones IP a MAC. Este protocolo realiza un broadcast a todos los hosts en la red LAN si no los tiene listados en su tabla. Cuando recibe una respuesta de que una dirección MAC dada posee determinada IP, entonces la agrega a su tabla ARP para posterior uso y así no necesita realizar broadcast de nuevo
- **¿Cuales son los tres componentes para la conexión del PPP?** Mecanismo de Encapsulación, Protocolo de Control de Enlace y Protocolo de Control de Red.
- **¿Qué es una netmask (mascara de red)?** Una mascara de red es una cadena de puntos decimales que es utilizada para enmascarar una dirección IP y distinguirla entre los bits de red y los bits de host.
- **¿Cómo funciona el enrutamiento?** Un paquete IP, si no esta destinado a un host de su misma red, es enrutado a través de un gateway a otra red. Como elegir la ruta depende de las entradas en la tabla de enrutamiento.
- **¿Por que usamos enrutamiento Dinámico?** Utilizamos la tabla de enrutamiento dinámico porque en grandes redes es extremadamente difícil mantener las tablas de enrutamiento dinámicas. En ese sentido, las tablas de enrutamiento son actualizadas por los protocolos de enrutamiento dinámico.
- **Dentro de una red Clase C, ¿Cómo podemos direccionar más de 255 máquinas?** Esto es posible utilizando *subnetting*. esto ayuda a utilizar un conjunto existentes de direcciones IP más eficientemente creando algunos de los bits del host de la dirección IP en bits de red.
- **¿En que se diferencian los conceptos de *supernetting* del de *subnetting*?** El *subnetting* da más espacio de direcciones sin cambiar la clase de la red (incrementando el número de IP's disponibles). Por otro lado, *supernetting* lleva más enrutamiento reduciendo el tamaño de las tablas de enrutamiento.
- **¿Por qué no podemos usar direcciones que terminen en 0 o 255 como direcciones de una subnet?** Las direcciones finalizadas en 0 y 255 son designadas para la ruta por defecto y las direcciones *broadcast* respectivamente.
- **Considerando RIP y OSPF ¿Cuál de estos protocolos de enrutamiento es más avanzado y por qué?** RIP es un miembro de el grupo de protocolos vector-distancia. Por otro lado OSPF es un miembro del más avanzado grupo de protocolos de estado de enlace. OSPF no transmite rutas a través de la red, pero en su lugar, actualiza el estado de los enlaces directamente conectados. Así, OSPF provee trafico reducido y más seguridad.
- **¿Después de cuantos saltos considerará RIP un destino no alcanzable?** Después de 16 saltos o más
- **¿Cuáles campos son contenidos en el cabezal IP?** Identificación, Compesación de fragmento, banderas de campo
- **¿Cuáles puertos son reservados para servicios bien conocidos?** 1024 hacia abajo
- **¿Cuáles son las afirmaciones verdaderas con respecto al encapsulamiento y desencapsulamiento de paquetes cuando viajan a través de un router?**. El router modifica el campo TTL, decreciendo de a uno. El router mantiene el mismo IP de origen y de destino. El router cambia la dirección física de origen a la dirección física de la interfaz de salida.
- **¿Qué son las métricas utilizadas por los protocolos de enrutamiento?** Una métrica es un valor usado por un protocolo de enrutamiento particular para comparar las rutas con las redes

remotas.

- **¿Qué significan las siglas OSPF y cuál es su utilidad?** *Open Shortest Path First* (frecuentemente abreviado OSPF) es un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - Link State Algorithm) para calcular la ruta más corta posible. Usa cost como su medida de métrica. Además, construye una base de datos enlace-estado (link-state database, LSDB) idéntica en todos los enrutadores de la zona. OSPF es probablemente el tipo de protocolo IGP más utilizado en grandes redes. Puede operar con seguridad usando MD5 para autentificar a sus puntos antes de realizar nuevas rutas y antes de aceptar avisos de enlace-estado. Como sucesor natural de RIP, acepta VLSM o sin clases CIDR desde su inicio. A lo largo del tiempo, se han ido creando nuevas versiones, como OSPFv3 que soporta IPv6 o como las extensiones multidifusión para OSPF (MOSPF), aunque no están demasiado extendidas. OSPF puede "etiquetar" rutas y propagar esas etiquetas por otras rutas.
- **¿Qué significan las siglas EIGRP y cuál es su función?** *Enhanced Interior Gateway Routing Protocol. E*s un protocolo de encaminamiento híbrido, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancias y del estado de enlace. Se considera un protocolo avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace. Algunas de las mejores funciones de OSPF, como las actualizaciones parciales y la detección de vecinos, se usan de forma similar con EIGRP. Aunque no garantiza el uso de la mejor ruta, es bastante usado porque EIGRP es algo más fácil de configurar que OSPF. EIGRP mejora las propiedades de convergencia y opera con mayor eficiencia que IGRP. Esto permite que una red tenga una arquitectura mejorada y pueda mantener las inversiones actuales en IGRP.
- **¿Qué significan las siglas BGP y cuál es su función?** El BGP o *Border Gateway Protocol* es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos. Por ejemplo, los ISP registrados en Internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP.
- **¿De qué forma el envenenamiento de ruta evita que se produzcan routing loops?** Las rutas que fallaron se publican con una métrica de infinito.
- **Un administrador de red usa el protocolo de enrutamiento RIP para implementar el enrutamiento dentro de un sistema autónomo. ¿Cuáles son las características de este protocolo?** Usa el algoritmo Bellman-Ford para determinar el mejor camino. Envía periódicamente tablas de enrutamiento completas a todos los dispositivos conectados.
- **Un router se inicia e ingresa al modo Setup. ¿Por qué?** La configuración no está en la NVRAM.
- **¿Qué protocolo de enrutamiento mantiene una tabla de topología separada de la tabla de enrutamiento?** EIGRP
- **¿Cuál es el método correcto del *horizonte dividido* con envenenamiento en reversa para la prevención de routing loop?** Asigna un valor que representa una métrica infinita a la ruta envenenada. Devuelve la ruta envenenada a la misma interfaz desde donde se recibió. El protocolo de vector de distancias emplea la regla de horizonte dividido que prohíbe a un router publicar una ruta por la misma interfaz por la que se aprendió en primer lugar. El horizonte dividido es uno de los métodos usados para prevenir el problema de ciclos de enrutamiento o "cuenta hasta el infinito"; debido a los altos tiempos de convergencia del protocolo de vector de distancias.
- **Un router obtuvo dos rutas de igual costo a una red remota a través de los protocolos EIGRP y RIP. Los dos protocolos están usando la configuración predeterminada. ¿Qué ruta a la red remota se instalará en la tabla de enrutamiento?** la ruta obtenida a través de EIGRP
- **En un entorno de prueba de laboratorio, un router detectó la red 172.16.1.0 a través de**

cuatro procesos de enrutamiento dinámicos diferentes. ¿Qué ruta se usa para alcanzar esta red? 172.16.1.0/24 [90/2195456] via 192.168.200.1, 00:00:09, Serial0/0/0

- **¿Cuales son las características de los routers que usan protocolos de enrutamiento de link-state?** Los routers que ejecutan un protocolo de *link-state* pueden establecer una topología completa de la red. Se usa el algoritmo *shortest path first.*
- **Modelo teórico de una red de datos:**
  - Modelo TCP/IP:
    - Proceso de Aplicación
    - Transmisión
    - Internet
    - Acceso a la Red
  - Modelo OSI:
    - Aplicación (Telnet/HTTP/SNMP/POP3)
    - Presentación (JPG/MP3)
    - Sesión (NTFS/X-Windows)
    - Transporte (TCP/UDP)
    - Red (IP/IPX/ICMP)
    - Enlace de datos (Ethernet/PPP/HDLC/Frame Relay)
    - Física (RJ-45/V-35)
- **Capa física del modelo OSI:**
  - Normativa EIA/TIA 568
  - Medios de Cobre:
    - Cable coaxial
    - Cable par trenzado de cobre
  - Fibra óptica:
    - Monomodo
    - Multimodo
  - Wireless:
    - Satélite
    - Wireless LAN por onda corta
    - Wireless LAN infrarrojo (IR)
    - Wireless LAN por spread spectrum (WLAN)
    - IEEE 802.11a
    - IEEE 802.11b
    - IEEE 802.11g
- **Elementos comunes de Ethernet:**
  - Estructura de la trama
  - Dimensiones de la trama
    - Mínima = 64 bytes
    - Máxima = 1518 bytes
  - Método de acceso al medio: CSMA/CD
  - Requerimiento de un spot time en conexiones half dúplex

CAPÍTULO 3

3.1 PROTOCOLOS Y SERVICIOS

¿Cómo definiría el término protocolo? Es un Conjunto de reglas que definen el proceso de la comunicación entre dos o más *host* dentro de una red

¿Qué es un servicio? Es un programa de aplicación que se ejecuta en un *host* con el fin de ser accedido por otro *host*. Los más comunes pueden ser: E-mail, transferencia de archivos, acceso remoto.

3.1.1 Telnet

El protocolo Telnet es un protocolo de capa de aplicación que emula una terminal remota a través de una red TCP/IP. El objetivo de este protocolo es definir una interfaz estándar para la intercomunicación entre sistemas finales, a través de una terminal virtual .

Antiguamente para iniciar una sesión remota se conectaba al servidor una terminal sin poder de procesamiento, llamada "terminal boba", por medio de un cable conectado al puerto serie y la comunicación se establecía a través de un protocolo de transmisión serie. El servidor servía de centro de la estrella donde convergían todas las terminales. Algunas desventajas de este sistema eran:

- la distancia entre las terminales y el servidor, limitada por el alcance del cable serial
- el costo asociado de mantener en el servidor un puerto serie por cada terminal remota

Con la llegada de las estaciones de trabajo y la difusión de las redes TCP/IP, las terminales remotas fueron reemplazadas por un software de terminal virtual, que se ejecuta en la estación y se comunica con el servidor a través de TCP/IP, utilizando el protocolo Telnet. Esta característica elimina la limitación de distancia entre las terminales y el servidor.

El protocolo Telnet se encuentra definido principalmente por los RFC 854 (TELNET Protocol Specifications) y 855 (TELNET Option Specifications). Se ejecuta sobre TCP y tiene asignado el número de puerto 23 .

El protocolo TELNET se basa en tres ideas principales:

- El concepto de "Terminal Virtual de Red" (NVT, Network Virtual Terminal). Una NVT es un dispositivo imaginario que mantiene una estructura básica común a todos los tipos de terminales. Cada host realiza la traducción desde su estructura hacia la NVT cuando transmite datos y desde la NVT hacia su estructura cuando recibe información.
- Una visión simétrica de terminales y procesos, es decir, asocia una terminal virtual con un proceso ejecutándose en la estación
- La negociación de opciones, la cual es utilizada por las estaciones para negociar las diferentes opciones que provee el protocolo, por ejemplo el tipo de terminal, una de las más comunes es VT100.

Proceso de conexión y funcionamiento: Para establecer una conexión Telnet entre un Cliente y un Servidor, primero debe establecerse una conexión TCP a través del saludo de tres vías. El cliente debe iniciar esta conexión haciendo una solicitud al puerto 23 del Servidor . Esta conexión se mantiene durante toda la sesión Telnet.

Una vez que finaliza el saludo de tres vías, se establece la conexión TCP, y el cliente y el servidor deben negociar las opciones específicas de Telnet. Cuando finaliza la negociación de las opciones, se comienza la transferencia de datos entre el cliente y el servidor.

Cada tecla que presiona el cliente no es procesada localmente, sino que viaja a través de la red hasta el servidor, donde es procesada por la aplicación Telnet, y transferida de vuelta al cliente para que proceda a mostrarla por pantalla, en caso que llegue un ENTER al servidor, procederá a ejecutar el comando formado por las letras que previamente le han llegado, y al igual que en el caso anterior, envía la respuesta al cliente para que la muestre por pantalla .

El protocolo Telnet provee autenticación de usuarios a través del ingreso de un nombre de usuario y una contraseña al iniciarse una sesión .

El mayor problema de seguridad de Telnet es que el tránsito de los datos se realiza en texto claro, es decir sin encriptar. Si estamos en una red de difusión, como Ethernet, Token Ring o FDDI, el tráfico que envía una estación es recibido por todas las demás que conforman la LAN y como los datos no viajan encriptados, cualquier estación podría leer las transacciones de otra estación.

3.1.2 HTTP

El protocolo de transferencia de hipertexto (HTTP, HyperText Transfer Protocol) es el protocolo usado en cada transacción de la Web (WWW). HTTP fue desarrollado por el consorcio W3C y la IETF, colaboración que culminó en 1999 con la publicación de una serie de RFC, siendo el más importante de ellos el RFC 2616, que especifica la versión 1.1.

HTTP define la sintaxis y la semántica que utilizan los elementos software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. Al cliente que efectúa la petición (un navegador o un spider) se lo conoce como "user agent" (agente del usuario). A la información transmitida se la llama recurso y se la identifica mediante un URL. Los recursos pueden ser archivos, el resultado de la ejecución de un programa, una consulta a una base de datos, la traducción automática de un documento, etc.

HTTP es un protocolo sin estado, es decir, que no guarda ninguna información sobre conexiones anteriores. El desarrollo de aplicaciones web necesita frecuentemente mantener estado. Para esto se usan las cookies, que es información que un servidor puede almacenar en el sistema cliente. Esto le permite a las aplicaciones web instituir la noción de "sesión", y también permite rastrear usuarios ya que las cookies pueden guardarse en el cliente por tiempo indeterminado.

Una transacción HTTP está formada por un encabezado seguido, opcionalmente, por una línea en blanco y algún dato. El encabezado especificará cosas como la acción requerida del servidor, o el tipo de dato retornado, o el código de estado.

El uso de campos de encabezados enviados en las transacciones HTTP le dan gran flexibilidad al protocolo. Estos campos permiten que se envíe información descriptiva en la transacción, permitiendo así la autenticación, cifrado e identificación de usuario.

Un encabezado es un bloque de datos que precede a la información propiamente dicha, por lo que muchas veces se hace referencia a él como metadato, porque tiene datos sobre los datos

3.1.3 HTTPS

Hypertext Transfer Protocol Secure (en español: Protocolo seguro de transferencia de hipertexto), más conocido por sus siglas HTTPS, es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP.

El sistema HTTPS utiliza un cifrado basado en SSL/TLS para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP. De este modo se consigue que la información sensible (usuario y claves de paso normalmente) no puede ser usada por un atacante que haya conseguido interceptar la transferencia de datos de la conexión, ya que lo único que obtendrá será un flujo de datos cifrados que le resultará imposible de descifrar.

Cabe mencionar que el uso del protocolo HTTPS no impide que se pueda utilizar HTTP. Es aquí, cuando nuestro navegador nos advertirá sobre la carga de elementos no seguros (HTTP), estando conectados a un entorno seguro (HTTPS).

Los protocolos HTTPS son utilizados por navegadores como: Safari, Internet Explorer, Mozilla Firefox, Opera y Google Chrome, entre otros.

Es utilizado principalmente por entidades bancarias, tiendas en línea, y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas.

El puerto estándar para este protocolo es el 443.

3.1.4 SHTTP

El protocolo fue diseñado por E. Rescorla y A. Schiffman de Enterprise Integration Technologies (EIT). para obtener conexiones de HTTP. S-HTTP provee una variedad amplia de mecanismos para tener prevista confidencialidad, autenticación, e integridad, La separación de política de mecanismo fue un cometido explícito.

S-HTTP es un superconjunto de HTTP, el cual permite mensajes para ser narrado de forma resumida de forma muy diversa. Las encapsulaciones pueden incluir cifrado, firma, o una autenticación basada en MAC. Esta encapsulación puede ser recursiva, y un mensaje puede tener varias transformaciones de seguridad aplicadas.

S-HTTP también incluye definiciones de encabezado para proveer la transferencia de clave, dar un certificado a la transferencia, y las funciones administrativas similares. S-HTTP parece ser sumamente flexible, lo cual permitirá al programador desarrollar aplicaciones web sin temor a que la aplicación sea vulnerada. S-HTTP también ofrece el potencial para el desenvolvimiento sustancial del usuario dentro de él, y el descuido de la autenticación y las actividades de cifrado.

S-HTTP no confía en un esquema particular de certificación de clave. Incluye soporte para RSA, hacia dentro se agrupa, fuera de banda y el cambio de clave kerberos. Las claves para las certificaciones pueden ser provistas en un mensaje, u obtenido en otro sitio. Como en SSL, las llaves públicas del cliente no son requeridas.

Las amenazas del S-HTTP son similares a las existentes contra el SSL. Sin embargo, la naturaleza más general de S-HTTP hace difícil de determinar exactamente cuáles son posibles. En el caso de un hacker, o del looker, el ataque contra un CA puede ser más difícil, debido a la existencia de CAs múltiples. Una clave se podía verificar teóricamente por varios CAs, haciendo un ataque infeasible.

El modo operacional por defecto de S-HTTP es substancialmente más resistente al ataque que el del SSL. Resiste el criptoanálisis claro de texto, hombre en el centro, y juega a nuevo ataques. Es más robusto que el SSL, porque se permite la renegociación y las recomprobaciones de la opción. Además, el costo del texto claro del criptoanálisis DES es substancialmente más alto que el de RC4-40. (Recuerde que el DES cifra por defecto para S-HTTP, y RC4-40 cifra por defecto para el SSL). Para romper una clave RC4-40 en aproximación con respecto a costos al mes es en promedio de $125. Para romper una clave del DES en costos de un mes es un aproximado de $10.000 (extrapolado de Wiener, 1994). Una clave DES de 56 bits cuesta un millón de dólares a la rotura sobre 7 horas. (Wiener, 1994) esta escala de costos va hacia arriba y hacia abajo en una forma lineal. (1/2 millón de dólares por máquina tomará 14 horas). Un mes tiene 720 horas (24 horas x 30 días), que es 102 períodos de 7 horas. El costo de romper el DES en un mes es casí cerca de $10 000, en comparación con $125 para 40 bits RC4.

El uso en el intercambio de la clave es potencialmente muy problemático; los autores no pasan bastante tiempo para asegurar que las claves se transfieren correctamente. Una transferencia incorrecta sería un esquema que envía B como Ea(B). Es decir, B dominante que substituye la clave A no se puede enviar usando la clave A para cifrarla. Si un atacante tiene llave quebrada A, entonces él tendrá B dominante, y el cambio de la llave es una pérdida de tiempo (con respecto a ese atacante). Esta equivocación fue incurrida a menudo por un japonés en la segunda guerra mundial. (Kahn) que esperaba que los programadores aprendan que de esto los errores de otros (especialmente los viejos errores de 50 años) son una apuesta pobre.

S-HTTP, es flexible, puede ofrecer a un programador bastantes variantes. Obviamente, no ofrece muchas opciones quebradas, sino que no parece hacer que cualquier cosa como los SSL con la actitud de "cifre todo y no lo que pueda". Un programador, especialmente uno no familiarizado con las aplicaciones de seguridad y criptografía, podría pensar que "usar S-HTTP me protegerá" y que no podrá proporcionar totalmente ninguna protección criptográfica para su información. La probabilidad de que esto suceda es discutible, pero es viable tener en consideración el problema.

3.2 PROTOCOLO SSH

El protocolo SSH (Secure Shell) fue creado con el fin de segurizar los datos en tránsito de una terminal remota. El funcionamiento es similar al de Telnet, con la diferencia que los datos que se transfieren entre el Cliente y el Servidor viajan encriptados. SSH soporta diferentes tipos de encriptación, lo que permite que el usuario seleccione su preferencia.

Existen dos versiones de SSH actualmente: SSH1 y SSH2. SSH1 soporta los algoritmos de encriptación Blowfish, DES, 3DES y RC4; mientras que SSH2 soporta 3DES, RC4 y Twofish (En el Modulo 2 - Capitulo 2 - Seguridad en los datos : Encriptación, podrá encontrar una descripción de las características de los algoritmos de encriptación mencionados).

En la actualidad SSH se ha convertido en el método seguro más utilizado para el acceso interactivo a sistemas remotos.

El protocolo SSH utiliza el puerto TCP 22 para realizar las conexiones . SSH se ocupa de la confidencialidad e integridad en el tránsito de datos entre el cliente y el servidor. Inicia una sesión encriptada entre el cliente y el servidor antes de transferir el nombre de usuario y la contraseña. De esta forma, si un usuario malicioso escucha el medio para capturar los datos que viajan en texto claro, no podrá comprender los datos transferidos por SSH.

El uso de SSH ayuda a protegerse de diferentes tipos de ataques, como *sniffing*, *IP spoofing* o la manipulación de datos por usuarios no autorizados.

SSH es una aplicación diseñada para substituir determinadas herramientas de acceso remoto usadas tradicionalmente en los sistemas Unix, como rsh(Remote Shell), rlogin(Remote Login) o rcp(Remote Copy), por nuevas versiones con servicios de seguridad.

El autor de la primera implementación del SSH, Tatu Ylönen, de la Universidad Tecnológica de Helsinki, publicó el año 1995 la especificación de la versión 1 del protocolo. Desde entonces se ha trabajado en la especificación de una nueva versión del protocolo, la 2.0, actualmente en fase de borrador a la espera de su publicación oficial como RFC. Aunque la funcionalidad que proporciona es básicamente la misma, la nueva versión incorpora muchas mejoras y es sustancialmente distinta de la anterior. La versión antigua y la nueva del protocolo se referencia habitualmente reverenciadas como SSH1 y SSH2, respectivamente.

Proceso de conexión y funcionamiento: El protocolo SSH necesita claves para poder encriptar la información que transmite. Estas claves deben ser conocidas por los dos extremos, por lo que deben ser transmitidas por la red. Este intercambio de claves debe ser previo a cualquier transferencia de información. Para evitar la escucha de las claves que se transmiten, se utiliza un esquema de claves asimétricas (se verá más adelante) que asegura que las claves transmitidas no podrán ser

interceptadas ni modificadas.

Una vez que se realizó el intercambio de claves, comienza la transferencia de datos, de manera similar a los demás protocolos.

El protocolo SSH provee un entorno seguro para la transferencia de información a través de una red no confiable. SSH permite asegurar:

- **Integridad**: Los datos transmitidos no pueden ser modificados por terceros.
- **Autenticación**: Los extremos son quien dicen ser (evita el robo de autenticidad)
- **Confidencialidad**: Los mensajes enviados no pueden ser leídos por terceros
- **No repudio**: Un mensaje que ha sido enviado no puede rechazarse
- **Rechazo de duplicados**: no permite que se envíe dos veces el mismo mensaje

SSH confía en que los dos extremos de la conexión son seguros, si alguno de ellos ha sido comprometido, todos los recursos que se utilicen sobre SSH también lo serán.

La aplicación define un protocolo propio para la transmisión segura de los datos, el protocolo SSH. Este protocolo se sitúa directamente por debajo de la capa de transporte, (concretamente del transporte TCP) y, como veremos en este apartado, proporciona servicios análogos a los del protocolo SSL/TLS. Aparte de establecer conexiones seguras, el protocolo SSH también ofrece otras funcionalidades como, por ejemplo, la re-dirección de puertos TCP o la comunicación entre clientes y servidores de ventanas X, a través de una conexión SSH.

De la misma forma que en SSL/TLS se distinguen dos subcapas en el nivel de transporte seguro, en SSH también se puede considerar una división en dos subniveles. Además, en SSH2 el nivel superior está estructurado en tres protocolos, uno por encima del otro.

3.2.1 Características de SSH

SSH proporciona servicios de seguridad equivalentes a los del protocolo SSL/ TLS.

Confidencialidad. SSH sirve para comunicar datos, que habitualmente son la entrada de una aplicación remota y la salida que genera, o bien la información que se transmite por un puerto redirigido, y la confidencialidad de estos datos se garantiza mediante el cifrado.

Como en el caso del protocolo SSL/TLS, en SSH se aplica un cifrado simétrico a los datos y, por lo tanto, será necesario realizar previamente un intercambio seguro de claves entre cliente y servidor. Una diferencia respecto a SSL/TLS es que en SSH2 se pueden utilizar algoritmos de cifrado distintos en los dos sentidos de la comunicación.

Un servicio adicional que proporciona SSH es la confidencialidad de la identidad del usuario. Mientras que en SSL 3.0 y TLS 1.0, si se opta por autenticar al cliente, éste tiene que enviar su certificado en claro, en SSH (y también en SSL 2.0) la autenticación del usuario se realiza cuando los paquetes ya se mandan cifrados. Por otro lado, SSH2 también permite ocultar ciertas características del tráfico como, por ejemplo, la longitud real de los paquetes.

Autenticación de entidad. El protocolo SSH proporciona mecanismos para autenticar tanto el ordenador servidor como el usuario que se quiere conectar. La autenticación del servidor suele realizarse conjuntamente con el intercambio de claves. En SSH2 el método de intercambio de claves se negocia entre el cliente y el servidor, aunque actualmente sólo hay uno definido, basado en el

algoritmo de Diffie-Hellman. Para autenticar al usuario existen distintos métodos; dependiendo de cuál se utilice, puede ser necesaria también la autenticación del ordenador cliente, mientras que otros métodos permiten que el usuario debidamente autenticado acceda al servidor desde cualquier ordenador cliente.

Autenticación de mensaje. Igual que en SSL/TLS, en SSH2 la autenticidad de los datos se garantiza añadiendo a cada paquete un código MAC calculado con una clave secreta. También existe la posibilidad de utilizar algoritmos MAC distintos en cada sentido de la comunicación.

Igual que SSL/TLS, SSH también está diseñado con los siguientes criterios adicionales:

- **Eficiencia**. SSH contempla la compresión de los datos intercambiados para reducir la longitud de los paquetes. SSH2 permite negociar el algoritmo que se utilizará en cada sentido de la comunicación, aunque solamente existe uno definido en la especificación del protocolo. Este algoritmo es compatible con el que utilizan programas como gzip(RFC 1950–1952).

  A diferencia de SSL/TLS, en SSH no está prevista la reutilización de claves de sesiones anteriores: en cada nueva conexión se vuelven a calcular las claves. Esto es así porque SSH está pensado para conexiones que tienen una duración más o menos larga, como suelen ser las sesiones de trabajo interactivas con un ordenador remoto, y no para las conexiones cortas pero consecutivas, que son más típicas del protocolo de aplicación HTTP (que es el que inicialmente se quería proteger con SSL). De todas formas, SSH2 define mecanismos para intentar acortar el proceso de negociación.

- **Extensibilidad**. En SSH2 también se negocian los algoritmos de cifrado, de autenticación de usuario, de MAC, de compresión y de intercambio de claves. Cada algoritmo se identifica con una cadena de caracteres que representa su nombre. Los nombres pueden corresponder a algoritmos oficialmente registrados, o bien a algoritmos propuestos experimentalmente o definidos localmente.

El protocolo de paquetes SSH se encarga de construir e intercambiar las unidades del protocolo, que son los paquetes SSH.

El protocolo de capa de transporte se encarga del establecimiento de la conexión de transporte, de la autenticación del servidor y intercambio de claves, y de las peticiones de servicio de los demás protocolos.

El protocolo de conexión gestiona las sesiones interactivas para la ejecución remota de comandos, mandando los datos de entrada de cliente a servidor y los de salida en sentido inverso. También se encarga de la redirección de puertos TCP.

3.2.2 Ataques contra el protocolo SSH

Muchas de las consideraciones sobre la protección que proporciona SSL/TLS son aplicables también al protocolo SSH. Este protocolo está diseñado para que un atacante no pueda leer el contenido de los mensajes ni alterarlos, y tampoco cambiar la secuencia de los mismos.

El protocolo SSH1 era vulnerable a ataques de repetición, eliminación o reordenación de paquetes porque no utilizaba números de secuencia, y también al reenvío de paquetes en sentido contrario si se utilizaba una sola clave de cifrado para ambos sentidos. Estos problemas ya no están presentes en SSH2.

La confidencialidad queda garantizada con el método de intercambio de claves basado en criptografía de clave pública, que protege contra los ataques “del hombre a medio camino” que hemos visto en el

apartado sobre SSL/TLS. Además, este método permite que el cliente se asegure de que se está conectando al servidor auténtico. Para comprobar que la clave pública que envía el servidor es realmente la suya, se pueden usar certificados, o bien una base de datos local del cliente en la que estén guardadas las claves de los servidores reconocidos. Y para autenticar al usuario mediante una clave pública (la suya o la del cliente desde el cual se conecta, dependiendo del método de autenticación), también existen las dos opciones: certificados o una base de datos de claves en el servidor.

Si no se usan certificados, el protocolo contempla la posibilidad (aunque no se recomienda) de dar por buena la clave pública de un servidor la primera vez que se establezca una conexión, sin necesidad de ninguna comunicación previa. Esto no es apropiado en un entorno donde la seguridad sea crítica, porque representa una vulnerabilidad a ataques “de hombre a medio camino”. En otros entornos, y mientras no se disponga de una infraestructura de claves ampliamente extendida, aceptar directamente claves recibidas por primera vez puede suponer un equilibrio entre comodidad de uso y seguridad.

Una característica interesante añadida a SSH2 es que las longitudes de los paquetes se envían cifradas. Un atacante que vea los datos intercambiados como un flujo de bytes no puede saber dónde empieza y dónde acaba cada paquete SSH2 (si tiene acceso al nivel de paquetes TCP puede intentar hacer deducciones, pero sin una certeza absoluta). Esto, juntamente con la posibilidad de incluir padding arbitrario (hasta 255 bytes) y enviar mensajes IGNORE, puede servir para ocultar las características del tráfico y dificultar los ataques con texto claro conocido.

3.2.3 OpenSSH

OpenSSH (Open Secure Shell) es un conjunto de aplicaciones que permiten realizar comunicaciones cifradas a través de una red, usando el protocolo SSH. Fue creado como una alternativa libre y abierta al programa Secure Shell, que es software propietario. El proyecto está liderado por Theo de Raadt, residente en Calgary.

Sus desarrolladores aseguran que OpenSSH es más seguro que el original, lo cual es debido a la conocida reputación de los desarrolladores de OpenBSD por crear código limpio y perfectamente auditado, lo que contribuye a que sea más seguro. Su seguridad también es atribuible al hecho de que su código fuente se distribuya libremente con una licencia BSD. Aunque todo el código fuente del SSH original también está disponible, existen restricciones con respecto a su uso y distribución, lo que convierte a OpenSSH en un proyecto mucho más atractivo a la hora de atraer nuevos desarrolladores.

Muchas aplicaciones pueden ser securizadas con OpenSSH, haciendo de este sistema una potente alternativa para sistemas VPN.

Cualquier aplicación que use conexiones por TCP (preferiblemente con un sólo puerto tcp) puede ser utilizada a través de túnel seguro- Algunos ejemplos de aplicaciones fácilmente tunelizables son el X Window System, http usando un proxy y VNC. El túnel para el X Window System se crea automáticamente entre dos ordenadores corriendo Unix, así que las aplicaciones con interfaz gráfico pueden ser ejecutadas desde ordenadores remotos simplemente escribiendo su nombres.

Entre las aplicaciones cuya tunelización es posible, aunque compleja, se encuentran el ftp (no es necesario, debido a la existencia de sftp) y SMB. Algunas aplicaciones llaman a OpenSSH para crear el túnel, tales como DistCC, CVS, rsync y fetchmail. Se pueden montar sistemas de archivos remotos a través de ssh usando shfs, lufs o podfuk.

El servidor OpenSSH autentica a los usuarios usando sus propios sistemas de autenticación, implementados en el propio software:

- Clave pública (id.rsa, authorized_keys)

- Contraseña
- Kerberos/GSSAPI

OpenSSH también puede usar PAM para llevar a cabo la autenticación. PAM permite la selección de métodos de autenticación y su política en tiempo de ejecución, permitiendo métodos avanzados de autenticación tales como:

- OTPW
- S/KEY
- OPIE

3.2.4 Finger

El protocolo de capa de aplicación Finger (definido por la RFC 1288), está diseñado para proporcionar información de los usuarios de una maquina local o de un servidor a través de la red TCP/IP. La información provista por el comando finger, depende de la implementación del servidor de finger. Generalmente, a través de consultas a un servidor Finger, se pueden visualizar desde los datos de un usuario particular hasta la lista de usuarios conectados a un host

Como vimos anteriormente, este protocolo proporciona información, a veces con gran detalle, de los usuarios que pertenecen a una maquina. Para hacerlo, se utiliza el comando finger desde un cliente, dándole como argumento un nombre de máquina y dominio precedido del símbolo @, y opcionalmente, un nombre de usuario. Desde el punto de vista de la seguridad, finger proporciona mucha información que podría ser de utilidad para un atacante. Una persona podría obtener nombres de usuario, hábitos de conexión, cuentas inactivas, incluso algunos administradores completan exhaustivamente la información de finger, con datos como sus oficinas y números telefónicos. Esta información podría ser fácilmente aprovechable por alguna entidad externa para practicar ingeniería social contra el personal de la organización.

Las principales características de finger que debería tener en cuenta son:

- No utiliza autenticación.
- No cifra los datos que transmite (por lo que pueden ser interceptados e interpretados).
- Muestra los nombres de usuarios actualmente conectados y desde dónde están conectados. Esto no sólo revela nombres válidos de usuarios en el sistema, sino que también puede ayudar a conocer la topología de la red privada.
- Brinda toda la información que el administrador (o los usuarios) hayan cargado sobre sus perfiles.

El servicio de finger, debe ser habilitado con mucha precaución en un servidor. Tenga en cuenta que el comienzo de un ataque consiste en recabar información y la función de este servicio es precisamente publicar información. Como se mencionó anteriormente, el servicio finger no incorpora un mecanismo de autenticación, por este motivo, si se necesita habilitar este servicio debería incorporar alguna herramienta que permita filtrar los accesos no deseados.

3.2.5 FTP

El protocolo FTP (File Transfer Protocol) es el estándar actual para la transferencia de archivos en redes TCP/IP. Este servicio utiliza el protocolo TCP para sus conexiones y un modelo cliente/servidor.

Las principales características de FTP son:

- Brinda un acceso interactivo: Aunque puede utilizarse software de aplicación para realizar las transferencias mediante FTP, la mayoría de las implementaciones de los sistemas operativos proporcionan una interfaz interactiva, es decir a través del uso de comandos, para acceder a servidores remotos.
- Permite especificar un formato de representación para la transferencia, optando entre texto o binario: Un usuario puede especificar si va a transferir un archivo de texto o binario, así como el formato de texto que utilizan.
- Realiza control de autenticación: Antes de realizar la transferencia de archivos, es obligatorio que cada cliente se autentique con el servidor proporcionando un nombre de usuario y contraseña válidos.

Antes de desarrollar la metodología y características de las conexiones en FTP es importante identificar dos implementaciones diferentes de este protocolo (ambas utilizan TCP para sus conexiones):

- FTP Estándar: Fue la primera implementación del protocolo. En las transferencias de archivos con FTP estándar el cliente inicia una conexión hacia el servidor (al puerto 21) y es el servidor quien posteriormente inicia una conexión hacia el cliente, desde el puerto 20 a un puerto establecido por el cliente en la conexión que realizó inicialmente.
- FTP Pasivo: El método de transferencias de archivo por FTP "Pasivo" es un mecanismo más seguro para la transmisión de información, definido por la RFC 959. Aquí el flujo de datos es configurado e iniciado por el programa FTP del cliente en lugar de ser el software FTP del servidor. Así, las conexiones se inician siempre desde el interior de la red hacia el servidor (cosa que con el FTP estándar no sucedía, ya que la conexión para el canal de datos, se realizaba desde el puerto 20 del servidor hacia un puerto del cliente).

Forma de conexión: Tanto en el uso de FTP estándar como FTP pasivo, el cliente inicia una conexión hacia el servidor al puerto 21 (convencionalmente asignado a ese servicio) utilizando TCP. Esta comunicación se suele llamar, canal de control (o conexión de control). Si se utiliza una comunicación por FTP estándar, el cliente utiliza este canal para enviar un paquete con el comando PORT y establecer el número de puerto que utilizará con el servidor para la transferencia de datos. Así, el servidor inicia una conexión desde el puerto 20 local (utilizando también TCP) hacia el número de puerto establecido por cliente en el canal de control. Este nuevo canal generalmente es llamado conexión de transferencia de datos.

Si en lugar de utilizar FTP estándar, se utiliza FTP pasivo, en lugar de enviar un paquete con el comando PORT el cliente envía el comando PASV. Este comando tiene como objetivo averiguar el puerto que usará el servidor para la conexión de transferencia de datos. Posteriormente el cliente inicia una conexión a ese puerto del servidor donde se realiza la conexión para la transferencia de datos.

Las conexiones de transferencia de datos pueden crearse de manera dinámica cuando se necesiten, pero la conexión de control continúa a través de toda la sesión del usuario. Una vez que la conexión de control desaparece, la sesión finaliza y el software en ambos extremos termina todos los procesos de transferencia de datos.

Como se describió anteriormente, las características del servicio FTP hacen que la autorización sea un proceso obligatorio, por lo cual sólo los clientes que cuenten con un usuario y contraseñas válidos en el servidor podrían tener acceso. Con el fin de facilitar el acceso a determinados archivos públicos, la mayoría de los servidores FTP permiten el acceso de un usuario anónimo, generalmente llamado anonymous. El acceso al FTP anónimo significa que el cliente no necesita tener un usuario y contraseña propios para utilizar el servicio, sino que ingresa como invitado con las restricciones que

imponga el administrador del servicio.

Se debe recordar que este servicio es autenticado, entonces podemos aprovechar esta característica para definir en forma cuidadosa los datos y directorios a los que tendrá acceso cada usuario, especialmente el usuario anónimo. Respecto a este último, si no son necesarios los accesos anónimos, convendrá deshabilitarlo. Por otro lado, si debe permitir los accesos anónimos, sería recomendable que los usuarios anónimos sólo puedan descargar información del servidor. Otra característica importante, respecto a la seguridad del protocolo, es que la transferencia de datos se realiza en texto claro, entonces, si nos encontramos en una red de difusión, como Ethernet, Token Ring o FDDI, cualquier estación podría interceptar e interpretar los datos, nombres de usuarios y contraseñas que se envíen por FTP

3.2.6 TFTP

El protocolo TFTP (Trivial File Transfer Protocol - Protocolo de Transferencia de Archivos Trivial) es un protocolo de transferencia de archivos muy simple . Utiliza el protocolo UDP y tiene las siguientes características:

- Provee control de errores para cada datagrama.
- No realiza una conexión entre el Cliente y el Servidor.
- No provee control de flujo.
- No provee acceso interactivo.
- No provee autenticación.

La simplicidad de este protocolo permite su implementación en dispositivos con escasos recursos, de memoria y almacenamiento, por ejemplo algunos modelos de routers lo utilizan para actualizar sus sistemas operativos. Generalmente se utiliza en ambientes controlados, por ejemplo dentro de una LAN, dado que no es confiable.

TFTP permite realizar transferencias de archivos entre un cliente y un servidor, el cliente realiza la solicitud inicial al puerto UDP número 69 del servidor. Debido a que su implementación es muy sencilla, prácticamente cualquier error causará la finalización de la transferencia; a excepción de la pérdida de un segmento, que causará la retransmisión del último transmitido.

Para iniciar una transferencia, el cliente envía una petición de lectura o escritura al servidor. Si el servidor acepta el requerimiento, se transfiere el archivo en bloques de tamaño fijo de 512 bytes. Cada bloque se enumera consecutivamente, comenzando desde 1. Cada paquete debe ser reconocido con un acuse de recibo antes que el siguiente sea transferido. Cuando se recibe un paquete con un tamaño menor a 512 bytes se asume que es el fin de la transferencia

Inicialmente, el cliente envía una solicitud al servidor al puerto UDP 69, el servidor responde a la solicitud asignando un puerto diferente, que se utilizará para el resto de la transferencia.

TFTP es un protocolo que no provee autenticación de usuarios, ni encriptación de datos en tránsito, por lo que puede considerarse un protocolo no seguro. Debido a esto es recomendable no implementar este servicio, por otro lado si es necesario para realizar transferencias entre dispositivos, debemos controlar los archivos y directorios que estarán expuestos. Generalmente, sólo se permite la lectura de archivos, pero no la escritura.

Las últimas versiones de TFTP se configuran de forma predeterminada para prohibir el acceso a cualquier directorio, excepto a /tftpboot. Este hecho es una buena medida, pero aún así los atacantes

pueden obtener cualquier archivo contenido en este directorio. Esto incluye la obtención de archivos delicados de configuración de routers, previa obtención del nombre del archivo que, generalmente, es "nombre del router".cfg. En muchos casos el intruso conseguiría acceder a las contraseñas del router y de las comunidades SNMP (En la sección 3.8 - SNMP, puede obtener información adicional sobre este protocolo) .

En algunas implementaciones de TFTP se puede especificar una lista de hosts, a través de direcciones IP o nombres DNS, que tendrán permitida o denegada la escritura y/o lectura de archivos, si no existe esta posibilidad, deberíamos contemplar alguna técnica auxiliar para controlar el acceso al servidor TFTP.

3.2.7 DHCP

El Protocolo de Configuración Dinámica de Hosts (DHCP) fue diseñado por la IETF como el sucesor del protocolo BOOTP para la configuración automática de hosts en una red TCP/IP. El protocolo DHCP mejora a su antecesor principalmente en dos aspectos:

- DHCP permite que el host reciba toda la información que pueda necesitar para su configuración de red en un solo mensaje (por ejemplo, además de su dirección IP, puede recibir la máscara de subred, la dirección de un gateway y de un servidor DNS)
- DHCP utiliza un mecanismo de asignación de direcciones IP en forma dinámica. Así, el servidor DHCP mantiene un conjunto de direcciones IP y a medida que los clientes le solicitan direcciones, se las asigna por un período de tiempo determinado.

DHCP está implementado según el modelo cliente - servidor, es decir, debemos tener un servidor DHCP configurado en nuestra red local. Actualmente es el protocolo de configuración dinámica más difundido y de uso generalizado. En redes TCP/IP extensas representa una herramienta de gran utilidad para los administradores de red, por un lado reduce la cantidad de errores en las configuraciones de los hosts y, por otro lado permite una utilización más eficiente de las direcciones IP. La configuración automática de hosts a través del protocolo DHCP fue un gran avance en contraste con BOOTP. Un servidor DHCP puede ser configurado para realizar asignaciones estáticas de IP a clientes según la dirección MAC de cada cliente, como así también puede entregar direcciones IP de un conjunto de direcciones en forma dinámica sin tener en cuenta quien se las pida. Las direcciones que entrega un servidor DHCP a los clientes son asignadas por un período de tiempo determinado. Según los requisitos o las necesidades de cada LAN el tiempo de asignación de la dirección puede variar de minutos a horas. Todo el proceso de comunicación entre el cliente y el servidor DHCP se realiza utilizando el protocolo UDP, a través del puerto 67 en el servidor

Cuando un cliente necesita configurarse en forma automática a través de DHCP, el proceso de solicitud y asignación de la configuración consiste en un diálogo entre el cliente y el servidor DHCP (o los servidores). El primer paso que realiza el cliente es enviar un mensaje de broadcast a toda la red local con el fin de encontrar algún servidor DHCP (el mensaje DHCPDISCOVER. En la figura se puede ver una descripción de los posibles valores a los tipos de mensajes DHCP). Una vez que el cliente envía el paquete DHCPDISCOVER, queda a la espera de respuestas de servidores DHCP que existan en la red. Los paquetes DHCPDISCOVER tienen como destino una dirección broadcast, con el fin de asegurar que todos los hosts de la red reciban el paquete.

Todos los hosts y servidores DHCP de la red local reciben el mensaje del cliente. Sólo los servidores DHCP interpretan el mensaje y le contestan al cliente enviando un paquete DHCPOFFER. El cliente puede recibir cero o más respuestas a su solicitud.

Cuando el cliente recibe las ofertas de los servidores, selecciona una (por ejemplo, la primera en llegar) y negocia con el servidor el tiempo de la dirección IP y demás información de configuración. Para esto, el cliente le responde a servidor DHCP seleccionado con un paquete DHCPREQUEST. La figura muestra la información que un cliente generalmente obtiene de un servidor DHCP.

Con el objeto de enviar un acuse de recibo al cliente el servidor le envía un paquete DHCPACK

Un cliente que recibió toda su configuración TCP/IP a través de DHCP y no necesita más acceso a la red antes que finalice el tiempo que el servidor le asignó su dirección, puede enviarle un paquete DHCPRELEASE con el fin de comunicarle que liberó su dirección IP. En el caso que el cliente de red necesite mantener acceso a la red por un tiempo posterior al asignado por el servidor, necesita renegociar su asignación. La figura muestra como un cliente realiza el período de renovación. Dentro de un ambiente DHCP hay que tomar ciertos recaudos para evitar el uso indebido.

Si revisamos el proceso utilizado por DHCP, podemos ver que el primer paquete enviado por una estación cliente DHCP (DHCP Discover), es un broadcast a toda la red. Este broadcast puede ser respondido por cualquier servidor que se encuentre en la red local. De esta manera una estación cualquiera que implemente un servidor DHCP podrá asignar direcciones IP a su parecer, provocando problemas de comunicación entre las estaciones de la red local .

Otro aspecto a tener en cuenta depende del tipo de asignaciones que estemos realizando.

- Si estamos realizando asignación dinámica de direcciones, podría suceder que una estación externa a nuestra red, se conecte a ella y reciba una dirección válida, obteniendo los mismos permisos y privilegios que una estación interna .
- Si estamos realizando asignación estática de direcciones, una estación maliciosa podría engañar al servidor DHCP cambiando intencionalmente la dirección MAC de sus tramas para obtener una dirección IP

3.2.8 SNMP

SNMP (Simple Network Management Protocol o Protocolo simple de administración de red) es un protocolo de capa de aplicación que facilita el intercambio de información entre dispositivos de red. SNMP permite a los administradores monitorear la performance de la red, el funcionamiento de los dispositivos, encontrar y solucionar problemas.

Existen actualmente tres versiones de SNMP: SNMP Versión 1 (SNMPv1), SNMP Versión 2 (SNMPv2) y SNMP Versión 3 (SNMPv3). Las tres versiones mantienen características en común, en SNMPv2 se agregaron nuevas operaciones sobre los dispositivos y en SNMPv3 se mejoró la seguridad del protocolo de administración.

El protocolo SNMP permite a un administrador de red supervisar y controlar el funcionamiento de uno o más dispositivos a través de una red. SNMP utiliza el protocolo UDP en el puerto 161

SNMP define tres elementos:

- Dispositivos administrados
- Agentes
- NMSs (Network Management Stations - Estaciones de administración de red)

Un dispositivo administrado es un host que contiene un agente SNMP. Los dispositivos administrados recolectan información la guardan y la dejan disponible para las NMSs. Routers, switches, hubs, estaciones de trabajo e impresoras pueden ser dispositivos administrados.

Un agente es un software que ejecutan los dispositivos administrados. Un agente tiene el conocimiento local de la información de red del dispositivo y la traduce en una forma compatible al protocolo SNMP.

Las NMSs proveen la mayor parte del procesamiento y requerimientos del sistema de administración. Pueden existir más de una NMS. Cada estación de administración se conecta a los dispositivos administrados y recolecta la información que tengan disponible. Así, las estaciones de administración concentran toda la información de los dispositivos de red administrados y la procesan para que sea fácilmente comprensible.

Una MIB (Management Information Base - Base de Información para Administración) es un conjunto de información organizada jerárquicamente. Esta información está compuesta por los objetos que son administrados de cada dispositivo, identificados por identificadores de objeto (OI).

Un objeto administrado (también llamado objeto MIB, objeto, o un MIB) es una característica específica del dispositivo administrado. Estos objetos administrados están formados por una o más variables que informan su estado. Dentro de una jerarquía MIB el dentificador de objeto (OI o Object ID) es único. La jerarquía MIB puede ser descripta como un árbol con una raíz sin nombre, de la cual se asignan niveles a diferentes organizaciones.

Los OI del primer nivel son asignados a diferentes organizaciones estándar, mientras que los objetos de niveles inferiores son asignados por organizaciones asociadas. Los fabricantes pueden definir ramas privadas que incluyan objetos administrados para sus productos específicos. Generalmente, las MIBs que no están estandarizadas son posicionadas en ramas experimentales.

Un ejemplo de un objeto administrado es ipAddrTable, que es un objeto de la categoría IP, que reporta el número IP asociado a cada interfaz. Este objeto puede ser identificado unívocamente por el nombre de su objeto: iso . identified-organization . dod . internet . mgmt . mib . ip . ipAddrTable o por su descriptor de objeto equivalente: 1.3.6.1.2.1.4.20

Aunque pueda parecer complejo el método para definir y llegar a un objeto, proporciona una herramienta muy poderosa que permite a las estaciones explorar las diferentes MIB de los distintos dispositivos en una forma rápida y simple.

SNMPv1 constituye la primera definición e implementación del protocolo SNMP, estando descrito en las RFC 1155, 1157 y 1212 del IETF (Internet Engineering Task Force). El vertiginoso crecimiento de SNMP desde su aparición en 1988, puso pronto en evidencia sus debilidades, principalmente su imposibilidad de especificar de una forma sencilla la transferencia de grandes bloques de datos y la ausencia de mecanismos de seguridad; debilidades que tratarían de ser subsanadas en las posteriores definiciones del protocolo.

SNMPv2 apareció en 1993, estando definido en las RFC 1441-1452. SNMPv1 y SNMPv2 tienen muchas características en común, siendo la principal mejora la introducción de tres nuevas operaciones de protocolo:

- GetBulk para que el gestor recupere de una forma eficiente grandes bloques de datos, tales como las columnas de una tabla. Inform para que un agente envíe información espontánea al gestor y reciba una confirmación.
- Report para que el agente envíe de forma espontánea excepciones y errores de protocolo.

SNMPv2 también incorpora un conjunto mayor de códigos de error y más colecciones de datos. En 1995 apareció una revisión de SNMPv2, denominada SNMPv2c, descripta en las RFC 1901-1910, que incluye una configuración más sencilla y mayor modularidad. La RFC 1446 describe también un mecanismo para la segurización en el protocolo SNMPv2 a través de MD5. La nueva y última versión de SNMP, SNMPv3, refuerza las prestaciones de seguridad, incluyendo autenticación, privacidad y control de acceso; y de administración de protocolo, con una mayor modularidad y la posibilidad de configuración remota .

SNMPv3 apareció en 1997, estando descrito en las RFC 1902-1908 y 2271-2275. Cabe destacar que SNMPv3 no se trata de un estándar que reemplaza a SNMPv1 y/o SNMPv2, sino que define una serie de capacidades adicionales de seguridad y administración a ser utilizadas en conjunto con SNMPv2 (preferiblemente) o SNMPv1. Estas mejoras harán que SNMP se constituya en un protocolo de gestión con altas prestaciones para todo tipo de redes.

El modelo de seguridad basado en usuario o USM (User-Based Security Model) proporciona los servicios de autenticación y privacidad en SNMPv3. El mecanismo de autenticación en USM asegura que un mensaje recibido fue trasmitido por el origen y además, que el mensaje no fue alterado durante su tránsito y que no fue artificialmente retardado o repetido.

Para conseguir la autenticación, el gestor y el agente que desean comunicarse deben compartir la misma clave de autenticación secreta configurada previamente fuera de SNMPv3 (no es almacenada en la MIB y no es accesible mediante SNMP). Por otro lado, la facilidad de privacidad de USM posibilita a los gestores y a los agentes encriptar mensajes para prevenir que sean analizados por intrusos. De nuevo, el gestor y el agente deben compartir una clave secreta configurada previamente (En el Modulo 2 - Capítulo 2- Seguridad de los datos : Encriptación, se describen en detalle los algoritmos de clave compartida).

El modelo de control de acceso basado en vistas o VCAM (Views-Based Access Control Model) permite proporcionar diferentes niveles de acceso a las MIB de los agentes para los distintos gestores en SNMPv3. Un agente puede, de este modo, restringir el acceso para determinados NMS a parte de su MIB o bien limitar las operaciones que podrán realizar. La política de control de acceso a ser utilizada por el agente para cada NMS debe estar configurada previamente; consistiendo básicamente en una tabla que detalla los privilegios de acceso para los distintos NMS autorizados. Mientras que la autenticación es realizada por usuario, el control de acceso es realizado por grupos, donde un grupo sería un conjunto de usuarios.

SNMP es un protocolo de requerimiento-respuesta. El sistema de administración genera un requerimiento, y los dispositivos administrados devuelven una respuesta. El acceso de las NMS a los dispositivos administrados está controlado por un nombre de "comunidad". Cada dispositivo tiene configurado una comunidad (o más) con un nombre que deben conocer las NMS para poder accederlo y obtener sus datos. Generalmente las comunidades que se utilizan son:

- *public*: generalmente configurada en los agentes para permitir el acceso de lectura a sus datos
- *private*: generalmente configurada en los agentes para permitir el acceso de lectura y modificación de sus datos

Los nombres de las comunidades pueden ser modificados en los agentes con el fin de impedir el acceso a una NMS que no conozca el nombre de la comunidad.

Cuando un agente y una NMS están configuradas en la misma comunidad, las NMS le envían solicitudes (a través de comandos) y esperan las respuestas del agente. Este comportamiento es implementado usando una de las cuatro operaciones:

- Get: es utilizada por la NMS para obtener el valor de una o más instancias de un objeto de un agente. Si el agente no puede proveer el valor de todas las instancias del objeto en una lista, no devuelve ningún valor.
- GetNext: es utilizada por la NMS para obtener los valores de la siguiente instancia en una tabla o lista.
- Set: es utilizada por la NMS para establecer los valores de las instancias de un objeto.
- Trap: es utilizada por los agentes para reportar de forma espontánea (no esperan la consulta de la NMS) ciertos eventos.

En la versión 2 de SNMP se incorporaron tres operaciones más:

- GetBulk: es utilizada para la recuperación de grandes bloques de datos en forma eficiente, tales como las columnas de una tabla.
- Inform: es utilizada para el envío de información espontánea al gestor y que reciba una confirmación.
- Report: es utilizada por el agente para el envío espontáneo de excepciones y errores de protocolo.

Se debe tener en cuenta que SNMPv1 y SNMPv2 no poseen encriptación de los datos que transmiten. En redes con medios compartidos, esto podría permitir que una persona no autorizada pueda estar "escuchando" y así recabar información (como modelos de dispositivos, direccionamiento, nombres de comunidades, etc.) que revele datos de la red .

Otro punto a tener en cuenta, es la falta de autenticación de SNMPv1 y SNMPv2, es decir, la única verificación que realizan los agentes SNMP antes de responder las solicitudes realizadas por la NMS es que concuerde el nombre de comunidad. Esto es muy importante si consideramos que la mayoría de las implementaciones de los dispositivos utilizan dos nombres por defectos para identificar la comunidad: public y private (el primer nombre de comunidad generalmente premite el acceso de sólo lectura a los datos mientras que el segundo tiene permisos de modificación). Así, un usuario malicioso podría intentar acceder a los dispositivos administrados adivinando el nombre de la comunidad y acceder a toda la información almacenada en los dispositivos. Por otro lado, la falta de autenticación entre las NMS y los dispositivos administrados permitiría a un atacante modificar la información que envían, tanto los dispositivos administrados como las NMS, y de esta forma reportar datos falsos pudiendo causar un caos en la administración de la red . A diferencia de sus predecesores SNMPv3 soporta autenticación, a través de MD5, y encriptación de datos, lo que permite crear un ambiente seguro ante los tipos de ataques arriba descriptos. Tenga en cuenta que SNMPv3 es un protocolo reciente, por lo que debe asegurarse que tanto sus dispositivos como sus estaciones de administración lo soporten.

3.2.9 DNS

En los comienzos de Internet, para identificar los diferentes hosts se utilizaba únicamente las direcciones IP. Esto evolucionó rápidamente en la utilización de nombres simbólicos de host. De forma que en lugar de identificar a un host con su dirección IP, se utilizaba un nombre compuesto por caracteres. Esto introdujo el problema de mantener la relación de direcciones IP a nombres de una forma centralizada y coordinada.

Inicialmente, la relación de nombres a direcciones IP se mantenía por el Network Information Center (NIC) en un solo archivo llamado HOSTS.TXT, que era tomado por todas las estaciones utilizando FTP. Debido al crecimiento explosivo de Internet, este mecanismo dejó de ser práctico y fue reemplazado por un nuevo concepto: El Sistema de Nombres de Dominio (DNS).

El sistema de nombres de dominio permite que una estación obtenga la dirección IP de un nombre dado de forma dinámica, sin necesidad de mantener un archivo centralizado con todas las relaciones . El sistema de nombres de dominio es un sistema distribuido, donde miles de servidores conforman la estructura del sistema, y cada uno mantiene sólo una porción del direccionamiento. Los mensajes DNS pueden ser transmitidos mediante TCP o UDP, en ambos casos se utiliza el puerto 53. Si se utiliza UDP, el tamaño máximo de segmento es de 512 bytes, mientras que si se utiliza TCP, en el comienzo del segmento se especifica el tamaño total.

En el estándar que define DNS, se especifica que para consultas comunes se debe utilizar preferentemente UDP. Si la respuesta debe ser separada (debido al límite de 512 bytes), se debe utilizar TCP. Se prefiere UDP sobre TCP debido a que UDP tiene menos overhead que TCP. En muy

raros casos una respuesta excede los 512 bytes. Para realizar las transferencias de zonas (veremos más adelante el concepto de zonas) se debe utilizar TCP, dado que en este caso, la cantidad de datos a transferir es mucho mayor que 512 bytes. El espacio de nombres de dominio es un espacio jerárquico, donde existen dominios y subdominios, conformando un árbol de dominios. Considere el dominio pc1.aula3.deptoinf.facultad.edu. Aquí, aula3.deptoinf.facultad.edu es el nombre de dominio de más bajo nivel, aula3 es un subdominio de deptoinf.facultad.edu, que a su vez es un subdominio de facultad.edu, un subdomino de edu. La jerarquía de nombres se puede representar a través de un árbol jerárquico

Dominios Genéricos: Los nombres compuestos por tres caracteres que conforman los dominios de más alto nivel, son llamados dominios genéricos, o dominios organizacionales.

Dominios nacionales: Existen también dominios de alto nivel para cada código de país conforme a la ISO 3166 (desde .ae para los Emiratos Árabes Unidos hasta zw para Zimbawe). Estos son llamados dominios nacionales o geográficos. La mayoría de los países, dentro de sus dominios, tienen una estructura similar a los dominios genéricos, así es como podemos encontrar dominios edu.ar, .com.uk, .gov.uy, etc.

El sistema de nombres de dominio utiliza un concepto de espacio de nombres distribuido. Los nombres simbólicos se encuentran agrupados en "zonas de autoridad", o como se las llama comúnmente, zonas. En cada una de estas zonas, uno o más hosts tienen la tarea de mantener la base de datos de nombres a direcciones IP y proveer la tarea de servidores para responder las consultas de otras estaciones. Estos servidores de nombres locales se encuentran interconectados a la jerarquía de nombres de dominio. Cada zona contiene una parte o una "rama" del árbol jerárquico, y los nombres dentro de la zona son administrados de forma independiente al resto de las zonas. El comienzo de todo el árbol es la zona "." o root. Dentro de una zona, pueden existir subdominios que pueden ser delegados a servidores diferentes. Consideremos por ejemplo una consulta para seguridad.proydesa.org.ar y que nuestro servidor no tiene la respuesta en su caché. La consulta será reenviada hasta el servidor raíz (.), quien reenviará la consulta al servidor que tenga la delegación para el dominio ar. Este servidor, a su vez, reenviará la consulta al servidor que tenga la delegación org, y así sucesivamente, hasta llegar al servidor que tenga la respuesta. Puede suceder que en alguno de estos pasos, algún servidor haya tenido en caché la respuesta, con lo que responderá con la dirección IP solicitada, en lugar de reenviarla a otro servidor.

Como resultado de este esquema, se obtienen las siguientes ventajas:

- En lugar de mantener una base de datos centralizada, la carga de mantenimiento se encuentra distribuida en múltiples servidores.
- La autoridad y responsabilidad para crear y modificar los nombres simbólicos se delega a los propietarios de la organización a la que pertenecen esos nombres.
- Desde el punto de vista del usuario es totalmente transparente: envía una solicitud, que es respondida por un servidor.

El proceso de resolución de nombres de dominio puede ser resumido en los siguientes pasos:

1. Un programa de usuario realiza una solicitud de resolución.
2. El cliente DNS (llamado resolver) revisa su tabla de caché para buscar si ya ha realizado la consulta. Si no la ha realizado, envía la solicitud al servidor DNS que tiene configurado.
3. El servidor recibe la solicitud y comprueba si la respuesta se encuentra dentro de su autoridad, si es así, responde la consulta. De otra forma, consultará a otros servidores disponibles, partiendo desde los servidores root, hasta conseguir la respuesta.
4. El programa de usuario recibirá la dirección IP del nombre consultado o un error si no se pudo

obtener. Normalmente, el programa no recibirá la lista de todos los servidores consultados.

Los mensajes de consultas y respuestas son transportados por UDP o TCP. Este proceso se realiza siguiendo un modelo cliente servidor. La función cliente es transparente para el usuario y es llamada por las aplicaciones para realizar las resoluciones. El servidor de nombres, es una aplicación servidora que provee las traducciones de nombres a direcciones IP.

Operación del resolver: Las consultas de nombres pueden ser de dos tipos: recursivas o iterativas. Un bit dentro de la solicitud especifica si el cliente solicita una consulta recursiva o iterativa. La diferencia entre las consultas se da cuando el servidor consultado no puede resolver la consulta. Si el cliente solicita una consulta recursiva (la mayoría de los casos) significa que el servidor deberá consultar hasta obtener una respuesta para la solicitud. Si el cliente solicita una consulta iterativa, el servidor enviará como respuesta la información que tenga disponible y una lista de servidores adicionales para que el cliente pueda consultar directamente.

Las respuestas de nombres de dominio, pueden ser de dos tipos: autoritativas o no-autoritativas. Un bit dentro de la respuesta especifica el tipo. Cuando un servidor recibe una consulta para un dominio de una zona sobre la que tiene autoridad, enviará una respuesta autoritativa. Cuando recibe una consulta para un dominio sobre el que no tiene autoridad, su acción depende del tipo de consulta:

- Si es una consulta de tipo recursiva, reenviará la consulta hacia otro servidor con autoridad, o hacia los servidores root. Si el segundo servidor no responde con una respuesta autoritativa (por ejemplo si ha delegado la zona a otro servidor), el proceso es repetido hasta obtener la respuesta. El servidor enviará esta respuesta de tipo no-autoritativa. Cuando un servidor o un resolver obtiene una respuesta, la guarda en caché para mejorar la performance de consultas posteriores. La entrada en caché será guardada por un período de tiempo especificado por el origen en un campo dentro de la respuesta (TTL). Típicamente 172800 segundos (dos días).
- Si es una consulta de tipo iterativa, enviará la información que tenga en su caché, más una lista de servidores de nombre para ser contactados para información autoritativa.

La base de datos distribuida del sistema de nombres de dominio está compuesta por registros de recursos (RR), los cuales se encuentran divididos en diferentes clases para diferentes tipos de redes. Aquí se estudiarán sólo los registros correspondientes a la clase Internet.

Los registros de recursos proveen un mapeo entre nombres de dominio y objetos de red. Los objetos de red más comunes son las direcciones de los hosts de internet, pero el sistema de nombres de dominio se encuentra designado para ubicar un amplio rango de objetos. Una zona consiste en un grupo de registros de recursos, comenzando con un registro "Start of Authority" (SOA). El registro SOA identifica el nombre de dominio de la zona. Deberá haber un registro Name Server (NS) para el servidor de dominio primario de la zona. También pueden existir registros NS para los servidores de nombres de dominio secundarios de la zona. Los registros NS son usados para identificar cuál de los servidores de dominio son "autoritativos" o tienen a cargo la zona. Luego, vienen los demás registros de recursos, que pueden mapear nombres a direcciones IP, o alias a nombres. El formato general de un registro de recurso se puede observar en la figura. Donde:

- Nombre: El nombre de dominio a ser definido. El DNS es muy general en las reglas de composición de sus nombres. Sin embargo, recomienda una sintaxis para los nombres de dominio que minimizarán la posibilidad que las aplicaciones que utilizan DNS interpreten erróneamente un nombre de dominio. Un nombre que cumple con la recomendación, debe consistir en una serie de etiquetas compuestas por caracteres alfanuméricos o guiones, con una longitud entre 1 y 63 caracteres, comenzando con un caracter alfabético. Cada etiqueta se encuentra separada por puntos ".". Los nombres de dominio no distinguen entre mayúsculas y minúsculas.

- TTL: El tiempo de vida en segundos en los que este registro deberá ser guardado en caché.
- Clase: Identifica la familia de protocolos. El valor usado generalmente es IN (Internet).
- Tipo: Identifica los diferentes tipos de recursos en este registro. Los diferentes tipos se encuentran descriptos por los RFC 1034, 1035 y 1706
- Rdata: El valor depende del tipo, por ejemplo:
    - A: una dirección IP (si la clase es IN)
    - CNAME: un nombre de dominio
    - MX: (Mail eXchanger) un valor de 16 bits que indica preferencia (valores más bajos indican mayor preferencia) seguido por un nombre de dominio
    - NS: un nombre de host
    - PTR: un nombre de dominio

El sistema de nombres de dominio provee mapeos de nombres simbólicos a direcciones IP y viceversa. El método para buscar un nombre de dominio dentro de la base de datos es relativamente simple, dada la estructura jerárquica. El proceso reverso, no puede seguir la jerarquía. Por lo tanto, existe otro espacio de nombres para mapeos reversos. El dominio se denomina in-addr.arpa (se utiliza arpa dado que Internet originalmente era ARPAnet).

Las direcciones IP normalmente se representan mediante cuatro números separados por coma, y existe un subdominio para cada jerarquía. Sin embargo, dado que los nombres de dominio tienen la parte menos significativa del nombre al comienzo (es decir, un nombre va de lo particular -un host- a lo general -el dominio-) y que las direcciones IP tienen sus bytes más significativos al comienzo (una dirección IP va de lo general -red- a lo particular -host-), las direcciones IP se escriben en orden inverso. Por ejemplo, el dominio del nombre de dominio correspondiente a 129.34.139.30 es 30.139.34.129.in-addr.arpa. Dada una dirección IP, el sistema de nombres de dominio puede ser usado para encontrar el nombre de host mapeado. Una consulta para encontrar un nombre de dominio asociado a una dirección IP se denomina consulta "pointer".

En internet se encuentra disponible mucha información sobre los diferentes dominios que existen. Una herramienta creada para la obtención de dicha información es el WHOIS. Existen muchas bases de datos WHOIS que se pueden consultar y que pueden proveer información sobre un dominio específico o sobre un bloque de direcciones IP. Para consultar las distintas bases de datos whois existen diferentes mecanismos. Se pueden realizar consultas mediante la página web perteneciente a la entidad ARIN (American Registry for Internet Numbers) o mediante un cliente whois instalado en una estación.

La información obtenida para un dominio puede contener lo siguiente:

- Registro: Información del registro y de los servidores whois
- Empresa: Información sobre la empresa propietaria del dominio
- Dominio: Información referente al dominio
- Bloque de direcciones IP: Bloque de direcciones IP asignado
- Punto de contacto: Información sobre la persona a cargo

Entidad	Descripción	Dirección
ARIN	American Registry for Internet Numbers	http://www.arin.net
APNIC	Asia Pacific Network Information Centre	http://www.apnic.net
LACNIC	Latin American and Caribbean IP address Regional Registry	http://www.lacnic.net
RIPE NCC	RIPE Network Coordination Centre	http://www.ripe.net
AfriNIC	African Network Information Center	http://www.afrinic.org

Existen diferentes tipos de amenazas al sistema de nombres de dominio, que en general no tienen como objetivo específico el servicio DNS, sino que son un paso intermedio en el proceso de un ataque. El mayor inconveniente de DNS es que no realiza autenticación ni cifrado de las consultas y las respuestas, y en general, sólo comprenden un mensaje UDP para la consulta y un mensaje UDP para la respuesta. Aquí listaremos las amenazas más importantes al sistema de nombres de dominio:

Modificación de un paquete: Una de las amenazas más simples contra DNS son las modificaciones de los paquetes enviados para realizar una consulta o una respuesta. En estos casos, el atacante modifica un paquete para inyectar información propia, por ejemplo, con el objetivo de engañar sobre una dirección IP.

Ataques basados en nombres: Otro tipo de ataques que pueden inyectar información falsa son los ataques basados en nombres, generalmente llamados "caché poisoning". Aquí, lo que realiza el atacante es agregar información a una respuesta, para "envenenar" la caché del resolver de una estación. De esta forma, se pueden agregar relaciones de nombres a direcciones IP a voluntad del atacante.

DNS Spoofing: Este ataque hace referencia al falseamiento de una dirección IP ante una consulta de resolución de nombre (esto es, resolver con una dirección falsa un cierto nombre DNS), o viceversa (resolver con un nombre falso una cierta dirección IP) debido a la falta de autenticación de este servicio. Esto se puede conseguir de diferentes formas, desde modificando las entradas del servidor encargado de resolver una cierta petición para falsear las relaciones dirección-nombre, hasta comprometiendo un servidor que infecte la caché de otro (lo que se conoce como DNS Poisoning); incluso sin acceso a un servidor DNS real, un atacante puede enviar datos falseados como respuesta a una petición de su víctima sin más que averiguar los números de secuencia correctos.

Denegación de Servicio: Así como cualquier otro servicio, el sistema de nombres de dominio es vulnerable a ataques por Denegación de Servicio (DoS). Aún peor, los servidores DNS pueden ser utilizados como amplificadores de DoS, dado que los paquetes de respuesta son significativamente mayores que los paquetes de solicitudes. Una alternativa para defendernos de los ataques al sistema de nombres de dominio es utilizar DNS Security (DNSSEC). DNSSEC es un método para suministrar autenticación a las consultas DNS. Esto asegura que los datos no han sido modificados durante el viaje desde el cliente hacia el servidor y viceversa. Cabe notar que este método sólo soluciona los ataques por modificación y basados en nombre, pero no realiza nada contra las denegaciones de servicio. Otra alternativa para solucionar los problemas de seguridad son las herramientas provistas

por las implementaciones de servidores DNS. En general, proveen filtros asociados a las transferencias de zonas (por ejemplo, sólo permitirán transferir zonas completas a los servidores propios), filtros para limitar las consultas, etc.

3.2.10 NetBIOS

El protocolo NetBIOS fue desarrollado por Sytec para IBM en 1983. En sus comienzos operaba sólo sobre un protocolo propietario de Sytec diseñado para las redes locales de IBM. Este protocolo, permitía una arquitectura de bus para la LAN con limitaciones de 70 a 80 estaciones.

Con el lanzamiento de Token-Ring, se implementó un emulador de NetBIOS que permitía su operación en estas nuevas redes. En 1985 se introdujo el protocolo NetBEUI (NetBIOS Extended User Interface) que permitió, entre otras cosas, la ampliación de hasta 260 dispositivos en un anillo y múltiples anillos conectados por puentes. En 1987, la RFC 1001 definió un estándar para los servicios de NetBIOS sobre TCP y UDP. Este protocolo actualmente es muy utilizado, junto con el protocolo SMB, por la familia de productos Microsoft para compartir recursos en redes LAN. En las secciones siguientes, se analizarán las principales características de NetBIOS y las funciones del comando NBTSTAT en un ambiente Microsoft NetBIOS provee los servicios de sesión descriptos en la capa 5 del modelo OSI. Es un protocolo de aplicación que permite compartir recursos en una red. Se encarga de establecer la sesión y mantener las conexiones.

Este protocolo no fue diseñando para hacer llegar sus datos hasta la estación destino, sea que se encuentre en una red LAN o WAN, por este motivo debe utilizar otro protocolo para transportar sus datos (por ejemplo, en redes LAN generalmente se utiliza el protocolo NetBEUI, y en las redes WAN el protocolo TCP/IP). Los protocolos que pueden prestar el servicio de transporte a NetBIOS son:

- IPX/SPX
- NetBEUI
- TCP/IP

El hecho de tener que ser transportado por otros protocolos se debe a que al operar en la capa 5 de OSI no provee un formato de datos para la transmisión, este formato es provisto por los protocolos antes mencionados. En lo que respecta al protocolo NetBIOS deben considerarse los siguientes servicios, que intervienen en el proceso de funcionamiento y conexión entre estaciones

- Servicio de Nombres (NBNS - NetBIOS Name Service): Este servicio se implementa para identificar los extremos de las conexiones. NetBIOS identifica las entidades que intervienen en una comunicación mediante nombres formados por 16 caracteres alfanuméricos. Utiliza dos tipos de nombres: nombres únicos de hosts, denominado "UNIQUE" y nombres de grupos, denominados GROUP, para asociar más de un host. Aunque en principio las especificaciones NetBIOS permiten nombres de 16 caracteres, Microsoft los limita a 15 y usa el caracter número 16 como un sufijo NetBIOS. Este sufijo es usado por el software de red de Microsoft para identificar el servicio o dispositivo registrado. Entonces, para conocer que representa un nombre NetBIOS, se deben analizar los primeros 15 caracteres (la parte que se lee fácilmente), el caracter 16 (normalmente expresado como dos dígitos hexadecimales) y el tipo de nombre (UNIQUE o GROUP). En la figura se pueden observar algunos ejemplos de sufijos NetBIOS y su significado.
- Servicio de Comunicación no orientado a la conexión: Conocido también como "Servicio de datagramas". En este servicio la estación envía los datos encapsulados en datagramas; es decir los mensajes son enviados en forma independiente, sin establecer una conexión con el destino.
- Servicio de Comunicación orientado a la conexión: Conocido también como "Servicio de conexión". Aquí se establece una conexión y un camino entre ambos hosts (que no son

necesariamente serán dos estaciones, puede ser entre una estación y un servidor). En este tipo de comunicación existe un intercambio seguro de datos, garantizado por el protocolo.

El comando **NBSTAT** (disponible en la mayoría de las implementaciones de sistemas operativos de Microsoft), muestra las estadísticas del protocolo y las conexiones actuales de TCP/IP usando NBT (NetBIOS sobre TCP/IP). La ejecución del comando se realiza desde la interfaz de línea de comandos con la siguiente sintaxis:

NBTSTAT [-a Nombreremoto] [-A dirección IP] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [intervalo]

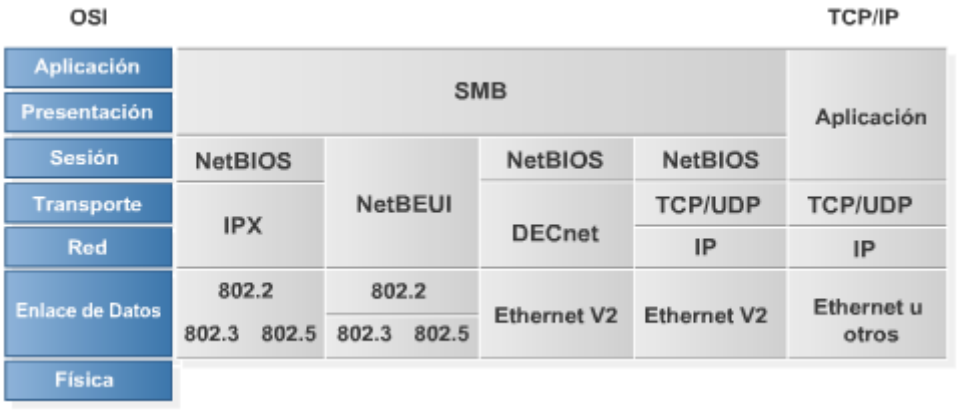
Donde:

- NombreRemoto: Nombre NetBIOS del host remoto.
- Dirección IP: Dirección IP del host remoto. Utilizaremos la opción -a o -A para indicar el equipo del cual queremos obtener los datos.
- intervalo: indica el intervalo en segundos que esperará para volver a mostrar las estadísticas seleccionadas. También se puede utilizar la combinación de teclas Ctrl+C para parar volver a mostrar los resultados.

Opción	Descripción
-a	Referencia el equipo del cual quiero obtener la infomación, ingresando su nombre NetBIOS
-A	Referencia el equipo del cual quiero obtener la infomación, ingresando su dirección IP
-c	Presenta una lista de los nombres remotos de la caché NBT y sus direcciones IP
-n	Presenta una lista de los nombres NetBIOS locales.
-r	Presenta una lista de los nombres resueltos por difusión y a través de WINS
-R	Purga y vuelve a cargar la tabla de nombres de la caché remota
-S	Presenta una lista de las sesiones con las direcciones IP de destino
-s	Presenta una lista de las sesiones convirtiendo las direcciones IP de destino en nombres de equipo NetBIOS.
-RR	Envía paquetes de Liberación de Nombres a WINS y después, inicia un Actualizar Nombres

3.2.11 SMB

SMB (Server Message Block) fue definido en 1987 por Microsoft/Intel como Microsoft Networks/Open Net-file Sharing Protocol. Sus posteriores desarrollos estuvieron a cargo de Microsoft y otros. Este protocolo permite a una aplicación o al usuario de una aplicación compartir archivos, discos, directorios, impresoras, puertos seriales, y realizar comunicaciones a través de una red. Está desarrollado siguiendo la arquitectura cliente-servidor, en otras palabras permite a un cliente leer, crear y modificar archivos de un servidor remoto; de esta forma el cliente sólo necesita que el servidor esté configurado para recibir y responder solicitudes SMB.



SMB se define con una estructura cliente-servidor, donde el cliente formula una solicitud y el servidor envía su respuesta. El servidor mantiene su sistema de archivos y otros recursos tales como: impresoras, mailslots, named pipes, APIs; disponibles para los clientes sobre la red. Los clientes se conectan al servidor usando TCP/IP, NetBEUI o IPX/SPX. Una vez que la conexión está establecida, el cliente envía comandos (llamados SMBs) al servidor para trabajar con el sistema de archivos.

Las principales implementaciones de SMB pertenecen a Microsoft y están incluidas en Windows for Workgroup 3.x, Windows 9x y Windows NT, por ejemplo, se están utilizando cuando se usa el File Manager o el Explorador de Windows, para visualizar y acceder a los recursos compartidos en otras estaciones. También existen numerosas implementaciones de SMB para otros sistemas operativos como UNIX, Linux, OS/2 y Digital. Como vimos, la relación entre los clientes y el servidor se realiza a través de solicitudes que los clientes formulan a los servidores. Los elementos del protocolo definidos para realizar estas tareas se conocen como solicitudes y respuestas, y reciben el nombre de SMBs

Los SMBs tienen un formato específico el cual es similar tanto para la solicitud como para la respuesta enviada por el servidor. Constan de una cabecera de tamaño fijo, un parámetro de tamaño variable y una porción para los datos. Una vez que se ha realizado la conexión con el servidor, el cliente está listo para solicitar los servicios, siendo necesario en primera instancia que el servidor y el cliente identifiquen qué variante del protocolo van a utilizar para comunicarse. Es decir que el primer paso es que se establezca el protocolo que va a permitir que ambos se entiendan, para ello el cliente envía un mensaje negprot SMB al servidor. Allí el cliente lista las versiones del protocolo que entiende, por su parte el servidor puede responder indicando cual versión quiere usar o 0XFFFF en el caso que no acepte ninguna de las opciones del cliente. Luego que el servidor acepta una versión para comunicarse con el cliente, le envía un mensaje negprot response informando sus capacidades (por ejemplo tamaño máximo del buffer), esto es para el caso de las últimas versiones.

Una vez que el protocolo se ha establecido, el cliente puede proceder a establecer una conexión con el servidor (loguearse) para lo cual utiliza un mensaje sessetupX SMB, en el cual se envía un nombre de usuario y la contraseña. La respuesta del servidor indica si la identificación fue validada, en cuyo caso le asignará un UID al cliente y podrá suministrarle la información solicitada. Una vez que el cliente se ha logueado en el servidor puede proceder a conectarse al sistema de archivos, para ello el cliente envía un mensaje tcon o tconX SMB donde especifica el nombre de la red a la que se quiere conectar. Una vez que esté conectado al sistema de archivos podrá operar directamente sobre los archivos del servidor, utilizando los mensajes, open SMBs para abrirlos, read SMBs para leerlos, write SMBs para escribirlos y close SMBs para cerrarlos luego que fueron utilizados.

El protocolo SMB presenta dos métodos de control de acceso a los recursos:

- Share level: cada recurso compartido puede tener una contraseña para acceder a los archivos que éste contenga. El usuario podrá acceder a los mismos siempre y cuando tenga ese permiso de entrada (la password). Para las primeras variantes de SMB (Protocolos Core y Core Plus) éste era el único modelo de seguridad disponible. En los sistemas operativos Windows 3.11 y Windows 95 es el nivel de seguridad por defecto.

- User level: en este nivel se protege a los archivos de cada usuario, además de la protección del nivel que se mencionó anteriormente. Está basado en los derechos de acceso del usuario, para ello es necesario que cada cliente se conecte al servidor con el fin de que sea autenticado, si tiene éxito el servidor le asignará un UID que deberá ser presentado en todos los siguientes accesos a los recursos del mismo. Este modelo de seguridad está disponible a partir de la tercera variante de SMB.

En una estructura de red con grupos de trabajo, cada estación mantiene su propia información de seguridad, es decir que la seguridad es distribuida. Si en lugar de utilizar grupos de trabajo se implementan dominios, la seguridad es administrada centralmente. Cada dominio tiene uno o más controladores de dominio, quienes mantienen información relacionada con los usuarios, como sus nombres, contraseñas, horas autorizadas de uso y grupos a los que pertenecen, entre otras opciones. Al utilizar una estructura de solicitud-respuesta para la comunicación de un cliente a un servidor, hay que tener en cuenta algunos temas relacionados con su seguridad. Por ejemplo, un usuario malicioso ubicado entre el cliente y el servidor puede engañar al cliente, tomando sus datos de autenticación, luego haciéndose pasar por el cliente puede acceder al servidor. Otro punto a tener en cuenta es la debilidad de los algoritmos de encriptación de password utilizados por los sistemas operativos Windows 9x y NT, esto permite que un atacante que capture las credenciales de un usuario cuando viajan a través de la red, pueda desencriptarlas a través de ataques por fuerza bruta o criptoanálisis. Los sistemas operativos Windows NT y 2000 incluyen APIs que proporcionan bastante información sobre cualquier máquina a través del puerto 139 en TCP (donde trabaja SMB) incluso a usuarios que no se hayan autenticado. Así, cualquier máquina que se conecte al puerto de un sistema NT/2000 podría obtener acceso al host y obtener información como recursos compartidos, nombres de usuarios, claves del registro, etc. Este acceso se conoce como acceso por sesión nula ya que no utiliza autenticación y por consigue acceso a los recursos típicos de estos sistemas operativos como IPC$, ADMI$, etc.

3.3 PREGUNTAS Y TIPS

- **En telnet: ¿En qué momento el cliente envía datos al servidor?** Por cada tecla que presiona el cliente
- **¿Para qué se utiliza el finger?** Para ver información sobre los usuarios conectados en el sistema. Para ver información detallada sobre un usuario en particular
- **¿Cuáles son características de FTP?** Se utiliza para la transferencia de archivo en redes TCP/IP, Brinda un acceso interactivo, Realiza en forma obligatoria un proceso de autenticación, Permite especificar el formato de la representación de los datos
- **¿Cuál es una característica de seguridad importante a tener en cuenta con el servicio FTP?** No encripta los datos que circulan entre el cliente y servidor
- **En TFTP, ¿qué sucede si se pierde un segmento?** Se retransmite el último segmento transmitido
- **¿Para qué se utiliza el protocolo DHCP?** Realiza la configuración TCP/IP de un host en forma automática
- **En SNMP: ¿Cuál es la función de un agente?** Recolectar información del dispositivo administrado en el que reside, guardarla y dejarla disponible para los NMSs en una MIB, Procesar y responder los mensajes de las NMS
- **En SNMP ¿En qué formato se guardan las variables de estado de cada dispositivo administrado?** En una Base de información jerárquica llamada MIB
- **¿Qué ventajas agregó SNMPv3 a las versiones de SNMP anteriores?** Mejoras en el servicio de Autenticación y Privacidad en las transacciones entre los agentes y la NMS
- **¿Cómo está organizado el espacio de nombres de dominio?** Es un espacio de nombres jerárquico
- **¿Cuáles son los tres servicios principales que implementa NetBIOS?** Servicio de nombres, servicio de conexión y servicio de datagramas
- **¿Para qué sirve el comando NBTSTAT?** Para reportar estadísticas y usos del protocolo NetBIOS
- **¿Cuál es una característica de seguridad a tener en cuenta con el protocolo SMB?** La contraseña es cifrada cuando circula por la red pero puede ser vista a través de fuerza bruta
- **¿Qué técnica utiliza SSH para asegurar la confidencialidad de los datos?** Encriptación
- **¿Qué ventajas tiene el TCP sobre el UDP?** TCP es más flexible y más confiable en corrección de errores y es el más utilizado.
- **Nombre un servicio de nombre alternativo**. Servicios NIS, NIS+ y WINS
- **Hay dos convenciones usadas al elegir un dominio. ¿Cuáles son?** Organizacional, tales como .com, .edu, .gov, y ubicación geográfica como .do .fr
- Un servicio FTP envía la información de usuario y password en texto plano!

CAPÍTULO 4

4.1 SEGURIDAD EN EL DISEÑO DE REDES

¿En qué capa del modelo OSI trabajan los switches? Al igual que los puentes trabajan en la capa 2 de enlace de datos

¿Qué dispositivos establecen dominios de colisión? Los Switchs y puentes segmentan las redes en distintos dominios de colisión.

¿En qué capa del modelo OSI trabajan los routers? En la capa 3 (capa de red)

¿Qué dispositivos establecen dominios de broadcast? Los routers son dispositivos que no reenvían loas broadcast y por lo tanto segmentan las redes en diferentes dominios de broadcast.

¿Para qué puede ser útil filtrar el tráfico en una red? Básicamente un filtro de tráfico se utiliza para:

- Control: decidir hasta donde acceder y hacia donde no
- Seguridad: permitir la entrada de datos solo de lugares confiables y a servicios específicos
- Registro: mostrar el flujo de paquetes que no cumplan con los parámetros normales

¿Qué significa AAA?

- *Authentication: Autenticación*
- *Authorization: Autorización*
- *Accounting: Auditoria*

¿Cuáles son los protocolos más usados para asegurar el acceso a la red? TACACS, TACACS+, RADIUS, Kerberos

Diseñar una red siempre ha sido difícil, pero hoy en día la tarea es cada vez más difícil debido a la gran variedad de opciones. A continuación se examinarán las principales metas del diseño de una red, cuales son las prioridades que se adaptan al desarrollo de la red, entre otras cosas. Un efectivo administrador de la red es también un cuidadoso planeador.

Metas en el diseño de una Red

El diseñador de la red debe siempre hacerse algunas preguntas básicas de la red antes de que empiece la fase del diseño. ¿Quién va a usar la red? ¿Qué tareas van a desempeñar los usuarios en la red? ¿Quién va a administrar la red? Igualmente importante ¿Quién va a pagar por ella? ¿Quién va a pagar la mantenerla? Cuando esas respuestas sean respondidas, las prioridades serán establecidas y el proceso del diseño de la red será mucho más productivo. Estas prioridades se convertirán en las metas del diseño. Vamos a examinar algunas de esas metas clave.

Desempeño (performance): Los tipos de datos procesados pueden determinar el grado de desempeño requerido. Si la función principal de la red es transacciones en tiempo real, entonces el desempeño asume una muy alta prioridad y desafortunadamente el costo de eleva súbitamente en este trueque desempeño/costo.

Volumen proyectado de tráfico: Algunos equipos de interconexión como los puentes, concentradores pueden ocasionar cuellos de botella (bottlenecks) en las redes con tráfico pesado. Cuando se está diseñando una red se debe de incluir el número proyectado de usuarios, el tipo de trabajo que los usuarios harán, el tipo de aplicaciones que se correrán y el monto de comunicaciones remotas (www, ftp, telnet, VoIP, realaudio, etc). ¿Podrán los usuarios enviar ráfagas cortas de información o ellos podrán enviar grandes archivos? Esto es particularmente importante para determinar el monto de gráficas que se podrán transmitir sobre la red. Si bien un diseñador de red no puede predecir el futuro, éste debe de estar al tanto de las tendencias de la industria. Si un servidor de fax o email va a hacer instalado en la red, entonces el diseñador deberá de anticipar que estos nuevos elementos no afecten grandemente al volumen actual de tráfico de la red.

Expansión futura: Las redes están siempre en continuo creciendo. Una meta del diseño deberá ser planear para el crecimiento de la red para que las necesidades compañía no saturen en un futuro inmediato. Los nodos deberán ser diseñados para que estos puedan ser enlazados al mundo exterior. ¿Cuantas estaciones de trabajo puede soportar el sistema operativo de red? ¿La póliza de precios del vendedor de equipos hace factible la expansión futura? ¿El ancho de banda del medio de comunicación empleado es suficiente para futuro crecimiento de la red? ¿El equipo de comunicaciones tiene puertos disponibles para futuras conexiones?

Seguridad: Muchas preguntas de diseño están relacionadas a la seguridad de la red. ¿Estarán encriptados los datos? ¿Qué nivel de seguridad en los passwords es deseable? ¿Son las demandas de seguridad lo suficientemente grandes para requerir cable de fibra óptica? ¿Qué tipos de sistema de respaldo son requeridos para asegurar que los datos perdidos siempre puedan ser recuperados? Si la red local tiene acceso a usuarios remotos, ¿Que tipo de seguridad será implementada para prevenir que hackers entren a nuestra red?

Redundancia: Las redes robustas requieren redundancia, sí algún elemento falla, la red deberá por sí misma deberá seguir operando. Un sistema tolerante a fallas debe estar diseñado en la red, de tal manera, si un servidor falla, un segundo servidor de respaldo entrará a operar inmediatamente. La redundancia también se aplica para los enlaces externos de la red. Los enlaces redundantes aseguran que la red siga funcionando en caso de que un equipo de comunicaciones falle o el medio de transmisión en cuestión. Es común que compañías tengan enlaces redundantes, si el enlace terrestre falla (por ejemplo, una línea privada), entra en operación el enlace vía satélite o vía microondas. Es lógico que la redundancia cuesta, pero a veces es inevitable.

Compatibilidad: hardware & software La compatibilidad entre los sistemas, tanto en hardware como en software es una pieza clave también en el diseño de una red. Los sistemas deben ser compatibles para que estos dentro de la red puedan funcionar y comunicarse entre sí, por lo que el diseñador de la red, deberá tener cuidado de seleccionar los protocolos mas estándares, sistemas operativos de red, aplicaciones (como un simple procesador de palabras). Así como de tener a la mano el conversor de un formato a otro.

Compatibilidad: organización & gente: Ya una vez que la red esta diseñada para ser compatible con el hardware y software existente, sería un gran error si no se considera la organización y el personal de la compañía. A veces ocurre que se tienen sistemas de la más alta tecnología y no se tiene el

personal adecuado para operarlos. O lo contrario, se tiene personal con amplios conocimientos y experiencia operando sistemas obsoletos. Para tener éxito, la red deberá trabajar dentro del marco de trabajo de las tecnologías y filosofías existentes.

Costo: El costo que implica diseñar, operar y mantener una red, quizá es uno de los factores por los cuales las redes no tengan la seguridad, redundancia, proyección a futuro y personal adecuado. Seguido ocurre que las redes se adapten al escaso presupuesto y todos las metas del diseño anteriores no se puedan implementar. Los directivos, muchas veces no tienen idea del alto costo que tiene un equipo de comunicaciones, un sistema operativo para múltiple usuarios y muchas veces no piensan en el mantenimiento. El costo involucrado siempre será un factor importante para el diseño de una red.

El paso de *Especificación de Requerimientos* es la etapa preliminar y es donde se especifican todos los requerimientos y variables que van a estar presentes en el diseño de una red. La Fase de Diseño, toma los elementos de la especificación para diseñar la red en base a las necesidades de la organización. Cualquier punto no previsto se revisa y se lleva a la fase anterior de Especificación de Requerimientos. La fase de Instalación se toman "los planos" de la fase de diseño y se empiezan a instalar físicamente los dispositivos y elementos de la red. Cualquier imprevisto se regresa nuevamente a la fase de Diseño o en su caso a la fase de Especificación. La fase de Pruebas es la fase final del proceso y consiste en realizar toda clase de pruebas a la red ya instalada para comprobar o constatar que cumple con las Especificaciones de Requerimientos. Ya realizadas las pruebas con éxito la red está lista para su uso. Cualquier imprevisto, se regresa a las fases anteriores.

4.1.2 Conmutación

La conmutación LAN es producida por dispositivos de capa 2 (switches y puentes). Estos dispositivos se ubican conectando a dos o más redes LAN. En esta unidad veremos los diferentes aspectos funcionales y la utilización de la conmutación como herramienta de seguridad en entornos LAN. Básicamente, los switches o puentes, leen las tramas que son transmitidas en un segmento LAN, y las retransmiten a los demás segmentos sólo si esto es necesario. Para poder tomar la decisión de reenviar o no una trama, deben crear una tabla donde asocien cada dirección MAC de la red a una interfaz (donde se encuentra conectada). Luego, cuando reciben una trama, leen el encabezado para conocer la dirección MAC destino de la trama. De acuerdo a la dirección destino seleccionará el puerto por el que la reenviarán.

4.1.3 Congestión y ancho de banda

Como hemos estudiado en unidades anteriores, en las redes Ethernet se comparte el medio, y la transmisión de un host puede colisionar con la transmisión de otro. Es decir que sólo un host puede transmitir a la vez, por lo que el ancho de banda asignado al segmento, sólo podrá ser utilizado por un host en un momento dado. Por ejemplo, si tenemos un segmento Ethernet de 10 Mbps, y tenemos 10 hosts, estadísticamente podemos decir que estamos asignando 1 Mbps a cada host.

Cuando una red se encuentra muy utilizada, las colisiones ocurrirán muy a menudo, y luego de una colisión viene una retransmisión, con lo que una trama de datos, puede llegar a ser transmitida hasta 16 veces si es que colisiona en cada transmisión. Esto produce un crecimiento exponencial de la utilización de una red Ethernet: cuantas más tramas, más colisiones, lo que produce más retransmisiones, por lo tanto, más tramas. Según pruebas realizadas, una red Ethernet se considera saturada si su utilización supera el 40%, con lo que de una red Ethernet de 10 Mbps se podrán utilizar como máximo 4 Mbps.

Desde el punto de vista de la seguridad, debe tener en cuenta que todas las estaciones que se

encuentran en su segmento podrán leer los datos que usted transmite o recibe.

4.1.4 Segmentación de la LAN

Para evitar el problema de la congestión y lograr asignar un mayor ancho de banda a cada estación de un segmento podemos dividir los segmentos para que sean más pequeños, es decir que contengan una menor cantidad de estaciones. Esto se denomina "segmentación LAN".

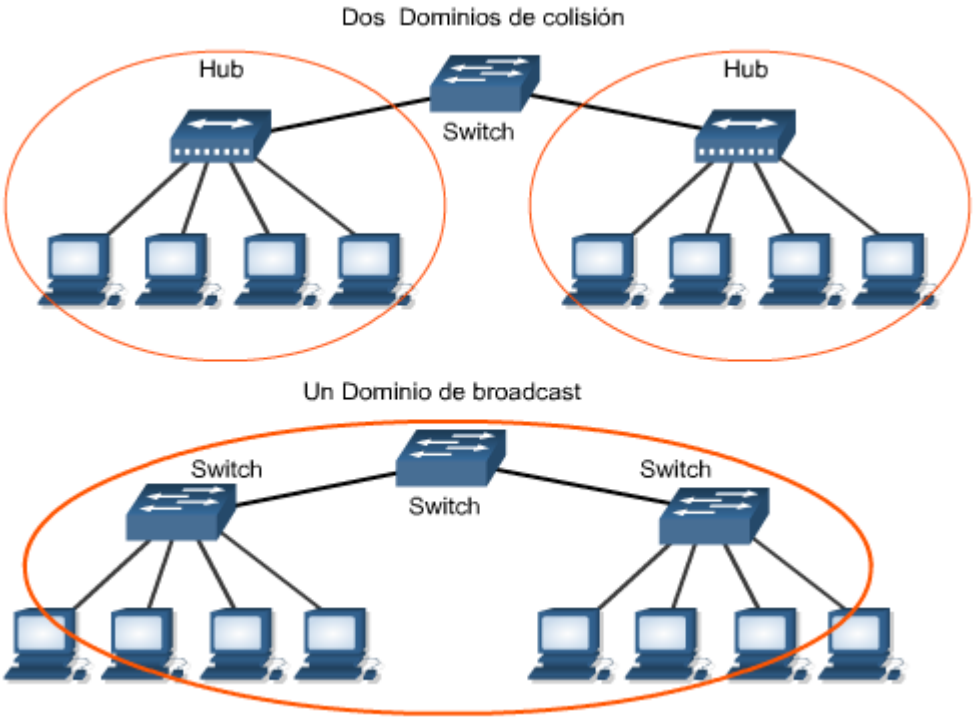
La segmentación de una LAN se puede realizar dividiendo un segmento en segmentos más pequeños, unidos por un dispositivo de capa 2 (switch o puente). Como el dispositivo de capa 2 sólo retransmite las tramas que así lo requieren, el tráfico de un segmento no congestionará otro segmento. Por este motivo, se dice que los dispositivos de capa 2 "dedican" el ancho de banda.

Cuando una estación envía una trama con destino *broadcast*, los dispositivos de capa 2 reenviarán esta trama por todos sus puertos.

4.1.5 Dominios de colisión versus dominios de broadcast

Como ya hemos estudiado, los dominios de colisión involucran todas las estaciones, dispositivos y medios que forman un segmento donde pueden ocurrir colisiones. Se pueden conectar diferentes segmentos, agregando más estaciones al mismo dominio de colisión, o agregando un dominio de colisión diferente. Los dispositivos de capa 1 extienden los dominios de colisión. Por ejemplo, si tenemos dos segmentos formados por 4 estaciones y un hub cada uno y los conectamos mediante otro hub, las 8 estaciones y los 3 hubs conformarán un solo dominio de colisión, es decir que el ancho de banda asignado al segmento será repartido entre las ocho estaciones.

Para segmentar un dominio de colisión, podemos utilizar un dispositivo de capa 2, con lo que las colisiones quedarán circunscriptas a cada segmento. Dado que los dispositivos de capa 2 reenvían los broadcast, definiremos un nuevo concepto: los "dominios de broadcasts". Un dominio de broadcast estará definido por todos los medios, estaciones y dispositivos que compartirán broadcasts de capa 2. Un dispositivo de capa 2 extiende los dominios de broadcast.



Si queremos segmentar un dominio de broadcast, deberemos utilizar dispositivos de capa 3 (routers). Al momento de diseñar la seguridad en su red LAN, deberá seleccionar la ubicación de los diferentes hosts que la conformarán y los dispositivos que los interconectarán. De acuerdo al tipo de seguridad que requiera la red, podrá utilizar dispositivos de capa 1 o 2.

4.1.5 Aprendizaje de un Switch

Los switches deben conocer qué estaciones tienen conectadas en cada uno de sus puertos, de forma de poder tomar las decisiones de reenvío de tramas. Deben lograr formar una tabla donde se relacionen las direcciones MAC de las estaciones a los puertos donde se encuentran.

Cuando el switch se enciende por primera vez, no cuenta con ninguna asociación MAC-Puerto. Debe ir aprendiéndolas a medida que recibe tráfico de las estaciones. Cada vez que una estación envía una trama, el switch lee la dirección MAC origen y la relaciona al puerto desde donde la recibió. De esta forma, va formando la tabla que utiliza para seleccionar hacia qué puerto reenviará una trama. Cuando recibe una trama con una dirección MAC destino que aún no conoce, el switch reenvía la trama hacia todos los puertos.

4.1.6 Métodos de conmutación

Para realizar el reenvío de una trama, un switch puede realizarlo mediante diferentes métodos de conmutación:

Por almacenamiento y reenvío (*store and forward*): se recibe la trama completa antes de realizar la conmutación. Una vez que recibió completamente la trama, de acuerdo a su dirección destino, la reenvía por el puerto correspondiente. Dependiendo del tamaño de la trama, variará el tiempo de conmutación. El tiempo será mayor para tramas más grandes, dado que se tardará más tiempo en la recepción completa. Dado que cuenta con la trama completa, el switch puede comprobar si la trama es correcta antes de reenviarla, con lo que sólo reenviará las tramas correctas.

Por método de corte (*cut through*): La conmutación se realiza sin esperar la recepción de la trama completa. Una vez que se recibió el encabezado (donde se encuentra la dirección MAC destino), se toma la decisión de reenvío y se realiza la conmutación a medida que se va recibiendo el resto de la trama. Esta técnica impone una latencia fija mínima para cualquier trama. La desventaja de este método es su falta de comprobación de errores. Existen dos variantes del método de corte: conmutación rápida (fast-forward) y libre de fragmentos (fragment free):

- **Conmutación rápida:** Sólo se espera recibir la dirección MAC destino para realizar la conmutación. Es el método de conmutación más veloz. Puede ocurrir que reenvíe tramas erróneas debido a colisiones.
- **Libre de fragmentos:** Espera a recibir los primeros 64 bytes de la trama, con lo que se asegura el tamaño de frame mínimo para no generar colisiones.

4.1.7 Redundancia sin bucles: Spannig Tree (STP)

En ambientes críticos es necesario crear enlaces redundantes entre switches para evitar que un problema en un enlace, deje fuera de servicio a un segmento o a toda la red. Estos enlaces redundantes pueden generar problemas de tráfico. Por ejemplo, si una estación envía un broadcast, y cada switch lo reenvía por todos sus puertos, se puede generar una multiplicación del broadcast. Esto se denomina "tormenta de broadcast". Otro problema que puede suceder es cuando una estación

envía una trama hacia un destino que no es conocido por los switches. Cada switch la reenviará por todos sus puertos, produciendo que los demás switches del segmento asocien la dirección MAC origen a cada puerto, y a su vez reenvíen esta trama por todos los suyos. Esto producirá cíclica mente el cambio en la tabla de asociación de direcciones MAC a puertos. La solución a estos problemas es el protocolo STP (Spanning Tree Protocol - Protocolo de árbol de extensión). Este protocolo, implementado en los switches, detecta y bloquea los enlaces redundantes, de forma que la topología formada contenga un único camino entre dos nodos cualesquiera. Un switch cumplirá el rol de "raíz" o centro de la topología, desde donde se desprenderán las "ramas" o enlaces hacia los demás switches. A esta topología se la llama árbol de extensión. Para determinar la topología Spanning Tree se utilizan tramas denominadas BPDU (Bridge Protocol Data Unit) que son enviadas y recibidas por todos los switches de la red a intervalos regulares. Si ocurre una falla en algún enlace, el protocolo STP re calculará el árbol de extensión, de forma de desbloquear los enlaces necesarios para brindar conectividad completa sin bucles.

4.2 LAN VIRTUALES (VLAN)

Una VLAN es una agrupación lógica de dispositivos o estaciones independiente de su ubicación física (por eso se denomina lógica). No necesariamente, estos dispositivos o estaciones estarán conectados al mismo switch, ni todos los enlaces de un switch formarán parte de esta agrupación.

Anteriormente vimos que los switches conforman un solo dominio de broadcast entre todos sus puertos. Esto no se cumple cuando tenemos VLANs: cada VLAN es un dominio de broadcast diferente. Los dispositivos o usuarios de una VLAN se pueden agrupar por funciones, departamentos, aplicaciones, etc., independientemente de la ubicación física de su segmento. La configuración de las VLANs se realiza en los switches. Las VLANs permiten armar varias redes dentro de un mismo switch. Estas redes no tendrán ninguna comunicación con las demás redes virtuales, es decir que desde el punto de vista de las estaciones es como si estuvieran en redes físicas diferentes . Esto brinda la flexibilidad de crear agrupaciones de usuarios de acuerdo a sus funciones o requerimientos, sin importar su ubicación física. Podemos crear redes que se encuentren distribuidas a lo largo de un edificio. Las VLANs no necesariamente se encuentran en un solo switch, sino que se pueden crear VLANs distribuidas a lo largo de varios switches. Esto se logra interconectando los switches mediante enlaces VLAN Trunking. Estos enlaces transportan la información de todas las VLANs entre los switches. Las VLANs se pueden crear de forma estática o dinámica. Estáticamente, el administrador de la red define en el o los switches los puertos que corresponderán a cada VLAN. Dinámicamente, se pueden crear VLANs de acuerdo a la dirección MAC o IP de cada estación. El puerto automáticamente detecta la estación conectada y de acuerdo a esa información se asocia dinámicamente a una VLAN

4.2.1 Diferencias entre las LAN conmutadas y las VLAN

En una red LAN conmutada todos los dispositivos conforman un gran dominio de broadcast. Esto puede generar una gran cantidad de tráfico innecesario entre las estaciones, y no permite aplicar políticas de seguridad por grupos de trabajo . Se considera una red "plana" debido a que todas las estaciones y dispositivos se encuentran en el mismo nivel de jerarquía.

Las VLANs permiten agrupar los usuarios de acuerdo a intereses comunes, o a recursos compartidos. De esta forma, el tráfico de una VLAN no afectará a las demás . Esta división en VLANs también permite la aplicación de políticas de seguridad apuntadas a grupos de trabajo o estaciones específicas . La comunicación entre las diferentes VLANs se debe llevar a cabo a través de dispositivos de capa 3 (Routers). Como veremos más adelante, en estos dispositivos podremos realizar filtrado de tráfico, para aplicar las políticas de seguridad necesarias.

Las diferencias entre VLANs y redes LAN conmutadas las podemos resumir en:

- Las VLANs funcionan a nivel de Capa 2 y Capa 3 del modelo de referencia OSI, mientras que las LAN conmutadas sólo funcionan en la capa 2.

- La comunicación entre las VLANs es implementada por el enrutamiento de Capa 3.
- Las VLANs proporcionan un método para controlar los broadcasts de red, las LAN conmutadas no realizan ningún control de broadcast.
- El administrador de la red asigna usuarios a una VLAN, en las LAN conmutadas y todos los usuarios se encuentran en la misma red. Las VLANs pueden aumentar la seguridad de la red, definiendo cuáles son los nodos de red que se pueden comunicar entre sí.

Desde el punto de vista del direccionamiento IP, las redes LAN conmutadas conforman sólo una subred, mientras que en una red dividida en VLANs, cada VLAN será una subred diferente.

4.2.2 Ventajas de las VLAN

Las ventajas de implementar VLANs en una red se pueden resumir en:

- Facilitan los agregados, desplazamientos y cambios de usuarios: Las VLANs ofrecen un mecanismo efectivo para controlar los cambios de usuarios y reducir en gran parte el costo asociado con las reconfiguraciones de hubs y routers. Un cambio de ubicación puede ser tan sencillo como conectar un usuario a un puerto del switch más cercano. Sólo el switch (si se han configurado VLANs dinámicas) detectará la nueva ubicación de la estación y la asociará a la VLAN correspondiente. No es necesario realizar un cambio de direccionamiento IP en la estación ni realizar cambios de configuración en los routers .
- Ayudan a controlar la actividad de broadcast: El tráfico de broadcast dentro de una VLAN no se transmite fuera de la VLAN. Las VLANs reducen sustancialmente el tráfico total de broadcast, liberan el ancho de banda para el tráfico real de usuarios, y reducen la vulnerabilidad general de las redes a las tormentas de broadcast.
- Permiten mejorar la seguridad de red: Limitan la cantidad de usuarios que pueden compartir información, evitan que un usuario se conecte sin recibir antes la aprobación del administrador de la red, permiten bloquear los puertos no utilizados en una VLAN.

4.2.3 Etiquetado: ISL versus 802.1q

Cuando se utilizan VLANs distribuidas, los enlaces de trunk deben transportar las tramas de todas las VLANs para luego ser distribuidas en los puertos que correspondan de cada switch. Cada trama debe llevar una identificación de la VLAN a la que corresponde. A esto se le llama "etiquetado de trama". Existen dos protocolos difundidos para realizar el etiquetado de tramas: ISL (Inter Switch Link) protocolo propietario de Cisco, y 802.1q, que es un estándar abierto definido por la IEEE. ISL encapsula la trama Ethernet en una trama ISL antes de transmitirla a través del enlace de Trunk . En el otro extremo, el switch des encapsula la trama y la envía únicamente a los puertos asocaciados a la VLAN indicada. El mayor inconveniente de ISL es que incrementa el tamaño de la trama. Si la trama tiene un tamaño de 1518 bytes, al agregarse el encabezado de ISL (30 bytes), tendrá un tamaño de 1548 bytes, tamaño inaceptable para una red Ethernet. IEEE 802.1q no encapsula la trama, sino que modifica el encabezado de la trama para agregar la información necesaria .

4.2.4 Transporte de las VLAN a través de backbones

Así como se utilizan los protocolos para realizar etiquetado de tramas entre switches, también se pueden utilizar para interconectar un router con varias VLANs. De esta forma, en lugar de utilizar una interfaz física para cada VLAN, se utiliza una sola interfaz física en el router que transfiere la

información correspondiente a todas las VLANs . A esta topología se la denomina comúnmente "Router on a stick". Al ser 802.1q un estándar abierto, existen implementaciones sobre diferentes Sistemas operativos (Microsoft Windows 2000, XP, Linux, Sun, etc.) y diferentes marcas de dispositivos (Cisco, 3com, Avaya, etc.), con lo que podemos realizar lo mismo si necesitamos conectar un servidor a varias VLANs simultáneamente

4.2.5 El papel de los Routers en las VLAN

Como hemos visto, para interconectar las VLANs, es necesario utilizar dispositivos de capa 3 (routers) que realizará el enrutamiento de los paquetes entre una VLAN y otra. El router hará su actividad normal si tiene una interfaz física conectada a cada VLAN, pero, ¿qué sucede cuando se utiliza un enlace de Trunk?. En este caso, en el router se crearán interfaces virtuales, una por cada VLAN. A cada interfaz virtual se le asignará una dirección IP . Estas interfaces virtuales se comportarán como interfaces físicas, desde el punto de vista del enrutamiento de paquetes, con lo que será totalmente transparente para las estaciones. En la figura se puede observar el flujo de los paquetes en una estructura de este tipo. Además de realizar el enrutamiento, en estos dispositivos podremos aplicar las políticas de seguridad a cada grupo de usuarios (VLAN) que necesitemos.

4.2.6 Filtrado de tráfico

Un método para impedir el acceso no autorizado a una red, parte de una red o un host, permitiendo por otro lado el acceso autorizado, puede ser establecer un filtro en el tráfico de datos. Por ejemplo, un administrador de red puede permitir que los usuarios tengan acceso a Internet, pero puede considerar no conveniente que los usuarios ubicados en Internet intenten realizar consultas de SNMP o administración remota a los dispositivos internos de la LAN

Los routers, los Firewall y algunos sistemas operativos proporcionan capacidades básicas de filtrado de tráfico, generalmente haciendo listas de filtros de paquetes. En las próximas secciones analizaremos las principales características del filtrado de tráfico y sus implementaciones más comunes. Desde un punto de vista global, el filtro de tráfico consiste en un conjunto de reglas que establecen qué tipo de tráfico se permite y cuál no. Para realizar el filtrado del tráfico, los dispositivos generalmente examinan la cabecera de los paquetes según van pasando, y decide la suerte del paquete completo según lo que establezcan las reglas de filtrado.

4.2.7 ¿Denegar o permitir?

La construcción de reglas de filtrado generalmente imponen una política que permite pasar algún tráfico en particular y deniegan otro. La construcción de estas reglas se pueden enfocar de dos maneras diferentes según las necesidades:

- Permitir el tráfico deseado y denegar todo el resto que no fue específicamente permitido
- Negar el tráfico que específicamente se quiere prohibir y permitir todo el resto

El primer método impone una política muy restrictiva e implica el conocimiento de todo el tráfico que desea estar permitido (el cual debe estar declarado en forma explícita en las reglas de filtrado). Este método puede ser el más indicado donde no se puede determinar con exactitud el tráfico no deseado. La conexión de una LAN a Internet puede ser un ejemplo donde este método funcionaría muy bien. El segundo método podría imponer una política más permisiva. Aquí se debe conocer con precisión cuál es el tráfico que quiere denegarse (debe declarase explícita mente en las reglas de filtrado) y todo lo que no esté denegado está permitido. Esta alternativa resulta muy conveniente cuando sólo se

quieren establecer filtros de tráficos a servicios exclusivos u orígenes determinados.

4.2.8 Posibles implementaciones en diferentes Sistemas Operativos

La mayoría de los sistemas operativos de red actuales incorporan sus propias implementaciones para el filtrado de tráfico. También, se encuentran disponibles en el mercado soluciones por software y hardware para la implementación de filtrado de paquetes en diferentes plataformas.

Linux: En Linux, el filtrado de paquetes está programado en el núcleo (como módulo o como componente estático). Según la versión del núcleo se puede utilizar el comando “iptables” o “ipchains" para configurar las reglas de filtrado. Linux utiliza tres conjuntos de reglas llamadas cadenas para aplicar los filtros según corresponda:

- Cadena INPUT: Contiene la lista de reglas que se aplican a los paquetes que llegan al host donde esté configurado el filtro y el destino del paquete es el mismo host.
- Cadena OUTPUT: Contiene la lista de reglas que se aplican a los paquetes que salen del host donde esté configurado el filtro.
- Cadena FORWARD: Contiene la lista de reglas que se aplican a los paquetes que llegan al host donde esté configurado el filtro pero el destino es algún otro host. Esta cadena se utiliza cuando el host que tiene las reglas de filtrado se comporta como un router

Windows: A través de la configuración avanzada de TCP/IP de Windows es posible establecer filtros básicos de paquetes.

Cisco IOS: El IOS de Cisco implementa el filtrado de paquetes a través de listas de control de acceso llamadas ACL. Estas listas contienen un conjunto de reglas que indican qué se debe hacer con cada paquete. Las ACL son aplicadas indicando la interfaz del dispositivo y el sentido del flujo de la información. Así, al momento de aplicar una lista de acceso se debe indicar en qué interfaz se posiciona el filtro y cuándo se va a tener en cuenta ese filtro: si para el tráfico que llegue a esa interfaz o el tráfico que salga de esa interfaz.

4.2.9 Implementación del filtrado de tráfico en Cisco IOS

Como vimos anteriormente, el IOS de Cisco implementa el filtrado de tráfico a través de listas de control de acceso llamadas ACL. Las ACL son listas de instrucciones que se aplican a una interfaz del router en un sentido determinado. Estas listas contienen un conjunto de reglas que le indican al router qué tipos de paquetes se deben aceptar y qué tipos de paquetes se deben denegar. La aceptación y rechazo se pueden basar en numerosos criterios, como la dirección IP origen, dirección destino, número de puerto, mensaje ICMP, entre otras opciones. Las ACL se deben definir por cada protocolo en cada interfaz del dispositivo. Esto significa que si un router está conmutando redes IP e IPX y desea establecer filtros para los dos protocolos, necesitará definir al menos dos listas de acceso.

4.2.10 Funcionamiento de las ACL

Una ACL es un grupo de sentencias que define el comportamiento del router ante la llegada y salida de paquetes por una interfaz. En principio, un router puede o no tener una ACL aplicada a la interfaz. Cuando llega un paquete, el router verifica si la interfaz de entrada tiene una ACL y está aplicada en

sentido entrante. Si existe, ahora se verifica si el paquete cumple o no las condiciones de la lista. Si el paquete es permitido, entonces se compara con las entradas de la tabla de enrutamiento para determinar la interfaz destino, y realizar el mismo proceso de análisis en esa interfaz. Si las reglas de la ACL indican que el paquete debe ser denegado, el router descarta el paquete y envía un aviso al emisor.

4.2.11 ACL estándar y extendidas

Según el grado de complejidad que se necesite al filtrar tráfico, el IOS de Cisco permite implementar dos niveles de listas de control de acceso:

- ACL estándar
- ACL extendidas

Las **ACL estándar** verifican sólo la dirección origen de los paquetes que se deben enrutar. Se deben usar cuando se desea bloquear o permitir todo el tráfico de una red o un host o también para permitir o denegar todo el conjunto de protocolos Internet (IP). Las **ACL extendidas** verifican las direcciones origen y destino de los paquetes. También pueden verificar protocolos, números de puerto y otros parámetros específicos (como tipo de mensajes ICMP o bits del encabezado de segmentos TCP). Esto ofrece mayor flexibilidad para describir las verificaciones que debe realizar la ACL y hace que se usen con mayor frecuencia para verificar condiciones, porque ofrecen una mayor cantidad de opciones de control que las ACL estándar. El tipo de ACL estándar se numera desde 1 a 99. Probablemente no pueda ofrecerle el tipo de control de filtrado de tráfico que se necesite ya que sus criterios son muy limitados. Las ACL extendidas usan un número dentro del intervalo del 100 al 199. A diferencia de las estándar con estas listas se pueden establecer filtros más complejos, por ejemplo, al filtrar números de puertos y se puede controlar el acceso a los servicios de una red a otra. En la figura se puede ver un ejemplo de la utilización de una lista de acceso estándar. Por filtrar sólo teniendo en cuenta la dirección origen de los paquetes, deben ubicarse lo más cerca posible del destino. De no ser así, no se podría asegurar que el destino del tráfico sea el esperado y se estaría filtrando tráfico erróneo.

Estándar	**Extendida**
Filtra según el origen	Filtra según el origen y destino
Permite o deniega una pila de protocolos completa	Especifica un protocolo y puerto particular
Rango 1 a 99	Rango 100 a 199

4.3 SEGURIDAD EN EL ACCESO

El proceso de establecer controles de acceso es crítico. El control de acceso define cómo los usuarios y los sistemas se comunican y de qué manera lo hacen.

El control de acceso protege la información de usuarios y sistemas no autorizados. El modelo AAA es el más utilizado para implementar confiabilidad, integridad y disponibilidad de los datos y recursos.

4.3.1 Introducción a AAA

AAA es un componente clave para comprender la seguridad en el acceso y en las redes. AAA es un

conjunto de siglas que identifican:

- *Authentication: Autenticación*
- *Authorization: Autorización*
- *Accounting: Auditoría*

AAA define un conjunto de procesos usados para proteger datos, equipos y confidencializar información. Uno de los objetivos de AAA es proveer:

- Confidencialidad: El contenido de los datos no debe ser revelado
- Integridad: El contenido de los datos debe permanecer intacto y no debe sufrir alteraciones
- Disponibilidad: El contenido de los datos debe estar accesible cuando se necesite

4.3.2 Arquitectura

AAA consiste de tres áreas separadas que trabajan en forma conjunta. Estas áreas proveen un nivel de seguridad básico en el control de acceso a los recursos y equipamientos de la red. Este control permite a los usuarios acceder a servicios en forma confiable y segura.

Autenticación: La autenticación puede ser definida como el proceso utilizado para verificar que una máquina o usuario que intenta acceder a un recurso es quien dice ser. El proceso de autenticación generalmente utiliza nombres de usuario, passwords, identificadores únicos, entidades certificantes, o algunos otros elementos para permitir verificar la identidad contra un dispositivo o software que analice y valide esas credenciales.

Autorización: La autorización o control de acceso puede ser definido como una política, componente de software o hardware que es usado para permitir o denegar el acceso a un recurso. Esto puede ser un componente avanzado como una tarjeta inteligente, un dispositivo biométrico o un dispositivo de acceso a la red como un Router, access point wireless o access server. También puede ser un servidor de archivos o recursos que asigne determinados permisos como los sistemas operativos de red (Windows 2000, Novell, etc.). También puede ser un conjunto de reglas que definen la operación de un componente de software limitando la entrada a un sistema o a la red.

Auditoría: Auditoría es el proceso de registrar eventos, errores, acceso e intentos de autenticaciones en un sistema. Es importante que usted pueda seguir un rastro del acceso, las tentativas del acceso, los problemas o los errores de los hosts, y otros acontecimientos que sean importantes para los sistemas que necesiten estar supervisados y controlados.

4.3.3 Métodos de autenticación

Autenticación, en su forma más básica, es simplemente el proceso de verificar la identidad de alguien o algo. Esto puede involucrar métodos complejos y seguros que sean costosos o métodos sumamente sencillos. Por ejemplo, si alguien que Ud. conoce personalmente se acerca a su puerta, usted lo reconoce visualmente entonces si lo desea lo deja entrar abriendo la puerta. Todos los procesos de autenticación siguen la misma premisa básica, que necesitamos probar quienes somos o quién es el individuo, el servicio, o el proceso, antes de que permitamos que utilicen los recursos.

La autenticación permite que un emisor y receptor de la información se validen como las entidades

apropiadas con las cuales desean trabajar. Si las entidades que desean comunicarse no pueden autenticarse correctamente, entonces no se puede confiar en la información provista por cada uno.

Un usuario puede ser identificado principalmente por tres cosas:

- Algo que el usuario conozca (por ejemplo, una contraseña)
- Algo que el usuario tenga (una tarjeta magnética)
- Algo que sea una propiedad intrínseca del usuario (Ej: la huella dactilar, el iris, la retina, la voz)

Una buena política de autenticación consiste en la utilización de más de uno de estos métodos.

Username y Password: La combinación de nombres de usuario y contraseñas es el método más común y más utilizado para realizar autenticación. La mayoría de los sistemas operativos implementan alguna forma de autenticación. Aunque éste es el método más común de autenticación, no significa que sea el mejor o que no tenga problemas. Desde un punto de vista de la seguridad, es importante comprender que la primera línea de defensa de un sistema es la creación y el mantenimiento de una política de contraseñas que se cumpla y tenga la flexibilidad necesaria para hacerla utilizable por los usuarios.

La mayoría de los sistemas operativos de red permiten definir estas políticas. Las políticas para definir las contraseñas de los usuarios pueden obligarlos a incluir:

- Cantidad mínima de caracteres y diferencias entre estos
- Caracteres en minúsculas y mayúsculas
- Números
- Caracteres especiales
- Palabras que no figuren en diccionario
- Palabras que no guarden relación con el nombre de usuario ni con datos personales relacionados (como fechas de cumpleaños, documento, etc.)
- Períodos de cambio de contraseña periódicos

Se debe tener en cuenta que mientras más elevado sea el nivel de seguridad que se desea implementar más complejo será definir contraseñas para los usuarios y memorizarlas, sin embargo este método es vulnerable frente a diversas técnicas de sniffing.

La idea básica de la autenticación basada en contraseñas es que el usuario *A* manda su identidad (su identificador de usuario, su nombre de login, etc.) seguida de una contraseña secreta *x* (una palabra o combinación de caracteres que el usuario pueda memorizar). El verificador *B* comprueba que la contraseña sea válida, y si lo es da por buena la identidad de *A*.

La manera más simple de comprobar una contraseña es que el verificador tenga una lista de las contraseñas asociadas a los usuarios, es decir, una lista de pares. Cuando A envía su contraseña, el verificador compara directamente el valor recibido x con el que figura en la lista.

Si se trata de las contraseñas correspondientes a usuarios de un sistema informático, es evidente que no pueden estar guardadas en un fichero de acceso público: es necesario que la lista esté protegida contra lectura. Pero si alguien encuentra la manera de saltarse esta protección (cosa que en ocasiones pasa en los sistemas multiusuario), automáticamente tendrá acceso a las contraseñas de todos los usuarios. Además, en estos sistemas normalmente hay un usuario administrador o “superusuario” que tiene acceso a todos los ficheros, y por tanto a las contraseñas de los usuarios. Un super-usuario que fuera mal intencionado podría hacer un mal uso de este privilegio. O un super-usuario que tuviera un momento de descuido podría dar pie a que otro usuario se aprovechara.

Existe un hecho que favorece al atacante en este caso: si los usuarios pueden escoger sus contraseñas, normalmente no usarán combinaciones arbitrarias de caracteres sino palabras fáciles de recordar. Por tanto, el espacio de búsqueda se reduce considerablemente. El atacante puede, pues, limitarse a probar palabras de un diccionario o combinaciones derivadas a partir de estas palabras. Por este motivo a este tipo de ataque se lo conoce como **ataque de diccionario**.

Una primera solución es restringir el acceso a la lista de contraseñas, protegiéndola contra lectura. Aun que en la lista aparezcan las contraseñas codificadas, el acceso a esta lista por parte de un atacante le permite realizar cómodamente un ataque de diccionario.

One time passwords: El envío de contraseñas en texto claro a través de redes permiten que algún usuario malicioso capture esa contraseña y la utilice posteriormente para obtener acceso a los sistemas. El sistema de clave de única vez hace que se genere una clave de acceso al momento que la necesite el cliente y posteriormente esa clave no tenga más validez.

El sistema S/Key utiliza algoritmos de hashing de una vía con el fin de crear un esquema de contraseñas de única vez (o también llamado One time passwords). En este sistema, las contraseñas son enviadas en texto claro a través de la red pero, luego que la password fue utilizada, caduca y no es válida para ser utilizada nuevamente. Una ventaja de S/Key es que protege el intento de acceso de un espía sin necesitar modificaciones del cliente.

El sistema S/Key tiene tres componentes principales:

- Cliente: Pide el login del usuario. No realiza ningún almacenamiento de contraseñas.
- Host: Procesa la contraseña. Almacena la contraseña de única vez y la secuencia del login en un archivo. También le provee al cliente el valor inicial para calcular el hash.
- Un calculador de claves: Es la función de hash para la contraseña de única vez.

Token cards: Otro sistema de autenticación de password de única vez que le agrega cierto grado de seguridad adicional es el uso de una token card o "tarjeta inteligente" y un servidor de token. Cada token card es programada para un usuario específico y además de esa tarjeta, cada usuario tiene un código de seguridad que le permite obtener de su tarjeta una clave de única vez. Las token cards y los servidores generalmente implementan estos pasos para autenticar a un usuario:

- Los usuarios generan una clave de única vez con la tarjeta usando un algoritmo de seguridad
- El usuario ingresa la contraseña de única vez en la pantalla de autenticación
- El cliente remoto envía la contraseña de única vez al servidor de token y al Servidor de Acceso (NAS)
- El servidor de token usa el mismo algoritmo para verificar si la password es correcta y autentica al usuario remoto

Los servidores de token, puede comportarse de tres formas diferentes:

- Basado en tiempo: Las tarjetas y el servidor tienen relojes que miden el tiempo transcurrido desde la inicialización. Cada cierto tiempo el número resultante se encripta y se muestra en la pantalla de la tarjeta; el usuario ingresa su PIN en el servidor junto con el número que se visualiza en su tarjeta. Como el servidor conoce el momento de inicialización de la tarjeta también puede calcular el tiempo transcurrido, dicho valor encriptado deberá coincidir con el introducido por el usuario para que éste sea aceptado.
- Por desafío y respuesta: En este sistema, la token card contiene una llave criptográfica. El servidor de token genera una cadena de dígitos aleatoria (desafío) y la envía al cliente remoto que intenta acceder a la red. El usuario remoto ingresa esa cadena de dígitos más su PIN en la

token card, la cual le aplica una función criptográfica (Ej: DES) con una llave almacenada, generando la contraseña (respuesta). El resultado de esa función es enviado nuevamente al servidor de token, quien realiza la misma función y si el resultado es igual, el usuario es autenticado.

- Sincronismo de eventos: La tarjeta y el servidor guardan la última contraseña utilizada. El usuario debe ingresar su PIN en la tarjeta; a partir del conjunto formado por el PIN y la última contraseña, se genera una nueva clave aplicando una función criptográfica (Ej: DES) a dicho conjunto, que será enviada al servidor para su verificación.

Identificación biométrica: Los sistemas biométricos se basan en características físicas del usuario a identificar . La autenticación basada en características físicas existe desde que existe el hombre y, sin darnos cuenta, es la que más utiliza cualquiera de nosotros en su vida cotidiana: a diario identificamos a personas por los rasgos de su cara o por su voz. Obviamente aquí el agente reconocedor lo tiene fácil porque es una persona, pero en el modelo aplicable a redes o sistemas el agente ha de ser un dispositivo que, basándose en características del sujeto a identificar, le permita o deniegue acceso a un determinado recurso. Aunque la autenticación de usuarios mediante métodos biométricos es posible utilizando cualquier característica única y mensurable del individuo (esto incluye desde la forma de teclear ante un ordenador hasta los patrones de ciertas venas, pasando por el olor corporal), tradicionalmente ha estado basada en cinco grandes grupos. El proceso general de autenticación sigue unos pasos comunes a todos los modelos de autenticación biométrica:

- Captura o lectura de los datos que el usuario a validar presenta
- Extracción de ciertas características de la muestra (por ejemplo, las minucias de una huella dactilar)
- Comparación de tales características con las guardadas en una base de datos
- Finalmente la decisión de si el usuario es válido o no.

Es en esta decisión donde principalmente entran en juego las dos características básicas de la fiabilidad de todo sistema biométrico (en general, de todo sistema de autenticación): las tasas de rechazo por no poder comprender los datos capturados y de falsa aceptación donde el sistema tomaría como válido a un usuario que no lo es.

	Ojo - Iris	Ojo - Retina	Huellas dactilares	Geometría de la mano	Escritura - Firma	Voz
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta
Prevención de ataques	Muy alta	Muy alta	Alta	Alta	Media	Media
Aceptación	Media	Media	Media	Alta	Muy Alta	Alta
Estabilidad	Media	Media	Media	Alta	Muy Alta	Alta
Identificación y autenticación	Ambas	Ambas	Ambas	Autenticación	Ambas	Ambas
Estándares	-	-	ANSI/NIST, FBI	-	-	SVAPI
Interferencias	Gafas	Irritaciones	Suciedad, heridas, asperezas ...	Artritis, reumatismo ...	Firmas fáciles o cambiantes	Ruido, resfriados ...

PAP: Ofrece un método de autenticación simple para que un host remoto establezca su identidad, utilizando el saludo de dos vías. PAP es utilizado por el protocolo PPP para autenticar el establecimiento de un enlace. El modo de trabajo de PAP consiste en enviar el par de datos usuario y

contraseña de forma reiterada a través del enlace hasta que se acusa recibo de la autenticación o la conexión se termina. Para que se validen los datos, en el otro extremo se debe tener registrado el mismo usuario y contraseña que se están enviando . PAP no es un protocolo de autenticación sólido. Las contraseñas se envían a través del enlace en texto no cifrado, y no hay protección contra la posibilidad de ver los datos en forma clara o los intentos de descubrimientos por fuerza bruta. El host remoto tiene control de la frecuencia y la temporización de los intentos de conexión. Otro punto a tener en cuenta es que PAP realiza la autenticación sólo al momento de establecer el enlace y una vez establecido el enlace, no vuelve a enviar el usuario y contraseña.

Las principales características de PAP son:

- Provee un método simple para que un nodo remoto establezca su identidad
- Utiliza intercambio de 2 vías
- El nodo remoto envía un nombre de usuario/contraseña reiteradamente hasta que se acusa recibo de la autenticación o la conexión se termina
- No es un protocolo de autenticación sólido
- Las contraseñas se envían en texto no cifrado
- No hay protección contra la reproducción o los intentos de descubrimiento mediante intentos reiterados de ensayo y error

CHAP: El mecanismo de autenticación utilizado por CHAP consiste en asegurar la identidad de los hosts remotos utilizando un saludo de tres vías Esto se realiza durante el establecimiento inicial del enlace y se puede repetir en cualquier momento una vez que se ha establecido el enlace.

A diferencia de PAP, en CHAP la contraseña nunca es enviada a través del enlace. El host envía un mensaje de comprobación al nodo remoto. El nodo remoto responde con un valor (este valor es el resultado de una función hash con la contraseña). El host compara el valor de la respuesta con su propio valor y si los valores concuerdan, se produce un acuse de recibo de la autenticación. De otro modo, la conexión no se establece.

CHAP ofrece funciones tales como verificación periódica para mejorar la seguridad. Esta característica, junto con la posibilidad de realizar autenticaciones una vez que el enlace está establecido y el no envío de las contraseñas en texto claro resulta que CHAP sea más efectivo que PAP.

4.3.4 Servidores de Acceso a la Red (NAS)

Como su nombre lo indica, la función de un servidor de acceso de red (NAS) es proveer a los usuarios remotos del acceso a los dispositivos y recursos.

Típicamente el NAS sería un router, ubicado en el perímetro de la red, quien provee dos tipos de accesos:

- Administración remota, o modo de caracteres: La administración remota contiene acceso en modo de caracteres. Esto incluye el acceso por consola, auxiliar, telnet o ssh.
- Acceso remoto a la red, o modo de paquetes: El acceso puede tomarse desde una línea analógica (a través de la red telefónica) o digital (a través de una conexión RDSI). El usuario remoto simplemente necesita el software de conexión, los protocolos adecuados y el enlace hasta el NAS. Esta tecnología es especialmente utilizada para empleados móviles, usuarios que residen en oficinas remotas y no requieran altos anchos de banda.

Si existiera un NAS brindando el acceso en una red, el administrador deberá almacenar los usuarios y

contraseñas en el NAS. Esto indica una autenticación local o base de datos de seguridad local. Las principales características de la seguridad local son:

- Usado para redes pequeñas
- Los usuarios y contraseñas son almacenados en el router
- No se requiere de una base de datos externa

El administrador del sistema debe configurar la base de datos local especificando los usuarios para cada uno que quiera conectarse a cada dispositivo. Existen protocolos para implementar bases de datos de seguridad remotas que serán vistos en secciones posteriores.

4.4 SEGURIDAD EN REDES INALÁMBRICAS

Un propósito principal de la seguridad es mantener afuera a los intrusos. En la mayoría de los casos, esto significa construir paredes fuertes y establecer puertas pequeñas bien protegidas para proporcionar acceso seguro a un grupo selecto de personas. Esta estrategia funciona mejor para las LANs cableadas que para las WLANs. El crecimiento del comercio móvil y de las redes inalámbricas hace que los modelos viejos sean inadecuados. Las soluciones de seguridad deben estar integradas sin fisuras y ser muy transparentes, flexibles y administrables.

Cuando la mayoría de la gente habla sobre seguridad, hacen referencia a asegurar que los usuarios puedan realizar sólo las tareas que tienen autorizado hacer y que puedan obtener sólo la información que tienen autorizado tener. La seguridad también significa asegurar que los usuarios no puedan causar daño a los datos, a las aplicaciones o al entorno operativo de un sistema. La palabra seguridad comprende la protección contra ataques maliciosos. La seguridad también comprende el control de los efectos de los errores y de las fallas del equipo. Todo lo que pueda proteger contra un ataque inalámbrico probablemente evitará también otros tipos de problemas.

Las WLANs son vulnerables a ataques especializados y no especializados. Muchos de estos ataques explotan las debilidades de la tecnología, ya que la seguridad de WLAN 802.11 es relativamente nueva. También hay muchas debilidades de configuración, ya que en algunas instalaciones no se utilizan las características de seguridad de las WLANs en todos los equipos. En realidad, muchos dispositivos son entregados con passwords de administrador predeterminadas. Finalmente, hay debilidades de políticas. Cuando una compañía no tiene una política de seguridad clara sobre el uso de la tecnología inalámbrica, los empleados pueden configurar sus propios APs. Un AP configurado por un empleado se conoce como un AP furtivo (rogue AP), y en general no cuentan con la configuración de seguridad apropiada.

Las redes LAN se han extendido hacia ambientes que podrían permitir el acceso no autorizado de dispositivos. Ejemplos de estos ambientes, son las redes LAN corporativas que se distribuyen hasta ambientes de acceso público, redes de servicios inalámbricos donde no se encuentran definidas sus fronteras, redes LAN de hoteles creadas para dar servicios a sus clientes, etc. En estos ambientes es necesario restringir el acceso a los servicios ofrecidos por la red LAN para permitir el acceso sólo a los usuarios habilitados. El estándar IEEE 802.1x - Port Based Network Access Control (Control de acceso a la red basado en puertos) define la forma en que se debe realizar la autenticación y autorización de los usuarios que acceden a una red LAN a través de un puerto con características punto a punto, y prohibir el acceso en caso que falle la autenticación y autorización. Los puertos incluyen los puertos de un switch, puente, o las asociaciones entre estaciones y access points de las redes inalámbricas IEEE 802.11. La autenticación IEEE 802.1x es una arquitectura cliente servidor provista a través de EAPOL (Extensible Authentication Protocol sobre LAN). El protocolo EAP lo veremos en la próxima sección. El servidor de autenticación autentica a cada cliente que se conecta a un puerto antes de proveerles acceso a los servicios ofrecidos por la red.

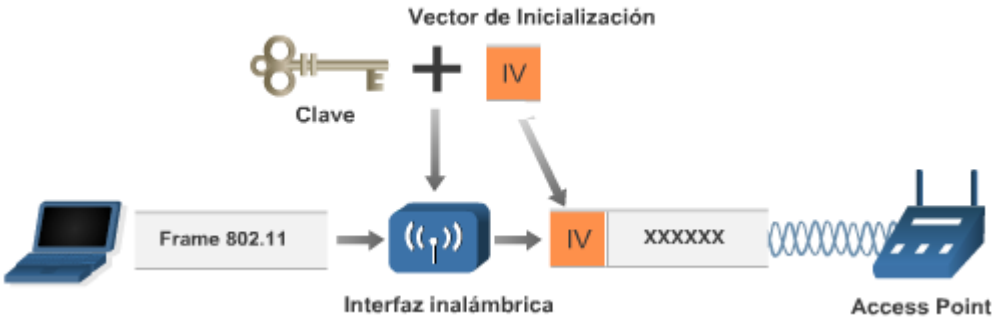
IEEE 802.1x contiene tres elementos principales :

1. Autenticador (Authenticator): El dispositivo que permite la autenticación del suplicante. Controla el acceso físico a la red basándose en la autenticación del suplicante. Es un intermediario entre el suplicante y el servidor de autenticación.
2. Suplicante (Supplicant): Cliente que solicita acceso a la red y responde los requerimientos del autenticador.
3. Servidor de autenticación (Authentication Server): Provee el servicio de autenticación al autenticador. Este servicio determina, dadas las credenciales del Suplicante, si está autorizado o no a acceder a los servicios ofrecidos por el Autenticador

La comunicación entre el suplicante y el autenticador se realiza mediante EAP sobre LAN. Puede soportar múltiples mecanismos de autenticación, como MD5, one time passwords, Token cards, etc.

4.4.1 WEP

El estándar IEEE 802.11 para las redes LAN inalámbricas incluye la definición de WEP (Wired Equivalent Privacy) para proteger a los usuarios autorizados de escuchas casuales. WEP realiza una encriptación de cada una de las tramas que se transmiten al aire. El estándar fija un tamaño de claves de 40 bits, pero algunos fabricantes las han extendido hasta más de 128 bits. Cuando se activa WEP, el cliente y el access point deben tener claves WEP coincidentes. WEP usa el método de cifrado RC4 (Rivest Cipher 4) creado por Ron Rivest de RSA Data Security, Inc.



La forma en que WEP utiliza el cifrado RC4 tiene muchas vulnerabilidades.

Una de las vulnerabilidades proviene del Vector de Inicialización. Para evitar ciertos inconvenientes, la IEEE estipuló el uso de un vector de inicialización (IV - initialization vector) que se concatena con la clave antes de generar el texto cifrado. El IV es transmitido en texto claro en el encabezado 802.11 de cada trama y se modifica para cada una. Tiene una longitud de 24 bits. Para realizar la desencripción, se realiza un esquema inverso. Los criptoanalistas Fluhrer, Mantin, and Shamir (FMS) publicaron un estudio donde demostraron que se puede obtener la clave con entre 100.000 y 1.000.000 de tramas. Este ataque se basa en ciertos patrones de los IV. A medida que se modifica el IV, se va proveyendo la información necesaria para obtener la clave. Existen implementaciones que permiten realizar una captura de tramas y realizar el cálculo de la clave WEP, las más difundidas son WEPCrack y Airsnort (ver vínculos).

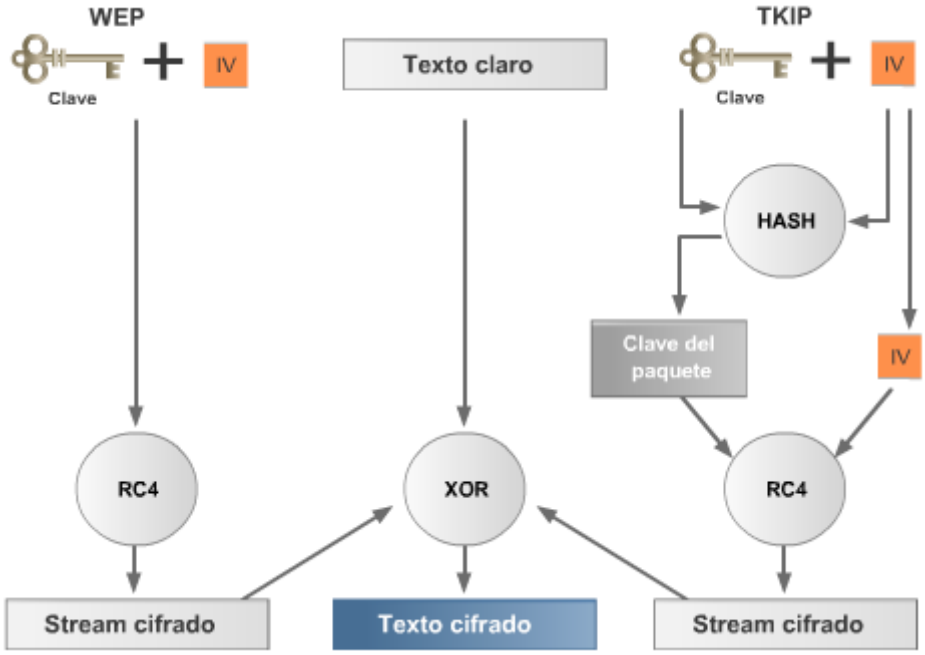
Otra vulnerabilidad de WEP es que WEP está apuntado a realizar autenticación de dispositivos y no de usuarios. Las claves WEP se deben configurar en los dispositivos (Interfaces inalámbricas y Access Points) en lugar de ser ingresadas por un usuario. El robo o acceso indebido a un dispositivo de un usuario malicioso estaría entregando las claves utilizadas en toda la red.

Para solucionar estos problemas se creó el estándar 802.11i, el cual aplica los conceptos vistos en 802.1x, más algunas modificaciones a WEP (TKIP) que veremos en las sección siguiente.

4.4.2 IEEE 802.11i

El estándar IEEE 802.11i incluye dos mejoras a la encriptación WEP:

1. TKIP (Temporal Key Integrity Protocol): mejoras por software a la implementación de RC4 utilizada por WEP
2. AES: algoritmo de cifrado más robusto que RC4



La primer mejora es una alternativa temporaria que permitiría mejorar la seguridad en las infraestructuras ya instaladas, sin necesidad de realizar un cambio de hardware. Casi cualquier dispositivo con soporte WEP, con una simple actualización del software o firmware podría implementar TKIP. El problema de WEP es que usa siempre la misma clave. TKIP define una clave temporal de 128 bits que se comparte entre clientes y access points. Esta clave es combinada con la dirección MAC del adaptador, y luego agrega un vector de inicialización de 128 bits (más de 5 veces superior al original) para producir la clave de cifrado . Este procedimiento asegura que cada estación utilizará claves diferentes para realizar el cifrado.

TKIP utiliza RC4 para realizar el cifrado, al igual que WEP, pero con la diferencia que cambia la clave temporal cada 10.000 paquetes, con lo que decrementa la posibilidad de filtrar información para realizar el cálculo de la clave.

La solución de raíz al problema de la encriptación es el reemplazo del algoritmo utilizado. Como reemplazo para RC4, 802.11i propone la utilización de AES, un algoritmo probada mente robusto. La gran desventaja de esta alternativa, es que para implementarla se debería cambiar la mayor parte del hardware actualmente instalado.

Hay personas entusiastas, dispuestas y calificadas para tomar ventaja de cada vulnerabilidad de WLAN. Ellas están constantemente tratando de descubrir y explotar nuevas vulnerabilidades. Se han escrito numerosos documentos sobre el tema de la seguridad del 802.11. Lo que sigue es un resumen de las principales vulnerabilidades:

- Control de acceso débil: Las credenciales de autenticación son presentadas por los dispositivos y no por usuarios de la red. Es decir que los privilegios estarán asociados a

dispositivos en lugar de usuarios.

- Encriptación de datos débil: Se ha comprobado que el sistema de encriptación definido en la primer especificación de 802.11 (WEP) es ineficiente como medio para cifrar datos.
- No hay integridad de mensajes - Se ha probado que el Valor de Control de Integridad (ICV) no es efectivo como medio para asegurar la integridad de los mensajes.

Los métodos de ataques inalámbricos pueden ser divididos en tres categorías:

- Reconocimiento
- Ataque de acceso
- Negación del Servicio [Denial of Service (DoS)]

Reconocimiento: El reconocimiento es el descubrimiento y mapeo no autorizado de sistemas, servicios o vulnerabilidades. También es conocido como reunión de información y normalmente precede a un ataque de otra índole. El reconocimiento es similar a un ladrón que revisa un vecindario buscando casas fáciles donde entrar. En muchos casos, los intrusos llegan hasta probar el picaporte de la puerta para descubrir áreas vulnerables, a las que pueden explotar en un momento posterior. La realización del reconocimiento comprende el uso de comandos o utilitarios comunes para conocer tanto como sea posible el sitio de la víctima. El *sniffing* inalámbrico es usado generalmente para este paso. La información reunida por las escuchas puede luego ser usada en futuros accesos o ataques DoS a la red. El usar encriptación y evitar protocolos que son fácilmente escuchados puede combatir las escuchas. Los analizadores de protocolos inalámbricos comerciales como ***AiroPeek***, ***AirMagnet***, o ***Sniffer Wireless*** se pueden usar para escuchar en las WLANs. Los analizadores de protocolos gratuitos como *Ethereal*, *Wireshark* o *tcpdump* soportan por completo las escuchas inalámbricas bajo Linux. Las escuchas inalámbricas se pueden usar para ver el tráfico de la red y descubrir los SSIDs en uso, las direcciones MAC válidas o para determinar si la encriptación está siendo usada. El reconocimiento inalámbrico a menudo es llamado ***wardriving***. Los utilitarios usados para explorar las redes inalámbricas pueden ser activos o pasivos. Las herramientas pasivas, como *Kismet*, no transmiten información mientras están detectando redes inalámbricas.

Algunas personas que usan herramientas WLAN están interesadas en recolectar información acerca del uso de la seguridad inalámbrica. Otros están interesados en encontrar WLANs que ofrezcan acceso libre a Internet o una puerta trasera fácil hacia una puerta corporativa.

Acceso: Rogue APs: La mayoría de los clientes se asocian al access point con la señal más fuerte. Si un atacante ubica un AP con el mismo SSID de la WLAN víctima, los clientes más próximos se asociarán al AP atacante en lugar del AP “oficial” de la red. El AP furtivo tendrá acceso al tráfico de red de todos los clientes asociados. Un AP furtivo puede ser usado para realizar ataques por ***man-in-the-middle*** contra tráfico encriptado en capa de aplicación, como **SSL** o **SSH**. El AP furtivo también puede usar *spoofing* de ARP e IP para engañar a los clientes y recibir conexiones desde ellos, obteniendo información como nombres de usuario, passwords e información confidencial. El AP furtivo puede también pedir sesiones no protegidas con la Privacidad Equivalente a la Cableada (WEP) con clientes durante la asociación. Ataques de Privacidad Equivalente a la Cableada (WEP) Los ataques contra la WEP incluyen Bit *Flipping*, *Replay Attacks*, y la colección Weak IV. Muchos ataques WEP no han salido del laboratorio, pero están bien documentados. Un utilitario, llamado ***AirSnort***, captura Vectores de Inicialización débiles para determinar la clave WEP que se está usando.

Denegación de Servicio: La DoS ocurre cuando un atacante desactiva o corrompe las redes, sistemas o servicios inalámbricos, con la intención de negar el servicio a usuarios autorizados. Los ataques DoS toman muchas formas. En la mayoría de los casos, la realización del ataque comprende simplemente ejecutar un *exploit*, un *script* o una herramienta. El atacante no necesita acceder previamente al objetivo, porque todo lo que se necesita normalmente es una forma de acceder a él.

Por estas razones y a causa del gran daño potencial, los ataques DoS son los más temidos, ya que son los más difíciles de evitar. Un utilitario, llamado ***Wlan Jack***, envía paquetes de desasociación falsos que desconectan a los clientes 802.11 del access point. Siempre que se ejecute el utilitario de ataque, los clientes no pueden usar la WLAN.

Otro tipo de ataques comprenden la inserción de señales en los canales utilizados por las redes WLAN, buscando lograr un alto nivel de ruido, para que las estaciones bajo ataque no puedan comunicarse. De hecho, cualquier dispositivo que opere a 2.4 GHz o a 5 GHz puede ser usado como una herramienta DoS.

El estándar IEEE 802.11 define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. Los protocolos de la rama 802.x definen la tecnología de redes de área local y redes de área metropolitana.

4.4.3 La rueda de la Seguridad WLAN

La mayoría de los incidentes de seguridad inalámbrica ocurren porque los administradores de sistemas no implementan contramedidas. Por lo tanto, la cuestión no es sólo confirmar que existe una vulnerabilidad técnica y encontrar una contramedida que funcione. También es crítico verificar que la contramedida está en su lugar y que funciona correctamente.

Aquí es donde la Rueda de la Seguridad WLAN, que es un proceso de seguridad continuo, es efectiva. La Rueda de la Seguridad WLAN no sólo promueve la aplicación de medidas de seguridad a la red, sino que lo más importante es que promueve el control y la aplicación de medidas de seguridad actualizadas en forma continua.

Para comenzar el proceso de la Rueda de la Seguridad, primero desarrolle una política de seguridad de WLAN que permita la aplicación de medidas de seguridad. Una política de seguridad debe realizar las siguientes tareas:

- Identificar los objetivos de seguridad inalámbrica de la organización
- Documentar los recursos a ser protegidos
- Identificar la infraestructura de la red con los mapas e inventarios actuales

Las políticas de seguridad proporcionan muchos beneficios. Ellas valen el tiempo y el esfuerzo necesarios para desarrollarlas. El desarrollo de una buena política de seguridad logra lo siguiente:

- Proporciona un proceso para auditar la seguridad inalámbrica existente.
- Proporciona un marco de trabajo general para implementar la seguridad
- Define los comportamientos que están o no permitidos
- Ayuda a determinar cuáles herramientas y procedimientos son necesarios para la organización
- Ayuda a comunicar un consenso entre un grupo de directivos clave y define las responsabilidades de los usuarios y de los administradores
- Define un proceso para manipular violaciones inalámbricas
- Crea una base para la acción lógica, si fuera necesario

Una política de seguridad inalámbrica efectiva trabaja para asegurar que los recursos de la red de la

organización estén protegidos contra el sabotaje y el acceso inapropiado, que incluye tanto el acceso intencional como el accidental. Todas las características de la seguridad inalámbrica deberían ser configuradas en conformidad con la política de seguridad de la organización. Si no está presente una política de seguridad, o si está desactualizada, se debería crear o actualizar antes de decidir cómo configurar o hacer uso de los dispositivos inalámbricos.

La seguridad no era una gran preocupación para las primeras WLANs. El equipo era propietario, costoso y difícil de conseguir. Muchas WLANs usaban el Identificador del Conjunto de Servicio [Service Set Identifier (SSID)] como una forma básica de seguridad. Algunas WLANs controlaban en acceso ingresando la dirección de control de acceso al medio (MAC) de cada cliente en los access points inalámbricos. Ninguna opción era segura, ya que el sniffing inalámbrico podía revelar las direcciones MAC válidas y el SSID.

El SSID es una cadena de 1 a 32 caracteres del Código Estándar Norteamericano para el Intercambio de Información [American Standard Code for Information Interchange (ASCII)] que puede ser ingresada en los clientes y en los access points. La mayoría de los access points tienen opciones como 'SSID broadcast' ['broadcast de SSID'] y 'allow any SSID' ['permitir cualquier SSID']. Estas características están normalmente activas por defecto y facilitan la configuración de una red inalámbrica. El usar la opción 'allow any SSID' permite que un cliente con un SSID en blanco acceda a un access point. El 'SSID broadcast' envía paquetes baliza que publican el SSID. El desactivar estas dos opciones no asegura a la red, ya que un sniffer inalámbrico puede fácilmente capturar un SSID válido del tráfico normal de la WLAN. Los SSIDs no deberían ser considerados una característica segura.

4.4.4 Filtrado de MAC

La autenticación basada en MAC no está incluida en las especificaciones de 802.11. Sin embargo, muchos fabricantes han implementado una autenticación basada en MAC. La mayoría de los dispositivos requieren que cada access point tenga una lista de direcciones MAC autorizadas. Algunos fabricantes también permiten que el access point consulte una lista de direcciones MAC en un servidor centralizado, como por ejemplo un servidor de autenticación RADIUS.

Las direcciones MAC no son un verdadero mecanismo de seguridad por estos motivos fundamentales:

- Lo que se está autenticando son dispositivos en lugar de usuarios. Si un atacante toma posesión de un dispositivo habilitado (placa pcmcia o usb, PDA, celular, etc.), podrá tener acceso a la red con los mismos privilegios que tenía su propietario.
- Cuando se transmite una trama, las direcciones MAC son visibles. Un atacante sólo necesitaría capturar una dirección MAC válida para poder acceder a la red. Es popularmente conocido que se puede transmitir tramas con una dirección MAC modificada.
- Aún cuando se logre que un usuario no habilitado no ingrese a la red, la protección que brinda el control de MAC es solo contra la propiedad de "autenticación" y no incluye protección contra la "privacidad" de la información en tránsito. Un atacante podría capturar todo el tráfico de una estación wlan sin necesidad de vulnerar el control de MAC, logrando por ejemplo, obtener una copia de todos los paquetes transmitidos y recibidos. Esto permitiría reconstruir páginas visitadas, emails enviados y recibidos, mensajería instantánea, y todo el tráfico no segurizado por capas superiores (VPN, SSL, SSH, etc).

Controlar el acceso a una red inalámbrica usando direcciones MAC es tedioso. Se debe mantener un inventario preciso y los usuarios deben reportar rápidamente la pérdida o el robo de equipo. En ciertos casos, la autenticación de direcciones MAC puede suplementar las características de seguridad, pero no debería ser nunca el único método en una WLAN.

4.4.5 WPA

Los diseñadores de red y los expertos en seguridad saben que no es suficiente arreglar las debilidades de WEP. La verdadera seguridad inalámbrica requiere más que sólo hacer dinámicas las claves WEP o mejorar el WEP. La verdadera seguridad inalámbrica debe poder autenticar a los usuarios, no sólo a los dispositivos. Las organizaciones deben decidir cuánta seguridad necesitan e incluirla en la política de seguridad inalámbrica. Algunas redes dependerán de soluciones VPN existentes para proporcionar seguridad adicional. Otras redes implementarán el control de acceso y los arreglos para WEP, que están incluidos en el Acceso Protegido Wi-Fi (WPA). WPA (Wi-Fi Protected Access) es un sistema para proteger las redes inalámbricas creado para corregir las deficiencias de WEP. Al popularizarse las debilidades de WEP, la IEEE comenzó a trabajar en un nuevo estándar, el IEEE 802.11i. En el tiempo intermedio en que se encontraba en desarrollo este nuevo estándar, nació WPA, como una solución temporal, que se puede implementar sin cambios de hardware en los dispositivos (pero sí requiere una actualización de software).

Los datos siguen siendo cifrados mediante RC4, pero se utilizan claves de 128 bits más un vector de inicialización de 48 bits (lo que da la friolera de 281.474.976.710.656 combinaciones). Otra mejora introducida por WPA es el protocolo TKIP (Temporal Key Integrity Protocol). TKIP se encarga de cambiar dinámicamente la clave utilizada para encriptar. Estos cambios se realizan cada 10.000 tramas, para evitar ofrecer la información suficiente a potenciales atacantes y no requieren ninguna acción de parte del usuario. Además de estas mejoras en la autenticación y en la encriptación, WPA incorpora mejoras en el control de integridad de los mensajes. Para mejorar este control de integridad, se cambió el algoritmo de CRC a un algoritmo específico para control de integridad (MIC - Message Integrity Code) llamado “Michael”. Además de mejorar la autenticación de cada mensaje, Michael incluye un contador en cada trama para evitar los ataques de *replay*. Una vez que se publicó el estándar 802.11i (Junio de 2004), WPA sufrió ciertas modificaciones convirtiéndose en WPA2. WPA2 implementa de manera completa 802.11i. La mayor diferencia es que se modificó el algoritmo de encriptación, utilizándose el potente AES (Advanced Encryption Standard) en lugar de RC4. Es muy probable que los dispositivos antiguos no soporten WPA2 debido a que se requieren cambios de hardware para su implementación.

WPA Corporativo: WPA fue diseñado para trabajar con un servidor de autenticación centralizado (RADIUS) mediante el protocolo de control de acceso 802.1x. Al trabajar de esta manera, a cada usuario se le puede asignar una contraseña diferente. Mediante 802.1x, la autenticación se realiza por usuario y no por dispositivo.

WPA Personal: WPA también provee un esquema de autenticación más sencillo para ambientes donde no se pueda costear un servidor de autenticación, donde todos los dispositivos deben compartir una misma clave pre-compartida (Pre Shared Key – PSK). En general se le denomina WPA hogareño o personal. En esta implementación se tienen los beneficios de seguridad mejorada al tener un esquema de encriptación (TKIP) y de control de integridad fuerte (Michael), pero tiene las siguientes desventajas:

- La autenticación se realiza por dispositivo
- Se debe configurar en todos los dispositivos la misma clave o No permite la implementación de diferentes políticas de seguridad

4.4.6 WPA2

WPA2 está basado en el nuevo estándar IEEE 802.11i. WPA, por ser una versión previa, puede ser considerado una “versión de migración”, dado que no incluye todas las características del 802.11i,

mientras que WPA2 se puede aceptar como la versión certificada del estándar. Al igual que su antecesor, la alianza Wi-Fi llama a la versión de clave pre-compartida WPA2-Personal y WPA-Personal, mientras que la versión con autenticación 802.1x se denomina WPA2Enterprise y WPA-Enterprise.

Existen algunas diferencias entre WPA y WPA2 que se detallan a continuación:

- CCMP se basa en el algoritmo de encriptación AES en su modo de operación CCM, con una longitud de clave y tamaño de bloque de 128 bits. AES es a CCMP lo que RC4 es a TKIP, pero al contrario de TKIP, que se diseñó para acomodarse al hardware existente para WEP, CCMP es un nuevo diseño.
- En WPA2 la computación de MIC utiliza el algoritmo CBC-MAC mientras que en WPA se utiliza el algoritmo Michael basado en las direcciones origen y destino de la trama, la MSDU y la Temporal MIC Key (TMK).
- En TKIP, el MIC se calcula en base a la MSDU, mientras que en CCMP se calcula en base a la MPDU. La diferencia entre MSDU y MPDU radica en que una MSDU representa a los datos antes de la fragmentación, mientras que una MPDU son múltiples unidades de datos luego de la fragmentación.

Los fabricantes comenzaron a producir la nueva generación de AP basados en esta arquitectura. La utilización de AES como algoritmo de encriptación, permite cumplir con los requerimientos de seguridad del gobierno de USA (FIPS 140-2), sin embargo es importante resaltar que los productos certificados para WPA proporcionan un adecuado nivel de seguridad de acuerdo a lo establecido en el estándar IEEE 802.11i.

4.4.7 Bluetooth

El Estándar Bluetooth, nacido en 1994 y formalizado en 1998 por el Bluetooth-SIG (Special Interest Group), es una tecnología inalámbrica de bajo costo, que opera en la banda no licenciada de 2.4Ghz de frecuencia (misma banda que utilizan algunos estándares de la tecnología 802.11).

Existen hoy en día tres versiones de Bluetooth (BT):

- **Bluetooth Protocolo V1.1** No provee compatibilidad para coexistir con 802.11
- **Bluetooth Protocolo V1.2** (2003) Data Rate 1Mbps
- **Bluetooth Protocolo V2.0 +EDR** (Enhanced Data Rate) (2004)

Data Rate 3Mbps: Uno de los hechos que hacen que esta tecnología sea de bajo costo, es la potencia necesaria para funcionar, tan sólo 0,1 Watts, que sin duda alguna reduce considerablemente el consumo de los equipos y que además permite ser incorporada en los teléfonos celulares y las PDA, sin que afecte en exceso el consumo de sus baterías. La tecnología BT permite la comunicación inalámbrica entre diferentes dispositivos que la incorporen, sin necesidad de línea de vista y son el reemplazo esperado de la tecnología infrarroja.

Cuando se conectan más de un dispositivo BT compartiendo el mismo canal de comunicación, forman una red denominada Piconet. Dichas redes están compuestas por un dispositivo Master quien impone la frecuencia de saltos para la Piconet y todos los demás dispositivos son los denominados Slaves (esclavos). Las Piconet solo pueden aceptar hasta 7 dispositivos Slaves conectados al mismo tiempo, sin embargo, son soportados hasta 200 dispositivos pasivos.

La pila del protocolo BT está conformada de la siguiente manera:

- Modo Descubrimiento
- Modo No Descubrimiento

Cabe mencionar que si algún dispositivo se encuentra en modo No Descubrimiento, igualmente puede ser mapeado siempre y cuando el atacante conozca la Mac Address del mismo. Básicamente los modelos de Seguridad de los dispositivos Bluetooth se clasifican en tres modos primarios:

- **Modo 1: Sin seguridad (Modo Default):** Esencialmente, los mecanismos de autenticación y cifrado están deshabilitados
- **Modo 2: Aplicación/ Nivel Servicio:** Ocurre en la capa L2CAP, nivel de servicios. Primero se establece un canal entre el nivel LM y el de L2CAP y recién entonces se inicializan los parámetros de seguridad. Como característica, el acceso a servicios y dispositivos es controlado por un Gestor de Seguridad por lo cual variando las políticas de seguridad y los niveles de confianza se pueden gestionar los accesos de aplicaciones con diferentes requerimientos de seguridad que operen en paralelo. Otra característica importante de este modo es que no hay ninguna codificación adicional de PIN o claves.
- **Modo 3: Autenticación vía PIN/ Seguridad a nivel MAC/ Encriptación:** Ocurre a nivel de Link y todas las rutinas se corren internamente en el chip BlueTooth por lo que nada se transmite en texto plano. A diferencia del Modo 2, los procedimientos de seguridad se inician antes de establecer algún canal y el cifrado se basa en la autenticación PIN y seguridad MAC. Básicamente, comparte una clave de enlace (clave de link) secreta entre dos dispositivos. Para generar esta clave, se usa un procedimiento de “paring” cuando los dos dispositivos se comunican por primera vez.

Es muy común encontrarse en los archivos almacenados en las PDA y en los Celulares, los usuarios y las contraseñas de las PC y hasta de los servidores que para no dejarlos anotados en un papel lo anotan en sus dispositivos móviles. Los lugares de mayor riesgo o donde es fácilmente posible obtener información como la mencionada anteriormente es en lugares públicos como por ejemplo: En el cine, En una plaza con mucha gente, En una biblioteca, En un centro comercial o en un bar, En un campo de fútbol, En alguna tienda de telefonía, tren, autobús.

Como podemos ver la información comprometida, puede o no ser de carácter corporativo, pero puede brindar al atacante de obtener datos que permitan desarrollar luego una estrategia de ataque más efectiva. Desde principios de 2003, comenzaron a hacerse públicas, algunas debilidades y vulnerabilidades que afectaban directamente a esta tecnología. La primera de ellas, fue descubierta por la gente de Atstake, y fue denominada *War Nibling*, y permite descubrir a todos los dispositivos que estén en el alcance del atacante estén estos en modo descubrimiento o no.

4.4.8 RFID

En la lucha eterna del equilibrio entre la seguridad y la funcionalidad, ya hemos visto pasar a varias tecnologías, solo por mencionar algunas 802.11, Bluetooth entre otras, pero como no podía ser de otra manera le llego el turno a RFID (Radio Frequency Identificación).

RFID, es una tecnología de identificación por radiofrecuencias, que permite el reconocimiento automático a distancia, basado en uno de sus principales componentes los TAGS (Etiquetas) de RFID, permitiendo esto un beneficio muy importante en lo que refiere a la logística, la distribución y la cadena de abastecimiento, pero como veremos más adelante la aplicación de esta tecnología, también está siendo adoptada en muchos otros aspectos y procesos, como el control de accesos y el pago electrónico y la identificación de documentación personal.

Tipos de etiquetas: Existen tres tipos de etiquetas, éstas se diferencian entre si por la frecuencia en la que operan, la cantidad de información que pueden contener, el tipo de funcionamiento y su durabilidad:

- **Etiquetas Pasivas:** Estas operan en la Frecuencia de los 13,56 MHZ y no tienen fuente de energía interna, sino que la pequeña corriente inducida en la antena, brindada por la señal entrante de la frecuencia radial, produce la energía suficiente para que el circuito integrado, pueda encenderse y comenzar a transmitir (Backscatter). Estas etiquetas son las de menos tamaño, por ende las más livianas y con una vida útil que puede ir hasta los 99 años.
- **Etiquetas Semipasivas:** Son muy similares a las etiquetas Pasivas, salvo por el agregado de una pequeña batería, esta batería mantiene una corriente continua en la memoria no volátil del circuito integrado, por lo cual la antena no debe preocuparse por recolectar la dicha corriente. La antena está más optimizada a su función de transmisión de radio frecuencia lo cual hace que sea más rápida y robusta que los Tags Pasivos.
- **Etiquetas Activas:** Las etiquetas activas poseen su propia fuente de energía y son capaces de alcanzar mayores distancias (10 metros aproximadamente), a poseer una batería su vida útil de es de hasta 10 años, estos economizan el consumo de energía, trabajando en intervalos definidos de operación.

RFID – Tipos de Frecuencias: Existen distintas frecuencias en las que los sistemas de RFID, pueden operar, cada una de ellas representa distintos pro y contras en base a su aplicación.

- ***Low Frequency*** *(125 a 134.2 kHz y de 140 a 148.5 kHz)*
- ***High Frequency*** *(13.56 MHz)*
- ***Ultra-High Frequency*** *(915 MHz, 433.92 MHz. o 315 MHz)*
- ***Microwaves***

Aplicaciones de RFID: Hoy en día, existen numerosas aplicaciones para estas tecnologías, pero la mas creciente, es el que está bajo el estándar EPC (Electronic Product Code), utilizada en la identificación de productos, la cual brinda una clave única para un producto, que permite detallar información sobre el mismo, en cualquier momento de la cadena de abastecimiento. Adicionalmente, entre otras aplicaciones podemos mencionar las siguientes:

- Implementaciones ganaderas, para la identificación de ganado, su historial, sus progenitores, sus descendientes y su producción.
- Identificación en medicamentos de la fecha de vencimiento o bien la información sobre los efectos secundarios del mismo.
- Medios de pago electrónico (Mastercard Paypass)
- Identificación de pacientes
- Identificación de convictos
- Identificación de billetes de alta denominación
- Identificación de pasaportes
- Identificación de registros de conducir
- Identificación de entradas a eventos deportivos y espectáculos (Mundial Alemania 2006)
- Sistemas de Control de acceso

Los sistemas RFID, se relacionan con varios procesos críticos, como el control de acceso físico, el seguimiento de productos, los sistemas de pago y otros más. Si bien, como vimos, los riesgos más publicitados de esta tecnología se relacionan con la privacidad, a continuación veremos algunos otros, que también deberían ser considerados.

> Relay Attacks en tarjetas de proximidad, Destrucción del TAG y Prevención de Lectura, RFID - SQL Injection, RFID – Virus, Algoritmos de Encriptación débiles, Sniffing, Spoofing

4.4.9 EAP, LEAP, PEAP

EAP (Extensible Authentication Protocol - Protocolo de autenticación extensible) es un protocolo de autenticación muy flexible, que generalmente corre sobre otros protocolos, como 802.1x, RADIUS, TACACS+, etc. EAP permite que el dispositivo autenticador sirva como intermediario entre el servidor de autenticación y el cliente a ser autenticado. Posibilita la distribución dinámica de claves WEP. Tanto el cliente, el autenticador y el servidor de autenticación deben soportar EAP.

En principio, cuando un usuario solicita conexión a un Access Point, comienza la fase de autenticación, que puede ser mutua, del cliente ante el servidor, y viceversa. Una vez que ambos extremos se han autenticado, comienza la fase de definición de claves, donde entre cliente y servidor definen una clave WEP para el tráfico de unicast. Esta clave es informada al Access Point, el cual enviará al cliente la clave WEP que utilizará para el envío de broadcasts. Para evitar que un usuario externo escuche esta clave, se encripta con la clave seleccionada para unicast que conocen sólo el Access Point, el cliente y el servidor de autenticación.

Cuando se utiliza 802.1x en una red inalámbrica, se pueden implementar diferentes variantes de EAP, las más conocidas son:

- LEAP (Lightweight EAP): También llamada EAP-Cisco, es la versión de Cisco de 802.1x EAP. Provee un método de distribución de claves WEP dinámicas, que varían por usuario y por sesión. De esta forma se decrementa la cantidad de tramas con la misma clave WEP, para evitar su cálculo.
- EAP-TLS (EAP-Transport Layer Security): algoritmo de autenticación basado en TLS que implementa autenticación basada en certificados digitales X.509 (se estudiarán mas adelante). Exige que todos los clientes y servidores tengan certificados digitales.
- PEAP (Protected EAP): basado en la autenticación EAP-TLS, PEAP permite utilizar diferentes tipos de autenticación del cliente, como EAP-GTC para one-time passwords y EAP-MD5 autenticación basada en passwords. De esta forma no se requiere que todos los dispositivos tengan certificados digitales.
- EAP-GTC (Generic Token Card EAP): provee autenticación basada en one-time password
- EAP-MD5: provee un método de autenticación basado en username y password.

4.4.10 TACACS+

TACACS+ (Terminal Access Controller Access Control System Plus) es una versión mejorada de TACACS. TACACS+ es un protocolo de Autenticación, Autorización, y Auditoría (AAA) que reside en un servidor centralizado. Existen al menos tres versiones de TACACS: TACACS, XTACACS y TACACS+:

TACACS es una especificación estándar de protocolo definido en el RFC 1492 que reenvía el nombre de usuario y contraseña a un servidor centralizado. Este servidor mantiene una base de datos TACACS con los usuarios. De acuerdo a los parámetros pasados, el servidor acepta o rechaza la autenticación, enviando un mensaje.

XTACACS define extensiones de Cisco al protocolo TACACS para soportar nuevas características. XTACACS es multiprotocolo y puede autorizar conexiones con SLIP, PPP, IPX, ARAP y Telnet. XTACACS soporta múltiples servidores TACACS, y syslog para el envío de información de auditoría. Actualmente, XTACACS se encuentra obsoleto, dados los nuevos requerimientos de AAA del mercado y a la existencia de TACACS+.

TACACS+ es una versión en constante mejora de TACACS que permite al servidor TACACS+ brindar servicios de AAA de manera independiente. Cada servicio puede ser usado con su propia base de datos o puede ser usado en conjunto con los demás servicios. TACACS+ no es compatible con XTACACS ni con la versión original de TACACS. Actualmente se encuentra como una propuesta en la IETF, por lo que no es un servicio estándar. TACACS+ permite la opción de encriptar toda la información que se intercambia entre el cliente y el servidor.

TACACS y sus diferentes versiones utilizan TCP como transporte, y tienen reservado el número de puerto 49.

4.4.11 RADIUS

RADIUS (Remote Authentication Dial-In User Service) es otra alternativa para realizar AAA. RADIUS es un protocolo AAA desarrollado por Livingston Enterprises, Inc (ahora parte de Lucent Technologies). Es un sistema de seguridad distribuida que seguriza el acceso remoto a redes y las protege de accesos no autorizados. RADIUS está compuesto por tres componentes:

1. Un protocolo basado en UDP
2. Servidor
3. Cliente

Según la definición del protocolo, RADIUS tienen reservados los números de puerto 1812 (para autenticación) y 1813 (para auditoría), pero existen muchas implementaciones que utilizan los puertos 1645 y 1646 respectivamente. El servidor es ejecutado en una computadora, generalmente dentro del sitio propietario de la red, mientras que el cliente reside en el NAS y puede estar distribuido en toda la red.

Modelo Cliente Servidor: El NAS opera como el cliente, reenviando la información de autenticación de los usuarios al servidor RADIUS configurado, y luego, actuando de acuerdo a la respuesta del servidor. Los servidores RADIUS son los responsables de recibir los requerimientos de los usuarios, autenticarlos, y devolver toda la información necesaria para que el cliente habilite los servicios correspondientes. El servidor RADIUS puede mantener una base de datos de los usuarios de forma local, utilizar la base de datos de Windows, o un directorio LDAP.

Seguridad de la red: Las transacciones entre el cliente y el servidor son autenticadas por un secreto compartido, que no se envía por la red. Las contraseñas son enviadas cifradas.

Métodos de autenticación flexibles: El servidor RADIUS soporta diferentes métodos para autenticar un usuario. Soporta PPP, PAP, CHAP, MS-CHAP, Unix login, etc.

4.4.12 TACACS+ versus RADIUS

Protocolo de capa de transporte: RADIUS utiliza UDP, mientras que TACACS+ utiliza TCP. Como UDP no brinda confiabilidad ni control de flujo, RADIUS debe implementar controles y retransmisiones, lo que lo vuelven más complejo que TACACS+ para su programación.

Encriptación de datos: RADIUS sólo soporta la encriptación de las contraseñas. Esto, a pesar de no proveer las contraseñas, puede permitir a un usuario malicioso conocer los movimientos de los accesos, ingresos, salidas, etc. TACACS+ soporta la encriptación de todo el tráfico entre el cliente y el servidor.

Autenticación y autorización: RADIUS combina la autenticación y autorización. En el mismo paquete donde se autentica a un usuario, se le informa de sus permisos. TACACS+ utiliza los tres servicios de manera independiente. Esto permite utilizar soluciones alternativas de autenticación, manteniendo TACACS+ como servicio de autorización y auditoría. Por ejemplo, utilizar autenticación Kerberos y autorización y auditoría TACACS+.

Soporte multiprotocolo: A pesar de que RADIUS es un protocolo flexible, no soporta algunos protocolos utilizados en ciertos ambientes:

- AppleTalk Remote Access (ARA) protocol
- NetBIOS Frame Protocol Control protocol
- Novell Asynchronous Services Interface (NASI)
- X.25 PAD connection

	TACACS+	RADIUS
Funcionalidad	AAA independientes	Combina Autenticación con Autorización
Protocolo de Transporte	TCP	UDP
Soporte de protocolos	Soporte Multiprotocolo	no ARA no NetBeui
Cifrado	Encripción del paquete completo	Encripción de la password
Auditoría	Limitada	Extensiva

Administración de Routers: RADIUS no permite asignar conjuntos de comandos habilitados o deshabilitados a los usuarios, por lo que no es útil para realizar autenticación de administradores de dispositivos. TACACS+ provee dos métodos para controlar esto. Un método es asignar niveles de privilegios a los comandos, que luego serán controlados por TACACS+ para comprobar si el usuario tiene permisos de ejecución. La otra forma es especificar en el perfil del usuario o del grupo de usuarios explícitamente el conjunto de comandos que puede ejecutar.

4.4.13 Kerberos

Kerberos fue creado en el Instituto de Tecnología de Massachusetts a comienzo de los 80´. La versión

actual de Kerberos es la versión 5, y ha sido publicada por la IETF como el RFC 1510. El sistema operativo Microsoft Windows 2000 utiliza a Kerberos como su técnica de autenticación.

El protocolo Kerberos depende de una técnica de autenticación que incluye secretos compartidos. El concepto básico es bastante simple: si un secreto es conocido sólo por dos personas, entonces cualquiera de las dos personas puede verificar la identidad de la otra confirmando que la otra persona conoce el secreto. Kerberos resuelve este problema con criptografía de clave secreta. En vez de compartir una clave de acceso, los extremos de la comunicación comparten una clave criptográfica, y usan el conocimiento de esta clave para verificar la identidad uno del otro.

Kerberos tiene tres componentes: un cliente, un servidor y una intermediario de confianza para mediar entre ellos. Este intermediario es el protocolo KDC (Key Distribution Center, Centro de Distribución de Claves). El KDC es un servicio que corre en un servidor físicamente seguro. Mantiene una base de datos con la información de las cuentas de sistema (usuarios, servidores, estaciones). Para cada cuenta, mantiene una clave conocida sólo por el KDC y la cuenta. Esta clave se usa en intercambios entre la cuenta y el KDC.

Cuando un cliente quiere hablar con un servidor, el cliente envía una solicitud al KDC, y el KDC distribuye una clave de sesión para que utilicen los extremos interesados (el cliente y el servidor) cuando se autentican uno al otro. La copia de la clave de sesión del servidor está encriptada con la clave compartida entre el KDC y el servidor. La copia de la clave de sesión del cliente está encriptada en la clave compartida entre el KDC y el cliente.

4.5 RECOMENDACIONES DE DISEÑO PARA REDES WLAN

La solución de seguridad para redes WLAN en un entorno empresarial es muy dependiente de las políticas de seguridad que se quieran implantar. A continuación, se indican recomendaciones de diseño de redes WLAN que garantizan diferentes niveles de seguridad empezando desde niveles básicos hasta niveles más completos y comparables a los niveles de seguridad de redes cableadas. No obstante, debe ser tenido en cuenta que la utilización de excesivas normas de seguridad podría reducir la eficiencia de funcionamiento de una red WLAN.

4.5.1 Recomendaciones de ingeniería social

- Educar al personal de la empresa para que no comente información sensible (contraseñas,..) con sus compañeros o gente desconocida, no escribir las contraseñas en papel, etc.
- Divulgar la información crítica (contraseñas administrativas,...) al mínimo personal posible.
- Algunos empleados pueden no darse cuenta de que un despliegue WLAN no autorizado (es decir, instalar puntos de acceso no autorizados conectados a la LAN o a la WLAN), puede aumentar los riesgos en la seguridad. Por ello, es conveniente fijar pautas claras que promuevan la cooperación activa. También sería conveniente emplear alguna herramienta que permita la detección de este tipo de equipos.

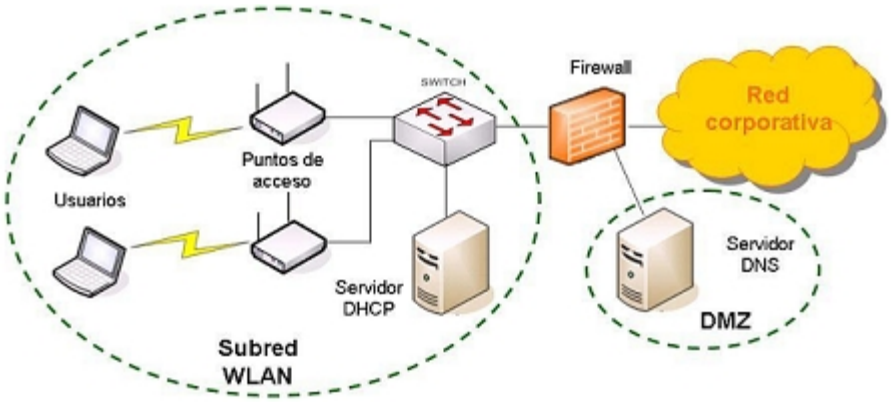
4.5.2 Recomendaciones de Red

- La implementación de una red WLAN no debe alterar arquitecturas y recomendaciones ya existentes en el lugar en el que se va a llevar a cabo el despliegue. Debe ser hecha respetando las políticas existentes en cuanto a seguridad.
- Las redes LAN no son substituidas por las redes WLAN. Las redes WLAN deben emplearse para aumentar la flexibilidad y la disponibilidad actuales de la red proporcionando una extensión a la red existente.

- Mantener una política de contraseñas adecuada. El administrador debe prestar atención a las contraseñas. Una contraseña debe ser suficientemente larga y contener caracteres no alfanuméricos y ser cambiada periódicamente. Una desventaja de este método es que los usuarios tienen dificultades para recordarlas y las escriben en el papel en lugar de memorizarlas.
- Realizar inspecciones físicas periódicas y emplear herramientas de gestión de red para revisar la red rutinariamente y detectar la presencia de puntos de acceso no autorizados.
- Utilizar perfiles de usuario que permitan el control de acceso para usuarios internos o empleados y usuarios invitados (clientes, proveedores, etc.)

4.5.3 Recomendaciones de arquitectura de red

- Las redes WLAN deben ser asignadas a una subred dedicada y no compartida con una red LAN. Entre la red WLAN y la red LAN deberá existir una estructura de firewall adecuada así como mecanismos de autenticación.
- Para proteger los servidores de la empresa de ataques DOS, los servicios que se desea prestar a los usuarios inalámbricos deben ubicarse en una DMZ que retransmita estas peticiones de los servicios a los servidores de la empresa. Por lo tanto, es recomendable emplear una red redundante para ofrecer alta disponibilidad.
- Cambiar los parámetros por defecto de los equipos.
- Comprobar regularmente si hay disponibles nuevas actualizaciones de seguridad para los equipos y y estudiar la aplicación de las mismas.
- Además de los puntos de acceso inalámbricos, elementos básicos a emplear en el despliegue de redes WLAN de forma eficiente y segura son los siguientes:
    - Switch de capa 2 ó de capa 3: Proporcionan conectividad Ethernet entre los puntos de acceso y la red corporativa.
    - Firewalls: La red WLAN es considerada insegura, por lo que todo el tráfico entre ella y la red corporativa debe ser filtrada. Filtrados especiales deben aplicarse a protocolos, direcciones IP origen y subredes destino.
    - Servidor de DHCP: Proporciona la configuración de direccionamiento IP para los usuarios inalámbricos. Su uso se recomienda por razones del escalabilidad.
    - Servidor del DNS.



Arquitectura básica de una red según recomendaciones

4.5.4 Recomendaciones sobre los puntos de acceso

- Seleccionar puntos de acceso que puedan ser actualizados (firmware y software).
- En el caso en que la red WLAN esté diseñada con puntos de acceso que se puedan configurar con diferentes modos de seguridad (WEP, WPA, IEEE 802.11i), se recomienda configurar la red con un único modo. Si es necesario configurar los puntos de acceso con diferentes modos de seguridad, es recomendable agrupar los puntos de acceso utilizando el mismo modo de seguridad en una subred. Por ejemplo, crear una subred para puntos de acceso que empleen WEP y otra para puntos de acceso que empleen WPA. Para facilitar la creación de subredes, Se recomienda que los puntos de acceso tengan la funcionalidad de soporte de múltiples SSID's. De esta forma, se pueden asociar diferentes políticas de seguridad a diferentes SSID's de un mismo punto de acceso.
- Habilitar el cifrado sobre el tráfico enviado por el interfaz aéreo siempre que sea posible.
- Asegurar físicamente los puntos de acceso, para evitar que personal no deseado tenga acceso a él.
- Las redes WLAN serán sólo accesibles por aquellos dispositivos asociados al SSID adecuado. Para evitar el acceso por parte de usuarios no deseados es fundamental deshabilitar el broadcast de SSID que, en general, llevan a cabo por defecto los puntos de acceso. Aunque este mecanismo de seguridad es fácilmente vulnerable, tal y como han demostrado numerosos estudios, su práctica sigue siendo recomendable puesto que supone un primer nivel de defensa contra ataques y permite evitar la conexión de usuarios de manera automática a la red, ya que aunque no hagan uso de ella para transmitir información, degradan la conexión de otros usuarios.
- Emplear puntos de acceso que permitan bloquear la comunicación entre usuarios conectados a un mismo punto de acceso.
- Emplear puntos de acceso inalámbricos que permitan activar la opción de 'intracell blocking' para evitar que un usuario conectado al mismo pueda acceder a máquinas de otros usuarios conectados a él.

4.5.5 Recomendaciones sobre protocolos y estándares

- Inhabilitar cualquier protocolo inseguro y no esencial. Comprobar los protocolos por defecto proporcionados por el fabricante.
- Emplear protocolos seguros de gestión como SSL o SSH cuando sea posible.
- En caso de que no sea posible emplear IEEE 802.11i, una alternativa a utilizar es WPA. WPA aporta mejoras importantes con respecto a WEP:
- IEEE802.11i y WPA utilizan autenticación basada en la combinación de IEEE802.1x y EAP. A la hora de seleccionar el tipo de EAP a emplear es conveniente tener en cuenta que los más seguros y flexibles son:
    - EAP-TLS en el caso de seleccionar autenticación de usuario mediante certificados.
    - EAP-TTLS y PEAP permiten la autenticación de usuario mediante nombre de usuario/contraseña. PEAP es compatible con las soluciones de Microsoft, pero EAPTTLS se puede utilizar con mayor número de mecanismos de autenticación.
- Cuando no sea posible la utilización de IEEE802.11i ni WPA, siempre es recomendable utilizar WEP.

- Emplear Listas de Control de Acceso (ACL) para que el acceso a la red sea restringido a los usuarios cuyas direcciones MAC están contenidas en la tabla ACL, la cual puede estar distribuida en los diferentes puntos de acceso o centralizada en un servidor. Esta medida es sólo recomendable cuando el número de usuarios es reducido.
- Para aumentar la seguridad de acuerdo a los escenarios de movilidad de determinados perfiles de usuarios, el uso de un IPsec VPN es altamente recomendado así como el uso de firewalls que filtren el tráfico entrante en la red de la empresa.
- Para evitar los ataques de diccionario o por fuerza bruta contra contraseñas se recomienda:
    - Llevar a cabo el bloqueo de cuentas de usuario por parte del servidor RADIUS tras una serie de intentos de autenticación fallidos.
    - Escoger contraseñas adecuadas.
    - Concienciar a la plantilla.
    - Emplear claves de usuario dinámicas, por ejemplo mediante autenticación OTP con PEAP y EAP-TTLS.
- Emplear EAP-TLS.

4.5.6 Recomendaciones de seguridad de los usuarios

- Inhabilitar el modo ad-hoc.
- Habilitar el cifrado sobre el tráfico enviado por el interfaz aéreo siempre que sea posible.
- Se recomienda la instalación de software de seguridad como antivirus y Firewalls.

4.5.7 Recomendaciones de protección física de la señal

- Tipo y ubicación de antenas estudiada para restringir el área de cobertura radio dentro del radio deseado.
- Empleo de materiales opacos en la construcción del edificio para atenuar la señal, y evitar que ésta se propague fuera del edificio.
- Equipos inhibidores de señal en zonas que no se desea tener cobertura.
- Herramientas de monitorización de la señal radio y de detección de puntos de acceso rogue.
- Vigilancia exterior.

4.5.8 Soluciones de seguridad en entorno empresarial

Dependiendo de la polítical de seguridad de la empresa es necesario aplicar medidas específicas de seguridad. A continuación, se analizan diferentes soluciones utilizando los mecanismos WEP, WPA, IEEE 802.11i e IPsec VPN.

WEP: Las redes WLAN IEEE 802.11 con el mecanismo de seguridad WEP habilitado, tienen que ser consideradas como inseguras puesto que WEP es un protocolo con numerosas vulnerabilidades probadas. Por ello, en una instalación en que los puntos de acceso sólo dispongan de cifrado WEP, es necesario aplicar medidas estrictas de seguridad para acceder a la red cableada. A pesar de su

vulnerabilidad, es recomendable emplear WEP cuando sea la única solución de seguridad implementable para evitar dejar la red WLAN abierta y completamente expuesta a posibles ataques.

Al ser WEP es un mecanismo de seguridad que presenta ciertas vulnerabilidades, para reforzar la seguridad proporcionada a una red WLAN por una solución WEP, es recomendable utilizar algún mecanismo adicional como es la solución VPN basada en IPsec.

Por último, a la hora de diseñar una clave WEP para la red es conveniente hacerlo asociándole valores hexadecimales, en lugar de caracteres ASCII, ya que el número de caracteres ASCII es limitado (el alfabeto ASCII consta de 127 caracteres, 255 si se emplean caracteres extendidos) y parte de la clave tendría asociado un valor nulo, vulnerabilidad de la que se suelen aprovechar las herramientas de descubrimiento de claves WEP. Además, es aconsejable emplear claves hexadecimales con valores no nulos en los bits de menos peso.

WPA: Un sistema de seguridad basado en WPA puede funcionar en los siguientes modos de operación:

- Modo WPA, sólo para usuarios con WPA.
- Modo mixto, para usuarios con y sin WPA.

Una red en modo mixto no es más segura que una red sin WPA, por lo que no se recomienda emplear este modo.

La Wi-Fi Alliance recomienda llevar a cabo el despliegue de una solución basada en WPA siguiendo los siete pasos que se detallan a continuación:

- Seleccionar el mecanismo de seguridad y credenciales
- Analizar las base de datos de autenticación de usuarios que se pueden utilizar
- Estudiar el Sistema operativo de los usuarios que van a utilizar esta solución
- Selccionar el Supplicant (software disponible en terminal de usuario para realizar la autenticación)
- Seleccionar el tipo de EAP
- Seleccionar el servidor de autenticación a utilizar

Tras realizar estos pasos, se conocerá qué elementos conformarán la solución y se estará preparado para implementar políticas de autenticación basadas en IEEE 802.1x y comenzar la instalación de la red WLAN.

En general, los elementos clave de la arquitectura de una solución de despliegue de redes WLAN que implementen un mecanismo de seguridad basado en WPA son los siguientes:

- Software específico en el dispositivo inalámbrico. La solución del software debe estar basada en un tipo de EAP que soporte el tipo de autenticación seleccionado. Para dotar de mayor seguridad a la red, el tipo de EAP debe proporcionar una autenticación mutua, por lo tanto, no es recomendable utilizar EAP-MD5.
- En caso de utilización de EAP-TLS, EAP-TTLS y PEAP se recomienda configurar los usuarios inalámbricos con un certificado de un servidor seguro y evitar que el usuario pueda modificar estos parámetros. Únicamente el administrador debe tener privilegios para poder modificar el certificado empleado. Si no se configura el certificado los ataques *Man In The Middle* son posibles.
- Puntos de acceso inalámbricos que soporten WPA y una conexión segura con un servidor

RADIUS. Los puntos de acceso se configuran para aceptar solamente conexiones WPA y rechaza conexiones WEP. En el caso de implementar esta solución en instalaciones nuevas, podría tenerse en cuenta la opción de adquirir equipos que únicamente sean compatibles con WPA. WPA ofrece mecanismos de seguridad mucho más robustos que los utilizados por WEP, en cuanto a la autenticación, integridad y confidencialidad.

- Servidor AAA. El servidor AAA proporciona la autenticación de usuarios a la red WLAN. El servidor AAA es el encargado de generar las llaves dinámicas utilizadas en el mecanismo WPA y envía estas llaves a los puntos de acceso. En caso de utilización de certificados, se recomienda que el servidor AAA contraste el estado del certificado del usuario contra un autoridad CRL (las principales Autoridades Certificadoras internacionales actualmente son Verising y Thawte) ó un servidor OCSP. Es posible llevar a cabo implementaciones con servidores AAA distribuidos para posibilitar reparto de carga así como confiabilidad a la red.

En función del método de autenticación utilizado pueden ser empleados opcionalmente los siguientes elementos adicionales:

- Servidor PKI. Proporciona certificados X.509 para la autenticación de usuario y de servidor. Necesario en caso de emplearse EAP-TLS, EAP-TTLS y PEAP.
- Proporciona autenticación OTP mediante servidores RADIUS. Puede emplearse con PEAP o EAP-TTLS.
- Servidor OTP

Adicionalmente, es recomendable proteger el modo EAP empleado (LEAP, PEAP, EAPTTLS) contra ataques de fuerza bruta. El servidor RADIUS debe bloquear las cuentas de usuario tras una serie de intentos de logueo fallidos. Cuando la cuenta de usuario esté bloqueada el usuario no puede ser autenticado (y por lo tanto no puede utilizar la red WLAN) hasta que no se lleven a cabo una serie de acciones administrativas. Esto permitirá al administrador de la red (y responsable de seguridad) llevar a cabo un análisis de la solución de seguridad empleada y si es necesario mejorarla. Para evitar este riesgo, se puede exigir a los usuarios inalámbricos llevar a cabo autenticación tipo OTP.

Las principales ventajas e inconvenientes de esta solución de seguridad son los siguientes:

- **Pros**:
    - Emplear una solución de seguridad que permite al personal acceder a todos los recursos de la red.
    - Permite definir diferentes perfiles de usuario.
- **Contras**:
    - Algoritmo de cifrado que emplea ha sido vulnerado.
    - Se aumenta la carga de trabajo del administración, ya que tiene que configurar el software específico WPA de los dispositivos inalámbricos.
    - Dependiendo del método EAP utilizado requiere el uso de certificados en la parte usuario.

Para instalaciones que dispongan de usuarios y puntos de acceso WEP sería conveniente migrar los puntos de acceso de un mecanismo de seguridad WEP a uno basadao WPA para dotar la red WLAN de una mayor nivel de seguridad. No obstante, si no fuera posible llevar a cabo esta migración, es posible un entorno heterogéneo que combine soluciones basadas en WEP y WPA simultáneamente o configurar los puntos de acceso para que trabajen en modo mixto WEP-WPA, de forma que soporten usuarios WPA y usuarios WEP. Es importante destacar que, sólo es posible desplegar una red en

modo mixto WEP-WPA. Para evitar comprometer la seguridad de la red debido a la vulnerabilidad de WEP no es posible hacerlo en modo mixto WEP-WPA2.

Es recomendable que los puntos de acceso que sólo soporten WEP y que no sea posible actualizarlos con “parches” WPA sean situados en la misma subred para formar así una subred WEP-LAN con políticas de seguridad independientes del resto de puntos de acceso.

En cualquier caso, la consecuencia directa de soportar ambos tipos de usuarios es que el nivel de seguridad de la red WLAN será el del mecanismo WEP. Por ello, se recomienda migrar todos los puntos de acceso y usuarios a WPA en lugar de mantener un entorno mixto.

IEEE802.11i

Los elementos clave de la arquitectura de una solución de despliegue de redes WLAN que implementen un mecanismo de seguridad basado en IEEE 802.11i son los mismos que empleados en una solución WPA. La única diferencia es que los puntos de acceso deben soportar el estándar IEEE 802.11i.

Una de las principales diferencias entre IEEE 802.11i y WPA se encuentra en el algoritmo de cifrado utilizado, IEEE 802.11i utiliza AES y WPA, al igual que WEP, utiliza RC4. Por lo que sí que existen puntos de acceso que soportan el modo mixto WEP-WPA, pero no que soporten el modo mixto WEP-IEEE 802.11i.

- **Pros**:
    - Emplear una solución de seguridad que permite al personal acceder a todos los recursos de la red.
    - Permite definir diferentes perfiles de usuario.
- **Contras**:
    - Puntos de acceso de determinados fabricantes no soportan la actualización software al mecanismo IEEE802.11i, en estos casos es necesario el cambio de los puntos de acceso desplegados por otros nuevos que sí soporten IEEE802.111i.
    - Sobrecarga de configuración de usuarios WPA, interno tipo empleado e invitados.
    - Dependiendo del método EAP utilizado requiere el uso de certificados en la parte del software del dispositivo inalámbrico.

IPSec VPN

Como se ha comentado anteriormente, para equipos IEEE 802.11 que tienen solamente WEP como mecanismo de seguridad, es necesario proteger el acceso a red con otros mecanismos adicionales. En estos casos, el uso de un VPN IPsec es altamente recomendable.

Cabe destacar que una solución VPN basada en IPsec es compatible con el uso de WPA e IEEE 802.11i.

La utilización de las soluciones VPN basadas en IPsec es especialmente recomendable en el caso en que la plantilla de la empresa sea itinerante, para proporcionar seguridad al conectarse a Internet o a la red de la empresa desde otras redes que no se la propia red de su empresa.

Los elementos clave de la arquitectura de una red WLAN en la que se emplea una solución VPN

basada en la tecnología IPsec para asegurar el tráfico de datos son los siguientes:

- Dispositivos inalámbricos. Proporcionan conectividad inalámbrica a los puntos de acceso.
- Software específico IPsecVPN instalado en el dispositivo inalámbrico. Es el extremo del túnel IPsec en el dispositivo de usuario. El usuario inicia la sesión VPN a través de este software específico y es el concentrador VPN el encargado de autenticar y validar el acceso del usuario a la red WLAN.
- El punto de acceso inalámbrico proporciona conectividad Ethernet a la red corporativa. Si el punto de acceso tiene capacidades de filtrado, se puede filtrar el tráfico para permitir únicamente los protocolos DHCP e IPsec.
- Gateway/concentrador IPsec VPN. Autentica y valida a los usuarios inalámbricos. Puede realizar también funciones de servidor DHCP para los usuarios inalámbricos.
- Firewall. Se recomienda ubicar un Firewall después del concentrador VPN que aplique políticas de seguridad al flujo no cifrado.

Existe una variedad de mecanismos de autenticación a utilizar cuando se emplea el mecanismo VPN basado en IPsec:

- Servidor RADIUS
- Servidor PKI. Proporciona certificados X.509 para la autenticación de usuario y de servidor. Se recomienda que los certificados de usuario sean accesibles solamente mediante hardware protegido con contraseña como, por ejemplo, smart-cards o llaves USB.
- Servidor OTP. Proporciona autenticación OTP mediante servidores RADIUS.

Se recomienda utilizar políticas basadas en certificados para establecer los túneles IPsec en lugar de llaves pre-compartidas. Emplear llaves pre-compartidas es peligroso, porque si un atacante las obtiene, es difícil detectar que las llaves están comprometidas. Por lo que implica sobrecarga en el mantenimiento al obligar periódicamente las llaves precompartidas. Además, se recomienda que el concentrador VPN compruebe el estado de los certificados de usuario contra las autoridades CRL (las principales Autoridades Certificadoras internacionales actualmente son Verisign y Thawte) ó un servidor de OCSP.

Las principales ventajas e inconvenientes de esta solución de seguridad VPN basada en IPsec son los siguientes:

- **Pros**:
    - Emplear una solución de seguridad que permite al personal acceder a todos los recursos de la red.
    - Permite definir diferentes perfiles de usuario.
    - Reutilización de la VPN fuera del entorno empresarial.
- **Contras**:
    - Necesidad de un concentrador VPN.
    - Sobrecarga de configuración de usuarios VPN.
    - Excluye a los invitados.
    - Es una solución costosa.

Las redes WLAN desplegadas en sitios públicos son conocidas como Hotspots y suelen ofrecer conectividad a Internet en hoteles, aeropuertos, centros de reuniones, etc. También están emergiendo las redes WLAN conocidas como Hotzones que no son otra cosa que la extensión de los hotspots fuera de los citados recintos o edificios cubriendo zonas amplias de una ciudad.

Son redes cuyo propósito es proveer servicio al público en general, tanto usuarios particulares como empresariales, usuarios con diferentes tipos de dispositivos inalámbricos, muy diversos niveles de conocimientos informáticos y, en muchos casos, sin permisos de administrador en sus dispositivos, lo que implica limitaciones en sus dispositivos a la hora de cambiar parámetros de configuración.

Las posibles limitaciones en cuanto a la configuración del dispositivo de usuario, así como la necesidad de ofrecer un servicio fácil de usar, hacen que las soluciones de seguridad recomendadas para entornos empresariales, como por ejemplo WEP, WPA, IEEE 802.11i o WPA2 tengan difícil aplicación en entornos públicos.

La seguridad de una red empresarial no significa tener un firewall en una caja o tener un antivirus, tiene mucho qué ver con el diseño de la estructura de la red y la manera de operación de la empresa y su manera de hacer negocios.

4.6 PREGUNTAS Y TIPS

- **¿Qué sucede cuando un switch recibe una trama con dirección MAC destino broadcast?** La reenvía por todos sus puertos
- **En un dominio de colisión, todo el tráfico que envían o reciben las estaciones puede ser escuchado por las demás estaciones.** Verdadero
- **¿Cómo hace el switch para aprender la ubicación de los hosts?** Cada vez que recibe una trama, lee su dirección origen y la asocia al puerto
- **¿Cuál es el método de conmutación más confiable?** Por almacenamiento y reenvío
- **¿Cuál es el objetivo del protocolo STP Spanning Tree Protocol?** Definir una topología de árbol para evitar los bucles
- **¿Podría implementar un servicio de AAA donde utilice Kerberos para realizar autenticación y TACACS+ para autorización y auditoría?** Si es correcto
- **¿Qué es una VLAN?** Una agrupación lógica de dispositivos o estaciones independiente de su ubicación física
- **¿Cómo se transmiten las tramas en los enlaces de VLAN Trunking?** Se les agrega una "etiqueta" indicando a que VLAN corresponden
- **¿Cómo se interconectan las diferentes VLANs?** Mediante un dispositivo de capa 3
- **¿Para qué se puede utilizar el filtrado de tráfico?** Para decidir qué tipo de paquetes pasan y cuáles no
- **¿Cómo se le llaman en el IOS de Cisco al conjunto de reglas que determinan si un paquete está permitido o denegado?** Listas de control de acceso
- **¿En qué sentido analiza el conjunto de reglas de una ACL el IOS de Cisco?** En forma secuencial de la primera a la última
- **¿Qué sucede con un paquete que al ser comparado con las sentencias de una ACL no concuerda con ninguna?** Se deniega
- **¿Qué significa AAA?** Authentication - Authorization – Accounting
- **En un sistema con Token Cards, el usuario ¿de dónde obtiene su contraseña de única vez?** De la Token Card y su código
- **¿Qué significan las siglas NAS?** Network Access Server
- **¿Cómo envía las contraseñas PAP para autenticar el establecimiento del enlace?** Envía la contraseña en texto claro sin cifrar
- **¿Cómo envía las contraseñas CHAP para autenticar el establecimiento del enlace?** Calcula un hash de la contraseña y envía ese hash
- **¿Cuál es el objetivo de IEEE 802.1x?** Define la forma en que se debe realizar la autenticación y autorización de usuarios que acceden a una red LAN
- **¿Qué mejoras a WEP se incluyen en el nuevo estándar 802.11i?** Cambiar RC4 por AES, El agregado de TKIP
- **¿Qué sistema de control de acceso le permite al propietario de un recurso establecer el permiso de acceso a un recurso?** El propietario de un recurso es responsable por los privilegios de acceso mediante DAC (Discretionary Access Control)
- **¿Qué algoritmo de encriptación recomienda IEEE 802.11i?** AES

CAPÍTULO 5:

5.1 ATAQUES Y CONTRAMEDIDAS

El conocimiento de los diferentes ataques y sus características, le permiten a un analista en seguridad estar más prevenido y mejor preparado ante la posibilidad de que sus sistemas sean atacados.

¿Cómo definiría un "ataque" y que consecuencias podría tener? Un ataque ocurre cuando una persona intenta acceder, modificar o dañar un sistema o entorno. Puede realizar una interceptación, modificación, interrupción o falsificación de los datos.

¿Qué factores considera que pueden incrementar el riesgo de recibir un ataque?

- Falta de políticas y/o normativas
- Protocolos
- Ambiente multilenguaje y multiproveedor
- Dispersión geográfica
- Falta de actualización del software base
- Uso incorrecto de las aplicaciones
- Errores en los programas
- Errores de configuración
- Passwords
- Falta de supervisión y/o controlado

¿Cómo aprenden las direcciones MAC los switches? A medida que reciben tráfico de las estaciones. Cada vez una estación envía una trama, el switch lee la dirección MAC origen y la relaciona al puerto desde donde la recibió. De esta forma, va formando la tabla que utiliza para seleccionar hacia que puerto reenviará una trama. Cuando recibe una trama con una dirección MAC destino que aún no conoce el switch reenvía la trama hacia todos los puertos.

¿Qué es una VLAN? Es una agrupación lógica de dispositivos o estaciones independiente de su ubicación física. No necesariamente, estos dispositivos o estaciones están conectados al mismo switch, ni todos los enlaces de un switch formarán parte de esta agrupación. La configuración de las VLANs se realiza en los switchs.

¿Cómo se realiza la asignación dinámica de direcciones IP? Se puede realizar mediante DHCP, este permite que el host reciba toda la información que pueda necesitar para su configuración de red en un solo mensaje, utiliza un mecanismo de direcciones IP en forma dinámica.

El servidor DHCP mantiene un conjunto de direcciones IP y a medida que los clientes le solicitan direcciones se las asigna por un período de tiempo determinado.

DHCP está implementado según el modelo cliente-servidor, es decir, debemos tener un servidor DHCP configurado en nuestra red local. Actualmente es el protocolo de configuración dinámica más difundido y de uso generalizado.

5.1.1 Introducción

Con la expansión de redes actuales, el incremento de la velocidad en los accesos y en el uso de los servicios de networking, los ataques encuentran un escenario cada vez más amplio y accesible a través de las redes. La amenaza de los ataques a redes, servidores, y estaciones de trabajo actualmente pueden provenir de diversos sitios y se deben aplicar, mantener y monitorear todas las medidas necesarias para mantenerse seguros de un ataque.

Mantener la seguridad, hoy por hoy consiste en participar de una batalla diaria entre la gente que desea atacar a los sistemas y la gente que desarrolla productos y servicios para ayudar a protegerlos. Piense que su red es, entonces, el campo de batalla.

Las redes de ordenadores se encuentran expuestas a ataques informáticos con tanta frecuencia que es necesario imponer una gran cantidad de requisitos de seguridad para la protección de sus recursos. Aunque las deficiencias de estos sistemas se pueden comprobar mediante herramientas convencionales, no siempre son corregidas. En general, estas debilidades pueden provocar un agujero en la seguridad de la red y facilitar entradas ilegales en el sistema.

La mayoría de las organizaciones disponen actualmente de mecanismos de prevención y de mecanismos de protección de los datos integrados en sus redes. Sin embargo, aunque estos mecanismos se deben considerar imprescindibles, hay que estudiar como continuar aumentando la seguridad asumida por la organización.

Así, un nivel de seguridad únicamente perimetral (basado tan solo en la integración en la red de sistemas cortafuegos y otros mecanismos de prevención) no debería ser suficiente. Debemos pensar que no todos los accesos a la red pasan por el cortafuegos, y que no todas las amenazas son originadas en la zona externa del cortafuegos. Por otra parte, los sistemas cortafuegos, como el resto de elementos de la red, pueden ser objeto de ataques e intrusiones.

Una analogía que ayuda a entender la necesidad de incorporar estos elementos podría ser la comparación entre la seguridad de una red informática y la seguridad de un edificio: las puertas de entrada ejercen un primer nivel de control de acceso, pero normalmente no nos quedamos aquí; instalaremos detectores de movimiento o cámaras de vigilancia en puntos claves del edificio para detectar la existencia de personas no autorizadas, o que hacen un mal uso de los recursos, poniendo en peligro la seguridad. Además, existirán vigilantes de seguridad, libros de registro en los que se apuntará a todo el personal que accede a un determinado departamento que consideramos crítico, etc. Toda esta información se procesa desde una oficina de control de seguridad donde se supervisa el registro de las cámaras y se llevan los libros de registro.

Todos estos elementos, proyectados en el mundo digital, configuran lo que se conoce en el ámbito de la seguridad de redes informáticas como mecanismos de detección.

5.1.2 ¿Qué es un ataque?

Un ataque ocurre cuando una persona o un grupo de personas intenta acceder, modificar o dañar un sistema o entorno. Estos ataques pueden ser simples y no estar relacionados o pueden ser más complejos y ejecutados en forma organizada.

Un ataque ocurre de diferentes formas y por distintas razones. Estos ataques generalmente intentan lograr algunos de estos objetivos:

- Un **ataque de acceso**: es un ataque donde alguien quiere acceder a sus recursos. Ataca la privacidad.
- Un **ataque de modificación**: es un ataque de alguien que quiere modificar los datos de su sistema. Ataca la integridad.

- Un **ataque de denegación de servicio**: Es un ataque de alguien que quiere interrumpir algún servicio de networking. Ataca la disponibilidad.
- Un **ataque de fabricación**: consiste en falsificar la información. Ataca la autenticidad.

5.1.2 Motivaciones

Las personas que ataquen los sistemas se ven motivados por diferentes razones:

- Por diversión o desafío: Un usuario malicioso podría intentar atacar cualquier sitio sólo con el fin de divertirse o probar que puede hacerlo.
- Por venganza: Un empleado descontento o algún empleado de la competencia podría atacar sus sistemas para tomar venganza de alguna situación que lo haya desfavorecido.
- Por terrorismo: Alguna organización que tenga fines políticos y/o religiosos puede comprometer la información o la estabilidad de su sistema para imponer su ideología.
- Rédito económico: Algún usuario malicioso podría comprometer el funcionamiento de sus sistemas o alterar la información de los mismos con el fin de verse favorecido económicamente.
- Ventaja competitiva: Una empresa de la competencia podría acceder a sus sistemas para recabar información de índole estratégico empresarial y ubicarse en una mejor posición competitiva.
- Poder: Algunas personas podrían intentar acceder a la información sensible que reside en sus sistemas sólo para tener el conocimiento de esa información.

5.1.3 Amenazas primarias

Las amenazas representan el posible peligro del sistema. Pueden provenir de personas (Hacker, Cracker), de programas o de desastres naturales. Equivalen a los factores que se aprovechan de las debilidades del sistema. Por otro lado las contramedidas son las técnicas de protección del sistema contra las amenazas.

Un analista de seguridad deberá identificar las amenazas en sus sistemas y establecer las contramedidas
necesarias para que no se concreten.

Entre las amenazas más comunes podemos encontrar:

- Eavesdropping
- Acceso no autorizado
- Denegación de Servicio
- Denegación de Servicio Distribuida

5.1.4 Debilidades en la seguridad de redes

Actualmente las redes están formadas por un gran conjunto de dispositivos. Los diferentes niveles de seguridad que se quieran implementar en una red (desde el acceso a ésta hasta la verificación de la integridad de los datos que circulan) dependen, en gran medida, de la seguridad de esos dispositivos.

Las debilidades en la seguridad de las redes van a estar originadas en gran medida por las

vulnerabilidades de los dispositivos presentes en la red. Una vulnerabilidad representa el punto o aspecto del sistema que es susceptible de ser atacado. Equivale al conjunto de debilidades del sistema.

Un analista de seguridad, debe mantenerse constantemente al tanto de las vulnerabilidades más recientes en los dispositivos que forman su red. De ésto depende que se comprometa la seguridad de los dispositivos y, por ende, de la red.

5.2 FACTORES QUE CONTRIBUYEN A LA EJECUCIÓN DE ATAQUES

En esta sección estudiaremos las principales causas que contribuyen a la inseguridad en las redes.

Los problemas de inseguridad actuales no se encuentran favorecidos únicamente por usuarios maliciosos, sino que muchas veces se encuentran ayudados por desinteligencias propias del administrador de la red, por malas implementaciones de las aplicaciones, desconocimiento, negligencia, etc.

Para esta sección, hemos catalogado los principales factores que pueden generar problemas de seguridad en las siguientes categorías:

- Falta de políticas y/o normativas
- Protocolos
- Ambiente multilenguaje y multiproveedor
- Dispersión geográfica
- Falta de actualización del software de base
- Uso incorrecto de las aplicaciones
- Errores en los programas
- Errores de configuración
- Passwords
- Falta de supervisión y/o control

5.2.1 Falta de políticas y/o normativas

Muchas organizaciones han incorporado su estructura informática de acuerdo a cómo surgieron sus necesidades. Así es como fueron creando poco a poco su red local, sus servidores, usuarios, acceso a Internet, servicios a terceros, etc. Muchas veces, este crecimiento no ha sido planificado, por lo que no se crea la documentación asociada, ni se tienen en cuenta las restricciones necesarias.

No es extraño entonces, encontrarnos con una gran estructura, donde los usuarios no tienen en claro cuáles son sus permisos, sus obligaciones y sus restricciones.

Es necesario crear las normativas o políticas que rijan el comportamiento de los usuarios, donde se exprese en forma explícita los roles de cada usuario y las penalidades en caso de que se incurra en alguna falta. Esta normativa debe ser refrendada por los niveles superiores de la organización, y deberá ser firmada por todos los usuarios de la red.

Algunas normas comunes en este tipo de políticas son:

- Perfiles, derechos y directorios de acceso de cada usuario
- Uso del correo electrónico (utilizarlo sólo con fines comerciales y no personales)

- Prohibición de instalación de software no autorizado
- Prohibición de instalación de hardware no autorizado
- Publicación de los directorios a los que se les realizará una copia de respaldo

De esta forma el usuario conoce sus derechos y obligaciones, y los administradores de la red tienen una base para realizar los controles necesarios sin que esto pueda incurrir en una violación de la privacidad de los usuarios.

5.2.2 Protocolos

Aún cuando mantengamos nuestro software libre de problemas de implementación, nuestras configuraciones totalmente libres de errores, y todos los usuarios protegidos con contraseñas de alta complejidad, podemos ser vulnerables. Esto es debido a que muchas vulnerabilidades se encuentran asociadas a las definiciones de los protocolos.

Es necesario diferenciar entre la definición de un protocolo y su implementación. La definición de un protocolo generalmente es creada por entidades generadoras de estándares, como la IETF (Internet Engineering Task Force) que define protocolos a través de los documentos RFC. Las implementaciones son creadas por las entidades desarrolladoras de software. Así es como tenemos, por ejemplo, diferentes implementaciones de TCP, existe una implementación de Microsoft, de Solaris, Linux, SCO, IBM, Cisco, etc. Muchas veces, las diferentes implementaciones no se comportan de la misma manera, a pesar de ser conformes a la definición del protocolo. Si la definición del protocolo o la implementación tienen un problema de seguridad, nuestra red será vulnerable.

Cuando se crearon los protocolos que hoy sirven de base para Internet, tuvieron como objetivo la alta disponibilidad, y no la seguridad. Así es como podemos encontrar múltiples problemas de seguridad en su definición. A medida que se han encontrado las vulnerabilidades, algunos protocolos han evolucionado en nuevas versiones, se han creado protocolos complementarios para segurizarlos o, sencillamente, se difundió el problema pero no se modificó el protocolo.

Un ejemplo claro de este tipo de problemas es el protocolo más difundido globalmente: IP. El protocolo IP transporta los datos encapsulados en texto plano, con lo que cualquier usuario que escuche la red, podrá interpretar la información. Tampoco realiza ningún control sobre el emisor, así es como cualquier usuario puede cambiar su dirección IP y hacerse pasar por otro usuario (esto se denomina "spoofing"). Actualmente se encuentra en investigación la nueva versión del protocolo IP: IP versión 6, que define las herramientas necesarias para evitar estos problemas. Dado que IPv6 aún no se encuentra implementado mundialmente, se ha creado un protocolo complementario a la versión actual de IP, que sirve de solución temporal a los problemas de seguridad de IP: IPSec.

	IP	IPSEC	IPv6
Autenticación	No	Si	Si
Privacidad	No	Si	Si
No repudio	No	Si	Si
Detección de duplicados	No	Si	Si
Funciona sobre	Protocolos de capa 2 (Ethernet, PPP, Frame Relay, etc)	Sólo sobre IP	Protocolos de capa 2 (Ethernet, PPP, Frame Relay, etc)

5.2.3 Ambiente multilenguaje y multiproveedor

Actualmente existen múltiples proveedores de múltiples servicios. Esto trae importantes beneficios al momento de realizar una compra de una plataforma o un sistema de base, dado que podemos seleccionar lo que se ajuste mejor a nuestras necesidades. El problema que esto trae aparejado es que se necesitarán diferentes herramientas de control y/o administración y personal especializado en cada una de las plataformas en uso dentro de la organización. Cuanta mayor sea la diversidad de plataformas, mayor será la cantidad de problemas de seguridad y mayor será el riesgo al que estaremos expuesto. Las empresas desarrolladoras de software y hardware van evolucionando en el tiempo y son muy dinámicas. Se fusionan con otras empresas, son absorbidas y eliminadas del mercado, se dividen, etc. Debido a esto, es imposible mantenerse siempre bajo la misma plataforma.

5.2.4 Dispersión geográfica

Debido a la descentralización en las operaciones de las organizaciones y a la búsqueda de una mayor cobertura, muchas corporaciones mantienen sucursales distribuidas a lo largo de varias ciudades y países. Esta dispersión puede resultar muy beneficiosa en términos comerciales, pero al distribuir la red en múltiples puntos, significa que se deberán controlar múltiples puntos de ingreso. Si la red se encuentra en diferentes países, puede variar la legislación, y probablemente variarán las formas en que se deban realizar los controles de seguridad. Como medida de seguridad, muchas organizaciones definen un único punto de entrada y salida de datos a la red. De esta forma sólo es necesario hacer el control y la administración en un solo punto. La desventaja de este esquema es que, de acuerdo a las distancias, puede resultar muy costoso mantener los enlaces intersucursales.

5.2.5 Falta de actualización del software de base

A medida que se utilizan los diferentes software de base se van descubriendo fallos en la programación que pueden debilitar la seguridad del sistema, la red, o la organización completa. Estos fallos, una vez descubiertos y publicados, son generalmente corregidos mediante actualizaciones provistas por las empresas desarrolladoras.

Es responsabilidad del administrador mantenerse al día con las actualizaciones para el software de base que esté utilizando. Actualmente, muchos sistemas proveen herramientas automáticas para la búsqueda de las actualizaciones necesarias. De esta forma se facilita la tarea del administrador. Aún manteniéndose al día con las actualizaciones, pueden existir fallos detectados pero no publicados, o publicados pero no corregidos, con lo que es necesario mantenerse informado con las últimas noticias en fallas e implementar medidas de seguridad alternativas para protegerse, como filtrado de paquetes, listas de control de acceso, etc.

5.2.6 Uso incorrecto de las aplicaciones

Es necesario realizar un estudio para conocer qué tipo de aplicaciones podemos utilizar, de acuerdo a nuestro objetivo y al entorno en que las utilizaremos. Debemos evitar el uso de una aplicación para un fin diferente para el que fue creada.

Un ejemplo de esto, es el uso de SMB para compartir archivos mediante Internet . El protocolo SMB fue creado para su utilización dentro de una red LAN confiable, si se lo utiliza mediante redes no confiables, corremos el riesgo de compartir archivos hacia terceras personas, dar acceso a los recursos de nuestra red, o aún incluso perder nuestra información.

Otro ejemplo podría ser el uso de una consola remota Telnet para realizar configuraciones de equipos

a través de Internet. Ya hemos visto los problemas de seguridad que tiene Telnet, por lo que corremos el riesgo de difundir nuestras configuraciones a cualquier usuario malicioso que lo desee. En lugar de Telnet, se debería utilizar SSH.

5.2.7 Errores en los programas

Así como existen errores en el software de base, también existen errores en el software de aplicación que pueden comprometer la seguridad de nuestro sistema o de nuestra red. No sólo es necesario conocer las aplicaciones que estamos utilizando, sino también las aplicaciones instaladas para mantenerlas actualizadas. Existen herramientas para detectar las vulnerabilidades asociadas tanto a las aplicaciones como al software de base. Las más difundidas son Nessus, LANguard Network Security Scanner y Retina

5.2.8 Passwords

El problema de seguridad más común no proviene de fallos en implementaciones o problemas de seguridad de los protocolos utilizados, sino que proviene de contraseñas inseguras o fáciles de adivinar. Este inconveniente es muy fácil de solucionar (sólo es necesario cambiar la contraseña), pero muy difícil de concientizar a los usuarios de la red a utilizar contraseñas complejas, variantes en el tiempo. Es necesario hacer responsable al usuario de las acciones que se realicen con su nombre de usuario y contraseña. De esta forma, el usuario tendrá más cuidado al momento de distribuir sus datos.

Un usuario malicioso que quiera conocer la contraseña de otro usuario, podría realizar repetidos intentos hasta obtener el ingreso. Por lo que también es necesario realizar un control de la cantidad de intentos fallidos de ingreso. En general se permiten sólo tres intentos fallidos, luego de eso, se puede deshabilitar la cuenta por un tiempo determinado o hasta que el administrador la vuelva a habilitar.

La mayoría de los sistemas operativos de red permiten definir una política de contraseñas. En general, se puede definir la longitud máxima y mínima, el período máximo en que estará activa (pasado ese período deberá ser cambiada), el período mínimo en que estará activa (el tiempo que debe transcurrir antes que un usuario esté habilitado para cambiar su contraseña), un control de complejidad (para evitar contraseñas triviales), un control de historial (para evitar que se repitan las contraseñas), etc.

Valores de una política de contraseñas seguras:

- Longitud mínima: 8 caracteres
- Longitud máxima: -
- Período máximo: 30 días
- Período mínimo: 1 día
- Control de complejidad: Habilitado
- Historial de contraseñas: Habilitado
- Cantidad de contraseñas en el historial: 10

5.2.9 Falta de supervisión y/o control

Una vez que hemos implementado nuestras políticas de seguridad en el sistema o en la red, es

necesario realizar controles periódicos para asegurarnos que se han implementado de forma correcta y que no han surgido nuevos problemas. Si esto no se realiza, nunca podremos detectar intentos de ingresos (fallidos o exitosos), usos abusivos de los recursos por parte de los usuarios, u otros inconvenientes. Los diferentes sistemas proveen de herramientas para registrar los eventos que suceden. Estos archivos deben ser supervisados periódicamente. Se puede definir un host como base central para los logs, donde se recibirán los logs de toda la red. De esta forma, un solo host centralizará los eventos de todos los dispositivos. Cuando se almacenan registros que sólo son informativos (estadísticas, etc) suele bastar con almacenarlos en el mismo dispositivo donde se generan. Cuando se almacenan por motivos de seguridad, sin embargo, se recomienda guardar una copia en otra máquina (el servidor de logs). El motivo es que si hay una intrusión en el dispositivo podrán borrar o modificar los registros, pero esas mismas actividades quedarán registradas en el servidor de logs, avisando así a los operadores.

Normalmente, la máquina que reciba los logs no se debe utilizar para otra cosa (para no ser susceptible de ataques) ni debe poder recibir logs desde fuera de la red local (para evitar ataques por saturación).

5.3 FASES DE UN ATAQUE (Hacking Ético)

En esta sección estudiaremos cuáles son los pasos que realiza un intruso para atacar un sistema. Es importante conocer la forma en que proceden los intrusos para conocer la forma de detenerlos. En general, los intrusos realizan las mismas actividades cuando desean ingresar o atacar a un sistema, por lo que podemos generalizar los pasos en:

- Reconocimiento - Investigación
- Escaneo
- Penetración – Obtención de acceso
- Mantenimiento de acceso – Extensión de la influencia
- Borrado u ocultamiento de huellas

Para cada uno de estos pasos, estudiaremos el comportamiento del intruso y las técnicas que podemos utilizar para detectarlo y detenerlo.

5.3.1 Reconocimiento - Investigación (Footprinting)

Siempre antes de realizar un ataque, los intrusos realizan un estudio del objetivo. Este estudio involucra diferentes herramientas y técnicas para conocer el ámbito del objetivo, cuáles y dónde se encuentran sus servicios, los posibles agujeros de seguridad, etc. Es en esta parte donde el atacante obtiene, reúne y organiza toda la información posible sobre su objetivo o su víctima, mientras más información obtiene con mayor precisión puede lanzar un mejor ataque.

Generalmente este paso consiste en obtener la siguiente información:

- **Información de la empresa objetivo**: A través de consultas en buscadores de Internet se puede obtener el perfil de la empresa. En general esta información es pública y no es crítica, pero permite al atacante conocer cuáles pueden ser las implicancias de su ataque, el país donde se encuentra la empresa, lo que permitirá conocer el ámbito legal en que se encuentra.
- **Información del dominio objetivo**: Conociendo el nombre de la empresa, como hemos visto, se puede obtener su información de dominio a través de consultas tipo WHOIS.
- **Información de los servidores**: Una vez que el intruso obtuvo el dominio, puede realizar consultas NSLOOKUP para conocer cuáles son los servidores que tiene la empresa. En general, en este punto, el atacante seleccionará uno o varios servidores que serán objetivo del

ataque.

- **Identificación de la plataforma**: Uno de los principales datos que buscan de sus objetivos es la plataforma sobre la que trabajan (Windows, Linux, Novell, etc.). Esto se puede realizar mediante la utilización de técnicas de ***OS fingerprint.***
- **Identificación de los servicios**: Otra información importante que buscan obtener los atacantes son los servicios que ofrecen los servidores objetivos. Esto se puede realizar mediante escaneadores de puertos (port-scanners).

La fase de recogida de información podría empezar con la utilización de todas aquellas aplicaciones de administración que permitan la obtención de información de un sistema como, por ejemplo, ping, traceroute, whois, finger, rusers, nslookup, rcpinfo, telnet, dig, etc.

La simple ejecución del comando ping contra la dirección IP asociada a un nombre de dominio podría ofrecer al atacante información de gran utilidad. Para empezar, esta información le permitirá determinar la existencia de uno o más equipos conectados a la red de este dominio.

Una vez descubierta la existencia de, como mínimo, uno de los equipos del dominio, el atacante podría obtener información relacionada con la topología o la distribución física y lógica de la red, mediante alguna aplicación de administración como, por ejemplo, traceroute. Mucha de la información, antes mencionada, como Domain Names, algunas direcciones IP, País, Ciudad, e información de contacto los Crackers la obtienen buscando en las bases de datos de WHOIS. Las bases de datos WHOIS mantienen detalles de direcciones IP registradas en 5 regiones del Mundo. Estas bases de datos son manejadas por 5 organizaciones llamadas Regional Internet Registry (RIR).

Las 5 bases de datos WHOIS están localizadas en:

1. América del Norte (ARIN)
2. América del Sur, América Central y el Caribe (LACNIC)
3. Europa, el medio Este y Asia Central (RIPE NCC)
4. Asia del Pacifico (APNIC)
5. África (AfriNIC)

Tipos de DNS Records

- A (address) – Dirección IP del Host
- MX (mail exchange) – Dominio del mail exchanger
- NS (name server) – Dominio del nombre del servidor
- CNAME (canonical name) -- Provee nombres o alias adicionales para localizar una computadora
- SOA (start of authority) – Indica la autoridad para un dominio
- TXT (text) – Record de texto genérico
- HINFO (host info)– Información del Host con el tipo de CPU y OS

Herramientas en línea (Online) para Footprinting:

- SamSpade (www.samspade.org) Herramienta WHOIS
- DNSstuff (www..dnsstuff.com/) Múltiples herramientas para extraer información de los DNS

- People Search (People.yahoo.com) Buscador de personas e información de contacto
- Intellius (www.intellius.com) Buscador de persona e información de contacto
- NetCraft (www.netcraft.com) Detector de OS
- Whois (www.whois.org) Herramienta WHOIS

Herramientas de programas (software) para Footprinting:

- ***SamSpade:*** Esta herramienta provee información sobre el DNS, WHOIS, IPBlock y permite hacer Ping, Dig, Trace, etc.
- **Web Data Extractor Tool:** Esta herramienta extrae data de los meta tags, enlaces, email, números telefónicos, fax, entre otras cosas y permite almacenarlos en el disco duro.
- **Spiderfoot:** Esta herramienta provee información sobre sub-dominios, versión del web server, dominios similares, emails y bloques de red (Netblocks)
- **DNS Enumerator:** Es una herramienta automatizada para le extracciones de su-dominios.
- **Traceroute:** Herramienta de línea de comandos que viene instalada en la mayoría de los OS se usa para encontrar la ruta de un sistema, muestra los detalles de paquetes IP que viajan entre dos sistemas. Puede trazar el número de routers (enrutadores) por donde viajan los paquetes y la duración del tiempo en tránsito del viaje entre dos routers. Traceroute trabaja explotando una característica del Internet Protocol (IP) llamada TTL (Time To Live).
- **NsLookup:** Nslookup es una herramienta valiosa para hacer consultas a los DNS para la resolucion de nombres de Host. Viene instalado en los sistemas operativos UNIX y Windows y se puede accesar a travez del command prompt.
- **3D Traceroute:** Es un trazador de ruta en 3 dimensiones que te permite monitorear visualmente conectividades de Internet (websites), escanear puertos, WHOIS, entre otras cosas.
- **GEOSpider:** GEOSpider te ayuda a detectar, identificar y monitorear tu actividad de red en un mapa mundial. Puedes ver websites, y localizaciones mundiales de direcciones IP. También puede trazar un Hacker, investigar un website y trazar su nombre de dominio.

Contramedidas: Como primer contramedida, es necesario restringir la información que se difundirá, especialmente a través de los servicios de DNS y WHOIS. También se pueden incluir filtrado de paquetes, para evitar la detección de la plataforma y los servicios y un Sistema de Detección de Intrusos (IDS) para detectar cuándo se está produciendo un escaneo de puertos, por ejemplo.

5.3.2 Escaneo (Scanning)

Cuando hablamos de la fase de “Escaneo”, generalmente nos referimos a una etapa previa al ataque, en la cual el atacante hecha mano a una serie de herramientas genéricamente referidas como scaners y escanea la red o sistema objetivo con el fin de obtener información específica, sobre la base obtenida en el paso previo de “Reconocimiento”. Como parte de las tareas a desarrollar durante esta etapa, el atacante intentara identificar diversos puntos de entrada al sistema objetivo, recorriendo en forma lógica su superficie. Las herramientas utilizadas para la tarea, serán entre otras:

Dialers: Herramientas automáticas de discado telefónico, utilizadas para escanear números telefónicos correspondientes a un área o compañía determinada por medio de la utilización de un MODEM (Practica a menudo referida como “wardialing”). Su principal objetivo, es el de hallar dentro

del rango especificado, maquinas de fax, computadoras, o sistemas de comunicaciones, sobre los cuales sea posible a partir de un ataque posterior, conseguir algún tipo de acceso. (Eh: Toneloc, Tmap)

Network Mapping Tools: Herramientas automáticas relacionadas con el descubrimiento de host y/o sistemas. Como resultado de la ejecución de este tipo de herramientas, el atacante a menudo es capaz de construir un mapa de la red objetivo. Este tipo de herramientas reúnen las características necesarias como para consultar que hosts se encuentran disponibles, que servicios en ellos se ejecutan y mucha información adicional, de suma importancia para el atacante. (Ej.: Cheops-NG).

Port scanners: Un port scanner o escaner de puertos, es una herramienta diseñada específicamente para indagar un host, acerca de sus puertos abiertos. Como tal, esta herramienta suele ser de suma utilidad para el atacante, a la hora de identificar los puertos abiertos del host objetivo, así como también los servicios que en él se encuentran corriendo. (Ej.: Nmap)

Vulnerability Scanners: Los scanners de vulnerabilidades, son herramientas diseñadas para buscar e identificar vulnerabilidades y/o debilidades en una aplicación, host o red. Estos se componen básicamente de un conjunto de herramientas de descubrimiento, y escaneo, más una base de datos de vulnerabilidades conocidas, contra las cuales se intenta hacer corresponder cada uno de los hallazgos. (Ej.: Nessus). Al término de esta fase, el atacante debería haber sido capaz de obtener el conjunto de información necesaria, a efectos de decidir el o los puntos específicos que intentará vulnerar. Dicha información incluye pero no se limita a: Sistemas Telefónicos a la espera de comunicaciones entrantes, puertos de servicios abiertos-cerrados-filtrados, posibles vulnerabilidades relacionadas con los servicios ofrecidos por el sistema, red o host objetivo. Algunos de los tipos de ataque mediante scanners son: Escaneo de conexión TCPconnect, Escaneo TCP reverse ident, FTP bounce attack, Escaneo UDP ICMP port unreachable, Fingerprinting, Escaneo TCP SYN, Escaneo TCP FIN, Stealth Port Scanning, Escaneo de fragmentación, Eavesdropping-Packet Sniffing, Snooping, Downloading.

Contramedidas: Entre las contramedidas básicas relacionadas con la mitigación del riesgo en esta fase, se puede mencionar el filtrado de puertos, la eliminación en el sistema de los servicios innecesarios, la implementación de sistemas de detección y prevención de intrusos, etc.

5.3.3 Obtención de acceso – Penetración (Gaining Access)

Este es quizás el paso más crítico en un ataque. En esta situación el atacante intentará acceder al objetivo. Para realizar este paso, utilizan diferentes técnicas:

- Explotación de vulnerabilidades: si existe algún producto instalado que permita la ejecución de código arbitrario, ésta es una puerta abierta al acceso de intrusos.
- Debilidad de contraseñas: Una contraseña débil puede permitir el ingreso de intrusos.
- Servicios mal configurados: Un servicio que no esté adecuadamente configurado puede permitir que intrusos hagan uso abusivo del mismo, o incluso, que ejecuten código arbitrario.
- Decepción o engaño: Ataque contra las personas.

Un ataque puede comenzar con la obtención de un usuario y contraseña de un servicio. El atacante puede lograr acceder a un entorno restringido. Desde este entorno, puede obtener más información, que luego le servirá para acceder a mayores servicios. Recuerde que un atacante no tiene apuro, y

puede dedicar todo su tiempo para encontrar la información que necesite.

Contramedidas: Las contra medidas para estas técnicas ya las hemos estudiado, pero no está de más repasarlas:

- Actualización constante del software instalado
- Definición de políticas de contraseñas
- Ejecución periódica de análisis de vulnerabilidades y auditoria de código
- Ejecución de procedimientos de hardening
- Filtrado de paquetes
- Implementación de HIDSs+, NIDSs e IPSs
- Procedimientos de revisión periódica de logs

Como contra medida general, siempre tenemos que tener en cuenta al filtrado de paquetes y la revisión periódica de los archivos de logs para conocer los eventos que han sucedido en el sistema.

Escalada de privilegios: Este tipo de ataque, puede ser el siguiente paso de un atacante luego de haber obtenido acceso a un sistema, ya que permite obtener permisos como "Administrador" al equipo, de ese modo no se tienen derechos restringidos.

Un atacante puede causar la mayoría del daño consiguiendo privilegios administrativos en una red. Hay varias utilidades que un atacante puede utilizar para ganar privilegio administrativo. Por ejemplo, la utilidad **Getadmin.exe** en sistemas Microsoft, es usada para otorgar a usuarios comunes privilegios administrativos agregando a estos usuarios al grupo de administradores. Esta utilidad funciona con todas las cuentas excepto con la cuenta de Guest.

Es importante observar que cualquier cuenta se haya concedido el "*Debug Programs right*". Siempre se podrá ejecutar satisfactoriamente Getadmin.exe, incluso después de la aplicación del hotfix. Esto es porque el "*Debug Programs righ*t" habilita al usuario a adjuntar cualquier proceso. El "*Debug Programs right*" es inicialmente otorgado a Administradores y debe ser utilizado únicamente con usuarios altamente confiables. También, si Getadmin.exe se ejecuta con una cuenta que sea ya un miembro del grupo local de los administradores, continua funcionando (incluso luego de aplicar el hotfix).

Como ejemplo, por defecto Windows XP instala el software de ayuda y accesibilidad que se activa pulsando la tecla SHIFT 5 veces seguida. Si lo haces verás que aparece una ventana que te permite configurar la aplicación. El fichero que se ejecuta es sethc.exe ubicado en C:\WINDOWS\SYSTEM32. El ataque consiste en sustituir sethc.exe por cmd.exe (esto se puede hacer con un disco de arranque ntfsdos o con un LIVE CD de Linux como Knoppix) y así cuando pulsemos la tecla SHIFT 5 veces seguidas se nos abrirá la shell de comandos, desde la cual podemos hacer TODO lo que queramos con el equipo. La cosa está en pulsar 5 veces la tecla SHIFT antes de iniciar sesión, y se nos abrirá la shell con permisos de ADMINISTRADOR.

5.3.4 Mantener acceso – (Maintaining access)

Una vez que un atacante ha logrado ingresar a un sistema generalmente realiza actividades para evitar ser detectado y deja herramientas o puertas traseras en el sistema para poder mantener un acceso permanente, quizás para conseguir más información, o como plataforma de ataque hacia otros sistemas.

Para evitar ser detectado, en general un atacante busca los archivos de auditoría o log del sistema, para borrarlos o modificarlos ocultando su acceso y sus actividades. En Linux, esto se puede hacer

desactivando el servicio syslog y borrando los archivos de log (generalmente ubicados en /var/log/*) , mientras que en Windows, se puede realizar borrando el contenido del Visor de Sucesos.

Cuando el intruso desee incorporar herramientas para accesos posteriores, corre el riesgo que un administrador las detecte y se conviertan en la demostración que ha ingresado al sistema. Para evitar esto, siempre dejan sus herramientas en directorios ocultos o difíciles de acceder. En Windows NT/2000 esto se puede realizar ocultando los directorios (muy sencillo de detectar), o mediante las facilidades provistas por NTFS, se puede concatenar un archivo detrás de otro mediante la herramienta cp.exe del NT Resource Kit, y quedar oculto a los ojos de los administradores. Esta herramienta no modifica el archivo original, con lo que no se detectarán cambios. En Linux, se pueden utilizar directorios dentro de /dev/, donde existen links hacia los diferentes dispositivos. Este directorio muchas veces no es tenido en cuenta por los administradores, por lo que puede convertirse en un buen lugar para ocultar herramientas.

Es importante tener presente que con frecuencia, el objetivo final de un ataque puede no ser el primer sistema atacado, sino que por el contrario, este puede ser el primero de una serie de saltos intermedios, necesarios para atacar con éxito el objetivo final, sin ser rastreados.

Esta situación puede generar que nuestro sistema termine siendo víctima, y a la vez se convierta en atacante. Si no son tomadas las medidas necesarias, podríamos eventualmente vernos envueltos en un ataque, con las implicancias legales que ello significa. Un ejemplo claro respecto de lo mencionado, son los ataques de Denegación de Servicio Distribuida, que se desarrollarán más adelante.

Contramedidas: Si no se pudo evitar el ingreso, es necesario detectarlo para evitar futuros ingresos. Para lograr detectarlo, es necesario evitar el borrado de los archivos de log. Para evitar que un intruso elimine los archivos de log, se puede optar por mantenerlos guardados fuera del lugar donde se generan. Hemos visto anteriormente cómo podemos armar una arquitectura donde todos los archivos de auditoría sean guardados en un servidor de log. De esta forma, si se eliminan los logs del dispositivo atacado, quedará la copia en el servidor de logs.

Es complicado evitar la copia de archivos, pero puede detectarse la modificación de ellos. Existen herramientas que crean un hash de los archivos de sistema, y avisan al administrador en caso de detectar una modificación. Un ejemplo de este tipo de herramientas es Tripwire.

5.3.5 Ocultamiento de huellas (Covering tracks)

Una vez que un atacante ha logrado ingresar a un sistema generalmente realiza actividades para evitar ser detectado. Bajo el término “Borrado u Ocultamiento de Huellas” o “Covering tracks”, solemos referirnos a la fase en la cual el atacante lleva a cabo una serie de pasos, con el fin de ocultar cada una de las acciones llevadas a cabo tanto al momento de ganar acceso al sistema objetivo, así como también respecto de su permanencia.

Para evitar ser detectado, en general un atacante busca los archivos de auditoria o log del sistema, para borrarlos o modificarlos ocultando su acceso y sus actividades. Cuando el intruso instala en el sistema atacado, herramientas destinadas a operar de algún modo o a asegurar su entrada en accesos posteriores, corre el riesgo que las mismas sean detectadas por un administrador y se conviertan en prueba suficiente a la hora de demostrar que un ingreso no autorizado ha sido llevado a cabo. A fin de evitar tal situación, el atacante suele dejar sus herramientas en directorios ocultos o de difícil acceso. En Windows NT/2000 esto se puede realizar ocultando los directorios (muy sencillo de detectar), o mediante las facilidades provistas por NTFS, se puede concatenar un archivo detrás de otro mediante la herramienta cp.exe del NT Resource Kit, y quedar oculto a los ojos de los administradores. Esta herramienta no modifica el archivo original, con lo que no se detectarán cambios. En Linux, se pueden utilizar directorios dentro de /dev/, donde existen links hacia los diferentes dispositivos. Este directorio muchas veces no es tenido en cuenta por los administradores, por lo que puede convertirse en un buen lugar para ocultar herramientas. Al margen de estas técnicas,

un atacante podría ser capaz de utilizar técnicas mucho más avanzadas a la hora de ocultar su acceso, tal como la programación de componentes a nivel del kernel del sistema operativo.

Contramedidas: Una vez que el atacante ha logrado vulnerar la seguridad de nuestro sistema y ha sido capaz de acceder el host objetivo, lo mejor es considerar la posibilidad de instalar nuevamente el sistema a partir de las copias de oro del software de base, los aplicativos que sobre él se encuentran corriendo y los datos almacenados como parte de nuestra política de resguardo. No obstante se debe notar que la implementación de sistemas centralizados de logging, procesos adecuados de hardening y sistemas de integridad de archivos, deberían ser considerados siempre que sea posible a fin de detectar un ataque, minimizar el impacto del mismo o al menos colaborar a su eventual investigación.

5.3.6 Simulación de un Ataque

El intruso comenzará su ataque obteniendo el rango de direcciones IP donde se encuentra alojado el servidor de la web www.victima.com. Para ello, será suficiente realizar una serie de consultas al servidor de DNS de la compañía. A continuación, realizará una exploración de puertos en cada una de las direcciones IP encontradas en el paso anterior. El objetivo de esta exploración de puertos es la búsqueda de servicios en ejecución en cada una de las máquinas del sistema, mediante alguna de las técnicas vistas en los módulos anteriores.

Gracias a los mecanismos de prevención instalados en una red a modo de ejemplo (el sistema cortafuegos y las listas de control), la mayor parte de las conexiones serán eliminadas. De esta forma, el atacante sólo descubrirá dos de las máquinas de la red (el servidor de DNS y el servidor web). El atacante decide atacar el servidor de HTTP. Para ello, tratará de descubrir que tipo de servidor está funcionando en este equipo (le interesa el nombre y la versión del servidor en cuestión), ya que es muy probable que existan deficiencias de programación en la aplicación que está ofreciendo dicho servicio. Por otra parte, el atacante también intentará descubrir el sistema operativo y la arquitectura hardware en la que se ejecuta el servidor. Esta información será importante a la hora de buscar los exploits que finalmente utilizará para realizar el ataque de intrusión. Para obtener toda esta información, el atacante tiene suficiente con las entradas de DNS que la propia compañía le está ofreciendo (a través de los campos HINFO de las peticiones). De esta forma, el atacante descubre que el servidor web está funcionando bajo una arquitectura concreta y que en este servidor hay instalado un determinado sistema operativo.

Otra fuente de información para descubrir el sistema operativo y la aplicación que ofrece el servicio web, y contrastar así la información ya obtenida, podrían ser las cabeceras de las respuestas HTTP que el servidor envía a cada petición de HTTP o HTTPS).

El atacante, que colecciona un amplio repertorio de aplicaciones para abusar de este producto, acabará obteniendo un acceso con privilegios de administrador. Supongamos, por ejemplo, que dicha intrusión la realiza gracias a la existencia de un buffer mal utilizado que existente en la aplicación en cuestión.

La primera observación que podemos indicar de todo el proceso que acabamos de describir es que los mecanismos de prevención de la red permiten la realización de este abuso contra el servidor de HTTP, ya que la forma de realizar el desbordamiento de buffer se realizará mediante peticiones HTTP legítimas (aceptadas en las listas de control del sistema cortafuegos).

Así pues, sin necesidad de violar ninguna de las políticas de control de acceso de la red, el atacante puede acabar haciéndose con el control de uno de los recursos conectados a la red de la compañía.

Una vez comprometido el servidor de HTTP, el intruso entrará en la fase de ocultación y comenzará a eliminar rápidamente todas aquellas marcas que pudieran delatar su entrada en el sistema. Además, se encargará de instalar en el equipo atacado un conjunto de *rootkits*. Una rootkit es una recopilación de herramientas de sistema, la mayoría de ellas fraudulentas, que se encargarán de dejar puertas abiertas en el sistema atacado, para garantizar así futuras conexiones con la misma escalada de

privilegios, así como ofrecer la posibilidad de realizar nuevos ataques al sistema o a otros equipos de la red (denegaciones de servicio, escuchas en la red, ataques contra contraseñas del sistema, etc).

Una vez finalizada la fase de ocultación de huellas, el atacante dispone de un equipo dentro de la red que le podrá servir de trampolín para realizar nuevos ataques e intrusiones en el resto de equipos de la compañía. Además, operando desde una máquina interna de la red, el atacante ya no estará sujeto a las restricciones impuestas por los sistemas de prevención.

Finalmente, una vez llegados a este punto el atacante dispondrá sin ningún problema de los datos que los clientes tienen almacenados en la base de datos.

Este ejemplo nos muestra como la existencia de un sistema cortafuegos (u otros mecanismos de prevención) y la utilización de comunicaciones cifradas (como un mecanismo de protección de datos) no es suficiente a la hora de defender nuestros sistemas de red.

5.4 EFECTOS DE UN ATAQUE

Como vimos anteriormente, la seguridad debe proveer integridad, disponibilidad y confidencialidad de la información. Un ataque puede tener diferentes efectos. En las siguientes secciones estudiaremos cada uno de estos efectos con mayor profundidad.

5.4.1 Interceptación

En un entorno de seguridad informática, nos referimos a interceptación cuando un usuario no autorizado obtiene acceso a la información. Estos tipos de ataques resultan complejos de detectar, sobre todo si es pasivo y el atacante no deja huellas.

En las siguientes secciones se analizarán, entre otros, los siguientes ataques de interceptación y sus contramedidas:

- Eavesdropping
- STP Manipulation
- CAM table overflow

5.4.2 Modificación

En un ataque por modificación, un usuario malicioso generalmente obtiene acceso no autorizado a un recurso con los privilegios necesarios para cambiar el entorno y lo hace para su beneficio. Modificar un flujo de datos en una transmisión de red o archivos en un servidor pueden ser ejemplos de estos ataques. En estos casos, la detección puede ser más sencilla que en la interceptación porque existe información que se modifica. De todas formas, la detección de modificación requiere un estudio exhaustivo por parte de un analista en seguridad.

5.4.3 Interrupción

La interrupción consiste en dañar o dejar sin funcionamiento un sistema completo o parte de éste. Para un atacante, puede ser un desafío, una venganza o la forma de facilitarle el acceso a algún otro recurso. Si bien la detección es inmediata, los daños ocasionados por la suspensión del servicio y el tiempo de recuperación pueden ser muy importantes y se deben tomar la mayor cantidad de recaudos posibles para evitar sufrir un ataque de este tipo.

5.4.4 Falsificación

La falsificación puede aplicarse a la creación de nuevos objetos dentro del sistema, o simplemente participar en una conversación simulando ser otro interlocutor. Un ejemplo muy común es un usuario malicioso, quien altera su identidad simulando ser un host determinado con el fin de obtener algún beneficio propio. Existen diferentes técnicas de detectar los intentos de falsificación y se revisarán posteriormente en las siguientes secciones.

5.4.5 Reconocimiento

El reconocimiento es el descubrimiento no autorizado de la topología de la red, sus sistemas, servicios o vulnerabilidades. Este proceso (que consiste en obtener información) en la mayoría de los casos precede a un ataque por denegación de servicios (DoS). Es importante notar que los atacantes se aprovechan de las debilidades presentes en la red y de la publicación de información que se haga. El reconocimiento es algo similar a un ladrón oportunista, que constantemente rastrea el panorama buscando alguna debilidad (como una puerta abierta, o un descuido) para aprovecharse. Como se mencionó anteriormente, el reconocimiento es el descubrimiento no autorizado de la topología de la red, sus sistemas, servicios o vulnerabilidades

Este proceso consiste generalmente en estos pasos:

- El usuario malicioso (intruso) típicamente realiza barridas de ping a la red destino para determinar qué direcciones IP están siendo utilizadas. Las barridas de ping consisten en enviar paquetes ICMP echos a cada uno de los números IP que forman la red de la víctima.
- Una vez que el atacante puede determinar qué hosts son utilizados, se utiliza un localizador de puertos disponibles (port scanner) para determinar qué servicios están activos en cada una de las direcciones IP.
- Cuando se obtuvo la lista de puertos disponibles en cada IP, resta conectarse a las aplicaciones de cada uno de los puertos donde se encontró algún servicio. Así se podrá determinar el tipo y versión de cada uno, como también el tipo y versión del sistema operativo del host.

Basado en esta información, el intruso puede determinar si existe alguna posible vulnerabilidad que pueda explotar. Para realizar cada paso del reconocimiento de una red, existen numerosas herramientas o alternativas. Algunas herramientas ya integran toda la secuencia de pasos: detectan los hosts alcanzables en una red, y por cada uno de estos realizan una búsqueda de sus servicios y vulnerabilidades. Utilizando, por ejemplo, las herramientas **nslookup** y **whois**, un atacante puede determinar también el rango de direcciones IP asignados a una corporación o entidad.

Sondeo ICMP: Un sondeo ICMP revelaría en redes potencialmente débiles y poco protegidas, información sobre sus equipos. Existen varios tipos de mensajes ICMP, pero a nosotros nos interesan especialmente cuatro de ellos, que son los que resultan verdaderamente útiles para rastrear una red.

- *Echo request:* También conocidos como paquetes ping. Mediante *Nmap*, podemos realizar barridos ping para identificar de una manera sencilla los equipos de la red.
- *Timestamp request:* Son solicitudes de tiempo y se utilizan para obtener el tiempo que tarda nuestro equipo en obtener una respuesta del equipo victima.
- *Information request:* Este mensaje se ideó en un principio para localizar sistemas autoconfigurables en el momento de arranque, consiguiendo de esta manera descubrir direcciones de red.

- *Subnet address mask request:* Estos mensajes revelan información sobre la mascara de subred utilizada por el equipo analizado. Esto servirá al atacante para realizar el mapa de la estructura de la red y sus subredes.

Barrido ICMP: Permite realizar barridos ICMP con el fin de localizar maquinas internas. Un barrido ICMP consiste en enviar mensajes de tipo 8 "echo request" a todas las direcciones IP internas de la red. Con *Nmap* se realizaría con el comando:

```
$ sudo nmap -sP 192.168.2.0/24 Starting Nmap 4.62 ( http://nmap.org ) at
2008-12-22 01:46 CET n hostname -- replacing with '*' Host (192.168.2.1)
appears to be up. MAC Address: 00:XX:XX:XX:XX:XX Host 192.168.2.100 appears
to be up. Host 192.168.2.103 appears to be up. Host 192.168.2.114 appears
to be up. Host 192.168.2.116 appears to be up. Host 192.168.2.117 appears
to be up. Host 192.168.2.124 appears to be up. Nmap done: 256 IP addresses
(7 hosts up) scanned in 2.142 seconds
```

Con el argumento -sP, estamos indicando a Nmap que realice un barrido ping en la red. Un administrador competente, habrá filtrado el tráfico ICMP en los Firewalls y en el router, por ello esta técnica quedaría obsoleta y habría que condimentarla con algo más. Podríamos añadir al comando el argumento "-PI", que enviará paquetes de sondeo TCP ACK y SYN al puerto 80 de cada equipo:

```
$ sudo nmap -sP -PI 192.168.2.0/24 Starting Nmap 4.62 ( http://nmap.org )
at 2008-12-22 01:46 CET n hostname -- replacing with '*' Host (192.168.2.1)
appears to be up. MAC Address: 00:XX:XX:XX:XX:XX Host 192.168.2.100 appears
to be up. Host 192.168.2.103 appears to be up. Host 192.168.2.107 appears
to be up. Host 192.168.2.114 appears to be up. Host 192.168.2.116 appears
to be up. Host 192.168.2.117 appears to be up. Host 192.168.2.124 appears
to be up. Host 192.168.2.136 appears to be up. Host 192.168.2.141 appears
to be up. Nmap done: 256 IP addresses (7 hosts up) scanned in 6.053 seconds
```

Como se apreciar, hemos obtenido más información con este comando que con el anterior.

Rastreo Vainilla connect(): TCP es un protocolo de control en el que por medio de banderas (flags) se controla la conexión realizada, indicando cuando se inicia, cuando se establece, cuando finaliza... En el protocolo TCP, para indicar que se va a establecer una conexión, se envía un paquete con flag SYN de sincronización de los *sequence numbers* (números de secuencia) a un puerto determinado, la maquina receptora, si tiene ese puerta abierto, enviará un paquete con flag SYN para sincronizar los números de secuencia y un paquete con flag ACK para afirmar que la conexión ha sido realizada, finalmente, el primer equipo (cliente) enviará un paquete con flag ACK para asegurar que la conexión se ha establecido también por parte del cliente. Sin embargo, si el cliente envía un paquete con flag SYN a un puerto que se encuentra cerrado o filtrado, el servidor responderá con un paquete con flag RST.

Rastreo de flag SYN medio abierto: para sincronizar una conexión entre dos equipos utilizando el protocolo TCP/IP, el cliente manda al servidor un SYN, el servidor responde con un SYN/ACK en el caso de que el puerto esté abierto y con un RST si está cerrado. En el caso de que esté abierto y se envíe el SYN/ACK, el cliente concluye con un ACK. La técnica de rastreo de flag SYN medio abierto se distingue de la Vainilla connect() en que esta última, si el puerto está abierto, el cliente responde con un flag ACK. En SYN medio abierto, en caso de que se encuentre abierto el puerto, en lugar de

responder con un ACK se responde con un RST, lo que provoca que se reinicie bruscamente la conexión. Estos dos métodos son fácilmente detectados por los IDS, así que no son aconsejables en caso de querer realizar un análisis sigiloso. Para realizar estos rastreos podemos utilizar Nmap con el argumento -sS: **`$ nmap -sS 192.168.2.156`**

En *Nmap* se puede ajustar la política de tiempos con el argumento "-T". Con el argumento "-T sneaky" se puede llegar a burlar la seguridad de los Firewalls. Esto consiste en enviar muy rápidamente paquetes SYN a diferentes puertos, lo que provocará un desbordamiento de SYN (un tipo de DoS).

Métodos de rastreo sigiloso: Estos tipos de métodos, aprovechan la estructura de la propia pila TCP/IP para escanear sin ser detectados (en algunas ocasiones, ya que dependerá del IDS y sobretodo del SO). Cuando en los métodos anteriores enviábamos paquetes SYN a un host y este nos respondía con el conocido SYN/ACK, daba a conocer que el puerto en cuestión estaba abierto, pero cuando respondía con un RST, daba a entender que el puerto estaba cerrado o filtrado. Muchos IDS son capaces de detectar paquetes con el indicador SYN recibidos y lo que harán será avisar al administrador de sistema diciéndole: "Están evaluándonos!", a lo que el administrador del sistema responderá tomando mayores medidas de seguridad.

Rastreo TCP con indicador inverso: Este rastreo va a consistir en enviar sondeos con indicadores de tipo FIN, URG, PUSH y NULL. Existen tres tipos de sondeos:

- Sondeo FIN = Consistirá en enviar paquetes con el indicador FIN.
- Sondeo XMAS = Consistirá en enviar paquetes con los indicadores FIN, URG y PUSH.
- Sondeo NULL = Consistirá en enviar paquetes con el indicador NULL.

Cuando enviemos uno de estos indicadores, si el puerto se encuentra abierto, no se obtendrá respuesta alguna. Sin embargo, si el puerto se encuentra cerrado, recibiremos un paquete RST. Esto viene definido por el estándar RCF 793, que indica que si no se percibe ninguna respuesta del puerto analizado, significa que el puerto está abierto o que el equipo se encuentra apagado. Lo que estamos haciendo es enviar paquetes "basura" que difícilmente van a ser detectados por los IDS. En equipos con sistemas Microsoft Windows, no se recibe respuesta alguna cuando se intenta conectar a un puerto cerrado. Por eso esta técnica sólo es eficaz con plataformas UNIX.

Para realizar uno de estos sondeos podemos utilizar *Nmap* con sus respectivos argumentos:

- Sondeo FIN = se utilizará el argumento -sF.
- Sondeo XMAS = se utilizará el argumento -sX.
- Sondeo NULL = se utilizará el argumento -sN.

Rastreo con indicador ACK: Otra técnica sigilosa es la de enviar paquetes con indicador ACK y luego analizar la información de los paquetes RST recibidos. Esta técnica explota vulnerabilidades de la pila TCP/IP de sistemas BSD. Existen dos modos de hacerlo:

- ***Análisis del TTL:*** El TTL es el tiempo de vida de los paquetes recibidos (Time To Live). Para realizar este ataque, hay que enviar miles de paquetes con indicador ACK a diferentes puertos del equipo víctima. Después habrá que analizar los resultados. *Nmap* nos permite hacer esto con el argumento "sA". A la hora de analizar las respuestas habrá que fijarse en el TTL del paquete.
- ***Análisis del campo WINDOW:*** Para realizar este ataque se llevará a cabo un procedimiento similar al anterior, enviando muchos paquetes ACK y analizando el campo WINDOW del paquete respuesta. Por norma general, los puertos cerrados tienen un valor WINDOW de 0.

Para realizarlo podemos utilizar *Nmap* con el argumento -sW.

Rastreo de rebote FTP (FTP bounce): Muchos servidores web tienen su propio servidor FTP y en muchas redes podemos localizar ordenadores que hacen de servidores de archivos y utilizan el protocolo FTP para desarrollar dicha misión. Es posible que tengamos localizado un servidor FTP desactualizado que permita realizar este tipo de ataques. Existe une defecto en la forma en la que los servidores FTP gestionan las conexiones mediante el comando PORT, que envía datos a equipos y puertos especificados por el usuario.

Esto es lo que sucede cuando se lleva a cabo este ataque:

1. El atacante conecta con el puerto del servidor FTP (por defecto el 21). Introduce el modo pasivo, el servidor por tanto es forzado a enviar datos utilizando DTP al puerto especificado por el atacante en un objetivo.
2. El atacante intenta conectar con un puerto específico TCP del servidor objetivo mediante el comando PORT.
3. Se crea una conexión con el equipo objetivo especificado por el comando PORT anterior, mediante el comando LIST. Si se observa una repuesta 226, el puerto está abierto, si la repuesta es 425, el puerto está cerrado o filtrado.

Todo esto lo podemos hacer con Nmap mediante el siguiente comando:

```
$ nmap -P0 -b usuario:contraseña@servidor:puerto ipdestino
```

En realidad el argumento que realiza el escaneo FTP bounce es el "-b". El "-P0" sirve para especificar a Nmap que no queremos que realice un ping.

Contramedidas: El descubrimiento se basa en alcanzar máquinas de una red y explorar su contenido. Una alternativa para evitar el descubrimiento es establecer filtros de tráfico. El filtrado de tráfico puede actuar como una barrera que impida los paquetes ICMP echos (generalmente utilizados en la primer fase del descubrimiento) como también un delimitador del área donde se brindan los servicios. La mayoría de las implementaciones de los servicios permiten también definir un rango de hosts permitidos y un rango de hosts denegados para acceder a sus servicios.

5.4.6 Escuchas de Red

Uno de los primeros ataques contra las dos primeras capas del modelo TCP/IP son las escuchas de red. Se trata de un ataque realmente efectivo, puesto que permite la obtención de una gran cantidad de información sensible. Mediante aplicaciones que se encargan de capturar e interpretar tramas y datagramas en entornos de red basados en difusión, conocidos como escuchas de red o *sniffers*, es posible realizar el análisis de la información contenida en los paquetes TCP/IP que interceptan para poder extraer todo tipo de información.

Las *escuchas* son un ataque pasivo que tienen como objetivo final monitorizar la red para capturar información sensible como, por ejemplo, la dirección MAC o IP origen y destino, identificadores de usuario, contraseñas, clave WEP, etc.

Las escuchas se consideran un paso previo a ataques posteriores, como por ejemplo la inyección y modificación de mensajes sin necesidad de descifrar claves, SSID, etc. lo que supone una importante fisura en cuanto a seguridad.

Para que un dispositivo tenga la capacidad de llevar a cabo escuchas en una red WLAN, debe tener instalada (o integrada) una tarjeta WLAN que actúa en “modo promiscuo” o en “modo monitor”. Estos modos de operación permiten recibir todo el tráfico que circula por la red.

Un ***sniffer*** no es más que un sencillo programa que intercepta toda la información que pase por la interfaz de red a la que esté asociado. Una vez capturada, se podrá almacenar para su análisis posterior. De esta forma, sin necesidad de acceso a ningún sistema de la red, un atacante podrá obtener información sobre cuentas de usuario, claves de acceso o incluso mensajes de correo electrónico en el que se envían estas claves. Este tipo de técnica se conoce como *sniffing*.

Algunos ejemplos de sniffer para WLANs disponibles para distintos sistemas operativos son los siguientes:

- Windows: Netstumbler, Airopeek, AirLine
- GNU/Linux: AirSnort, Kismet, Airtraf
- Sistema Operativo MAC: iStumbler, KisMAC, MacStumbler
- Pocket PC: “Ministumbler”.

Las técnicas de ***sniffing*** también se conocen como técnicas de ***eavesdropping*** y técnicas de ***snooping***. La primera, *eavesdropping*, es una variante del *sniffing*, caracterizada por realizar la adquisición o intercepción del tráfico que circula por la red de forma pasiva, es decir, sin modificar el contenido de la información.

Por otra parte, las técnicas de *snooping* se caracterizan por el almacenamiento de la información capturada en el ordenador del atacante, mediante una conexión remota establecida durante toda la sesión de captura. En este caso, tampoco se modifica la información incluida en la transmisión.

La forma más habitual de realizar técnicas de *sniffing* en una red, probablemente porque está al alcance de todo el mundo, es la que podríamos denominar *sniffing software*, utilizando las aplicaciones ya mencionadas.

Una de las aplicaciones más conocidas, en sistemas Unix, es ***Tcpdump***. Captura todos los paquetes que llegan a nuestra máquina y muestra por consola toda la información relativa a los mismos. Se trata de una herramienta que se ejecuta desde la línea de comando y que cuenta con una gran cantidad de opciones para mostrar la información capturada de formas muy diversas. *Tcpdump* es una herramienta muy potente y es la base para muchos otros sniffers que han aparecido posteriormente. Otra herramienta muy conocida es ***Ettercap***. Esta aplicación, que también funciona desde consola, ofrece un modo de ejecución interactivo en el que se muestran las conexiones accesibles desde la máquina donde se encuentra instalado y que permite seleccionar cualquiera de ellas para la captura de paquetes. *Ettercap* es una aplicación muy potente que permite utilizar la mayor parte de las técnicas existentes para realizar tanto *sniffing* como *eavesdropping* y *snooping*.

5.4.7 Wardriving

Es un caso particular del ataque anterior (escuchas de red) donde individuos equipados con material apropiado (dispositivo inalámbrico, antena, software de rastreo y unidad GPS) tratan de localizar en un vehículo, moto, caminando, puntos de acceso inalámbricos.

5.4.8 Descubrimiento de ESSID ocultos

En general en una red WLAN el proceso de conexión de un usuario consiste en la autenticación y asociación del mismo a un punto de acceso. Para ello, es necesario que el usuario conozca previamente la existencia de una red WLAN.

El SSID (Service Set IDentifier) es un código incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID. Dependiendo de si la red inalámbrica funciona en modo ad-hoc o en modo Infraestructura, el SSID se denomina BSSID (Basic Service Set Identifier) o ESSID (Extended Service Set IDentifier) respectivamente. El BSSID suele ser la dirección MAC del equipo y, por lo tanto, es única. El ESSID es el nombre de 32 caracteres de la red. Todos los puntos de acceso de una red deben tener el mismo ESSID.

A menudo al ESSID se le considera como el nombre de la red y es el parámetro clave para llevar a cabo el descubrimiento de una red WLAN por parte de un usuario. Así, existen dos procesos mediante los cuales el usuario puede identificar la existencia de una o varias redes WLAN en modo infraestructura. Dichos procesos de descubrimiento de red son los siguientes:

- ***Escaneo Pasivo***: El dispositivo de usuario espera recibir la señal del punto de acceso. Los puntos de acceso emiten BEACON FRAMES cada cierto intervalo fijo de tiempo. Las BEACON FRAMES son anuncios de la red emitidos por el punto de acceso inalámbrico que normalmente contienen el ESSID. Los usuarios escuchan estos BEACON FRAMES e identifican al punto de acceso. En ese momento ya puede iniciarse el proceso de asociación y autenticación.
- **Escaneo Activo:** La estación lanza tramas a un punto de acceso determinado y espera una respuesta. El usuario también puede enviar una trama PROVE REQUEST con un determinado ESSID para ver si algún el punto de acceso inalámbrico responde.

No emitir BEACON FRAMES o emitirlos sin el ESSID permite que sólo aquellos usuarios que conozcan el ESSID de la red WLAN se puedan conectar a ella, ya que obligan a llevar a cabo el descubrimiento de red mediante el envío de tramas PROVE REQUEST con un determinado ESSID por parte del usuario. Este tipo de redes se conocen como redes WLAN cerradas. Sin embargo, es posible descubrir el ESSID de una red aún en estas circunstancias con dispositivos operando en modo monitor y capturando tramas PROVE REQUEST de otros usuarios de la red. El envío de este tipo de tramas se puede forzar mediante un ataque de denegación de servicio en el que desasociamos a un usuario válido de la red para que vuelva a intentar conectar se a la misma.

5.4.9 Eavesdropping

Eavesdropping es el proceso de escuchar una conversación o parte de ésta. En eavesdropping, la persona que "escucha" o tiene acceso a los datos de esta conversación, lo hace sólo porque ninguna de las partes que integran la conversación ha tenido en cuenta que sus datos pueden ser leídos . Es decir, la posibilidad de tomar e interpretar los datos es por un descuido de las partes.

Como vimos anteriormente, la interceptación o eavesdropping, es un proceso mediante el cual un agente capta información (en claro o cifrada) que no le iba dirigida. Esta captación puede realizarse por muchísimos medios (por ejemplo, capturando las radiaciones electromagnéticas o simplemente interpretando las señales eléctricas de los cables) . Aunque no es un ataque que represente un daño o una baja en un servicio, lo más peligroso del eavesdropping es que resulta muy difícil de detectar mientras que se produce, de forma que un atacante puede capturar información privilegiada sin que nadie se dé cuenta. Un medio de interceptación bastante habitual es el ***sniffing***. Este método consiste en capturar tramas que circulan por la red mediante un software que corre en una máquina conectada al segmento de red o bien mediante un dispositivo que se engancha directamente el cableado. Estos dispositivos, denominados *sniffers* de alta impedancia, se conectan en paralelo con el cable de forma que la impedancia total del cable y el aparato es similar a la del cable solo, lo que hace difícil su detección.

Otro punto a tener en cuenta cuando estudiamos eavesdropping es la imposibilidad de establecer límites concretos en redes wireless. En este tipo de infraestructura, realizar eavesdropping es mucho

más sencillo ya que no se requiere ningún acceso físico al medio, el medio donde se transportan los datos está disponible siempre. Cualquier usuario malicioso con una placa de red compatible con la tecnología wireless que se utilice, tiene la posibilidad de "ver" las tramas que circulan desde los Access Points y las placas, si es que no se han implementado las medidas de seguridad adecuadas.

Contramedidas: Ya que los ataques de eavesdropping son, por lo general, difíciles de detectar, es importante considerar algunos puntos claves para evitar o facilitar que se produzca en una red. Algunos de estos puntos son:

- No permitir la existencia de segmentos de red de fácil acceso ya que representan el sitio indicado para que un atacante se conecte y capture tráfico. No obstante esto puede resultar difícil en redes ya instaladas pero puede ser tenido en cuenta para instalaciones nuevas.
- Utilizar cifrado para realizar las comunicaciones o el almacenamiento de la información. Para cifrar la información se puede utilizar un software o dispositivos de cifrado (utilizar dispositivos involucran una alternativa más costosa pero más eficiente que el uso de software).
- No permitir tomas de red libres habilitadas, donde un usuario malicioso puede conectarse para capturar tráfico. Es recomendable analizar regularmente la red para verificar que todas las máquinas activas están autorizadas.
- Realizar autenticación a nivel de la capa de enlace. Por ejemplo, en wireless la utilización de 802.11i permite disponer de una capa más de seguridad en el acceso a la red

5.4.10 Técnicas de detección de Sniffers

Las técnicas de detección de sniffers se basan en la búsqueda del problema que varía según se tenga acceso local al ordenador o haya que descubrirlo de algún ordenador remoto, esta última es la variante más usual aunque la más compleja. El objetivo de la mayoría de pruebas es conseguir que la máquina que tiene la tarjeta de red en modo promiscuo se traicione a sí misma, revelando que ha tenido acceso a información que no iba dirigida a ella y que, por tanto, tiene un sniffer, lamentablemente es un objetivo que puede llegar a ser imposible por su complejidad. Si la búsqueda es una consulta directa sobre un ordenador, lo que tendremos que hacer es mirar el estado de las diferentes interfaces de redes que tengamos en dicho equipo, la forma más habitual es utilizar el comando ipconfig.

En el caso de que no podamos acceder y consultar el estado de las interfaces de red, entonces utilizaríamos algún defecto en la implementación concreta del protocolo TCP/IP por algún programa/comando, las técnicas de búsqueda de sniffer en este caso se dividen en dos: las dependientes del sistema operativo y las que no lo son. La ventaja de las técnicas que dependen del sistema operativo es su excelente rendimiento cuando explora máquinas que tienen el mismo sistema operativo del que la técnica obtiene partido, la principal desventaja es el gran número de falsos negativos que ocasiona debido a que en muchos casos las implementaciones de la pila TCP/IP varían entre versiones del mismo sistema operativo. Como ejemplos destacar el filtrado de paquetes en kernels de Linux.

En condiciones normales, los paquetes son aceptados o rechazados a nivel hardware por la tarjeta de red según la MAC address de destino que aparezca en el frame Ethernet. Sólo si esa MAC address es la de la propia máquina o la de broadcast, el paquete es aceptado (copiado) y procesado (se pasa al kernel); en caso contrario, se rechaza (se ignora). Para cada PC del segmento de red que se desee analizar se crea un paquete con una MAC address de destino que no exista en el segmento, cualquier máquina con la tarjeta de red en modo no promiscuo rechazará directamente un paquete que tiene como destino una que no es la suya ni la de broadcast, y no procesará el paquete, mientras que una tarjeta en modo promiscuo pasará el paquete al kernel, este analizará el paquete exclusivamente según los datos del paquete IP que encapsule, el paquete es un ping completamente normal que es contestado por la máquina que tiene el sniffer revelando así su estado.

Filtrado de paquetes broadcast en algunos drivers de Windows: La idea es la misma que en el filtrado de paquetes en kernels de Linux, la característica a considerar en este caso es cómo el driver del sistema operativo decide cuándo un paquete va dirigido a la dirección broadcast ff:ff:ff:ff:ff:ff, cuando la tarjeta de red está en modo no promiscuo, se verifican los seis octetos mientras que en estado promiscuo sólo se verifica el primero de ellos, este hecho facilita mucho la detección de sniffers. Se crea un paquete dirigido a la MAC address ff:00:00:00:00:00, cualquier tarjeta en modo no promiscuo lo va a rechazar automáticamente, mientras que una tarjeta en modo promiscuo con un sistema operativo Windows que use el driver afectado confundirá ese paquete con uno dirigido a broadcast, y lo procesará. Las técnicas no dependientes del sistema operativo son menos fiables y menos concluyentes, suelen basarse en suposiciones del comportamiento de determinados sniffers, convirtiendo estas técnicas inútiles en determinados ambientes. A destacar como ventaja no suelen provocar falsos negativos.

Test DNS: En este método, la herramienta de detección en sí misma está en modo promiscuo. Creamos numerosas conexiones TCP/IP falsas en nuestro segmento de red, esperando un sniffer pobremente escrito para atrapar esas conexiones y resolver la dirección IP de los inexistentes host. Algunos sniffers realizan búsquedas inversas DNS en los paquetes que capturan. Cuando se realiza una búsqueda inversa DNS, una utilidad de detección de sniffers huele la petición de las operaciones de búsqueda para ver si el objetivo es aquel que realiza la petición del host inexistente.

Test de ping: Este método confía en un problema en el núcleo de la máquina receptora. Podemos construir una petición tipo "ICMP echo" con la dirección IP de la máquina sospechosa de hospedar un sniffer, pero con una dirección MAC deliberadamente errónea. Enviamos un un paquete "ICMP echo" al objetivo con la dirección IP correcta, pero con una dirección de hardware de destino distinta. La mayoría de los sistemas desatenderán este paquete ya que su dirección MAC es incorrecta. Pero en algunos sistemas Linux, NetBSD y NT, puesto que el NIC está en modo promiscuo, el sniffer analizará este paquete de la red como paquete legítimo y responderá por consiguiente. Si el blanco en cuestión responde a nuestra petición, sabremos que está en modo promiscuo. Un atacante avanzado puede poner al día sus sniffers para filtrar tales paquetes para que parezca que el NIC no hubiera estado en modo promiscuo.

Test ICMP: Ping de Latencia. En éste método, hacemos ping al blanco y anotamos el Round Trip Time (RTT, retardo de ida y vuelta o tiempo de latencia) Creamos centenares de falsas conexiones TCP en nuestro segmento de red en un período de tiempo muy corto. Esperamos que el sniffer esté procesando estos paquetes a razón de que el tiempo de latencia incremente. Entonces hacemos ping otra vez, y comparamos el RTT esta vez con el de la primera vez. Después de una serie de tests y medias, podemos concluir o no si un sniffer está realmente funcionando en el objetivo o no.

Test ARP: Podemos enviar una petición ARP a nuestro objetivo con toda la información rápida excepto con una dirección hardware de destino errónea. Una máquina que no esté en modo promíscuo nunca verá este paquete, puesto que no era destinado a ellos, por lo tanto no contestará. Si una máquina está en modo promiscuo, la petición ARP sería considerada y el núcleo la procesaría y contestaría. Por la máquina que contesta, sabremos que la máquina está en modo promiscuo.

Test Etherping: Enviamos un ping echo al host a testear con una IP de destino correcta y dirección MAC falseada. Si el host responde, es que su interfaz está en modo promiscuo, es decir, existe un sniffer a la escucha y activo.

5.5 ATAQUES DE ACCESO Y SUS CONTRAMEDIDAS

Un ataque por acceso consiste en que un atacante obtiene los privilegios necesarios para acceder a dispositivos o recursos de red en forma ilícita. Generalmente para conseguir el acceso a un sistema los métodos más utilizados son:

- Explotar contraseñas triviales: Aplicar fuerza bruta, diccionarios o herramientas de crack.
- Explotar servicios mal configurados: Servicios como TFTP, FTP anónimo y acceso remoto al registro. Relaciones de confianza entre dominios. Servicios de archivos compartidos.
- Explotar fallas de aplicaciones.
- Acceso a aplicaciones fuera del dominio, desbordamientos de buffers: Examinar y explotar fallas de protocolos.
- Ingeniería social: Engañar a los usuarios simulando ser personal de seguridad con el fin de obtener información. Buscar nombres de usuarios y contraseñas anotadas en los lugares de trabajo. Examinar los papeles arrojados a la basura para encontrar información.

El acceso a datos no autorizados puede resultar en una simple lectura de datos (en algunos casos es tan fácil como encontrar carpetas compartidas en Windows, Unix o Macintosh con acceso público sin contraseñas). También puede resultar en la modificación, copia o eliminado de información.

5.5.1 Man-in-the-middle (Hombre en el medio)

Un ataque man-in-the-middle requiere que el atacante tenga acceso a los paquetes que atraviesan la red, se interponga en una "conversación" y actúe como intermediario entre el emisor y el receptor de los paquetes. Un ejemplo podría ser algún usuario malicioso que hubiera realizado un ataque de DHCP starvation (visto anteriormente) y configure a los hosts de la red indicando su propia dirección IP como puerta de enlace. Con cada host que tome esta configuración, el atacante recibirá todas los paquetes destinados a otras redes, el atacante podrá reenviarlo posteriormente modificando la información que contiene o simplemente obteniendo la información de los datos que envía. Con estos ataques, se puede robar información, robar una sesión para obtener acceso a recursos, realizar un análisis de tráfico para obtener información sobre redes y usuarios, denegación de servicios (DoS) o corrupción de los datos transmitidos.

Los entornos que operan sobre redes WLAN facilitan la captura y redirección de sesiones ya que una estación inalámbrica que transmite no es capaz de detectar la presencia de estaciones adyacentes con la misma dirección MAC o IP.

Así, por ejemplo, una estación inalámbrica podría suplantar la identidad del punto de acceso para conseguir las credenciales válidas del usuario, para posteriormente hacerse pasar ante el verdadero AP como un usuario válido y como un punto de acceso, ante el usuario final.

Para llevar a cabo este ataque es necesario que el dispositivo atacante cuente con dos interfaces WLAN:

- Con una simulará ser un punto de acceso.
- Con la otra simulará ser un usuario válido.

El atacante envía una trama de disasociación a la víctima para que busque un punto de acceso al que conectarse. Posteriormente hace creer a la víctima que es el punto de acceso original, pero operando en otro canal, obtiene de la víctima la información necesaria para conectarse a la red y se conecta al punto de acceso original con la otra tarjeta, haciéndose pasar por un usuario válido.

Contramedidas: Para evitar los ataques de man-in-the-middle resulta fundamental poder asegurar que los extremos de una comunicación son quien dicen ser. Esto se puede lograr utilizando autenticación mediante una entidad certificante.

5.5.2 Explotación de las relaciones confianza

Este tipo de ataque consiste en aprovecharse de las relaciones de confianza entre hosts de la red para lograr un acceso no autorizado. Generalmente el segmento de servidores es protegido por algún Firewall y los hosts del segmento confían entre sí. Si un usuario malicioso pudiera atacar a sólo uno de los servidores comprometería la seguridad de la red completa.

Otra forma de un acceso involucra la escalación de privilegios. La escalación de privilegios ocurre cuando un usuario obtiene privilegios o derechos para la ejecución de comandos o acceso a archivos que le están asignados por el administrador. Una vez que un usuario malicioso escala en los niveles de privilegios, puede instalar sniffers, crear cuentas con accesos ocultos, utilizarla para un DDoS y eliminar archivos (o parte de estos) del registro del sistema.

Los sistemas más comunes que implementan relaciones de confianzas son:

- Active Directory y Dominios en entornos Windows
- NFS y NIS en entornos UNIX

Contramedidas: Para evitar ataques por abuso de relaciones de confianza lo más importante es mantener a todos los hosts del dominio (que forman la relación de confianza) lo más protegidos posibles. Esto implica las actualizaciones más recientes de seguridad en los servicios y sistemas operativos como también la implementación de técnicas de Firewall para evitar los accesos no autorizados. Otro punto a tener en cuenta es no ejecutar servicios que no sean estrictamente necesarios. Aunque los servicios se ejecuten sólo para un dominio de confianza, piense que si el servicio no es necesario, es una posibilidad más de acceso a nuestro host para un atacante.

5.5.3 Manipulación de datos

Mediante la manipulación de datos, un intruso podría capturar tráfico, modificar información de acuerdo a sus intereses, o replicar información.

Los ataques por manipulación de datos más difundidos son:

- Graffitis: Un intruso obtiene acceso a un servidor web y deja su mensaje en el sitio de la compañía atacada modificando sus páginas web.
- Modificación de información en un host de red: El intruso altera archivos en el host accedido, como archivos de contraseñas, para posibilitarse accesos futuros.

Algunas herramientas utilizadas para realizar estos ataques son:

- Analizadores de protocolos con capacidades de capturar contraseñas a medida que son transmitidas por el medio.
- Crackeadores de passwords, que contienen algoritmos que permiten la desencripción de contraseñas. Dependiendo del tipo de contraseña, pueden realizar una desencripción por criptoanálisis, o por fuerza bruta

Contramedidas: Para evitar la manipulación de datos en tránsito, la contramedida ideal es la

utilización de encriptación de los datos que se transmiten.

Si nos interesa tener control sobre los archivos de sistema para detectar cualquier modificación, se puede utilizar software específico, como ya hemos visto, que permite mantener un hash de los archivos críticos, con lo que cualquier modificación no autorizada generará un hash diferente al guardado, lo que permitirá su detección.

5.5.4 Puntos de acceso no autorizados (Rogue Aps)

Si se consigue tener acceso a la instalación física de una red WLAN, éste es uno de los ataques más nocivos. Un Rogue AP es un punto de acceso que se conecta sin autorización a una red existente. Estos puntos de acceso no son gestionados por los administradores de la red y es posible que no se ajuste a las políticas de seguridad de la red. De esta forma se abre una puerta a todo tipo de ataques indeseados, puesto que permite a cualquiera con un terminal WLAN conectarse a la red, y vulnera todos los mecanismos que se basan en el cifrado de información entre extremos (WEP, WEP2, WPA, etc.). En general los rogue APs suelen emitir con más potencia que los puntos de acceso válidos de la red para que los usuarios se conecten a ellos por defecto. Existen numerosas herramientas para detectar los puntos de acceso rogue. Estas soluciones están basadas en un punto de acceso que realiza labores de escaneo y envía los datos a un sistema central que es el encargado de decidir si un punto de acceso es rogue o no. Algunas herramientas de este tipo permiten, además, deshabilitar este tipo de puntos de acceso. Ejemplos soluciones que ofrecen estas funcionalidades son las ofrecidas por fabricantes como Airwave, Airmagnet, Wimetrics o Airdefense.

5.5.5 IP spoofing

En un ataque de falsificación de IP (IP spoofing), el intruso cambia la dirección IP de los paquetes transmitidos, falsificando la dirección IP origen para hacerse pasar por otro usuario. De esta forma, el intruso asume la identidad de un usuario válido y obtiene los privilegios de acceso de ese usuario. Durante un ataque de IP spoofing, el atacante, desde una red externa, pretende hacerse pasar por un usuario de confianza. El atacante podría utilizar una dirección IP dentro del rango de direcciones de la red, o utilizar una dirección externa que es de confianza y tiene permitido el acceso a los recursos de la red.

Normalmente, un ataque de IP spoofing se encuentra limitado a la inserción de datos o comandos dentro de un flujo de datos existente de una aplicación cliente-servidor, o una conversación par a par. El atacante, simplemente envía la información, pero no espera respuesta alguna, dado que el sistema atacado, enviará la respuesta a la dirección IP origen, y no al atacante.

Para lograr una comunicación bidireccional, el atacante debería cambiar las tablas de enrutamiento de los dispositivos intermedios entre él y el objetivo, de forma de crear un camino de vuelta para los paquetes con su dirección IP falsificada.

Así como el eavesdropping, los ataques por IP spoofing no se encuentran limitados a atacantes externos. Este ataque puede ser usado por usuarios internos de la red para lograr ciertos privilegios asignados sólo a unas direcciones IP.

Además de esta técnica, otra forma más sencilla es la de redefinir la dirección física o MAC de una interfaz inalámbrica por una dirección MAC válida dentro del sistema atacado. Para ello, basta con emplear un sniffer que permita capturar alguna MAC válida en el sistema y posteriormente esperar a que ésta deje de transmitir en el sistema o emplear un ataque DoS contra ella para desconectarla de la red y utilizar su dirección MAC. Esta práctica permite romper filtros basados en direcciones MAC. Con cualquiera de estas técnicas, el atacante será capaz de recopilar información sensible como contraseñas, números de cuenta, etc.

Contramedidas: Para evitar ataques por IP spoofing, se pueden crear filtros de paquetes específicos, que no permitan el ingreso de paquetes con dirección IP origen de la red que quieren acceder. Para evitar los ataques internos, la asignación de privilegios debería realizarse en base a un nombre de usuario u otro método de autenticación, y no a una dirección IP.

5.5.6 DNS Poisoning

NS cache poisoning / DNS Poisoning / Pharming es una situación creada de manera maliciosa o no deseada que provee datos de un Servidor de Nombres de Dominio (DNS) que no se origina de fuentes autoritativas DNS. Esto puede pasar debido a diseño inapropiado de software, falta de configuración de nombres de servidores y escenarios maliciosamente diseñados que explotan la arquitectura tradicionalmente abierta de un sistema DNS. Una vez que un servidor DNS ha recibido aquellos datos no autentificados y los almacena temporalmente para futuros incrementos de desempeño, es considerado envenenado, extendiendo el efecto de la situación a los clientes del servidor.

Normalmente, una computadora conectada a Internet utiliza un servidor DNS proporcionado por el proveedor de servicios de Internet (ISP). Este DNS generalmente atiende solamente a los propios clientes del ISP y contiene una pequeña cantidad de información sobre DNS almacenada temporalmente por usuarios previos del servidor. Un ataque de envenenamiento (poisoning attack) de un solo servidor DNS de un ISP puede afectar a los usuarios atendidos directamente por el servidor comprometido o indirectamente por los servidores dependientes del servidor.

Para realizar un ataque de envenenamiento de caché, el atacante explota una vulnerabilidad en el software de DNS que puede hacer que éste acepte información incorrecta. Si el servidor no valida correctamente las respuestas DNS para asegurarse de que ellas provienen de una fuente autoritativa, el servidor puede terminar almacenando localmente información incorrecta y enviándola a los usuarios para que hagan la misma petición.

Esta técnica puede ser usada para reemplazar arbitrariamente contenido de una serie de víctimas con contenido elegido por un atacante. Por ejemplo, un atacante envenena las entradas DNS de direcciones IP para un sitio web objetivo, reemplazándolas con la dirección IP de un servidor que él controla. Luego, el atacante crea entradas falsas para archivos en el servidor que él controla con nombres que coinciden con los archivos del servidor objetivo. Estos archivos pueden contener contenido malicioso, como un virus o un gusano. Un usuario cuya computadora ha referenciado al servidor DNS envenenado puede ser engañado al creer que el contenido proviene del servidor objetivo y sin saberlo descarga contenido malicioso.

Como parte del proyecto Golden Shield, China, de forma regular hace uso de envenenamiento de DNS para redes o sitios específicos que violan las políticas bajo las cuales el proyecto opera.

La primera variante del envenenamiento de caché de DNS involucra redirigir el nombre del servidor del atacante del dominio hacia el servidor de nombres del dominio objetivo, luego se asigna a dicho servidor de nombres una dirección IP especificada por el atacante.

La segunda variante de envenenamiento de caché DNS involucra redirigir el servidor de nombres de otro dominio hacia otro dominio no relacionado a la petición original de una dirección IP especificada por el atacante.

La tercera variante de envenenamiento de caché de DNS, que es denominada falsificación de DNS (DNS Forgery) involucra hacer demorar la respuesta real hacia una consulta recursiva DNS hacia el servidor DNS. Las consultas DNS contienen un número identificador (nonce) de 16 bits, utilizado para identificar las respuestas asociadas a una respuesta dada. Si el atacante puede predecir exitosamente el valor de dicho número identificador y devolver la respuesta primero, el servidor aceptará la respuesta del atacante como válida. Si el servidor elige aleatoriamente el puerto origen de respuesta, el ataque se volverá más dificultoso, dado que la respuesta falsa debe ser enviada por el mismo puerto desde donde la consulta se originó.

Enviando un número de peticiones simultáneas de DNS al servidor para forzarlo a enviar más

consultas recursivas, la probabilidad de predecir exitosamente uno de los números identificadores se incrementa. Esta modificación es una forma de ataque de cumpleaños (birthday attack).

Contramedidas: Muchos ataques de envenenamiento de caché puede ser prevenidos simplemente por servidores DNS siendo menos confiables que la información pasada por ello por otros servidores DNS, e ignorando cualquier registro DNS retornado y que no sea directamente relevante a la consulta. Por ejemplo, versiones recientes de BIND ahora contienen código que evalúa estos casos. Como se mencionó anteriormente, la selección aleatoria del puerto origen de consultas DNS, combinada con el uso de números aleatorios critográficamente seguros para elegir el puerto y el número identificador de 16 bits puede reducir grandemente la probabilidad de ataques de carrera DNS exitosos.

Una versión segura de DNS, DNSSEC, utiliza firmas criptográficas electrónicas validadas con un certificado digital confiable para determinar la autenticidad de los datos. DNSSEC puede contener ataques de envenenamiento de caché.

Este tipo de ataque puede ser mitigado también por las capas de transporte o aplicación para conseguir validación extremo a extremo (end-to-end validation) una vez que una conexión es establecida en extremo. Un ejemplo común de esto es el uso de Seguridad de Capa de Transporte y firmas digitales. Por ejemplo, usando la versión segura de HTTP, HTTPS, los usuarios pueden verificar si el certificado digital es válido y pertenece al dueño esperado de un sitio web. De manera similar, el programa de inicio de sesión remoto SSH verifica certificados digitales en los extremos (si los conoce) antes de proseguir con una sesión. Para aplicaciones que descargan actualizaciones automáticamente, la aplicación puede alojar una copia local del certificado digital de los datos y validar el certificado almacenado en la actualización de software contra el certificado alojado.

5.5.7 DNS rebinding

DNS rebinding es un ataque basado en DNS de código embebido en páginas web aprovechándose de la política del mismo origen de los navegadores. Normalmente las peticiones del código embebido en las páginas web (Javascript, Java, Flash..) están limitadas al sitio web desde el que se han originado (política del mismo origen). DNS rebinding puede mejorar la habilidad de Malware basado en Javascript para penetrar en redes privadas transtornando la política del mismo origen. Usando DNS rebinding un atacante puede sortear Firewalls, navegar en intranets corporativas, mostrar documentos sensibles, y comprometer máquinas internas sin parchear. El atacante registra un dominio el cual delega a un servidor DNS que él controla. El servidor está configurado para responder con un parámetro TTL muy corto, que previene que la respuesta sea cacheada. La primera respuesta contiene la dirección IP de el servidor con el código malicioso. Las consiguientes respuestas contienen direcciones IP de redes privadas falsas (RFC 1918) presumiblemente detrás de un Firewall que es la meta del atacante. Dado que las dos son respuestas DNS completamente válidas, autorizan al script el acceso a hosts dentro de la red privada. Devolviendo múltiples direcciones IP, el servidor DNS habilita al script para escanear la red local o realizar actividades maliciosas.

Contramedidas: Las siguientes técnicas pueden ser utilizadas para prevenir ataques de DNS rebinding:

- DNS pinning - fijando una dirección IP al valor recibido en la primera respuesta DNS. Esta técnica puede bloquear algunos usos legítimos del DNS dinámico.
- Bloqueando la resolución de nombres externos en direcciones internas en los servidores de nombres locales de la organización.
- Los servidores pueden rechazar peticiones HTTP con una cabecera de Host irreconocible.

5.5.8 Pharming

Pharming es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (domain name) a otra máquina distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio.

La palabra Pharming deriva del término farm (granja en inglés) y está relacionada con el término "phishing", utilizado para nombrar la técnica de ingeniería social que, mediante suplantación de correos electrónicos o páginas web, intenta obtener información confidencial de los usuarios, desde números de tarjetas de crédito hasta contraseñas.

El origen de la palabra se halla en que una vez que el atacante ha conseguido acceso a un servidor DNS o varios servidores (granja de servidores o DNS), se dice que ha hecho un farming.

En una conferencia organizada por el Antiphishing Working Group, Phillip Hallam-Baker definió este término como "*un neologismo de mercadotecnia diseñado para convencer a banqueros y empresarios de comprar nuevos equipos o accesorios de seguridad*".

Si buscamos en un diccionario de inglés el término pharming, lo encontraremos definido como "la producción de fármacos a partir de plantas y animales modificados genéticamente".

Todos los ordenadores conectados a internet tienen una dirección IP única, que consiste en 4 octetos (4 grupos de 8 dígitos binarios) de 0 a 255 separados por un punto (ej: 127.0.0.1). Estas direcciones IP son comparables a las direcciones postales de las casas, o al número de los teléfonos.

Debido a la dificultad que supondría para los usuarios tener que recordar esas direcciones IP, surgieron los Nombres de Dominio, que van asociados a las direcciones IP del mismo modo que los nombres de las personas van asociados a sus números de teléfono en una guía telefónica.

Los ataques mediante pharming pueden realizarse de dos formas: directamente a los servidores DNS, con lo que todos los usuarios se verían afectados, o bien atacando a ordenadores concretos, mediante la modificación del fichero "hosts" presente en cualquier equipo que funcione bajo Microsoft Windows o sistemas Unix.

La técnica de pharming se utiliza normalmente para realizar ataques de phishing, redirigiendo el nombre de dominio de una entidad de confianza a una página web, en apariencia idéntica, pero que en realidad ha sido creada por el atacante para obtener los datos privados del usuario, generalmente datos bancarios.

Contramedidas: Anti-Pharming es el término usado para referirse a las técnicas utilizadas para combatir el pharming. Algunos de los métodos tradicionales para combatir el pharming son la utilización de software especializado, la protección DNS y el uso de addons para los exploradores web, como por ejemplo toolbars. El software especializado suele utilizarse en los servidores de grandes compañías para proteger a sus usuarios y empleados de posibles ataques de pharming y phishing, mientras que el uso de addons en los exploradores web permite a los usuarios domésticos protegerse de esta técnica. La protección DNS permite evitar que los propios servidores DNS sean hackeados para realizar ataques pharming. Los filtros anti-spam normalmente no protegen a los usuarios contra esta técnica.

5.5.9 Replay

En un ataque de repetición de sesión, un atacante registra (monitorea y captura) todo los paquetes y

comandos que un usuario utilice en una sesión entre un cliente y un servidor. Así, la sesión puede ser "repetida" por el atacante utilizando la misma información que pudo obtener anteriormente.

Contramedidas: Para evitar la repetición de sesión se debe utilizar algún protocolo que no permita la interpretación de paquetes duplicados. También se puede utilizar una entidad certificante que asegure la identidad de los extremos con el fin de rechazar cualquier intento de conexión por un host que no es quien dice ser.

5.5.10 TCP/IP Hijacking

Un ataque del tipo TCP Hijacking, Session Hijacking o active sniffing como suele conocerse, suele ser un problema a menudo relacionado con aplicaciones basadas en TCP/IP tal como una sesión Telnet o una aplicación de comercio electrónico basada en la web. A fin de llevar adelante el Hijack (secuestro) de una conexión TCP/IP, el atacante debe primero ser capaz de interceptar los datos de un usuario legítimo, para luego insertarse en esta sesión. Una forma sencilla de ver este ataque, es por medio de un ejemplo conceptual el cual incluya un atacante el cual logra acceso a un host de la red, para “lógicamente” desconectar este de dicha red. Acto seguido, el atacante inserta otra máquina con la misma dirección IP y continua el dialogo con el interlocutor del sistema desconectado ocupando su lugar. Si esto pudiera ser realizado con la suficiente rapidez, el atacante podría ganar acceso a la sesión que involucraba al sistema desconectado y su interlocutor, siendo que el Server podría no notar lo ocurrido y responder como si se tratara de un cliente confiable. Si bien es cierto que este tipo de ataques suelen ser algo sofisticados, la verdad es que con la aparición de diferentes herramientas en condición de automatizar los mismos, pueden en ciertos casos ser llevados a cabo con relativa facilidad. Hunt por ejemplo, es una de las herramientas que implementan monitoreo y secuestro de sesión, la cual funciona excepcionalmente bien con sesiones Telnet y FTP.

Contramedidas: Una de las principales contramedidas a la hora de prevenir secuestros de sesión en conexiones TCP/IP, radica en la utilización de sesiones encriptadas y de métodos de autenticación fuertes. La utilización de protocolos tales como IPSec o Kerberos, permiten entre otras funciones servir como contramedida para la ejecución de ataques de secuestro de sesión.

5.5.11 Bluejacking

El término bluejacking se refiere a una técnica consistente en enviar mensajes no solicitados entre dispositivos Bluetooth, como por ejemplo teléfonos móviles, PDAs o portátiles. La tecnología Bluetooth tiene un alcance limitado de unos 10 metros normalmente en dispositivos pequeños (como teléfonos móviles) aunque otros aparatos más grandes (como portátiles) con transmisores más potentes pueden alcanzar los 100 metros. Hay quien piensa que el término bluejacking viene de Bluetooth y "hijacking". Aunque suena lógico un bluejacker no intercepta nada: únicamente utiliza una característica en su dispositivo, y en el del receptor. Ambas partes mantienen el control absoluto sobre su dispositivo, y el bluejacker no puede hacer nada, ni siquiera ver la información personal contenida. Bluejacking es bastante inofensivo, pero como mucha gente no sabe qué ocurre piensan que su teléfono móvil tiene un virus o alguien entró a el. Normalmente un bluejacker sólo enviará un mensaje de texto, aunque en los modelos de teléfonos más recientes es posible enviar también imágenes y sonido.

Actualmente hay varios programas utilizados para esta práctica (como Bluetooth Messenger, Easy Jack, etc.), aunque el más utilizado es Mobiluck. Ahora se está empezando a utilizar BT Info, que hace muchas más cosas: apaga el teléfono de la víctima, explora su agenda y sus sms, y hasta puede llamar y enviar mensajes.

5.5.12 Bluesnarfing

Bluesnarfing es el robo de información de un dispositivo inalámbrico a través de una conexión Bluetooth, ya sea entre teléfonos, portátiles o PDAs. Esto permite acceso al calendario, la lista de contactos, correos y mensajes de texto. Bluesnarfing es mucho mas serio en relación al Bluejacking, pero ambos “explotan” otros dispositivos Bluetooth sin su conocimiento. Cualquier dispositivo que tenga encendido el Bluetooth y este se encuentre en Modo Descubierto (osea que puede ser encontrado por otros dispositivos en el rango) puede ser atacado. Apagando esta opción puede protegerse de la posibilidad de ser Bluesnarfiado. Siendo esto una invasión de la privacidad, el Bluesnarfing es ilegal en algunos países. Dentro de este Rango de Herramientas Encontramos al Mismo BT Info (Super Bluetooth Hack), el BT File Manager, el BT Explorer, Miyux y otra gran variedad de utilidades.

5.5.13 Bluebugging

Alguna gente considera el Bluebugging como una forma de Bluesnarfing. Pero la naturaleza de este es muy diferente. Blue Bugging fue inventado en 2004, mas o menos un año despues de que empezara el Bluesnarfing. Mientras el bluesnarfing se trata de robar cosas o archivos del dispositivo de la victima, el Blue Bugging hace un trabajo diferente. Toma el control del móvil de la victima, y por medio de comandos hace lo que el BlueBugger desee (dentro de este rango tenemos al BT Info o Super Bluetooth Hack). Para decirlo en palabras fáciles, significa que el bluebugger toma el control de tu teléfono, y lo usa para enviar mensajes o para hacer una llamada. Mientras al principio el bluebugging requería que el bugger(literalmente) usara un dispositivo previamente acomodado, las nuevas herramientas del bluebugging han hecho la mayor parte del trabajo, lo que significa que cualquiera con el conocimiento y la herramienta adecuada puede tomar control de tu teléfono. Las posibilidades y consecuencias de esto, están a la Imaginación.

5.5.14 Bluetiming o Toothing

Podría decirse que es una variante del BlueJacking, la cual se dice, es para promover encuentros del tipo sexual (citas, encuentros y esas cosas) mediante la cual un dispositivo Bluetooth es usado para “descubrir” otros dispositivos bluetooth en el rango, y les envía un mensaje sugestivo, algo así como: Hablamos ? Donde nos vemos ?. Se crea una red de encuentros furtivos con otros dispositivos bluetooth, generalmente en areas con mucha afluencia de publico como Centros Comerciales y parecidos, la cual no solo es para encuentros y charlas, sino también para compartir cosas, lo que a logrado que se desarrollen aplicaciones dentro de la categoría MoSoSo (Software para sociabilidad movil, Mobile Social Software en Ingles.) dentro de las cuales podemos contar el Mobiluck, el Bluejack, y los recientes Chat2u o Bluetooth Messenger. También tenemos aquí al “Sensor” de Nokia.

5.5.15 Auto rooters

Los auto-rooters son programas que permiten automatizar el proceso de un ataque y penetración. Generalmente realizan una búsqueda de vulnerabilidades en un rango de direcciones IP, y donde encuentran una vulnerabilidad, aplican el exploit correspondiente para lograr un acceso. Una vez que se logró el acceso a una estación, servidor o dispositivo, pueden realizar diferentes acciones:

- Copiar software para permitir accesos futuros (llamados rootkits)
- Capturar datos que viajen por la red, mediante un sniffer
- Modificar información

- Instalar software zombies que esperarán por órdenes para realizar un ataque por DdoS.

Estas herramientas son extremadamente peligrosas, porque automatizan el proceso de un atacante y permiten realizar ataques masivos indiscriminados. Todas las fases de un ataque pueden verse reducidas a minutos con estas herramientas. Generalmente, los autorooters se encuentran enfocados en la búsqueda de sólo una vulnerabilidad, pero se han reportado casos de búsqueda de múltiples vulnerabilidades.

Contramedidas:

- Un Firewall con las reglas de filtrado correctas permitirá un control excelente de las conexiones entrantes/salientes de la red. Esto impedirá el acceso o difusión de un autorooter.
- Intrusion detection systems: A pesar que no pueden detener directamente el accionar de un autorooter, pueden alertar sobre su detección.
- Deshabilitar servicios no utilizados: Esto es esencial, no sólo para la defensa ante autorooters sino como defensa para todo tipo de ataques.
- Antivirus: Muchos autorooters son detectados por antivirus. Tener una buena política de antivirus en su corporación podrá ayudarlo a detener la distribución de un autorooter.
- Mantener actualizado el sistema: Mediante las herramientas provistas por los desarrolladores o con filtros especiales en caso que exista una solución.

5.5.16 SQL Injection

Los ataques de SQL Injection, se han vuelto muy populares en los últimos años. En términos simples, es una técnica que los atacantes suelen utilizar para ejecutar consultas SQL arbitrarias sobre una aplicación conectada a una base de datos, a partir de la inyección de código SQL dentro de una aplicación. Este tipo de ataques, consiste básicamente en la modificación del comportamiento de las consultas propias de cada aplicación, mediante la introducción de parámetros no deseados en los campos a los que tiene acceso el usuario.

A pesar de lo que suele creerse, los ataques de SQL Injection no se deben de modo primario, a un bug o falla en el motor de base de datos. Por el contrario, estos se deben a errores de programación, esencialmente relacionados con la ausencia de controles estrictos de validación de entradas en las aplicaciones que se comunican con bases de datos.

Si bien el recurso de explotar validaciones de entradas pobremente construidas, no es para nada novedoso dentro del ambiente de la seguridad de la información, este tipo de ataques en particular tiene connotaciones diferentes desde el punto de vista del nivel de penetración que se puede lograr muchas veces con solo disponer de un navegador de Internet y algunos conocimientos básicos respecto de la forma en la que se construyen sentencias lógicas en lenguaje SQL. Puesto que como hemos mencionado anteriormente, SQL Injection no se trata de la vulnerabilidad de alguna base de datos en particular, sino que por el contrario su explotación se encuentra relacionada con el aprovechamiento de malas prácticas de programación, generalmente en rutinas de validación; es posible la utilización de técnicas de SQL Injection, tanto en Oracle como en MS-SQL como así también en MySQL, aunque en cada caso, los metacaracteres utilizados a tal efecto y su interpretación, posiblemente difieran de una base a otra. Este tipo de errores puede permitir a usuarios malintencionados acceder a datos a los que de otro modo no tendrían acceso y, en el peor de los casos, modificar el comportamiento de nuestras aplicaciones.

Contramedidas: Puesto que SQL Injection es un ataque que se aprovecha de malas prácticas de

programación, la principal contramedida es preventiva y se encuentra relacionada con la codificación segura de aplicaciones. La implementación de un estricto control de entrada de datos, es la principal contramedida cuando de prevenir la inyección de código se trata. No obstante, a continuación se mencionan algunas máximas:

- “Escape” las comillas simples.
- Rechace lo que conoce como “Bad Input”
- Solo permita el acceso de “Good Input”
- Siempre que sea posible, utilice stored procedures, pero no confíe en ellos en un ciento por ciento. Su mala utilización, puede hacer que estos también sean susceptibles a SQL Injection.
- Realice auditorias de código en forma periódica

5.5.17 Blind SQL Injection

Ataque a ciegas de inyección SQL, en inglés, Blind SQL injection es una técnica de ataque que utiiliza inyección SQL cuando una página web por motivos de seguridad no muestra mensajes de error de la base de datos al no haber un resultado correcto mostrándose siempre el mismo contenido (solo habrá respuesta si el resultado es correcto). Sentencias del tipo "Or 1=1" o "having 1=1" ofrecen respuestas siempre correctas por lo que son usadas como comprobación. El problema para la seguridad de la página está en que esta técnica es utilizada en combinación con diccionarios o fuerza bruta para la búsqueda carácter por carácter de una contraseña, un nombre de usuario, un número de teléfono o cualquier otra información que albergue la base de datos atacada; para ello se utiliza código SQL específico que "va probando" cada carácter consiguiendo resultado positivo cuando hay una coincidencia. De esta manera se puede saber por ejemplo que una contraseña comienza por "F...", luego "Fi...", luego "Fir..." hasta dar con la palabra completa. Existen programas que automatizan este proceso de "adivinación" letra por letra del resultado de la consulta SQL que un intruso podría enviar.

5.5.18 XSS (Cross Site Scripting)

Conocido como “XSS” a fin de evitar confundir este tipo de vulnerabilidades con “Cascading Style Sheets (CSS)”, un término común para referirse a las “Hojas de Estilo en Cascada” las cuales constituyen un mecanismo para asociar estilos de composición a documentos estructurados del tipo HTML o XML, “Cross Site Scripting” es sin dudas hoy en día, el ataque más común a nivel de aplicación. Como característica principal, podemos destacar que XSS es un tipo de vulnerabilidad del tipo “Client Side” (Del lado del cliente) que a diferencia de muchas otras, no afecta tanto a los servidores que contienen la aplicación vulnerable, sino que por el contrario a menudo los principales damnificados son los usuarios que navegan dichas aplicaciones a través de Internet.

Los ataques en condición de aprovechar este tipo de vulnerabilidades, se basan en técnicas por medio de las cuales se fuerza a un sitio web a repetir el código ejecutable suministrado por un atacante, el cual se carga en el navegador del usuario. El código normalmente está escrito en HTML o JavaScript, pero también puede extenderse a VBScript, ActiveX, Java, Flash, o cualquier otra tecnología soportada por el navegador.

En líneas generales, XSS es una vulnerabilidad que radica en la pobre validación de entrada que los desarrolladores codifican en sus aplicaciones, en relación al input llevado a cabo por el usuario, generalmente a través de formularios o de las propias URLs.

Por lo general, los tipos de recursos más susceptibles a contener vulnerabilidades explotables de XSS, son aquellos que toman el ingreso del usuario y lo publican o reproducen en forma dinámica, sin realizar las validaciones correspondientes sobre dicha entrada, resultando en caso de que este input contenga un script, que el mismo se ejecute en el navegador del usuario dentro del contexto de

seguridad de la página web visitada, pudiendo realizar en el ordenador del usuario, todas y cada una de las acciones que le sean permitidas a ese sitio web, como por ejemplo interceptar entradas del usuario víctima o leer sus cookies. Algunos ejemplos en donde con frecuencia suelen existir condiciones de XSS se cuentan: Webloga, Web bulletin boards, Chat rooms, Libros de Visita, Clientes de Web Mail, Motores de búsqueda, Formularios de Confirmación en diferentes aplicaciones. Cualquier aplicación que refleje el input del usuario sin validar su contenido.

Por último, es importante mencionar que en ataques reales, el ingreso del script malicioso no lo genera el usuario que ve la página, sino un atacante, el cual consigue de algún modo que el script se ejecute en el navegador del usuario. La víctima ejecuta el código de manera indirecta cuando confiadamente hace clic sobre un enlace fraudulento, el cual puede estar presente en el sitio web del atacante, en un mensaje de correo electrónico o de un grupo de noticias, etc.

En resumen, un ataque de Cross Site Scripting funciona de la siguiente forma:

- El usuario sigue un enlace, que incluye codificada una cadena de entrada como argumento de entrada a algún parámetro de la página del sitio web.
- El sitio web no valida (o lo hace pobremente) la entrada anterior y genera dinámicamente una página HTML que incluye el código introducido en el enlace por el atacante.
- Este código se ejecuta en el navegador de la víctima, con los mismos privilegios que cualquier otro código legítimo del mismo sitio web.

Contramedidas: El objetivo principal al intentar proteger una aplicación contra problemas de XSS, no es otro que el de codificar aplicaciones en forma segura, las cuales implementen y refuercen el concepto de validación de entradas de modo efectivo. Hoy en día algunos lenguajes han comenzado a implementar opciones especiales a fin de verificar el input antes de que este sea publicado en nuestro html, de este modo se obtiene un segundo control, transformando la validación de entrada en el primero de ellos y el “encoding” de la información a publicar en el segundo.

5.5.19 Cross Site Request Forgery

El CSRF (del inglés Cross-site request forgery o falsificación de petición en sitios cruzados) es un tipo de exploit malicioso de un sitio web en el que comandos no autorizados son transmitidos por un usuario en el cual el sitio web confía. Esta vulnerabilidad es conocida también por otros nombres como XSRF, enlace hostil, ataque de un click, cabalgamiento de sesión, y ataque automático. Un ataque CSRF fuerza al navegador web validado de una víctima a enviar una petición a una aplicación web vulnerable, la cual entonces realiza la acción elegida a través de la víctima. Al contrario que en los ataques XSS, los cuales explotan la confianza que un usuario tiene en un sitio en particular, el cross site request forgery explota la confianza que un sitio tiene en un usuario en particular.

Las vulnerabilidades CSRF se conocen desde 1990. CSRF no se puede tracear porque es llevada a cabo por la dirección IP de un usuario legítimo. Esto puede llevar a confusión en investigaciones forenses, donde será necesaria la intervención de expertos en seguridad informática para determinar casos particulares de ataques CSRF. Los exploits de este tipo de ataque apenas se conocen públicamente, en el año 2007 hay unos pocos ejemplos bien documentados.

5.5.20 Cross Site Tracing

XST (Cross Site Tracing) es una vulnerabilidad informática derivada de XSS (Cross Site Scripting). Esta vulnerabilidad surge a causa de algún error de filtrado y del uso del comando TRACE de HTTP 1.1 con el fin de incrementar el riesgo para el servidor.

Un ataque cross-site tracing explota controles ActiveX, Flash, Java y otros que permiten la ejecución

de una llamada HTTP TRACE. Este tipo de ataque no es nuevo; fue descubierto por el investigador de seguridad Web Jeremiah Grossman en 2003, y permite a un atacante conseguir acceso a las cookies e información de credenciales de autenticación de un individuo.

El llamado HTTP TRACE le pide a un servidor Web que conteste el contenido de las solicitudes al cliente. La solicitud completa, incluyendo los encabezados HTTP, que pueden incluir información sensible como cookies o información de autenticación, es devuelta en el cuerpo de la entidad de una respuesta TRACE. La solicitud es usada principalmente por los desarrolladores para probar y depurar aplicaciones HTTP y por defecto está disponible en la mayoría de los programas de servidores Web.

Una forma de llevar a cabo un ataque XST es crear una página que incluya algún JavaScript que contenga la solicitud TRACE. El JavaScript entonces puede explotar cualquier vulnerabilidad cross-domain en el navegador del visitante para recolectar las credenciales en cache de cualquier sitio, incluyendo aquellos que utilizan SSL.

Otro método más comúnmente usado toma el snippet JavaScript que contiene la solicitud TRACE y lo inyecta en la aplicación Web vulnerable. El JavaScript será capaz de enviar los encabezados de las solicitudes de la víctima, incluyendo la información de cookie etiquetada como “httpOnly”, al atacante. “httpOnly” es un parámetro adicional agregado a los cookies, que oculta a los cookies de los scripts y es soportado por la mayoría de los navegadores; el método TRACE, sin embargo, puede ser usado evitar esta protección.

Contramedidas: Para impedir este tipo de ataque, es esencial que los métodos PUT, DELETE, CONNECT y TRACE estén deshabilitados en sus servidores Web ya que todos representan un riesgo de seguridad. Si una aplicación necesita uno o más de estos métodos, tal como los servicios Web REST (que puede necesitar PUT o DELETE), es importante verificar que su uso sea apropiadamente limitado a los usuarios confiables y en condiciones seguras. Para deshabilitar el soporte de HTTP TRACE en un servidor Apache, fije TreaceEnable en Off. Si está corriendo IIS en un servidor Windows, use la herramienta URLScan para rechazar las solicitudes HTTP TRACE o para permitir solo los métodos necesarios para satisfacer los requerimientos de su sitio y de su política de seguridad. Es fácil para un atacante, o para un administrador de sistema, verificar si un servidor Web soporta el método TRACE. Usando utilitarios tales como el Netcat de fuente abierto – un servicio de redes que puede leer las conexiones de red con TCP o UDP – los atacantes pueden usar el método OPTIONSS de HTTP para obtener la lista de métodos soportados por el servidor Web.

5.5.21 Parameter/URL/Form Tampering

Bajo el término “Parameter Tampering” se conoce a un tipo de ataque, el cual relacionado inicialmente con aplicaciones web, se encuentra basado en la alteración de los datos, generalmente enviados por el servidor, del lado del cliente. Al nivel más básico, el proceso de alteración de los datos por parte del usuario es sumamente sencillo. Cuando un cliente realiza una petición HTTP por medio de los métodos GET o POST, el servidor procesa el requerimiento y como resultado envía la página HTML que corresponda, la cual puede entre otras cosas, contener valores en campos ocultos los cuáles si bien no son visualizados desde el navegador, son de hecho efectivamente enviados al realizarse el submit de dicha página (por ejemplo como parte de un formulario). Lo mismo, podría ocurrir, en aquellos casos donde los campos del formulario enviado al usuario, resultaran ser valores “preseleccionados” tal como en el caso de listas desplegables, checkbox, radio buttons, etc.; los valores de dichos campos podrían ser manipulados por el usuario, permitiendo por ejemplo, que él decida asignar valores diferentes a los asignados inicialmente por el desarrollador de la aplicación, consiguiendo en definitiva realizar una petición HTTP con datos por él alterados.

El principal problema detrás del tampering en aplicativos web, radica en el hecho de que muchos desarrolladores confían en la utilización de campos ocultos o fijos, para llevar adelante operaciones críticas. Las vulnerabilidades de parameter tampering, suelen a menudo ser reconocidos como ataques a la lógica de la aplicación y se originan una vez más… en malas prácticas de programación y

una pobre validación de entradas.

Entre los ejemplos más básicos de “Parameter Tampering”, se encuentra el cambio del lado del cliente de los parámetros en los campos de un formulario o la propia modificación de atributos en una URL determinada, con el objeto de manipular de uno u otro modo el resultado lógico de la aplicación.

En cuanto al uso de campos ocultos, el ejemplo más típico es el de la utilización de los mismos al publicar el valor de determinados artículos en un portal de ventas on-line. Si para fijar el precio de los mismos, se utilizaran campos ocultos en los formularios, un usuario malicioso podría eventualmente interponer una aplicación que actúe de proxy http tal como “Paros” entre su browser y el servidor web, para entonces capturar el tráfico, editar el valor existente en el campo oculto (no visualizado a través del navegador, pero accesible al interceptar el tráfico pues viaja como valor oculto del formulario) y finalmente enviar al servidor el formulario con los valores de precio del producto (del campo supuestamente oculto) modificado. Una acción de este tipo, permitiría que un atacante decida el precio a pagar por cualquiera de los artículos dispuestos en la página web del portal de ventas on-line, siempre que no se cuenten con validaciones del lado del servidor y se haya deslindado esta responsabilidad del lado del cliente.

Contramedidas: A fin de evitar el tampering, se debe evitar el uso de campos ocultos para manejar cualquier tipo de información sensible. Al mismo tiempo, las validaciones en cada uno de los parámetros utilizados en una página web, deben encontrarse correctamente validados.

5.5.22 Wardialing

Hace algunos años, cuando Internet aún no se encontraba desarrollada como en la actualidad, gran parte de las comunicaciones de datos, eran realizadas a través de la red telefónica por medio de la utilización de módems. Debido a ello, era muy común encontrar centros de cómputos donde se apilaban una gran cantidad de módems conectados a un pool pre-establecido de números telefónicos, de forma tal que por ejemplo, sucursales dispersas pudieran establecer una comunicación con los mismos, para una vez conectados acceder a los recursos de la red interna de la organización. A fin de llevar a cabo este tipo de funciones, varias compañías de desarrollo de software comenzaron a comercializar productos (Remote Control, PCAnywhere, etc.) que fueran capaces de, contando con una porción CLIENTE (REMOTE) y una porción SERVIDOR (HOST), brindarles la capacidad a los usuarios de aprovechar sus módems para establecer comunicaciones de datos entre equipos.

En la actualidad, si bien es cierto que tras el auge de Internet, gran parte de las comunicaciones de datos son cursadas a través de dicha red, también lo es el hecho de que aún existen aplicaciones o soluciones que involucran la posibilidad de recibir conexiones de datos a partir de una comunicación del tipo Dial-Up por medio de la utilización de módems. Un ejemplo de este tipo de aplicaciones, se encuentra en centrales telefónicas las cuales a menudo poseen módems de servicio conectados a líneas dedicadas a fin de que técnicos puedan accederlas remotamente con el objeto de brindar mantenimiento , realizar cambios de configuración, etc.

Ahora bien, a que nos referimos cuando hablamos de Wardialing? básicamente al hecho de barrer o escanear grandes rangos de números telefónicos, utilizando para tal fin un MODEM en conjunto con algún tipo de herramienta de software capaz de tomar un listado de teléfonos preestablecidos, discar los mismos e intentar detectar el tipo de dispositivo que se encuentra a la escucha en el otro extremo, para finalmente grabar un archivo de log en donde el atacante/auditor pueda a posterior, conocer en forma exacta si efectivamente existe algún dispositivo o software a la escucha, esperando conexiones entrantes. Al margen de esta operación básica, algunas de las herramientas de Wardialing más potentes, tienen la capacidad de reconocer la existencia de los paquetes de software comerciales más importantes e incluso intentar lograr acceso, mediante la utilización de usuarios y contraseñas por default en tales productos. A pesar de lo que pudiera parecer a simple vista, hoy en día aún sigue siendo probable hallar dado un rango telefónico, dispositivos a la espera de comunicaciones entrantes. Muchas veces, usuarios corporativos instalan módems en sus Workstation, de modo tal de

poder accederlas remotamente desde sus hogares, sin el consentimiento del administrador de seguridad y violando las políticas internas. Este hecho, podría permitir que un atacante en su etapa de reconocimiento, encuentre este tipo de conexiones por medio de técnicas de Wardialing y se aproveche de ellas ganando acceso no autorizado a la red corporativa.

Contramedidas: Las políticas corporativas, deberían prohibir en forma explícita a sus empleados la instalación de módems en sus terminales. Por su parte, los analistas de seguridad deberían practicar evaluaciones periódicas, mediante técnicas de Wardialing, a efectos de detectar posibles puntos de entrada en su rango telefónico. Entre los objetivos posibles por parte de un atacante, podrían encontrarse dispositivos tales como: equipos de FAX y centrales telefónicas. Se recomienda evitar siempre que sea posible, la utilización de los servicios de acceso remoto de administración a centrales telefónicas corporativas, sobre todo aquellas vinculadas con la red de datos.

5.5.23 Ingeniería Social

El término "Ingeniería social" incluye a un conjunto de técnicas y habilidades sociales realizadas por el atacante para obtener información de terceros. Estas técnicas o habilidades, incluyen generalmente un engaño o parcialización de la verdad con el objetivo de obtener la confianza de la persona con los conocimientos a obtener. Una vez que se ha obtenido la confianza de la persona, se procede a obtener la información considerada importante.

La ingeniería social se da muchas veces vía telefónica, correo electrónico o a través de sesiones de chat, donde la verdadera personalidad del atacante queda oculta. Un ejemplo típico de Ingeniería social, es cuando el atacante llama a un usuario de la red, simulando ser del departamento de informática, y le exige que le informe de su nombre de usuario y contraseña. Si el usuario que está siendo víctima del engaño, no conoce la estructura de la organización, es muy probable que le brinde al atacante la información solicitada. De esta forma, el atacante, con sólo conocer el número telefónico de la víctima, y sin realizar ninguna acción sospechosa sobre la red, podrá tener acceso con los privilegios de un usuario interno. La ingeniería social termina cuando se obtiene la información buscada. Las actividades que se realicen con la información obtenida ya no entran en el marco de la Ingeniería social.

Contramedidas: Aquí, la mejor contramedida es la educación de los usuarios de la red y la implementación de planes efectivos de concientización. En la política que firman los usuarios, se debe especificar que el nombre de usuario y contraseña no pueden ser transmitidos mediante otro medio que no sea persona a persona. De esta forma se evitará también que posibles escuchas de la red intercepten la información.

5.5.24 Dumpster Diving – Trashing

Aunque parezca desagradable, la búsqueda de datos dentro de la basura puede proveer información importante para comenzar un análisis. Tomar objetos de la basura es completamente legal, por lo que no existe una forma de evitarlo. Quizás la información obtenida no sea la necesaria para realizar un ataque, pero por ejemplo, puede ofrecer información para realizar Ingeniería Social. Datos tales como agendas con números de teléfono, memos, organigramas, resúmenes de ventas, planificaciones de reuniones, hardware fuera de uso, manuales de uso, etc. pueden ser un muy buen paso para comenzar la investigación. Las planificaciones de vacaciones, pueden decirnos qué usuarios se encuentran fuera de la organización, los manuales o políticas nos pueden informar sobre la estructura de seguridad y permisos que tienen los usuarios, el hardware en desuso, se puede utilizar para poder recuperar la información que tenía. Quizás dentro del disco obtengamos nombres de usuarios, contraseñas, etc.

Contramedidas: A fin de minimizar el riesgo de que un atacante pudiera obtener información a partir de documentos desechados por la organización, deberían existir procedimientos claros en cuanto a la destrucción de documentos y eliminación de información digital (wipe) del material de almacenamiento desechado.

5.5.25 Shoulder Surfing

"Shoulder Surfing", suele ser el termino para describir un particular tipo de ataque que se aprovecha de la ingenuidad de los usuarios de sistemas. Tal como su nombre lo indica, este tipo de ataque consiste en "mirar por encima del hombro", es decir espiar físicamente a los usuarios, para obtener generalmente nombres de usuario o claves de acceso a un sistema. El "Shoulder Surfing" no solo se ve beneficiado por la ingenuidad de los usuarios de un equipo; en determinadas circunstancias son los propios desarrolladores de software los que diseñan aplicaciones susceptibles de sufrir ataques de este tipo. Un claro ejemplo, lo representan aquellas aplicaciones que muestran transparentemente en pantalla, las contraseñas al ser tipiadas. Cualquier individuo situado cerca de un usuario el cual este haciendo uso de esta aplicación, podría eventualmente leer claramente esa clave.

Contramedidas: Tal como lo mencionáramos cuando nos referimos a los ataques de ingeniería social en general, a fin de prevenir el shoulder surfing, se debe principalmente trabajar en la implementación de planes de educación y concientización de usuarios. Desde el punto de vista técnico, se debe evitar la utilización de cualquier tipo de aplicación en la cual el ingreso de las passwords tipiadas pueda ser observado en pantalla.

5.5.26 Brute Force (Fuerza Bruta)

En términos simples, la definición de ataque por fuerza bruta, refiere a la acción de intentar tantas combinaciones de contraseñas como sean necesarias hasta dar con la correcta. Si bien es cierto que frente a un conjunto infinito de posibilidades, la probabilidad de dar con la contraseña correcta es nula, también lo es el hecho que generalmente la mayoría de las contraseñas que suelen utilizarse, poseen entre 4 y 16 caracteres. Puesto que tan solo cerca de 100 valores diferentes pueden ser utilizados para cada uno de los caracteres que conforma una contraseña, en el peor de los casos deberían intentarse entre 100^4 y 100^16 combinaciones hasta dar con el valor correcto, tarea que con el poder de cómputo actual, podría ser llevada a cabo sin mayores inconvenientes en un tiempo razonable.

Siempre que se mencione la posibilidad de lanzar un ataque de contraseñas, es importante tener en cuenta lo que en criptografía se conoce como "Keyspace" o "Espacio de Claves", término que se refiere al conjunto de posibles valores usados para construir una clave. Por su parte, otro termino asociado "Work Factor" o "Factor de Trabajo" se refiere al tiempo estimado, esfuerzo y recursos necesarios para romper un criptosistema. Si bien es cierto que los ataques a contraseñas por fuerza bruta suelen en algunos casos ser la única opción en determinados casos, lo cierto es que dicho proceso suele ser considerado costoso en tiempo computacional (dado que utilizan el método de prueba y error), por tanto suele ser la última opción cuando de atacar contraseñas se trata. Por último, es posible decir que un ataque por fuerza bruta, teóricamente siempre arrojara un resultado positivo en cuanto a lo que hallar la clave correcta se refiere, no obstante en términos prácticos puede que el tiempo y esfuerzo invertido en tal tarea, termine por no ser efectivo. Dicho de otro modo, puede que para cuando terminemos por romper una contraseña la información que estemos tratando de acceder, ya no posea el mismo valor que cuando el ataque fue lanzado.

Hoy en día es posible encontrar muchas herramientas en capacidad de lanzar ataques de fuerza bruta contra contraseñas. Entre las más importantes se cuentan: LOphtCrack, Brutus y John the Ripper.

Contramedidas: El establecimiento de contraseñas duras de romper, tal como aquellas que combinan una longitud de entre 7 y 16 caracteres, siendo estos un conjunto de símbolos no imprimibles, letras mayúsculas, minúsculas y números, suele ser una buena contramedida. No obstante, quizás la más efectiva contra ataques de fuerza bruta, no sea otra que el bloqueo de cuentas luego de una serie determinada de intentos fallidos.

5.5.27 Híbridos

Hoy en día, la mayoría de las herramientas avanzadas de cracking de contraseñas brindan al atacante o analista de seguridad, no solo la posibilidad de lanzar ataques basados en diccionario o fuerza bruta, sino que además incorporan la característica de ejecutar lo que se conoce como ataques híbridos, los cuales no son otra cosa que una técnica consistente en la combinación de de los ataques de fuerza bruta y diccionario. Cuando un ataque hibrido es lanzado, un archivo de diccionario es utilizado, pero a la vez sobre él se realizan una serie de permutaciones y variaciones intentando ampliar su rango de acción no solo a las palabras conocidas contenidas en el diccionario seleccionado, sino a su vez intentando algún tipo de variación que pudiera coincidir con el criterio utilizado por el usuario al momento de seleccionar su contraseña. Al momento de configurar este tipo de ataques, es posible al igual que en los ataques de fuerza bruta, el set de caracteres que se utilizará al momento de combinar estos con las búsquedas de diccionario.

Contramedidas: Los ataques de tipo híbrido, suelen ser efectivos sobre todo cuando se intenta hallar algunas de las combinaciones que con mayor frecuencia utilizan los usuarios al momento de seleccionar sus contraseñas tal como la mezcla de una palabra de uso común con una cifra numérica o un conjunto de caracteres alfabéticos (Ej.: ”Irresponsable123456”). Nuevamente, las contramedidas a aplicar siguen siendo principalmente aquellas mencionadas en el indicador “Fuerza Bruta”, aunque a menudo suele ser recomendado el armado de contraseñas basadas por ejemplo en la selección de una frase larga de varias palabras, para luego tomar sus iniciales al momento de establecer una clave (Ej.: “El mar nunca ha estado mejor que el día de hoy, no crees?” à “Emnhemqeddhn?”)

5.5.28 Back doors

Los backdoors (o puertas traseras) son accesos no convencionales a un sistema. Los backdoors generalmente son instalados por intrusos para tener un acceso permanente al sistema atacado.

Existen backdoors con gran difusión, apuntados a usuarios de internet, como el BackOrifice , Netbus o SubSeven. Estos backdoors permiten tomar el control de una estación Windows y realizar diferentes actividades, como enviar mensajes, copiar o borrar archivos, cambiar configuraciones, etc.

Aparte de los backdoors, otros ataques muy comunes que es conveniente analizar son:

- TCP session hijacking: En este caso, un usuario malicioso se interpone en el medio de una sesión TCP de dos hosts. Como la autenticación de los servicios ocurre generalmente al comienzo de la conexión, esto le permite al atacante obtener acceso en el host destino.
- Redirección de puertos: La redirección de puertos consiste en asociar un puerto específico en un host a algún otro puerto del mismo host o a algún otro puerto de algún otro host. De esta forma, cuando se accede a un puerto determinado del primer host, en realidad se accede a algún otro servicio del mismo host o de algún otro. Los Firewalls generalmente filtran los paquetes según los protocolos y puertos que utilicen, por lo que la redirección de puertos es un mecanismo que le permite a un atacante que consiga acceso a un host detrás del Firewall superar en gran medida las limitaciones que el Firewall le imponía.

- Ataques a contraseñas: Los ataques de contraseñas generalmente consisten en la prueba metódica una a una de un conjunto de contraseñas sobre un destino determinado. En la medida que el destino del ataque no imponga un número máximo de intentos de accesos fallidos, el atacante podrá seguir intentando validar su acceso con la verificación de contraseñas nuevas hasta conseguirlos. El origen de las contraseñas que son probadas pueden ser obtenidos de algún diccionario de palabras comunes o simplemente generadas en forma secuencial por el atacante.

Contramedidas: Firewalls: Los backdoors abren puertos para aceptar las conexiones de los intrusos, de esta forma, si tenemos reglas apropiadas, podremos filtrar los posibles intentos de acceso. Antivirus: Los antivirus actuales detectan los backdoors más conocidos, sobre todo para plataforma Win32.

5.6 ATAQUES DE CAPA 2 Y SUS CONTRAMEDIDAS

Como los routers, tanto los switches capa 2 como los de capa 3 tienen algunas consideraciones de seguridad que se deben tener en cuenta. En las secciones posteriores se verán los ataques o vulnerabilidades más comunes relacionado con la capa 2 y los switches (como principales dispositivos de esa capa). A continuación se analizarán los siguientes temas:

- La sobrecarga en la tabla CAM de los switches
- El acceso a diferentes VLANs
- La utilización de STP para modificar el árbol de expansión
- La falsificación de direcciones MAC
- La inundación y saturación del servidor DHCP

5.6.1 CAM table overflow

Como hemos estudiado anteriormente, cuando un switch recibe una trama hacia un destino que no conoce, la reenvía por todos sus puertos. El switch va aprendiendo dónde está ubicada cada dirección MAC a medida que recibe tramas de esa dirección. Esta información la guarda en una tabla llamada CAM. Las entradas que no se referencian por un tiempo, son borradas de la tabla.

Las tablas CAM tienen un tamaño limitado, si se ingresa la cantidad suficiente de entradas, se puede llenar la tabla hasta el punto que no se acepten nuevas entradas. Esto puede ser utilizado por un intruso para inundar el switch con una gran cantidad de direcciones MAC inexistentes hasta que la tabla CAM se llene. Cuando esto ocurre, el switch comenzará a reenviar las tramas por todos los puertos, dado que no podrá aprender nuevas asignaciones, y las asignaciones antiguas irán venciendo y serán borradas, lugar que ocuparán las MAC inexistentes. Este proceso hará que el switch se comporte como un hub. El intruso, debe realizar esta inundación de forma continua para evitar que el switch borre las entradas inexistentes mas viejas y comience a aceptar direcciones MAC existentes. Este ataque es conocido como "CAM Table overflow" o "Desborde de Tabla CAM". Este ataque sólo puede realizarse dentro de una sola VLAN, con lo que el intruso, sólo podrá capturar el tráfico de una VLAN en particular.

Contramedidas: Para protegernos de este tipo de ataques podemos configurar seguridad por puertos en el switch. Esta opción permite especificar la dirección MAC asociada a un puerto, o la cantidad de direcciones MAC que podrán ser aprendidas por un puerto específico. Cuando el switch detecta una dirección MAC inválida puede filtrar la trama sospechosa, o bloquear el puerto.

Dependiendo del tipo de organización, puede convertirse en un dolor de cabeza asociar una dirección MAC por puerto, dado que ante cada cambio de puerto, deberá reconfigurarse el switch. Una opción más flexible, es limitar la cantidad de direcciones que podrá aprender un puerto.

5.6.2 VLAN hopping

VLAN hopping es un ataque donde un host envía paquetes destinados a otro host ubicado en una VLAN diferente, donde normalmente no podría ser alcanzado directamente. El atacante intenta establecer con el Switch un enlace de trunk para enviar y recibir información de cualquier y a cualquier VLAN. Esto es conocido como Switch Spoofing. Con Switch Spoofing el atacante intenta engañar al switch, haciéndose pasar por uno de estos. Este método requiere que el atacante sea capaz de procesar y generar tramas ISL o 802.1q con el protocolo DTP (Dinamyc Trunk Protocol). Así, un usuario malicioso hace que su host se vea como un puerto de trunk de un switch, y cuando establece el enlace es capaz de ver todas las VLANs.

Switch Spoofing: Aquí el atacante configura su sistema para simular un Switch. Esto requiere que su adaptador de red sea capaz de emular la señalización 802.1q el protocolo del IEEE para etiquetado de tramas y comunicación de VLANs a nivel de trunking. Usando este método, el atacante puede aparecer como un switch con un puerto de trunk, si lo logra podrá conocer todo el tráfico de VLANs que exista, pudiendo capturar la información contenida en las diferentes tramas.

Double Tagging: Otro tipo de ataque de VLAN hopping, involucra la trasmisión de tramas con un doble etiquetado (tagging) 802.1q. De esta manera, el primer switch que recibe la trama interpreta el primer etiquetado y reenvía dicha trama a los puertos configurados con la VLAN nativa del atacante, pero incluye en el reenvío a los puertos de trunk. El segundo switch que recibe la trama a través del puerto de trunk, interpreta el segundo etiquetado, reenviando esta trama a la VLAN destino. A fin de mitigar el ataque de VLAN hopping, se requiere realizar cambios en la configuración de VLAN. Uno de los más importantes, es utilizar un identificador de VLAN dedicado para todos los puertos de trunk. También deshabilitar todos los puertos no utilizados y asignarlos a una VLAN sin uso. Todos los puertos de usuario, es decir donde existen hosts conectados, deben ser configurados en modo de notrunk, desactivando específicamente el Dynamic Trunk Protocol (DTP) en dichos puertos.

Private VLAN: Consiste en un mecanismo que permite restringir las comunicaciones entre hosts situados en la misma subred IP. Limitan los puertos dentro de una VLAN, que pueden comunicarse con otros puertos de la misma VLAN. Puertos aislados (isolated ports) dentro de una VLAN, pueden comunicarse solamente con puertos promiscuos (promiscuous ports). Puertos de comunidad (community ports) pueden comunicarse solamente con otros puertos de la misma comunidad o con puertos promiscuos. Puertos promiscuos pueden comunicarse con cualquier tipo de puertos.

Ataque Private VLAN Proxy: En este tipo de ataque, se envía tráfico a un host conectado a un puerto promiscuo, por ejemplo un router. El atacante envía un paquete con la direcciones origen IP y MAC de su propia estación, la dirección IP de destino de la víctima, pero la dirección MAC de destino del router. El switch reenvía la trama al router, pues éste está ubicado sobre un puerto promiscuo, estando permitido este diálogo en Private VLAN. El router interpreta la dirección IP de destino y rutea el paquete sobrescribiendo la dirección MAC de destino con la del host víctima. Ahora el switch reenvía la trama hacia el puerto donde está situado el host víctima. Este ataque sólo permite inyectar tráfico a la víctima, pues cualquier intento de envío de tráfico de respuesta por parte de la víctima, será bloqueado por la configuración de la Private VLAN.

Este escenario no es una vulnerabilidad propia de Private VLAN, debido a que las reglas de envío de tráfico de una Private VLAN se cumplen, sin embargo se produce una violación de la seguridad. A fin

de mitigar este ataque, pueden configurarse ACLs en el router, como así también VLAN ACLs.

Contramedida: Para evitar un ataque de VLAN hopping es necesario realizar modificaciones en las configuraciones de VLAN. Uno de los elementos más importantes es utilizar identificadores de VLAN dedicados para todos los puertos que sean de Trunk. También, se deben desactivar todos los puertos no utilizados del switch y ubicarlos en una VLAN no utilizable. Los puertos para dar servicio a los usuarios se deben configurar deshabilitando explícitamente el modo trunk, desactivando DTP en estos puertos.

5.6.3 STP manipulation

Otro ataque sobre los switches consiste en interceptar y generar tráfico del protocolo Spannig Tree. Como vimos en el capítulo anterior, este protocolo se utiliza en redes conmutadas para evitar la formación de bucles en la topología de la red. Así, en un estado inicial todos los switches realizan un proceso de determinación de una topología libre de bucles y luego envían y escuchan constantemente paquetes STP (llamados BPDU) para verificar la convergencia de la red. Los switches identifican un único switch como root bridge (switch raíz del árbol) y bloquean todos los otros caminos redundantes para evitar los bucles.

Con un ataque STP, un usuario malicioso intenta ser el switch raíz de la topología. Para hacer esto, el atacante inunda toda la red con BPDUs con el fin de que todos los switches de la red tengan que recalcular la topología de la red. Los BPDU enviados por el atacante anuncian que su sistema tiene un menor bridge ID, convirtiéndolo en el candidato a ser raíz.

Si el atacante consigue tomar el rol de switch raíz prodrá ver las tramas que circulen entre los switches conectados a él.

Contramedida: Para contrarrestar la manipulación del STP, puede configurar los switches con el fin de delimitar el uso del protocolo STP o indicar en cada puerto del switch si desde éste puede llegar al switch raíz o no. En dispositivos Cisco puede utilizar los comandos root guard y bpdu guard con el fin de asegurar la ubicación del switch raíz en la red y asegurar los bordes de propagación de STP. El comando root guard permite asegurar la ubicación del switch raíz de la red. El comando BPDU GUARD está diseñado para permitir a los administradores de redes mantener la topología de red predictiva. Mientras BPDU GUARD le puede parecer innecesario porque puede asignar prioridad cero a los dispositivos (recuerde que cero representa la menor prioridad, y el switch que tenga menor prioridad será raíz), pero tienen que tener en cuenta que el bridge ID se forma por la prioridad y la dirección MAC, lo que no garantiza que sea siempre el candidato a switch raíz.

5.6.4 MAC address Flooding

El ataque de MAC Flooding, intenta explotar las limitaciones de recursos que los switches de diferentes vendedores poseen, en referencia a la cantidad de memoria asignada para la MAC Address Table, es decir, el lugar donde se almacenan las direcciones físicas aprendidas por el dispositivo y el identificador de puerto físico correspondiente.

Como ya se mencionó anteriormente, cuando un switch inicia su funcionamiento, no conoce qué dispositivos se encuentran conectados al mismo, reenviando las tramas recibidas por todos sus puertos, a excepción de aquel por donde dicha trama arribó. A medida que se va generando tráfico, el switch aprende las direcciones MAC de los distintos host conectados, registrando esta dirección junto al puerto de conexión en un área de memoria, conocida como MAC Address Table. A partir de aquí, cuando la dirección MAC de destino de una trama se encuentra en la mencionada tabla, el switch reenviará la misma al puerto correspondiente y ya no por todos sus puertos, aumentando

significativamente el rendimiento de la red.

La MAC Address Table es limitada en tamaño, si una cantidad excesiva de entradas se registran y su tamaño está al límite, las entradas más antiguas se eliminan, liberando espacio para las más nuevas. Típicamente un intruso tratará de inundar el switch con un gran número de tramas con direcciones MAC falsas, hasta agotar la MAC Address Table, por ejemplo utilizando la herramienta macof, creada en 1999 e incorporada en dsniff. Cuando esto ocurre dicha tabla estará completa de direcciones erróneas, cualquier nueva trama que reciba, aunque sea real, no encontrará el puerto asociado a la dirección en dicha tabla, motivo por el cual seguirá su procedimiento lógico, es decir, reenviará dicha trama por todos los otros puertos, convirtiéndose en un hub. Si el atacante no mantiene la inundación de direcciones falsas, el switch puede eventualmente eliminar las entradas erróneas por exceso de tiempo de vida y aprender nuevamente las direcciones reales de la red, normalizando su funcionamiento.

Este tipo de ataque puede ser mitigado, activando la configuración de seguridad que caracteriza a la mayoría de los switches administrables. Por ejemplo se puede configurar la dirección MAC que estará conectada a cada puerto del switch, o bien, se puede especificar hasta cuántas direcciones MAC podrán aprender los puertos del dispositivo y hasta también la acción a ejecutar ante una violación de seguridad, como bloquear la dirección MAC errónea o bloquear el propio puerto. En un Cisco Catalyst estas funciones de seguridad se denominan Port Security.

5.6.5 MAC address spoofing

La dirección MAC (Media Access Control) es un identificador único que se asigna a todas y cada una de las tarjetas de red existentes. Este identificador se graba en una memoria especial de las mismas. Lo hace el propio fabricante de la tarjeta o dispositivo, y consiste en una serie de números que identifican unívocamente a esa tarjeta de red.

De esta secuencia de números se pueden deducir una serie de datos, como por ejemplo el fabricante (marca de la tarjeta). También es conocida como la dirección física, dirección hardware, etc.

Su formato es el siguiente: 12:34:56:78:9A:BC

Se trata de una codificación hexadecimal en pareja de 48 bits de información. Los 24 primeros bits (tres primeras parejas de números) identifican al fabricante del hardware, y los 24 bits restantes corresponden al número de serie asignado por el fabricante, lo que garantiza que dos tarjetas no puedan tener la misma dirección MAC.

Los ataques por MAC address spoofing (Falsificación de dirección MAC) se basan en el uso de una dirección MAC de otro host para hacer que el switch objetivo envíe las tramas al intruso en vez de enviarlas al host destino real. Si el intruso envía una trama con la dirección MAC origen de otro host, hará que el switch sobrescriba la tabla CAM para reenviar las tramas hacia ese puerto. Hasta que el host que está siendo falsificado no envía una trama (que volverá a sobrescribir la tabla CAM), no recibirá más trafico.

5.6.6 ARP poisoning (Envenenamiento de la tabla ARP)

El envenenamiento ARP (en inglés Address Resolution Protocol o Protocolo de resolución de direcciones) es una técnica usada por atacantes en redes internas cuyo fin es obtener el tráfico de red circundante, aunque no esté destinado al sistema del propio intruso. Con este método, el atacante puede conseguir derivar la información hacia su propia tarjeta de red y así conseguir información sensible, bloquearla o incluso modificarla y mostrar datos erróneos a las víctimas.

Esta técnica no se basa en una vulnerabilidad concreta que pueda llegar a desaparecer con el tiempo, sino que se basa en un fallo de diseño de las redes TCP (Transmission Control Protocol), y por tanto, es un método de ataque siempre válido y eficaz a menos que se tomen medidas específicas contra él.

Es una variación del ataque por falsificación de dirección MAC inserta entradas en la tabla ARP de las estaciones de usuarios. Como hemos visto, ARP es utilizado por las estaciones para asociar direcciones IP con direcciones MAC. Este ataque se lleva a cabo enviando un ARP Reply a una estación asociando la dirección IP del objetivo del ataque a la dirección MAC del intruso. En este caso, no se utiliza una dirección MAC falsificada, sino que se "envenena" la tabla ARP de las demás estaciones. Es utilizado para obtener una dirección MAC desconocida a partir de una dirección IP conocida dentro de una LAN, donde los hosts de la misma subred residen. Normalmente una estación enviará para esto una solicitud ARP, mediante una trama broadcast a todas las demás estaciones y recibirá una respuesta ARP conteniendo la dirección MAC buscada, por parte de la estación que tiene la dirección IP conocida. Dentro de este esquema, existen respuestas ARP no solicitadas llamadas ARP gratuitos, que pueden ser explotados maliciosamente por un atacante para enmascarar una dirección IP sobre un segmento. Típicamente, esta acción es ejecutada para posibilitar un ataque denominado Man in the Middle (MITM), en el cual el atacante engaña a los dispositivos que entablarán una comunicación a través de la red, enviando su propia dirección MAC mediante ARP gratuitos. Cada estación involucrada (un cliente y un servidor o una estación con su default gateway) almacena en su ARP caché la dirección IP del otro host, pero asociada a la dirección MAC del atacante, con lo cual el tráfico pasa por éste antes de dirigirse a su destino, posibilitando la captura de datos.

Contramedidas: El uso de seguridad por puerto en el switch puede defendernos de un ataque de falsificación de MAC, dado que nos permitiría fijar una dirección MAC por puerto, pero, como vimos, esto puede ser muy poco flexible ante cambios de usuarios o estaciones en una organización porque requeriría una reconfiguración del switch para cada cambio. Para defendernos de ataques por envenenamiento de ARP, podemos achicar los tiempos de espera en las estaciones para borrar las entradas, o una mejor solución sería cambiar la forma en que trabaja ARP: no debería aceptar respuestas ARP a solicitudes que no ha realizado, pero este cambio involucraría cambiar la implementación de TCP/IP en todas las estaciones.

El uso de autenticación entre los dos extremos involucrados en la comunicación proveería una defensa ante los ataques por suplantación de identidad, y con el uso de encriptación de los datos no permitiríamos que se filtre información a terceros no deseados. Esto se debe realizar en las capas superiores, dado que no hay una solución directa en capa 2.

Una solución que puede ser usada para mitigar este tipo de ataque, es el uso de la técnica conocida como Dynamic ARP Inspection (DAI), quien determina la validez de un paquete ARP basado en la relación existente entre una dirección MAC con una dirección IP, almacenada previamente en una base de datos por acción de otra técnica de seguridad conocida como DHCP snooping. DAI puede también validar tráfico ARP a través de Listas de Control de Acceso (ACL), especialmente para estaciones que tengan direccionamiento IP estático.

Es posible indicar al sistema operativo que la información en la caché ARP es estática y por tanto, no debe ser actualizada con la información que le provenga de la red. Esto prevendrá el ataque, pero puede resultar problemático en redes donde se actualicen los sistemas conectados a la red de forma regular.

Los switch de gama alta, poseen funcionalidades específicas para prevenir este tipo de ataques. Es necesario configurarlos adecuadamente para que mantengan ellos mismos una asociación IP-MAC adecuada y prevengan estos ataques.

Una adecuada segmentación de las subredes con routers y redes virtuales (otra de las funcionalidades de algunos switch) es la mejor prevención.

Existen herramientas que permiten conocer si una tarjeta de red en una subred se encuentra en modo promiscuo. Esto puede indicar la existencia de un ataque de envenenamiento ARP.

5.6.7 DHCP Starvation

El ataque por DHCP starvation consiste en que un usuario malicioso realice el envío de solicitudes DHCP falsificando la dirección MAC. Si se envían bastantes solicitudes, el atacante puede saturar el espacio de direcciones disponibles del servidor DHCP para un período determinado de tiempo. Así, el atacante podría configurar un servidor DHCP malicioso para responder a las nuevas solicitudes DHCP de clientes en la red. Tenga en cuenta que agotar todas las direcciones IP del servidor no es necesario para introducir un servidor DHCP malicioso (recuerde que en una red puede haber más de un servidor DHCP que realicen ofertas a una solicitud del cliente, y será el cliente quien seleccione la respuesta). Con la ubicación de un servidor DHCP malicioso en la red, un atacante puede enviarle a los clientes otra información de red. Una respuesta DHCP generalmente incluye al gateway por defecto y la información del servidor DNS, el atacante entonces podría simular ser el gateway por defecto y el servidor DNS realizando un ataque conocido como "man-in-the-middle" (hombre en el medio).

Contramedidas: Las técnicas para contrarrestar los ataques por inundación de la tabla CAM también pueden ser aplicadas a los ataques de DHCP starvation, por ejemplo, limitando el número de direcciones MAC en los puertos del switch. Otro punto a tener en cuenta surge de la RFC 3118, Autenticación para Mensajes DHCP, que hace más complicado el ataque de inundación y agotamiento al servidor DHCP. Finalmente, la opción 82 de DHCP, puede contribuir a prevenir este ataque especificando determinada información en los clientes para el servidor DHCP. Así, el servidor podría utilizar esta información para implementar políticas de asignación de direcciones.

DHCP snooping proporciona un alto grado de seguridad al filtrar los mensajes DHCP que arriban desde puertos no declarados para procesar este tipo de tráfico. De esta manera, sólo los puertos autorizados, por estar conectados a los verdaderos DHCP, pueden transmitir este tipo de mensajes, actuando como un Firewall. De esta manera un administrador puede diferenciar entre interfaces de no confianza, conectadas a usuarios finales, de interfaces de confianza conectadas a los verdaderos servidores DHCP.

DHCP snooping permite construir una tabla de asignaciones de direcciones IP, debido a que registra el intercambio de mensajes DHCP que ocurre cuando un servidor asigna estas direcciones IP a las estaciones que lo solicitan. Dicha tabla contiene la siguiente información:

- Dirección MAC de la estación de trabajo
- Dirección IP otorgada
- Tiempo de vida o alquiler de la dirección IP
- Tipo de enlace o binding
- Número de VLAN a la que pertenece la estación
- Identificador del puerto al que está conectado la estación

De esta manera, DHCP snooping permite también mitigar los ataques de ARP spoofing.

5.6.8 Buffer Overflow

Más allá de sus buenas intenciones, al igual que el resto de los seres humanos, los desarrolladores de

software pueden cometer errores. En muchos casos, estos errores pueden terminar en debilidades o vulnerabilidades, que aprovechadas por un atacante podrían terminar por comprometer un sistema por completo. Este tipo de ataque puede ocasionar negaciones de servicio o habilitar que determinado código no autorizado se ejecute en modo privilegiado. Al nivel más básico, Un Buffer Overflow, se produce cuando un programa, producto de su codificación, es poco estricto en la gestión de su espacio de memoria o no comprueba adecuadamente la longitud de las entradas recibidas como parte de su operación.

Si una aplicación no verifica la cantidad de información que está siendo ingresada, o lo hace incorrectamente, el atacante podría ingresar más datos de los esperados, de modo tal que estos terminen sobrescribiendo otros segmentos de memoria.

Un buffer no es otra cosa que un área temporal de memoria, utilizada por un programa para almacenar datos o instrucciones. A fin de crear un ataque de buffer overflow, el atacante simplemente debe escribir más datos de los que caben en el área de memoria asignada por el programa para una operación determinada, de modo tal de sobrescribir lo que allí se encuentre. Estos datos extra pueden ser tan solo caracteres sin sentido que podrían hacer que el programa falle, o eventualmente instrucciones que dispuestas del modo indicado, podrían desviar el flujo del programa a un punto en el cual el atacante sea capaz de, al controlar el mismo, ejecutar cualquier acción sobre el equipo atacado.

Un aspecto importante, radica en el hecho que aún hoy en día, donde los lenguajes de desarrollo más modernos (Java, C#, etc.) incluyen características que imposibilitarían a priori y en condiciones normales, la existencia de condiciones de desbordamiento de buffer, este tipo de bugs aún suelen ser encontrados con frecuencia. Adicionalmente, podemos mencionar que errores de BoF (Buffer Overflow), históricamente representan el tipo de bug más popular de todos los tiempos, relacionado con la codificación de software.

Contramedidas: La principal contramedida contra Buffer Overflows, se encuentra relacionada con la prevención. Aspectos tales como la utilización de prácticas de programación segura, el reemplazo de funciones inseguras tales como por ejemplo strcpy y strcat por strncpy y strncat respectivamente, la utilización de flags especiales en algunos de los compiladores mas comunes respecto de la prevención de aspectos de corrupción de memoria, el correcto chequeo respecto del largo del input dispuesto por el usuario en las aplicaciones y la adopción cuando sea posible de lenguajes tales como Java, C# etc., deberían contribuir notablemente a la reducción de este tipo de issues.

5.6.9 Denegación de Servicio (DoS)

Los ataques de DoS (Denial of Service - Denegación de Servicio) están apuntados exclusivamente a afectar negativamente el funcionamiento un servicio ofrecido por algún sistema o dispositivo de red. Un ataque de DoS exitoso afectará tanto al servicio que lo volverá totalmente inalcanzable. Este tipo de ataques no involucran un acceso al sistema, sino que buscan la degradación del servicio. Estos ataques generalmente son apuntados hacia un servidor o grupo de servidores específico, pero también pueden ser ejecutados contra routers, switches, hosts específicos, o contra la infraestructura de toda una red. Las motivaciones que llevan a que un atacante realice una DoS pueden ser por venganza, envidia, para desacreditar una compañía u organización, afectar sus negocios, o simplemente aburrimiento o búsqueda de desafíos.

A pesar que los ataques de Denegación de Servicio no generan un riesgo de pérdida de información o divulgación de información confidencial, pueden actuar como una herramienta efectiva para ocultar otras actividades intrusivas que se pueden realizar simultáneamente.

Es difícil de medir las implicancias de un ataque de denegación de servicio. Como mínimo son avergonzantes, y como máximo pueden afectar un comercio hasta cerrarlo. Las empresas que comercian a través de Internet (Amazon, eBay, etc.) son las más vulnerables a estos ataques. Si un sitio se encuentra inaccesible, seguro habrá un sitio alternativo a un par de clicks de distancia.

Mientras se realiza el ataque de DoS contra un objetivo, puede realizarse el verdadero intento de intrusión hacia otro objetivo. Cuando se realiza una Denegación, inmediatamente se toma conocimiento (una vez que la denegación es exitosa) y los administradores deben abocarse a la reparación. Este caos generado puede ser que genere una relajación de las medidas de seguridad hasta lograr levantar nuevamente el servicio, y esto puede ser aprovechado por los atacantes para ingresar al objetivo real.

Los ataques de DoS pueden generarse de diferentes maneras:

Por explotación de errores de aplicaciones: Se envían paquetes mal formados que generan una caída de la aplicación.

Por mensajes de control: Se envían paquetes con mensajes de control para que los dispositivos interrumpan la operación de la red.

Por inundación (IP Flooding): Consumen los recursos con una gran cantidad de paquetes. Un ejemplo de este tipo de ataques es el SYN Flood. Este ataque consiste en enviar masivamente peticiones de conexiones TCP (con el código SYN activado). Para cada petición de conexión, el receptor debe reservar una porción de memoria. Si se realiza una cantidad suficiente de peticiones de conexión, el receptor consumirá toda su memoria y no podrá responder a nuevas peticiones.

Este ataque se realiza habitualmente en redes locales o en conexiones con un gran ancho de banda. Consiste en la generación de tráfico basura con el objetivo de conseguir la degradación del servicio. De esta forma, se resume el ancho de banda disponible, ralentizando las comunicaciones existentes de toda la red.

Podemos pensar en la utilización de este ataque principalmente en redes locales cuyo control de acceso al medio es nulo y cualquier máquina puede ponerse a enviar y recibir paquetes sin que se establezca ningún tipo de limitación en el ancho de banda que consume.

Algunos de los métodos más conocidos son:

- **Ping de la muerte**: La utilidad ping sirve principalmente para saber si un host está activo y además podemos determinar el delay existente hasta ese host. En este ataque, básicamente se le envía un paquete ICMP de ping a un host esperando su respuesta. La diferencia está en que si se le envía un paquete muy grande, éste puede llegar desordenado por lo que el host pide al origen que le vuelva a enviar una parte o la totalidad del paquete, produciendo así un datagrama ICMP muy grande que ocasionará su caída.

  Al igual que otros ataques de denegación existentes, utiliza una definición de longitud máxima de datagrama IP fraudulenta.

  La longitud máxima de un datagrama IP es de 65535 bytes, incluyendo la cabecera del paquete (20 bytes) y partiendo de la base de que no hay opciones especiales especificadas. Por otra parte, recordemos que el protocolo ICMP tiene una cabecera de 8 bytes. De esta forma, si queremos construir un mensaje ICMP tenemos disponibles 65535 - 20 - 8 = 65507 bytes.

  Debido a la posibilidad de fragmentación de IP, si es necesario enviar más de 65535 bytes, el datagrama IP se fragmentará y se reensamblará en el destino.

  El ataque ping de la muerte se basa en la posibilidad de construir, mediante el comando ping, un datagrama IP superior a los 65535 bytes, fragmentado en N trozos, con el objetivo de provocar incoherencias en el proceso de reensamblado.

  Si, por ejemplo, construimos un mensaje ICMP de tipo *echo-request* de 65510 bytes mediante el comando ping -s 65510, los datos ICMP podrán ser enviados en un único paquete fragmentado en N trozos (según la MTU de la red), pero pertenecientes al mismo datagrama

IP. Si hacemos la suma de los distintos campos del datagrama, veremos que los 20 bytes de cabecera IP más los 8 bytes de cabecera ICMP, junto con los datos ICMP (65510 bytes) ocuparán 65538 bytes. De esta forma, el ataque consigue provocar un desbordamiento de 3 bytes. Este hecho provocará que al reconstruir el paquete original en el destino, se producirán errores que, si existen deficiencias en la implementación de la pila TCP/IP del sistema, podrían causar la degradación total del sistema atacado.

- **Syn flood**: El Syn Flood o TCP/SYM Flood es uno de los más famosos de los ataques tipo Denial of Service. Se basa en un "saludo" incompleto entre el host atacante y el objetivo del ataque. El Cliente envía un paquete SYN pero no responde al paquete ACK del 2º paso del saludo de tres vías TCP, ocasionando que el servidor permanezca a la escucha un determinado tiempo, reservando recursos para la nueva conexión, hasta cancelar la llamada. Si se envían muchos saludos incompletos, se consigue que el servidor se paralice o por lo menos se ralentice. El ataque de TCP/SYN Flooding sea provecha del número de conexiones que están esperando para establecer un servicio en particular para conseguir la denegación del servicio.

  Cada vez que se procesa una conexión, deben crearse datagramas IP para almacenar la información necesaria para el funcionamiento del protocolo. Esto puede llegar a ocupar mucha memoria. Como la memoria del equipo es finita, es necesario imponer restricciones sobre el número de conexiones que un equipo podrá aceptar antes de quedarse sin recursos.

  Cuando un atacante configura una inundación de paquetes SYN de TCP, no tiene ninguna intencióin de complementar el protocolo de intercambio, ni de establecer la conexión. Su objetivo es exceder los límites establecidos para el número de conexiones que están a la espera de establecerse para un servicio dado.

  Esto puede hacer que el sistema que es víctima del ataque sea incapaz de establecer cualquier conexión adicional para este servicio hasta que las conexiones que esten a la espera bajen el umbral.

  Hasta que se llegue a este límite, cada paquete SYN genera un SYN/ACK que permanecerá en la cola a la espera de establecerse. Es decir, cada conexión tiene un temporizador (un límite para el tiempo que el sistema espera, el establecimiento de la conexión) que tiende a configurarse en un minuto.

  Cuando se excede el límite de tiempo, se libera la memoria que mantiene el estado de esta conexión y la cuenta de la cola de servicios disminuye en una unidad. Después de alcanzar el límite, puede mantenerse completa la cola de servicios, evitando que el sistema establezca nuevas conexiones en este puerto con nuevos paquetes SYN.

  Dado que el único propósito de la técnica es inundar la cola, no tiene ningún sentido utilizar la dirección IP real del atacante, ni tampoco devolver los SYN/ACK, puesto que de esta forma facilitaría que alguien pudiera llegar hasta el siguiendo la conexión. Por lo tanto, normalmente se falsea la dirección de origen del paquete, modificando para ello la cabecera IP de los paquetes que intervendrán en el ataque de una inundación SYN.

- **Land attack**: Este ataque consiste en un error en la implementación de la pila TCP/IP en sistemas Windows. Aquí el atacante envía a algún puerto abierto de un servidor (generalmente al 113 o al 139) un paquete, maliciosamente construido con la IP y puerto origen igual que la IP y puerto destino. Al final la máquina termina por colapsarse.

- **Teardrop**: Los ataques Teardrop I y Teardrop II afectan a fragmentos de paquetes. En este caso, un atacante puede enviarles paquetes manipulados a sistemas Windows con el fin de adulterar los números de fragmentos de los paquetes. Algunas implementaciones de colas IP no vuelven a recomponer correctamente los fragmentos ya que se superponen, haciendo que el sistema se cuelgue. El Windows NT 4.0 es especialmente vulnerable a este ataque. Aunque existen parches que pueden aplicarse para solucionar el problema.

  El ataque Teardrop intentará realizar una utilización fraudulenta de la fragmentación IP para

poder confundir al sistema operativo en la reconstrucción del datagrama original y colapsar asi el sistema.

- **Snork**: El ataque Snork se basa en una utilización malintencionada de dos servicios típicos en sistemas Unix: el servicio CHARGEN (CHARacter GENerator, generador de caracteres) y el servicio ECHO. El primer servicio se limita a responder con una secuencia aleatoria de caracteres a las peticiones que recibe. El segundo servicio, ECHO, se utiliza como sistema de pruebas para verificar el funcionamiento del protocolo IP. Así, esta denegación de servicio se basa en el envío de un datagrama especial al ordenador de destino, que una vez reconocido, enviará una respuesta al equipo de origen.

  El ataque Snork consiste en el cruce de los servicios ECHO y CHARGEN, mediante el envío de una petición falsa al servicio CHARGEN, habiendo colocado previamente como dirección de origen la dirección IP de la máquina que hay que atacar (con el puerto del servicio ECHO como puerto de respuesta). De esta forma, se inicia un juego de ping-pong infinito. Este ataque se puede realizar con distintos pares de equipos de la red obteniendo un consumo masivo de ancho de banda hasta degradar el rendimiento de la misma.También se puede realizar contra una misma máquina (ella misma se envía una petición y su respuesta) consiguiendo consumir los recursos (especialmente CPU y memoria) de este equipo.

El tráfico generado por DoS puede ser:

- **Aleatorio**. Cuando la dirección de origen o destino del paquete IP es ficticia o falsa. Este tipo de ataque es el más básico y simplemente busca degradar el servicio de comunicación del segmento de red al que está conectado el ordenador responsable del ataque.
- **Definido o dirigido**. Cuando la dirección de origen, destino, o incluso ambas, es la de la máquina que recibe el ataque. El objetivo de este ataque es doble, ya que además de dejar fuera de servicio la red donde el atacante genera los datagramas IP, también tratará de colapsar al equipo de destino, sea reduciendo el ancho de banda disponible, o bien saturando su servicio ante una gran cantidad de peticiones que el servidor será incapaz de procesar.

Los datagramas IP utilizados podrían corresponder a:

- **UDP**. Con el objetivo de generar peticiones sin conexión a ninguno de los puertos disponibles. Según la implementación de la pila TCP/IP de las máquinas involucradas, las peticiones masivas a puertos específicos UDP pueden llegar a causar el colapso del sistema.
- **ICMP**. Generando mensajes de error o de control de flujo.
- TCP. Para generar peticiones de conexión con el objetivo de saturar los recursos de red de la máquina atacada.

Una variante del *IP Flooding* tradicional consiste en la utilización de la dirección de difusión de la red como dirección de destino de los datagramas IP. De esta forma, el encaminador de la red se verá obligado a enviar el paquete a todos los ordenadores de la misma, consumiendo ancho de banda y degradando el rendimiento del servicio.

También existen otras variantes en las que se envían peticiones ICMP de tipo *echo-request* a varios ordenadores suplantando la dirección IP de origen, sustituida por la dirección de difusión (*broadcast*) de la red que se quiere atacar. De esta forma, todas las respuestas individuales se ven amplificadas y propagadas a todos los ordenadores conectados a la red.

Debido a que en general estos ataques no realizan ninguna acción declarada como prohibida, o denegada, son ataques difíciles de detectar.

Para defendernos de los ataques de DoS por explotación de vulnerabilidades, como lo hemos visto

anteriormente, es imperioso mantener los sistemas libres de vulnerabilidades mediante las últimas actualizaciones.

Para defendernos de los ataques de DoS por mensajes de control, necesitaremos crear los filtros de paquetes apropiados.

Para defendernos de los ataques de DoS por inundación, existen dispositivos llamados IDS (Intrution Detection Systems) que veremos más adelante, que ayudan a detectar a un ataque de este tipo en proceso. Analizan el flujo de datos buscando patrones de ataques. Otra alternativa es restringir la cantidad de conexiones simultáneas que atenderá un servidor.

El peligro de los ataques de denegación de servicio viene dado por su independencia de plataforma. Como sabemos, el protocolo IP permite una comunicación homogénea (independiente del tipo de ordenador o fabricante) a través de espacios heterogéneos (redes Ethernet, ATM, ...). De esta forma, un ataque exitoso contra el protocolo IP se convierte inmediatamente en una amenaza real para todos los equipos conectados a la red, independientemente de la plataforma que utilicen.

Las formas de ataque DoS más comunes en redes WLAN son los siguientes:

- ***Radio jamming***. Interferir el espectro con una señal de alta potencia inhabilitando que el usuario legítimo acceda al servicio.
- ***Wireless DoS***. Es inherente al protocolo IEEE 802.11. Como las tramas de gestión no están protegidas por privacidad, autenticación e integridad, cualquier atacante puede realizar un ataque Wireless DoS sin más que mandando tramas de disociación a cualquier usuario de la red WLAN.

  En general, para llevar a cabo este tipo de ataques es necesario configurar el interfaz WLAN modo Master y con la MAC del AP (con un sniffer).

5.6.10 Denegación de Servicio Distribuido (DdoS)

Un tipo de ataque de DoS más reciente es la Denegación de Servicio Distribuida (DDoS) que utiliza múltiples computadoras para atacar a una sola entidad. Básicamente el DDoS es un ataque similar al DoS, donde se intenta consumir todos los recursos de una víctima hasta agotar su capacidad de procesamiento o llegar a un desborde. A diferencia del DoS en este caso no enfrentamos a múltiples atacantes y desde cada uno de estos se intenta inundar a la víctima, ocasionando así una avalancha mucho mayor de paquetes sobre el destino del ataque.

En los ataques por DDoS, el atacante se suele aprovechar de los hosts de usuarios hogareños que están conectados en forma permanente (como los que utiliza conexiones DSL o por cable). Este tipo de hosts, generalmente, no están lo suficientemente protegidos, entonces un usuario malicioso podría cargar en docenas o miles de estos hosts un software de ataque.

El programa de ataque permanece latente en las computadoras hasta que reciben una señal del usuario malicioso (no necesariamente el mismo que haya instalado el software de ataque en los hosts). Esta señal, le indica a todos los hosts (comúnmente llamados zombis) en forma simultánea que deben comenzar el ataque hacia un destino determinado.

Un punto a tener en cuenta es que las máquinas utilizadas finalmente para realizar el ataque son, generalmente, máquinas de usuario hogareños. Al momento de comenzar el ataque no se le realiza ningún aviso previo al usuario y cuando se completa el ataque, el programa instalado generalmente se elimina del sistema o infecta al usuario con algún virus que destruya la evidencia el rastro. A diferencia de los ataques por DoS, los ataques por DDoS son en la mayoría de los casos por inundación.

Si el atacante tiene un ancho de banda para el acceso a la red menor al de la víctima, resultaría muy complicado poder "inundarlo" hasta saturarlo. Con el ataque distribuido en un gran número de hosts el atacante logra generar el tráfico suficiente para ahogar a la víctima.

Así, consumen los recursos de una víctima enviando más paquetes de los que pueda procesar. Un

ejemplo de este tipo de ataques es el SYN Flood (ya visto en el ataque por DoS). Este ataque consiste en enviar masivamente peticiones de conexiones TCP (con el código SYN activado). Para cada petición de conexión, el receptor debe reservar una porción de memoria. Si se realiza una cantidad suficiente de peticiones de conexión, el receptor consumirá toda su memoria y no podrá responder a nuevas peticiones.

Un ataque muy común de DDoS es el ataque ***Smurf***.

- Este sistema de ataque se basa en transmitir a la red una trama ICMP correspondiente a una petición de ping. Esta trama lleva como dirección de origen la dirección IP de la víctima, y como dirección de destino la dirección broadcast de la red atacada. De esta forma se consigue que por cada trama que se transmite a la red, contesten a la víctima todos aquellos sistemas que tienen habilitado el poder contestar a paquetes destinados a la dirección broadcast de la red.

  Como dirección de origen se pone la dirección IP de la m;aquina que debe ser atacada. En el campo de la dirección IP de destino se pone la dirección de difusión de la red local o red que se utilizará como trampolín para colapsar a la víctima.

  Con esta petición fraudulenta, se consigue que todas las máquinas de la red respondan a la vez a una misma máquina, consumiendo todo el ancho de banda disponible y saturando el ordenador atacado.

Otro ataque por DDoS muy conocido es el ***TFN*** (*Tribe Flood Network*).

- En este ataque, un usuario malicioso obtiene acceso privilegiado a múltiples hosts e instala un software que realice Syn Flood (visto anteriormente) sobre un destino en particular al momento de recibir la orden del atacante. Así, el atacante envía la instrucción a los hosts zombies y éstos realizan un SYN Flood sobre la víctima, ocasionando que quede fuera de servicio.

Otro ataque conocido es el **Trin00**

- TRIN00 es un conjunto de herramientas *master-slave* utilizadas para sincronizar distintos equipos que cooperarán, de forma distribuida, en la realización de una denegación de servicio. Las primeras implementaciones de TRIN00 fueron implementadas únicamente para sistemas Sun Solaris (en los que se produjeron los primeros ataques conocidos).

  El primer paso para realizar un ataque con TRIN00 consiste en la instalación de las herramientas en los equipos desde los que partirá el ataque. Para ello, el atacante necesitará obtener privilegios de administrador en estos equipos (que habrá conseguido mediante técnicas de *sniffing*, explotación de servicios, ...). Estos sistemas deberían ser equipos interconectados en grandes redes corporativas con un gran ancho de banda y en los que el origen del ataque pudiera pasar desapercibido entre cientos o millares de sistemas dentro la misma red. El atacante tratará de realizar un ataque de intrusión a un primer equipo de estas redes, desde donde continuará con la búsqueda de nuevos equipos vulnerables y procederá a su infección de igual manera como se realizó con el primer equipo.

  Para realizar las intrusiones, el atacante llevará a cabo una búsqueda de vulnerabilidades en los equipos existentes en la red, generando una lista de equipos potencialmente débiles en los que tratará de introducirse y ejecutar las herramientas necesarias para provocar la escalada de privilegios.

  Desde el primer equipo infectado por TRIN00, el atacante tratará de distribuir las herramientas a cada una de las demás máquinas infectadas. También se encargará de la ejecución de tareas periódicas para tratar de esconder los rastros de la intrusión que puedan delatar la entrada en el sistema y la detección del origen del ataque.

Evitar un ataque de inundación no resulta muy sencillo. Algunos servicios en los sistemas operativos permiten definir el número máximo de conexiones, o la capacidad máxima que puede consumir en el host, pero no todos lo hacen. La mayoría de los sistemas son susceptibles entonces a sufrir este tipo

de ataques. Además, continuamente son descubiertos nuevos bugs (fallas de seguridad) en los servicios o el mismo sistema operativo. Afortunadamente, la mayoría de los desarrolladores han implementado técnicas de actualización periódicas con el fin de minimizar los efectos de estos ataques. Un analista de seguridad debe mantener actualizados todos sus sistemas con las últimas mejoras de seguridad para cada sistema. Otro punto a tener en cuenta para no sufrir ataques de inundación, es configurar los routers de borde para que ajusten la velocidad de arribo de determinados tipos de paquetes (por ejemplos, limitar la velocidad de ICMP y TCP Syn).

Fortaleciendo el Protocolo TCP/IP en Windows contra ataques DoS

Hasta la fecha era muy difícil impedir un ataque DoS a ordenadores basados en la arquitectura NT, como Windows 2000 o XP; no ocurre así lo mismo con el kernel de Linux. Sin embargo, existe un modo de fortalecer la pila del protocolo TCP/IP en Windows; ya sea en redes internas o redes conectadas a Internet.

Se abre, por tanto, Regedit y en la clave:

`HKey_Local_Machine/System/CurrentControlSet/Services/Tcpip/Parameters`

Se colocan los siguientes valores DWORD:

- **`EnableICMPRedirect = 0`**

  Se deshabilitan las redirecciones ICMP, impidiendo que un ataque se redirija a un tercero.

- **`SynAttackProtect = 2`**

  Establece el límite SYN, para que no se cree una situación en la que la conexión TCP se bloquee en un estado semi abierto. La configuración predeterminada es 0. Un valor de 2 controla la caducidad de las conexiones abiertas y medio abiertas.

- **`TCPMaxConnectResponseRetransmissions = 2`**

  Determina las veces que TCP transmite un mensaje SYN/ACK que no es respondido. TCP retransmite confirmaciones hasta alcanzar el número de este valor.

- **`TCPMaxHalfOpen = 500`**

  Número de conexiones que el servidor puede mantener en estado semi abierto antes de que TCP/IP inicie la protección contra ataques SYN.

- **`TCPMaxHalfOpenRetired = 400`**

  Número de conexiones que el servidor puede mantener en estado semi abierto, incluso después de retransmitir una conexión. Si se sobrepasa esta entrada, TCP/IP inicia la protección contra ataques SYN.

- **`TCPMaxPortsExhausted = 5`**

  Número de solicitudes de conexión que el sistema rechazará antes de que TCP/IP inicie la protección contra ataques SYN.

- **`TCPMaxDataRetransmissions = 3`**

  Número de veces que TCP retransmite un segmento de datos desconocido en una conexión existente.

- **`EnableDeadGWDetect = 0`**

  Determina si el ordenador tiene que detectar puertas de enlace inactivas. Un valor de 1 implica que el sistema solicite a TCP que cambie a una puerta de enlace de reserva en caso de conexiones con problemas. Las puertas de enlace de reserva están definidas en la

Configuración TCP/IP, en Red, del Panel de control.

- **`EnablePMTUDiscovery = 0`**

  Determina si está habilitado el descubrimiento MTU de ruta de acceso, donde TCP descubre el paquete de mayor tamaño en la ruta a un host remoto.

- **`DisableIPSourceRouting = 2`**

  Determina si un ordenador permite que los clientes conectados establezcan la ruta que los paquetes deben seguir hasta su destino. Un valor de 2 impide el enrutamiento de origen de los paquetes IP.

- **`NoNameReleaseOnDemand = 1`**

  Determina si el ordenador libera su nombre NetBIOS a otro ordenador que lo solicite o si un paquete malintencionado quiere apropiarse del nombre NetBIOS.

- **`PerformRouterDiscovery = 0`**

  Determina si el ordenador realiza un descubrimiento del router de esta tarjeta. El descubrimiento solicita la información del router y agrega la información a una tabla de ruta -ARP-. El valor de 0 incluso impide el envenenamiento ARP.

A todo lo anterior, aún puede asegurarse más la pila TCP/IP para las aplicaciones socket de Windows (Winsock), como es el caso de los servidores web o FTP. Cabe añadir que el responsable de las conexiones a aplicaciones Winsock es el driver ***Afd.sys***. El problema de este driver es que en Windows 2000 y XP se modificó para admitir un número mayor de conexiones en estado semi abierto, sin denegar acceso a los clientes legítimos. En Windows 2003 se ha habilitado otro tipo de protección. Afd.sys puede usar la copia de seguridad dinámica del Registro, configurable, en lugar de hacerlo con la copia de seguridad estática. Y eso es lo que vamos a hacer en:

`HKey_Local_Machine/System/CurrentControlSet/Services/AFD/Parameters`

Colocando los siguientes valores DWORD:

- **`EnableDynamicBacklog = 1`**

  Alterna entre el uso de una copia de seguridad estática y una dinámica del Registro. El valor predeterminado es 0, lo que únicamente permite el uso de la copia de seguridad estática.

- **`MinimumDynamicBacklog = 20`**

  Número mínimo de conexiones permitidas a la escucha. Si las conexiones libres descienden por debajo de este valor se crea un subproceso para crear conexiones libres adicionales. Un valor demasiado grande reduce el rendimiento del ordenador.

- **`MaximumDynamicBacklog = 20000`**

  Número máximo de conexiones libres y medio abiertas. Más allá de este valor no habrán conexiones libres adicionales, al estar limitado.

- **`DynamicBacklogGrowthDelta = 10`**

  Número de extremos Winsock en cada conjunto de asignación solicitado por el ordenador. Un número demasiado elevado provoca que los recursos del sistema se ocupen de forma innecesaria.

La segunda macro de las mencionadas, Winsock_sec.vbs, configura automáticamente estos valores en el Registro de Windows 2000 y XP.

El fortalecimiento de la pila TCP/IP no es una panacea, pero servirá para la defensa de ataques

basados en DoS, sean del tipo que sea. Como siempre, el administrador de sistemas o el usuario, debería de activar, cuando menos, un Firewall, como medida adicional para evitar éste y otro tipo de ataques.

5.7 RESPUESTA ANTE INCIDENTES

Muy probablemente, pocas afirmaciones respecto de los diferentes aspectos relacionados con Seguridad de la Información, sean tan validos como el hecho de que no importa donde usted se encuentre, ni el nivel de seguridad que sus sistemas ostenten, muy probablemente alguna vez estos serán atacados y eventualmente su seguridad vulnerada. Consientes de tal situación, resulta imprescindible que nuestra organización se encuentre preparada para actuar del modo correcto, cuando llegue el momento de hacer frente a un incidente de seguridad.

A lo largo de los siguientes indicadores, intentaremos introducir las actividades relacionadas con las prácticas de respuesta a incidentes, los objetivos que con ellas se persiguen, el armado del equipo de respuesta a incidentes, las habilidades requeridas y los principales puntos involucrados en una respuesta efectiva. A fin de adentrarnos en los principales aspectos relacionados con la respuesta a incidentes, es de suma importancia comenzar estableciendo correctamente aquello que debe ser definido como un Incidente de Seguridad. En líneas generales, un Incidente de Seguridad puede ser definido como cualquier evento adverso que compromete o intenta comprometer la confidencialidad, integridad, disponibilidad, legalidad o confiabilidad de la información. Un incidente, también puede ser referido como cualquier violación a la política de seguridad de la organización A menudo suele cometerse el error de identificar como incidente, tan solo aquellos eventos más terribles y/o desastrosos, mientras que un incidente puede ser tan pequeño como la infección con virus de una notebook o un llamado a un usuario por parte de un tercero no identificado tratando de obtener algún tipo de información interna de la organización. Tal como veremos en breve, resulta de suma importancia que no solo se defina internamente en la organización, qué debe ser tomado como un incidente de seguridad y que no, sino que a su vez cada uno de los empleados de la misma conozcan exactamente que aspectos configuran un incidente, a fin de ser capaces de identificarlos y reportarlos.

5.7.1 Objetivos

En líneas generales, la “Respuesta a Incidentes” como tal, envuelve todas y cada una de las acciones tomadas frente a un incidente, durante y después de que el mismo haya ocurrido. Entre los objetivos primarios de una estrategia de “Respuesta a Incidentes” se encuentran:

- Proveer una manera efectiva y eficiente de enfrentar la situación de forma tal que sea posible reducir el impacto potencial en la organización
- Proveer a la gerencia de la información suficiente para que estos puedan decidir sobre el curso de acción apropiado
- Mantener o restaurar la continuidad del negocio
- Defenderse frente a ataques futuros.
- Disuadir a potenciales nuevos atacantes a través de la investigación, persecución y procesamiento.

Por su parte, la propia gestión de incidentes de seguridad de la información, a menudo comprende entre otras, las siguientes tareas principales:

- La detección y reporte del incidente
- La clasificación del incidente

- La respuesta al incidente
- El análisis del incidente
- El registro de incidentes
- El aprendizaje a partir de la experiencia

Por último, es importante mencionar, que el establecimiento de una correcta Gestión de Respuesta a Incidentes, puede permitir a la organización responder a los incidentes en forma sistemática, facilitar una recuperación rápida y eficiente de incidentes de seguridad, minimizando la perdida de información e interrupción de servicios, mejorar continuamente el marco de seguridad y el proceso de tratamiento de incidentes y manejar correctamente los aspectos legales que pudieran surgir en el tratamiento de incidentes.

Al momento de planificar una estrategia efectiva en relación a las prácticas de respuesta a incidentes, es requisito fundamental no solo trabajar en función de algún tipo de metodología o política formal al respecto, sino también contar con un equipo bien entrenado, conformado por personas con diferentes habilidades y conocedoras de los procesos de la organización.

Si bien el conjunto general de habilidades que se describirán en el próximo indicador, nos permitirán conocer en líneas generales, los perfiles que deben ser asociados a un equipo de respuesta a incidentes a partir de sus competencias y conocimientos, es importante notar que parte del éxito de toda estrategia de respuesta a incidentes, radica en contar con un equipo interdisciplinario el cual conjugue el valor de recursos capaces de aportar su conocimiento del negocio, con el expertise propio de campos tan diversos como son los de recursos humanos, legales, seguridad, tecnología, operaciones, etc.

5.7.2 Guía para una respuesta efectiva

Ya hemos mencionado en indicadores anteriores, los diferentes aspectos que relacionados con los diversos puntos en torno al proceso de respuesta a incidentes, no obstante a fin de que la estrategia sea considerada como tal, deben existir políticas, normas y procedimientos formales los cuales avalen dicha estrategia. A continuación mencionaremos algunos de los principales puntos a tener en cuenta en torno a la confección de estos documentos:

- La existencia de políticas, normas y procedimientos, son fundamentales en cualquier proceso o metodología y el manejo de incidentes no es la excepción a la regla.
- Políticas y procedimientos respecto de la respuesta a incidentes, deben ser desarrollados antes de que un incidente ocurra.
- “A pesar de que a simple vista la respuesta a incidentes parecería ser un proceso reactivo, en realidad debe ser referido como la ejecución reactiva de un plan proactivo”.
- Para las políticas y procedimientos relacionados con la administración de incidentes, rigen los mismos principios que para el resto de las políticas de la organización (Aprobación de la dirección, comunicación al equipo de trabajo, etc.)
- La correcta comunicación de las políticas relativas al manejo de incidentes, asegurara que potenciales incidentes sean reportados.

La elaboración de un plan efectivo de respuesta a incidentes, debe a su vez regirse por una serie de pasos, los cuales basados en las sentencias máximas expuestas en la política de respuesta a incidentes, permitan llevar a cabo el conjunto necesario de tareas a fin de tratar un incidente

determinado. Un ejemplo en cuanto a los posibles pasos a adoptar se menciona a continuación:

- Realizar una evaluación inicial
- Comunicar el incidente
- Contener el daño y minimizar el riesgo
- Identificar el tipo y gravedad del incidente
- Proteger las pruebas
- Notificar a los organismos externos, si corresponde
- Recuperar los sistemas
- Compilar y organizar la documentación del incidente
- Valorar los daños y costos del incidente
- Revisar las directivas de respuesta y actualización

Recomendaciones de Seguridad

- Defensa en profundidad
- Seguro por diseño
- Privilegios mínimos
- Aprender de los errores cometidos
- Mantener la seguridad
- Hacer que los usuarios se centren en la concienciación de seguridad
- Desarrollar y probar planes y procedimientos de respuesta a incidentes

Se deberá seguir el modelo de defensa en profundidad. Cada nivel del modelo está protegido por los niveles contiguos y depende de todos los niveles que se implementan. Hay un compromiso constante entre la funcionalidad y la seguridad. Ambos raramente se complementan. Aunque quizás en alguna ocasión lo importante haya sido la funcionalidad, ahora se busca definitivamente la seguridad. Así se facilita una implementación segura por diseño. El software y los sistemas son seguros de forma predeterminada y por diseño, con lo que se simplifica la creación de un entorno de red seguro. Los procesos y las aplicaciones que se ejecutan en un sistema logran este objetivo mediante un nivel definido de privilegios sobre el sistema. A menos que se configuren de otro modo, los procesos iniciados, mientras un usuario está conectado al sistema, se ejecutan con los mismos privilegios que tiene el usuario. Para impedir ataques accidentales, todos los usuarios del sistema deben iniciar sesión en él con los privilegios mínimos necesarios para realizar sus funciones. Los virus se ejecutan con los privilegios del usuario que haya iniciado la sesión. En consecuencia, los virus tendrán un ámbito mucho más amplio si el usuario inicia sesión como administrador. Las aplicaciones y los servicios también se deben ejecutar con los privilegios mínimos necesarios. Es muy importante que se entienda que la seguridad no es un objetivo: es un medio. Un entorno nunca es completamente seguro. Siguen apareciendo nuevos virus, revisiones y puntos débiles en los sistemas. Aprenda de la experiencia y conserve una documentación exhaustiva de todo lo que suceda. Para mantener la seguridad, implementar procedimientos de supervisión y auditoría, y comprobar que los resultados de estos procedimientos se procesan con regularidad.

Disponer de planes y procedimientos de respuesta a incidentes claros, completos y bien comprobados, es la clave para permitir una reacción rápida y controlada ante las amenazas.

5.8 MONITOREO DE TRÁFICO EN LA RED

Los sistemas de monitoreo se encargan de observar las conexiones dentro de una red y en algunos casos también son los responsables de dar aviso al administrador de la red e incluso bloquear una conexión. Entre las aplicaciones más utilizadas para el monitoreo de tráfico de red se encuentran:

Netstat: El comando Netstat es una aplicación utilizada para visualizar las conexiones de red al equipo, tablas de enrutamiento y listado de puertos abiertos. Está disponible en entornos Linux y Windows, basta con abrir una consola y escribir `netstat` para ver las opciones disponibles.

Se pueden realizar consultas de conexión, puertos activos y pasivos. Usándolo con las opciones –t, –u, –w, y –x se muestran las conexiones activas de puertos TCP, UDP, RAW o Unix. Si a su vez se incluye el modificador –a, se mostrará también una lista de los puertos que estén esperando una conexión (es decir, que estén escuchando). Esto dará una lista de todos los servicios que estén corriendo actualmente en el sistema. Si se ejecuta el comando Netstat usando el indicador -r se puede observar las tablas de enrutamiento al igual que se verifica con el comando route. Si se combina con el parámetro -i, Netstat presenta estadísticas de las interfaz físicas del host. Con la opción -a se muestra el estado de todos los sockets, todas las tablas de enrutamiento, y todas las interfaces lógicas y físicas.

Ntop: Ntop (Network Top) es una herramienta en sistemas Linux que permite monitorear en tiempo real usuarios y aplicaciones que estén consumiendo recursos de red y a su vez puede dar aviso de errores visualizados con un alerta del lado del cliente de la aplicación. Posee una interfaz la cual se accede vía web a través del puerto 3000 o de forma segura por medio del puerto 3003, desde donde se pueden obtener estadísticas mediante un conjunto de gráficos, los cuales agrupan las conexiones por protocolos, usuarios, etc. Es una aplicación fundamental para el administrador de redes que permite observar como está siendo utilizado el ancho de banda para verificar posibles abusos, vulnerabilidades o fallas en el esquema de red. Estos reportes se encuentran en forma de gráficos y resúmenes de tráfico histórico, detalle agrupado por origen del mismo (local, remoto, o ambos), sentido (Solo enviado, solo recibido, o ambos), filtro por protocolos y una serie de utilidades para exportar las estadísticas de tráfico recopiladas por ntop en forma de archivos de texto, XML y otras

Nessus: Nessus es una herramienta diseñada para realizar chequeos de vulnerabilidades conocidas de manera automática y corre sobre múltiples sistemas operativos.

El proyecto Nessus fue iniciado y liberado bajo licencia GPL en el año 1998 por Renaud Deraison. Gran parte de su éxito se debe a que una gran cantidad de desarrolladores colaboran con este trabajo, sobre todo en la construcción de plugins de detección. En octubre de 2005, Tenable Network Security cambió Nessus3 a una licencia propietaria aunque gratuita, donde se distribuyen los binarios pero no así sus fuentes, es por eso que para correr dicha versión es necesario descargarla y compilarla en muchas de las distribuciones Linux.

Está formado básicamente por tres partes que se describen a continuación:

- ***Servidor***: Es servidor de Nessus (nessusd) es el demonio que realiza los escaneos propiamente dichos.
- ***Cliente***: El cliente, que puede ser instalado en la misma máquina o en forma remota, es el encargado de realizar la interfaz con el administrador, ya sea en forma gráfica o de consola. Este, al momento de finalizado el escaneo, muestra un reporte que puede ser exportado en varios formatos como XML, LaTex y HTML, o utilizar la alternativa de generar una base de conocimiento para tomar como referencia en los próximos escaneos de vulnerabilidades.
- ***Pluggins***: Debido a su interfaz modular, basada en plugins, se puede hacer que esta herramienta realice el chequeo específico de ciertas características de conectividad de

servicios y aplicaciones escritos en un lenguaje propio llamado NASL (L (Nessus Attack Scripting, lenguaje de Scripting optimizado para interacciones personalizadas en redes.) los cuales pueden ser activados o desactivados personalizando, de esta manera, el chequeo a realizar. Hay que tener en cuenta que existen varios pluggins que pueden “confundir” al sistema de detección de intrusos que está siendo atacado donde sería posible la activación de un método de defensa que podría generar una eventual caída del sistema.

Nagios: El sistema de monitoreo Nagios es una aplicación open source que verifica el estado de los hosts y servicios especificados, y posee la capacidad de alertar (ya sea en forma gráfica, sonora, mediante mails al adminsitrador, sms, o incluso un sistema de desarrollo propio) cuando el comportamiento no sea el adecuado y cuando el mismo retorne a su estado normal.

5.9 PREGUNTAS Y TIPS

- **¿Cuales son factores que contribuyen a la inseguridad en las redes?** Falta de políticas y/o normativas, Uso incorrecto de las aplicaciones, Errores en los programas, Ambiente multilenguaje y multiproveedor
- **¿Por qué la falta de normativas o políticas de uso pueden ayudar a los ataques?** Porque no existen reglamentaciones de uso de la red, y los usuarios pueden realizar actividades que faciliten los ataques
- **¿Por qué se deben revisar las opciones de un software recién instalado?** Porque muchas aplicaciones inician con configuraciones inseguras
- **¿En qué orden se realizan las fases de un ataque?** Investigación, Penetración, Permanencia, Expansión, Logro del objetivo.
- **¿En qué consiste un ataque de interceptación?** Un usuario no autorizado obtiene acceso a la información o los datos.
- **¿Cuál opción describe más correctamente un ataque por interrupción?** Un usuario malicioso ataca a un sistema o parte de éste con el fin de dejarlo sin funcionamiento
- **¿Una de las fases del ataque es el reconocimiento, en qué consiste?** Es el descubrimiento no autorizado de la topología de la red, sus sistemas, servicios o vulnerabilidades
- **¿De qué forma se puede evitar el reconocimiento de la red?** Estableciendo filtros de tráfico
- **¿En qué consiste el eavesdropping?** En tomar datos que circulan por la red
- **¿Cuál de las siguientes opciones describe más exactamente man-in-the-middle?** Es un host que tiene acceso a los paquetes que atraviesan la red y se interpone en una conversación actuando como intermediario entre el emisor y el receptor con algún fin malicioso
- **¿Cómo podemos detectar una modificación de archivos dentro de nuestro sistema?** Utilizando software específico que genera un hash de cada archivo y reporta cuando hubo modificaciones
- **¿En qué consiste un ataque por IP spoofing?** El atacante falsifica su dirección IP para ganar los privilegios de otro usuario
- **¿Cómo puede defenderse de los ataques de CAM Table Overflow?** Mediante seguridad por puertos en los switches
- **¿Cuál de las siguientes opciones representan un problema de seguridad asociado a la utilización de STP?** Un usuario malicioso podría engañar a los switches de la red y podría transformarse en el switch raíz con el fin de ver las tramas que circulen entre switches
- **¿Qué debe enviar un intruso para realizar un ataque de MAC address spoofing?** Una trama cambiando su dirección MAC origen por la del objetivo
- **¿Qué puede conseguir un intruso mediante un ataque de ARP poisoning?** Redireccionar la dirección IP del objetivo hacia su dirección MAC
- **¿En qué se diferencia la Denegación de Servicio con la Denegación de Servicio Distribuida?** La DoS realiza el ataque desde un solo host, mientras que la DDoS utiliza múltiples hosts para realizar el ataque
- **¿Qué medida preventiva puede tomar para evitar sufrir un ataque de DoS o DDoS por inundación de ICMP o TCP Syn?** Configurar los routers de borde para regular el flujo de paquetes
- **¿Qué tipo de ataque requiere realizar un sniffing a la red?** Man-in-the-Middle

- **¿Qué tipo de ataque es el TCP/IP Hijacking?** Man-in-the-Middle
- **Snort, TCPDump y Wireshark son comúnmente usados para un Sniffing de Red**
- **SSH es un mecanismo que se puede usar para encriptar credenciales sobre FTP o Telnet**
- **¿Cuál es el principio de la seguridad que garantiza la exactitud de la información?** La Integridad
- En la práctica el bit ACK esta a 1 siempre, excepto en el primer segmento enviado por el host que inicia la conexión.!
- **¿Cuál es el puerto TCP por defecto cuando se protege el protocolo SMTP mediante SSL?** Puerto 25
- **¿Qué intenta explotar un ataque de tipo MAC Flooding?** La cantidad de memoria asignada para la MAC Address table
- Un CLR (*Common Language Runtime. Máquina virtual de Microsoft*) contiene una lista de las “llaves” tanto públicas como privadas!

CAPÍTULO 6

6.1 SEGURIDAD EN EL PERÍMETRO INTERNO Y EXTERNO DE LA RED

El perímetro de red es el área de una red que está más expuesta a un ataque del exterior. Los perímetros de red se pueden conectar a numerosos entornos diferentes, que van desde socios comerciales a Internet. Cada organización usa criterios distintos para definir su perímetro.

El compromiso de la seguridad en el perímetro puede resultar en:

- Ataque a la red corporativa
- Ataque a los usuarios remotos
- Ataque a un socio comercial
- Ataque desde una sucursal
- Ataque a servicios de Internet
- Ataque desde Internet

La mayoría de los expertos en seguridad se centran en el área desde la que cabe esperar que se origine un ataque, como Internet. Sin embargo, los intrusos también son conscientes de que ésta será la solución que probablemente utilice e intentarán atacar la red desde algún otro lugar. Es muy importante que todas las entradas y salidas de la red sean seguras.

Es improbable que uno sea el responsable de la implementación de seguridad de los socios comerciales; por lo tanto, no se puede confiar completamente en todo el acceso que se origine en ese entorno. Además, no se tiene control del hardware de los usuarios remotos, lo que constituye otro motivo para no confiar en el mismo. Las sucursales podrían no contener información confidencial y, por lo tanto, es posible que tengan una implementación menos segura. Sin embargo, podrían tener vínculos directos a la oficina principal que un intruso podría usar.

Es importante considerar la seguridad de la red en conjunto, no sólo en áreas individuales.

La protección del perímetro de red incluye:

- Servidores de seguridad
- Bloqueo de puertos de comunicación
- Traducción de direcciones IP y puertos
- Redes privadas virtuales
- Protocolos de túnel
- Cuarentena en VPN

La protección de los perímetros se puede llevar a cabo principalmente con servidores de seguridad. La configuración de un servidor de seguridad puede ser difícil desde el punto de vista técnico. Por lo tanto, los procedimientos deben detallar claramente los requisitos.

Los sistemas operativos recientes de Microsoft Windows facilitan el bloqueo de los puertos de comunicación innecesarios para reducir el perfil de ataque de un equipo.

La traducción de direcciones de red (NAT, Network Address Translation) permite a una organización disimular las configuraciones de direcciones IP y de puertos internos para impedir que usuarios malintencionados ataquen los sistemas internos con información de red robada. Los mecanismos de seguridad del perímetro pueden ocultar también los servicios internos, incluso aquellos que están

disponibles externamente, de modo que un intruso nunca se comunique de forma directa con ningún sistema que no sea el servidor de seguridad desde Internet.

Cuando los datos salen del entorno que está bajo la responsabilidad de uno, es importante que se encuentren en un estado que garantice su seguridad y que lleguen intactos a destino. Esto se puede conseguir mediante protocolos de túnel y cifrado, con el fin de crear una red privada virtual (VPN, Virtual Private Network).

El protocolo de túnel que emplean los sistemas de Microsoft es el Protocolo de túnel punto a punto (PPTP, Point-to-Point Tunneling Protocol), que utiliza Cifrado punto a punto de Microsoft (MPPE, Microsoft Point-to-Point Encryption), o Protocolo de túnel de nivel 2 (L2TP, Layer 2 Tunneling Protocol), que utiliza el cifrado de IPSec.

Cuando los equipos remotos establecen comunicación a través de una VPN, las organizaciones pueden seguir pasos adicionales para examinar esos equipos y garantizar que cumplan una directiva de seguridad predeterminada. Los sistemas que establecen la conexión se aíslan en un área independiente de la red hasta que se completan las comprobaciones de seguridad.

La protección del perímetro de una red es el aspecto más importante para parar un ataque del exterior. Si un perímetro sigue siendo seguro, la red interna se debe proteger contra ataques externos. Se enumeran abajo algunas maneras de implementar la defensa del perímetro:

- Packet Filtering
- Inspección de paquetes
- Intrusion Detection

Los ataques no provienen sólo de orígenes externos. Tanto si los ataques internos son genuinos como si son meros accidentes, muchos sistemas y servicios se dañan desde dentro las organizaciones. Es importante implementar medidas internas de seguridad orientadas a las amenazas mal intencionadas y accidentales.

El acceso a los sistemas y recursos de red internos permite a los intrusos obtener acceso fácilmente a los datos de la organización.

Mediante el acceso a la infraestructura de red también pueden supervisar la red e investigar el tráfico que se está transportando. Las redes totalmente enrutadas, aunque hacen que la comunicación sea más fácil, permiten a los intrusos tener acceso a los recursos de la misma red independientemente de si se encuentran o no en ella.

Los sistemas operativos de red tienen instalados muchos servicios. Cada servicio de red constituye un posible medio de ataque.

Uno puede tener una serie de redes en su organización y debe evaluar cada una individualmente para asegurarse de que está asegurada apropiadamente. Se enumeran abajo algunas maneras de implementar defensas de red:

- VLAN Access Control Lists
- Internal Firewall
- Auditing

- Intrusion Detection

Para proteger el entorno de la red interna, se debe requerir que cada usuario se autentique de forma segura en un controlador de dominio y en los recursos a los que tenga acceso. Utilizar la autenticación mutua, de modo que el cliente también conozca la identidad del servidor, con el fin de impedir la copia accidental de datos a los sistemas de los intrusos.

Segmentar físicamente los conmutadores, es decir, crear particiones de la red para impedir que toda ella esté disponible desde un único punto. Se puede crear particiones si se utilizan enrutadores y conmutadores de red independientes o si crean varias redes virtuales de área local (VLAN, Virtual Local Area Network) en el mismo conmutador físico.

Considerar cómo se van a administrar los dispositivos de red, como los conmutadores. Por ejemplo, el grupo de trabajo de red podría utilizar Telnet para tener acceso a un conmutador o enrutador y realizar cambios de configuración. Telnet pasa todas las credenciales de seguridad en texto sin cifrar. Esto significa que los nombres y las contraseñas de los usuarios son accesibles para cualquiera que pueda rastrear el segmento de red. Esto puede constituir una debilidad importante de la seguridad. Considerar permitir únicamente el uso de un método seguro y cifrado, como SSH de shell o acceso de terminal serie directo. También se deben proteger adecuadamente las copias de seguridad de las configuraciones de dispositivos de red. Las copias de seguridad pueden revelar información sobre la red que resulte útil a un intruso. Si se detecta una punto débil, se pueden utilizar copias de seguridad de la configuración de los dispositivos para realizar una restauración rápida de un dispositivo y revertir a una configuración más segura.

Restringir el tráfico aunque esté segmentado. Puede utilizar 802.1X para proporcionar un acceso cifrado y autenticado tanto en las LAN inalámbricas como en las estándar. Esta solución permite utilizar cuentas de Active Directory y contraseñas o certificados digitales para la autenticación. Si se utilizan certificados, se tendrá que integrar una infraestructura de clave pública (PKI, Public Key Infrastructure), en Servicios de Windows Certificate Server; para las contraseñas o certificados, también necesitará un servidor RADIUS integrado en el Servicio de autenticación Internet (IAS, Internet Authentication Service) de Windows. En Windows Server 2003 se incluyen IAS y Servicios de Certificate Server. Implementar tecnologías de cifrado y firma, por ejemplo la firma de IPSec o bloque de mensajes de servidor (SMB, Server Message Block), con el fin de impedir a los intrusos rastrear los paquetes de la red y reutilizarlos.

Los Firewalls e IDS son herramientas muy importantes que nos permiten agregar funcionalidades de seguridad a nuestro diseño, sobre todo nos permiten interactuar en forma dinámica con el entorno y responder rápidamente a los incidentes.

¿Qué es un ataque y cuáles son sus objetivos? Un ataque ocurre cuando una persona o un grupo de personas intenta acceder, modificar o dañar un sistema o entorno. Ocurre de diferentes formas y por distintas razones. Estos ataques generalmente intentan lograr algunos de de estos objetivos:

- *Un ataque de acceso:* es un ataque donde alguien quiere acceder a sus recursos
- *Un ataque de modificación:* es un ataque de alguien que quiere modificar los datos de su sistema
- *Un ataque de denegación de servicio*: Es un ataque de alguien que quiere interrumpir algún servicio de networking
- *Un ataque de fabricación:* consiste en falsificar la información, ataca la autenticidad.

¿Cómo pueden las PC de una red interna con direccionamiento privado acceder a Internet, si sus direcciones IP no son ruteables? El protocolo NAT (Network Address Translation) se caracteriza por permitir el uso en nuestras redes de números IP considerados como no ruteables (también

llamados privados) y poder conectarnos ainternet, esta posibilidad la brinda el protocolo al utilizar un mecanismo conocido como traslación, el cual permite que los paquetes con destino a Internet enviados desde una red privada, sean interceptados a fin de que en el paquete IP el número IP no ruteable sea remplazado por uno que sí lo es, con lo cual el paquete IP resultante queda listo para ser ruteado en Internet.

¿Qués es un PIX? Es un Firewall desarrollado por Cisco System, con poderosas características de análisis y filtrado de paquetes obtenidas a través de varias técnicas, entre ellas la inspección de pleno estado. Está implementado como un dispositivo independiente y completamente dedicado. Uno de los aspectos básicos de la seguridad es el control del tráfico que ingresa y egresa de nuestra red, así como también el monitoreo general de los sistemas, ya sea para conocer que las medidas de seguridad se encuentran establecidas como para detectar qué es lo que está sucediendo. Un error típico es creer que por tener implementadas estas medidas, el sistema ya será inmune a todo tipo de ataques. Antes que una intrusión suceda, se pueden poner en práctica una serie de controles para prevenir, disuadir y detectar anormalidades. Durante una intrusión, las medidas de detección podrán alertar la existencia de un atacante en base a los eventos producidos, ya sea en forma directa o mediante la correlación de un conjunto de ellos. Adicionalmente, durante la intrusión se puede recolectar toda la información disponible que pueda ser utilizada para el estudio de la técnica de ataque.

6.1.1 La problemática de los Firewalls

Comúnmente, se denomina Firewall o cortafuego a una pared hecha de material no combustible diseñado para impedir la extensión del fuego desde una porción de un edificio a otra. El objetivo es mantener las áreas peligrosas fuera del alcance de las áreas seguras. Al aplicar el término a una red de computadoras, un cortafuego proporciona un punto de defensa entre la red interna de la empresa y la red externa, donde están situados usuarios no confiables, y permite proteger el acceso de una red hacia la otra, es decir, es un sistema o grupo de sistemas que permite implementar una política de control de acceso entre dos o más redes. Entonces, un Firewall o cortafuego protege la red privada de una compañía contra el público o las redes compartidas con quienes está conectada. Un Firewall evalúa cada paquete que ingresa o sale de la empresa y lo compara con las políticas de seguridad de la red, implementadas a través de una colección de reglas, que reflejan las convenciones, y procedimientos d seguridad que gobiernan las comunicaciones hacia y desde una red. Podemos encontrarlos como una funcionalidad adicional en los propios Routers (software IOS Firewall de Cisco Systems), como una aplicación software ejecutándose en una PC (por ejemplo LINUX) o como dispositivos independientes y completamente dedicados (como los PIX de Cisco Systems).

6.1.2 Políticas de configuración

Como mencionamos anteriormente mediante el uso de un Firewall se aísla la red privada de los posibles daños que pueda sufrir por estar conectada a un sistema público inseguro (como puede ser Internet). Siguiendo las reglas que el administrador del sistema debe escoger cuidadosamente, se permite que los paquetes alcancen su destino, o bien se eliminen y descarten.

Las dos políticas principales de configuración para un Firewall son:

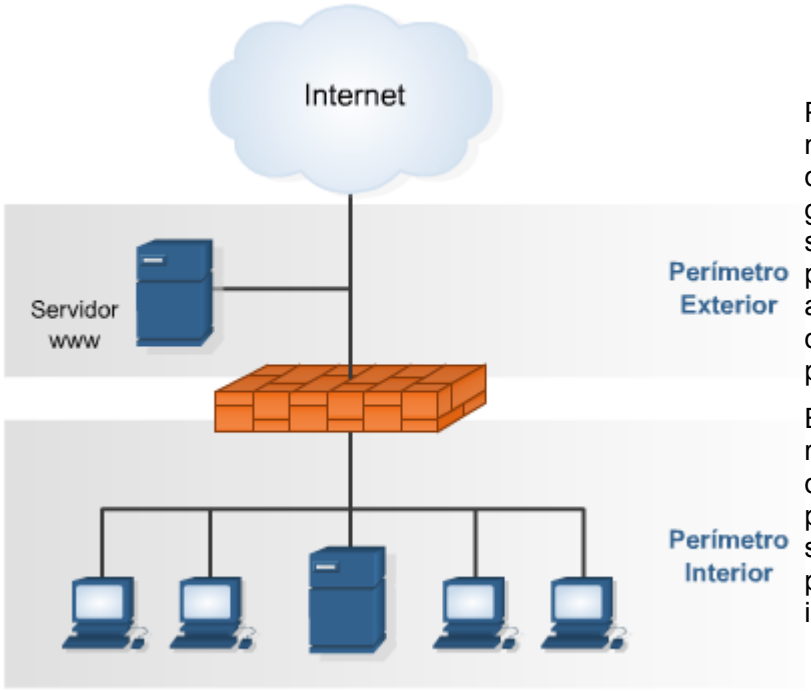
- permitir todo lo que no esté específicamente prohibido, o bien
- prohibir todo lo que no esté explícitamente permitido.

De las dos formas posibles de configurar un Firewall mencionadas anteriormente, la segunda es más recomendable, segura y restrictiva, y permitirá al administrador tener el control sobre las comunicaciones que entran y salen de la red.

6.1.3 Perímetro Externo e Interno

Generalmente las directivas marcadas dentro de la política de seguridad, fuerzan a diseñar la red separando los recursos en perímetros de seguridad. Cuando implementemos un Firewall, por lo menos encontraremos dos perímetros claramente definidos:

Un "perímetro interior", en el que se situarán todos los recursos sensibles a un posible ataque, pero de manera aislada al "perímetro exterior" donde se situarán los recursos menos sensibles, o que inevitablemente por motivos funcionales deban estar en contacto con el mundo exterior de forma menos rígida. El perímetro interior estará aislado o protegido del perímetro exterior y del resto de Internet, por medio del Firewall, donde se centralizarán la mayoría de las medidas de seguridad.



Por ejemplo, una empresa que necesitara publicar en Internet determinada información de interés general, podría implementar un servidor WWW y debería ubicarlo en el perímetro exterior. Esto permitiría aplicarle reglas de seguridad diferentes a las que le aplicamos al perímetro interior.

En este caso, deberíamos definir reglas donde se especifique que desde el perímetro exterior sólo se permitirán conexiones hacia el servidor WWW, de esta manera protejo los recursos de mi perímetro interior.

6.1.4 Topologías de seguridad

El término “topologías de seguridad” permite describir la manera en la cual se aíslan sistemas o redes, es decir, la forma de separar diferentes recursos. Cuando se habla de topologías o zonas de seguridad, es bueno pensar en estas zonas como si fueran distintos salones o habitaciones de una casa, a fin de facilitar su comprensión. En esta analogía, se pueden tener algunos salones donde nadie puede ingresar, también pueden existir otros salones donde el acceso será limitado a individuos o propósitos específicos, como así también hay salones para acceso al público en general. Es posible aislar redes de otras utilizando hardware y software, por ejemplo se puede utilizar un Router con capacidades de Firewall para esta tarea, configurando direcciones de red diferentes y haciendo invisible una de otra a menos que se permita expresamente el tráfico a través del Router.

Se pueden establecer cuatro zonas o topologías de seguridad diferentes:

- ***Internet:*** Como ya es sabido, Internet es una red global que permite conectar computadoras y redes situadas en todo el mundo. Este entorno debería asumirse como de bajo nivel de confianza, debido a que no se controla el tráfico que circula por la misma, ni se puede conocer de antemano las intenciones de los usuarios que se conectan a nuestros servicios públicos.
- ***Intranet:*** Conforman redes privadas implementadas y mantenidas por una misma empresa u organización. Una Intranet utiliza la misma tecnología que existe en Internet, como ser el uso

de hipervínculos o enlaces, acceso a diferentes clases de archivos multimedia, etc. Una misma Intranet puede estar conectada a través de Internet, pero sólo permitirá el acceso a usuarios previamente autenticados y autorizados.

- ***Extranet:*** Permite extender el alcance de una Intranet, a fin de incluir redes de partners. Una Extranet permite el acceso a la red privada de un partner mediante un enlace privado o utilizando un canal seguro a través de Internet. Una Extranet involucra la conexión entre redes no confiables, debido a que cada una de ellas se encuentra bajo una política de administración diferente.
- ***DMZ:*** Una zona desmilitarizada (DMZ) es un área donde se sitúan los servidores públicos, es decir, aquellos que deben ser accedidos por todo tipo de usuarios y desde cualquier parte. Aislando un server en la DMZ, se pueden ocultar otras redes o evitar el acceso a áreas críticas de nuestra red, reduciendo de esta manera la amenaza de intrusiones en los recursos internos. Normalmente su implementación se realiza mediante la utilización de Firewalls.

6.1.5 Defensa por Capas

CAPA 1: El perímetro del router de Internet (Externo): La primer capa de protección contra un ataque es el router externo. Un router configurado correctamente, puede evitar que el tráfico externo ingrese a una red haciendo spoofing de la red interna. Los routers pueden también utilizar listas de control de acceso (ACLs) para permitir, denegar, o simplemente identificar el tráfico. Igualmente, un paquete “fabricado a mano” para un ataque podría potencialmente fijar el bit de ACK en 1, y un router podría creer que este paquete es tráfico de la respuesta a una sesión que se originó dentro de la red.

El Switch (Interno): La primer capa de protección en una red es el switch en donde se conectan las computadoras. Una buena práctica es separar las diferentes bocas en varias VLANs forzando el tráfico entre las las mismas y generando un sistema de protección de capa tres del modelo OSI mediante ACLs en los routers. Con una buena implementación de estas VLANs podemos evitar el uso de ARP spoofing, técnicas usadas por muchas herramientas de captura de tráfico como Ettercap y DSNIFF.

CAPA 2: El perímetro del Firewall (Externo): Mediante un Firewall, fácilmente se pueden establecer reglas para hacer cumplir ciertas restricciones y más. En este ejemplo, el Firewall previene cualquier conexión de entrada a la red interna. Así mismo, este permite que los sistemas internos establezcan las conexiones de salida (y permite el tráfico de vuelta solamente para las conexiones iniciadas desde la red interna). También se puede tener un control detallado, habilitando procesos que inspeccionen el tráfico de red en la capa de aplicación. También se puede alterar automáticamente el contenido de cada paquete (como campos de IP) y hacer NAT.

Sistemas de Prevención de Intrusos de red (Interno): Como ya se comentó en el ejemplo anterior, estos IPSs se encuentran constantemente analizando el tráfico de la red, buscando patrones de potenciales ataques, los cuales, en algunos casos, se podrían contrarrestar disparando de manera automática acciones o reglas para actuar preventivamente ante este ataque.

CAPA 3: El Firewall de la DMZ (Externo): A veces, los usuarios externos necesitan tener acceso a ciertos recursos (como un servidor web, o un servidor de correo) que obligadamente los Firewall de la primera línea deben dejar pasar. Estos servidores se ubican en un área que no compromete el resto de la red privada.

Encriptación (Interno): Para asegurarse que la comunicación establecida sea privada a los usuarios que la originaron, y contemplando el posible caso de sufrir una captura de tráfico de red, es conveniente utilizar protocolos encriptados como Secure Shell (SSH) Secure Socket Layer (SSL), los cuales evitan que el tráfico interceptado sea interpretado por el atacante. En este ejemplo, encriptando el tráfico de red resulta casi imposible que un ataque interno obtenga, por ejemplo, las credenciales de logueo y minimiza o prácticamente elimina la posibilidad de sufrir un ataque del tipo *man-in-the-middle* en la organización.

CAP 4: Sistemas de Prevención de Intrusos de red (Externo): Los sistemas de prevención de intrusos (IPS) son dispositivos ubicados en puntos claves de una red interna, los cuales analizan continuamente el tráfico de la misma en búsqueda de patrones conocidos, guardados en una base de datos, para poder avisar y ejecutar acciones a tiempo para combatir actividades potencialmente maliciosas. En capítulos posteriores se describirán con más detalle diferentes herramientas de este tipo.

Autenticación Fuerte (Interno): Este tipo de autenticación se utiliza para proteger activos de alta criticidad para contrarrestar la posibilidad de que alguien utilice la contraseña obtenida de alguna manera (ya sea porque la observó cuando se escribía o por medio de alguna aplicación como keylogers). Una alternativa para implementar esto es utilizar contraseñas del tipo one-time, agregando al típico usuario y clave, una tarjeta Smartcard, un generador de token o una aplicación de software que otorguen un código único para ese logueo. Un buen ejemplo para citar es el caso de la implementación del e-token del home banking del HSBC, un llavero generador de códigos que se modifican constantemente y se utilizan en conjunto con un nombre de usuario (no el número de DNI como en la mayoría de los casos de home banking), una contraseña alfanumérica de más de seis dígitos, y obviamente el código generado por el e-token.

Capa 5: NetFlow (Analizadores de tráfico de alto nivel): Se utiliza para identificar determinados parámetros de una conexión y ubicar patrones conocidos, guardados en una base de datos, de actividades potencialmente anómalas. Los parámetros de conexión que generalmente se apartan son:

- Dirección IP Origen.
- Dirección IP Destino.
- Puerto Origen.
- Puerto Destino
- Protocolo
- Cantidad de Datos Transmitidos.

Capa 6: Antivirus: Otra línea de defensa muy importante se encuentra contenida en el Antivirus, el cual protege al sistema de virus, gusanos y troyanos, especialmente ahora que los sistemas de computadoras superan los límites de nuestras oficinas con el uso de computadores portátiles. Como complemento a este tipo de aplicaciones es recomendable la utilización de programas anti-spyware, anti-rootkit y anti-spam.

Capa 7: Sistemas de Prevención de Intrusos en Host: Los IPS de host corren de forma local en el sistema a proteger. Poseen mejoras significativas con respecto a los antivirus ya que cuentan con la habilidad de detectar código malicioso como keyloggeers o troyanos desde el mismo instante en que el atacante está instalándolos. Un IPS de host como el Cisco Security Agent (CSA) , ademas de lo anteriormente detallado, protege al sistema de otros tipos de ataque como buffer overflow y posee la

posibilidad de alertar al administrador de sistemas mediante el envío de mensajes de texto o e-mails.

6.1.6 ¿Qué no protege un Firewall?

Por un lado los Firewalls no pueden protegernos del tráfico que no pueden analizar, es decir, si existen caminos alternativos para el tráfico de forma que no atraviese el Firewall. Por ejemplo, muchas organizaciones toman extremas precauciones con las conexiones que se puedan producir a través de Internet, pero no ponen el mismo empeño en protegerse de conexiones telefónicas establecidas desde la red Interna.

Por otro lado, pensemos que la mayoría de las violaciones de seguridad modernas tienen que ver con el mal uso de servicios autorizados, como los servicios de acceso a las páginas web, servicios de correo, etc, contra lo que los Firewall poco pueden hacer. Por ejemplo los e-mail con virus o spam no serán detenidos por el Firewall.

Otro factor contra el que no nos pueden proteger es contra el robo de información, evidentemente de nada sirve que se instale una poderosa solución para proteger la red corporativa, si existen empleados que extraen información y la retiran en disquettes o CD.

Respecto de estas consideraciones, es importante recordar que la tecnología por sí sola no soluciona los problemas de seguridad, sino que debemos apoyarla con políticas y procedimientos correctos que sean conocidos y reforzados por toda la organización.

6.1.7 Construcción de un Firewall

En el sentido más general, un sistema cortafuegos consta de software y hardware. El software puede ser propietario, shareware o freeware. Por otro lado, el hardware podrá ser cualquiera que pueda soportar este software.

Actualmente, tres de las tecnologías más utilizadas a la hora de construir sistemas cortafuegos son las siguientes:

- Encaminadores con filtrado de paquetes (*routers*).
- Pasarelas a nivel de aplicación.
- Pasarelas a nivel de circuito.

Routers con filtro de paquetes: Se trata de un dispositivo que encamina el tráfico TCP/IP (encaminador de TCP/IP) sobre la base de una serie de reglas de filtrado que deciden que paquetes se encaminan a través suyo y cuales se descartan.

Las reglas de filtrado se encargan de determinar si a un paquete le está permitido pasar de la parte interna de la red a la parte externa, y viceversa, verificando el tráfico de paquetes legítimo entre ambas partes.

Los encaminadores con filtrado de paquetes, al trabajar a nivel de red, pueden aceptar o denegar paquetes fijándose en las cabeceras del protocolo (IP, UDP, TCP, ...), como pueden ser:

- Direcciones de origen y de destino.
- Tipos de protocolo e indicadores (flags) especiales.
- Puertos de origen y de destino o tipos de mensaje (según el protocolo).
- Contenido de los paquetes.
- Tamaño del paquete.

Una política de denegación por defecto suele ser más costosa de mantener, ya que será necesario que el administrador indique explícitamente todos los servicios que tienen que permanecer abiertos (los demás, por defecto, serán denegados en su totalidad).

En cambio, una política de aceptación por defecto es más sencilla de administrar, pero incrementa el riesgo de permitir ataques contra nuestra red, ya que requiere que el administrador indique explícitamente que paquetes es necesario descartar (los demás, por defecto, serán aceptados en su totalidad).

La construcción de un sistema cortafuegos mediante un encaminador confiltrado de paquetes es realmente económica, ya que generalmente suelen ser construidos con hardware ya disponible. Además, ofrece un alto rendimiento para redes con una carga de tráfico elevada. Adicionalmente, esta tecnología permite la implantación de la mayor parte de las políticas de seguridad necesarias.

Proxy a nivel de aplicación: Una pasarela a nivel de aplicación, conocida también como servidor intermediario (proxy), no encamina paquetes a nivel de red sino que actúa como retransmisor a nivel de aplicación. Los usuarios de la red contactaran con el servidor intermediario, que a su vez estará ofreciendo un servicio proxy asociado a una o más aplicaciones determinadas.

Una pasarela separa completamente el interior del exterior de la red en la capa de enlace, ofreciendo únicamente un conjunto de servicios a nivel de aplicación. Esto permite la autenticación de los usuarios que realizan peticiones de conexión y el análisis de conexiones a nivel de aplicación.

Estas dos características provocan que las pasarelas ofrezcan una mayor seguridad respecto a los filtros de paquetes, presentando un rango de posibilidades muy elevado. Por el contrario, la penalización introducida por estos dispositivos es mucho mayor. En el caso de una gran carga de tráfico en la red, el rendimiento puede llegar a reducirse drásticamente.

En la práctica, las pasarelas y los dispositivos de red con filtrado de paquetes son complementarios. Así, estos dos sistemas se pueden combinar, proporcionando más seguridad y flexibilidad que si se utilizara solamente uno.

El uso de las pasarelas proporciona varios beneficios. De entrada, una pasarela podría permitir el acceso únicamente a aquellos servicios para los que hay un servidor proxy habilitado. Así, si una pasarela contiene servicios intermediarios tan solo para los servicios HTTP y DNS, entonces sólo HTTP y DNS estarán permitidos en la red interna. El resto de servicios serían completamente rechazados.

Otro beneficio del uso de pasarelas es que el protocolo también se puede filtrar, prohibiendo asi el uso de distintos subservicios dentro de un mismo servicio permitido. Por ejemplo, mediante una pasarela que filtrara conexiones FTP, sería posible prohibir únicamente el uso del comando PUT de FTP, dejando habilitado el resto de comandos. Esta característica no sería posible haciendo uso únicamente de filtros de paquetes.

Adicionalmente, los servidores intermediarios también pueden implantar el filtro de conexiones por dirección IP de la misma forma que los filtros de paquetes, ya que la dirección IP está disponible en el ámbito de aplicación en el cual se realizará el filtrado.

Aun obteniendo más control global sobre los servicios vigilados, las pasarelas también presentan algunas problemáticas. Uno de los primeros inconvenientes que hay que destacar es la necesidad de tener que configurar un servidor proxy para cada servicio de la red que se debe vigilar (HTTP, DNS, Telnet, FTP, ...). Además, en el caso de protocolos cliente servidor como, por ejemplo, FTP, pueden llegar a ser necesarios algunos pasos adicionales para conectar el punto final de la comunicación.

Proxy a nivel de circuito: Las pasarelas a nivel de circuito son un híbrido entre los esquemas de filtrado de paquetes y el uso de servidores intermediarios. Una pasarela a nivel de circuito es un dispositivo similar al de pasarela a nivel de aplicación, donde el usuario establece primero una conexión con el sistema cortafuegos y éste establece la conexión con el equipo de destino.

Pero, en contraste con una pasarela tradicional, una pasarela a nivel de circuito opera de manera similar a un filtro de paquetes a nivel de red una vez que la conexión ha sido inicializada.

Zonas desmilitarizadas: En ciertas instalaciones, no es suficiente un único dispositivo cortafuegos. Aquellas redes formadas por múltiples servidores, accesibles públicamente desde el exterior, juntamente con estaciones de trabajo que deberían estar completamente aisladas de conexiones con el exterior, se beneficiarán de la separación entre dos grupos de sistemas cortafuegos.

Los sistemas cortafuegos focalizan las decisiones de seguridad en un único punto de choque, tratando de rechazar cualquier conexión que no esté expresamente permitida.

Mediante un escenario de configuración de filtrado de paquetes en sistemas cortafuegos simples, se podrán aplicar tecnológicamente las decisiones de una política de seguridad definida por la organización. También es posible la construcción de sistemas cortafuegos mediante tecnologías de servidores intermediarios o pasarelas, de manera que todo el tráfico recibido se pueda interpretar a niveles superiores del de red.

Así pues, la utilización de un sistema cortafuegos supone una barrera de control que mantendrá la red protegida de todos aquellos accesos no autorizados, actuando como un punto central de control y facilitando las tareas de administración. Por otro lado, por el hecho de situarse en un punto intermedio, los sistemas cortafuegos ofrecen otras funciones de seguridad interesantes como podrían ser la monitorización de las conexiones de red, el análisis de contenidos, la realización de controles de autenticación adicionales, la construcción de redes privadas virtuales, etc. También pueden realizar funciones no relacionadas directamente con la seguridad de la red, como la traducción de direcciones IP (NAT), la gestión de servicios de red, el control del ancho de banda.

6.1.8 Outsourcing

El outsourcing es la externalización de un determinado proceso en una empresa, es decir se contrata dicha actividad a una empresa externa, en vez de realizar el proceso con personal propio. Las tareas más susceptibles de ser externalizadas son las labores administrativas, la logística, partes de la producción y los sistemas de información. Respecto de esta última tarea podemos mencionar dos esquemas, el housing y hosting, ambos delegan la responsabilidad sobre el mantenimiento de equipos, de software, sistemas de seguridad y conexiones, copias de seguridad, etc.

En un esquema de housing la responsabilidad del proveedor sobre los problemas de seguridad residiría en la administración de la seguridad física de los servidores, de los routers y servidores DNS, sistemas de detección de intrusiones y en la instalación y configuración de Firewalls, es decir, de todos los componentes de conectividad que permiten que nuestros equipos funcionen adecuadamente. Estos componentes son comunes a los otros servers alojados por nuestro proveedor. Esta situación aumenta las probabilidades de "ser blanco" de ataques, ya que un router atacado por un "intruso", con el objetivo de afectar la disponibilidad de un servicio determinado alojado en los sistemas de nuestro proveedor, podría tener como consecuencia directa la indisponibilidad de nuestros servicios. De esta manera seríamos perjudicados por una acción emprendida contra otra empresa que comparte un mismo "sitio" con nosotros.

En el esquema de hosting la situación es un poco más comprometida porque no sólo tendremos que considerar los factores relativos a la seguridad física de un esquema de housing, sino que deberemos considerar también problemáticas de seguridad relativas al sistema operativo y aplicaciones, ya que estos elementos también son compartidos con las otras empresas. Es decir existe un punto particularmente débil en el esquema de hosting: las vulnerabilidades que pudiesen tener los servicios con los que compartimos el servidor. Si un sistema que se encuentra alojado en nuestro servidor posee una vulnerabilidad que permitiese por ejemplo, modificar archivos, estaríamos ante un grave problema de seguridad muy difícil de controlar.

Si la seguridad de nuestros servicios es un tema importante para la empresa, es muy recomendable

que evalúe todas las ventajas y desventajas respecto de la ubicación del mismo.

6.1.9 NAT

Recordemos que anteriormente comentamos que las direcciones IP son un recurso escaso, por este motivo, normalmente las empresas proveedoras de acceso a Internet entregan a sus clientes una dirección IP pública, indispensable para identificar a su computadora en el mundo Internet y excepcionalmente entregan direcciones múltiples. Entonces, NAT es un protocolo diseñado para aumentar el grado de eficiencia con la cual se usan las direcciones IP en Internet.

Por otro lado este protocolo se caracteriza por permitir el uso en nuestras redes de números IP considerados como no ruteables (también llamados privados) y poder igualmente conectarnos a Internet, esta posibilidad la brinda el protocolo al utilizar un mecanismo conocido como traslación, el cual permite que los paquetes con destino a Internet enviados desde una red privada, sean interceptados a fin de que en el paquete IP el número IP no ruteable sea remplazado por uno que sí lo es, con lo cual el paquete IP resultante queda listo para ser ruteado en Internet.

Entonces, las técnicas de NAT contribuyen a la seguridad de la red por dos razones fundamentales, la primera porque las estaciones de trabajo tienen por defecto asignados números IP no ruteables en Internet por lo tanto, nadie externo a su red puede alcanzar directamente sus estaciones de trabajo.

La segunda razón es porque utiliza un mecanismo inequívoco para controlar los paquetes que pueden ingresar desde Internet a la LAN del usuario, este mecanismo es la tabla de traslación, la cual sólo permite que ingresen a la LAN los paquetes que corresponden a respuestas a conexiones iniciadas por una máquina de la red LAN, o acceso a servicios publicados y que cuenten con una entrada inscripta en dicha tabla de traslación, si el paquete que llega no tiene una correspondencia exacta en la tabla de traslación el mismo es descartado. Adicionalmente, este paquete debe llegar dentro del intervalo de tiempo determinado por el sistema para tener abierta una entrada en la tabla de traslaciones.

6.1.10 NAC

Las soluciones de Control de Acceso a Redes (NAC) permiten únicamente a los dispositivos autorizados acceder y operar en una red. Si se aplica correctamente, NAC puede mejorar el perfil de seguridad de una red y reducir los riesgos a los que se enfrentan las empresas.

Los distintos enfoques de NAC han creado un importante y controvertido debate en toda la industria de seguridad de TI. Los beneficios de NAC son claros, aunque todavía no se han realizado de forma generalizada.

Actualmente muchas soluciones de NAC son todavía propuestas costosas que requieren una re-arquitectura de la red y están basadas en un conjunto de tecnologías bypassable. Al mismo tiempo, muchos proveedores ofrecen soluciones NAC que no proporcionan plena cobertura de la red y dejan a las empresas expuestas a vulnerabilidades.

La visibilidad y el descubrimiento de un dispositivo en tiempo real son la base para el proceso NAC, elimina uno de los puntos principales de ataque y permite la cobertura de NAC por toda infraestructura de la red. Si una solución NAC no puede identificar todos los dispositivos conectados a la red en tiempo real, es probable que la seguridad en nuestra red se vea decrementada. NAC debe ser tratada como una metodología de seguridad. Una buena solución NAC proporcionar un conocimiento profundo de la red por perfiles de dispositivos conectados a la red e identificar correctamente si dichos dispositivos son o no autorizados.

Las actuales tecnologías de control de accesos desaparecerán a medida que las empresas vayan adoptando sistemas de autenticación que operen en el extremo de las redes, de acuerdo con una reciente investigación, el mercado NAC se encuentra actualmente sumido en una gran confusión y

que los NACs actuales son meramente preventivos.

6.1.11 PAT

Es una técnica de traslación de direcciones que permite conectar múltiples estaciones de trabajo a Internet con una sola dirección IP ruteable, también se conoce con el nombre de masquerading o PAT. Esta técnica permite entre otras cosas, realizar un uso eficiente de las direcciones IP

Con esta técnica, el dispositivo que realiza el PAT, inscribe en su tabla de traslaciones por cada conexión una entrada que indica:

- El número IP de origen desde el cual se inició la conexión (número IP no ruteable)
- El número de puerto TCP/IP desde el cual se originó la conexión.
- El número de puerto TCP/IP con el cual se reemplazo el número de puerto de origen.

Con los dos primeros datos el sistema identifica hacia dónde tiene que ir dirigido el paquete internamente y con el tercer dato, el cual no se repite en ninguna de las conexiones establecidas hacia el exterior, el sistema diferencia a qué sistema interno, definido con los dos primeros valores, corresponde el paquete IP al momento que éste llega al dispositivo que hace PAT, de esta manera usando los puertos TCP/IP de origen del paquete IP el sistema puede multiplexar las conexiones de múltiples estaciones de trabajo para que en todas las conexiones el número IP no ruteable sea remplazado por una única dirección IP ruteable.

No todo el tráfico es soportado por PAT, en general cualquier tráfico TCP/UDP que no transporte el número IP de origen o destino en la parte de datos del paquete IP permite interactuar a dispositivos que estén protegidos por PAT, por ejemplo http, tftp, telnet, finger, NTP, NFS, rlogin, rsh, rcp, ICMP, FTP, Netbios sobre TCP/IP, Real Audio, CuSeeMe, Stream Works, H.323, Netmeeting, VDOLive, Vxtreme. Por otro lado, no son soportados por PAT, el tráfico IP multicast, Routing table updates, Transferencias de zona DNS, BOOTP, talk, ntalk, SNMP, Netshow.

6.2 TIPOS DE FIREWALL

Analizada la problemática de los Firewalls en la sección anterior, vamos a analizar ahora qué tipos de funcionalidades se necesitan para cubrir las necesidades encontradas y qué tipos de dispositivos pueden albergar dichas funcionalidades.

A partir de la identificación básica de una comunicación, es decir direcciones IP (de Capa 3) y puertos (de Capa 4) de origen y destino en ambos casos, se encuentra que en la práctica la ubicación y manejo de puertos es muy variable y no siempre previsible. Esto presenta un obstáculo para asegurar un buen nivel de seguridad procurando mantener abiertos al paso sólo los puertos estrictamente necesarios en cada conexión.

Surge entonces la necesidad de apelar a más información presente en los encabezamientos de las capas de los paquetes. Mientras alguna de esta información está presente en el encabezamiento IP, otra está en el del TCP, mientras que aparece claro que un conocimiento cabal de lo que hace o puede hacer una aplicación (y por lo tanto un posible ataque) sólo puede obtenerse llegando hasta la Capa de Aplicación de la pila de protocolos.

Tres aproximaciones se consideran en este punto: la más simple, el Filtro de Paquetes implementado generalmente en enrutadores; la más compleja, el Gateway de Aplicación basado en servicios proxy, Filtros Dinámicos o Adaptativos, y algo intermedio que hemos llamado genéricamente Inspección de pleno estado. Los Filtros de Paquetes son muy rápidos pero no ofrecen gran seguridad, mientras que los Gateways de Aplicación son relativamente lentos pero ofrecen el mayor nivel de seguridad posible. Entre tanto, los Filtros Dinámicos son los que han recibido más dedicación en los últimos tiempos en

la búsqueda de optimizar velocidad y seguridad

6.2.1 Filtros estáticos de paquetes

Se implementan a través de las denominadas listas de control de acceso o Access Control Lists (ACL). Esta técnica es la más antigua, además es la más simple y menos costosa para implementar, por lo cual encontraremos que es utilizada en gran cantidad de equipos que ofrecen funcionalidades de Firewall.

Esta técnica opera en la capa 3 y 4 del modelo OSI, donde se analizan ciertos valores contenidos en el paquete (por ejemplo, tipo de protocolo, dirección de origen, dirección de destino y puerto) y en función de éstos y las políticas de acceso, el dispositivo decide si deja pasar el paquete o lo descarta (para obtener mayor información sobre las Listas de Control de Acceso le recomendamos consultar el Capitulo 4.4 - Filtrado de Tráfico).

El principal problema de este tipo de Firewalls es la limitación a la hora de configurar reglas complejas y la poca capacidad para generar "logs" o registros de actividad. Otra limitación fundamental es la imposibilidad de filtrar tráfico en función de información contenida en niveles superiores, tales como URL's, o esquemas de autenticación fuertes. Por otro lado los paquetes son analizados uno a uno sin importar los análisis anteriores, por lo cual hacen un uso más extensivo de los recursos de procesamiento del hardware y no están capacitados para actuar contra ningún tipo de ataque moderno (denial of service, ip spoofing, etc.)

Su funcionamiento es habitualmente muy simple: se analiza la cabecera de cada paquete, y en función de una serie de reglas establecidas previamente, la trama es bloqueada o se le permite seguir su camino; estas reglas suelen contemplar campos como el protocolo utilizado (TCP, UDP, ICMP...), las direcciones fuente y destino, y el puerto destino. Además de la información de cabecera de las tramas, algunas implementaciones de filtrado permiten especificar reglas basadas en la interfaz del router por donde se ha de reenviar el paquete, y también en la interfaz por donde ha llegado hasta nosotros. Si se resolviera utilizar un router como filtro de paquetes, es recomendable bloquear todos los servicios que no se utilicen desde el exterior (ej.: NIS, NFS, X-Window, TFTP, etc.), así como el acceso desde máquinas no confiables hacia nuestra subred.

Cuando se especifican reglas de filtrado estático para las conexiones generadas por clientes de una red interna hacia una red externa (Ej. Internet), se deben permitir también las respuestas de los servidores. Debido a que al momento de crear el filtro estático no se puede conocer el puerto destino, porque es elegido aleatoriamente por el cliente, debemos permitir todos los paquetes que provengan de la red externa y tengan un puerto destino mayor a 1023. Este tipo de filtro demiasiado permisivo no es deseable, ya que podríamos estar permitiendo conexiones desde el exterior a servicios en estaciones internas que estén escuchando en puertos mayores a 1023 (Ej. backdoors).

Una solución a este problema en TCP, son algunas implementaciones de filtrado estático que permiten analizar los campos de código del encabezado TCP (SYN, ACK, FIN, etc.) entonces se podría permitir que sólo ingresen aquellos paquetes que contengan el código ACK=1. De esta forma estaríamos denegando un inicio de conexión (que contiene SYN=1, ACK=0) desde el exterior al interior. Esta solución no se puede implementar en UDP, debido a que no es orientado a conexiones.

6.2.2 Filtros dinámicos o adaptables

La configuración de los filtros dinámicos se basa en la aplicación de listas de acceso extendidas (desarrolladas durante el capitulo 4) para bloquear el tráfico que desea atravesar un dispositivo, generalmente un router. Aquellos usuarios que deseen atravesar el router, previamente deberán autenticarse realizando un Telnet, HTTP o FTP al dispositivo. Una vez que se han autenticado en forma exitosa, el Firewall finaliza la conexión Telnet y genera una nueva ACL que reflejará las restricciones que posea el usuario. Adicionalmente, se pueden configurar perfiles que permitan las

conexiones sólo durante cierto tiempo. Los filtros dinámicos son de utilidad porque a través de ellos podemos aplicar permisos a un usuario o grupo de usuarios, para garantizar un acceso seguro a un host ubicado en una red protegida, es decir, con los filtros dinámicos autentico al usuario y entonces le aplico una lista de acceso que le permite un acceso limitado a través del Firewall, sólo a ciertos hosts o subredes, y por un determinado período de tiempo.

6.2.3 Proxies o Gateways de aplicación

Los Proxies llamados también Gateways de aplicación (Application Gateways) son dispositivos que trabajan solamente en la Capa de Aplicación del modelo OSI. Esta característica es muy importante, porque permite a los proxies realizar filtros más detallados, por ejemplo un proxy HTTP podrá filtrar determinadas páginas, mientras permite otras, para un filtro de paquetes esto es imposible. Si queremos incorporar seguridad a determinadas aplicaciones basándonos en este tipo de sistema, deberemos implementar un proxy que administre las conexiones de cada aplicación. En toda aplicación basada en Proxy se establecerán dos conexiones TCP: una desde el originador del paquete hacia el Proxy y la otra desde el Proxy hacia el punto de destino. Ahora bien, como proporciona seguridad a nuesta red el Proxy, la respuesta es simple: el Proxy sólo deja pasar los paquetes que son la respuesta a una comunicación iniciada por algún usuario de la red, todos los paquetes que no tengan esta característica no podrán ingresar a la red.

Para la aplicación específica para la cual están implementados estos sistemas ofrecen mayor seguridad que un sistema basado en filtros de paquetes, sin embargo, su desventaja radica en que la protección sólo se aplica para la aplicación para la cual el Proxy ha sido instalado, por otro lado sólo existen Proxies creados para un número muy limitado de aplicaciones (por ejemplo HTTP, Telnet y FTP) con lo cual es imposible implementar políticas estrictas de seguridad.

Por otro lado al estar diseñado el Proxy según una arquitectura cliente – servidor, el sistema está expuesto a ataques del tipo denial of service, con lo cual toda la red podría quedarse sin servicio. Finalmente es fácil imaginarnos que su implementación es trabajosa y a medida que crece nuestra red, se torna extremadamente complejo tener un sistema de seguridad basado en proxies.

Existen diferentes implementaciones de Proxies, la más común son los servidores Proxy de capa de aplicación, pero existe otra implementación denominada SOCKS que operan en la capa de transporte. Al operar en capa 4, son independientes de la aplicación utilizada. Actualmente conviven dos versiones: SOCKSv4 y SOCKSv5. La diferencia entre ellas es que la versión 5 soporta autenticación de usuarios.

Algunas de las ventajas a mencionar son:

- Esconden la información de los clientes en la red privada.
- Se controlan los servicios y su uso desde un punto único.
- Si el proxy falla, la red aún así queda protegida.
- Pueden llevar registros de información muy útil.
- Pueden inspeccionar el contenido de las solicitudes al punto de bloquear el acceso a sites o porciones de código cuestionables.

Como contrapartida, algunas de las desventajas a mencionar son:

- Constituyen un punto único de falla.
- Cada servicio requiere de un proxy.
- Requiere modificación en los clientes.

- Los proxies analizan los pedidos de los clientes y de acuerdo a reglas preestablecidas autorizan o deniegan los mismos.
- Para ello abren el datagrama y analizan la dirección, puerto destino y el URL al que hace el pedido.

Suelen ser utilizados para controlar y monitorear el tráfico saliente de la red privada. Pueden llegar a dificultar las conexiones que se realizan a través de ellos. Para optimizar los tiempos de espera, utilizan una memoria intermedia (caché) que almacena los datos que se piden con mayor frecuencia. También pueden realizar un seguimiento exhaustivo de todos los datos que se transfieren, de manera que no quede duda posible acerca de si se ha transmitido determinada información a través de ellos. Asimismo, el administrador del sistema tiene que configurar las aplicaciones para que funcionen correctamente a través del servidor proxy. La forma en que funcionan es relativamente sencilla: cuando se solicita una conexión con una dirección externa a la red privada, el proxy actúa como intermediario. La conexión se realiza con el proxy, y es éste el que se conecta con la dirección remota. De esta forma, todos los datos de la comunicación tienen que pasar por el proxy, que puede almacenar todas las direcciones que se visiten e incluso puede denegar el acceso a algunas de ellas.

El uso de este tipo de dispositivos permite una autenticación mediante contraseña, de forma que sólo se permita realizar conexiones con el exterior de la red a determinados usuarios. Existe un tipo de proxy llamado "Sock", que únicamente tiene la misión de permitir las conexiones a través de un Firewall. No permite autenticación, aunque sí el registro de todas las conexiones realizadas. No obstante, en algunos productos existentes actualmente en el mercado, se ha incluido la característica de autenticación por contraseña de tipo "kerberos".

Firewalls basados en Proxies

Son aquellos dispositivos que estando conectados a ambos perímetros (interior y exterior), no permiten el paso de paquetes IP a través de ellos. Comúnmente, se denomina ip-forwarding desactivado.

La comunicación se produce por medio de programas denominados proxies, que se ejecutan en el Firewall. Este tipo de sistema también se denomina Bastion host. Desde el punto de vista conceptual, este tipo de Firewall funciona a nivel de aplicación.

Un usuario interior que desea hacer uso de un servicio exterior, deberá conectarse primero al Firewall, donde el proxy atenderá su petición, y en función de la configuración en dicho Firewall, se conectará al servicio exterior solicitado y hará de "puente" entre el servicio exterior y el usuario interior. Es importante notar que para la utilización de un servicio externo, han de establecerse dos (2) conexiones o sockets, una desde la máquina interior hasta el Firewall, y otra desde el Firewall hasta la máquina que albergue el servicio exterior.

En el caso de este tipo de Firewalls, los programas clientes deben estar configurados para redirigir las peticiones al Firewall, en lugar de al host final. Esto es común en navegadores WWW, como Netscape o Internet Explorer, y en clientes FTP, como WS_FTP y otros. En cambio, aplicaciones tipo TELNET, no suelen incluir este tipo de soporte, y para ello, lo habitual es conectar directamente con el Firewall y desde allí, el proxy permite especificar el destino final de la aplicación telnet en cuestión.

La capacidad de logging o registro de actividad es mucho mayor con este tipo de dispositivos. La información típica registrada por estos sistemas, va desde el nombre de usuario que ha conseguido autenticarse satisfactoriamente, hasta los nombres y tamaños de ficheros transmitidos vía FTP, pasando por los URL's solicitados a través del proxy HTTP.

Asimismo, un proxy puede estar basado en un programa (Layer 7 modelo OSI) que permite o niega el acceso a una aplicación determinada entre dos redes. Los clientes proxy se comunican sólo con los servidores proxy, que autorizan las peticiones y las envían a los servidores reales, o las deniegan y

las devuelven a quien las solicitó. En tal sentido, pueden escucharse definiciones que tipifican a los proxies como "intermediarios" entre los usuarios (normalmente de una red local) e Internet. No obstante, también existen en el mercado proxies basados en un dispositivo de hardware

Es por ello, que una de las funcionalidades reales de un Proxy es recibir peticiones de usuarios y redirigirlas a Internet. La ventaja que presenta es que con una única conexión a Internet se posibilita conectar varios usuarios.

Funcionalidades Asociadas

Normalmente, un proxy es a su vez un servidor de caché. La función de "la memoria caché" es almacenar las páginas Web a las que se accede más asiduamente en una memoria. Así cuando un usuario quiere acceder a Internet, accede a través del Proxy, que mirará en la caché para ver si tiene la página a la cual quiere acceder el usuario. Si es así, le devolverá la página de la caché y si no, será el Proxy el que acceda a Internet, obtenga la página y la envíe al usuario. Con la caché se aceleran en gran medida los accesos a Internet, sobre todo si los usuarios suelen acceder habitualmente a las mismas páginas.

El Proxy es "transparente" al usuario, los empleados en una empresa deberán configurar el navegador especificando que acceden a Internet a través de un Proxy (deberá indicarse la dirección IP del proxy y el puerto por el que se accederá).

Otros proxies recientemente aparecidos en el mercado realizan además funciones de filtrado, como por ejemplo, dejar que un usuario determinado acceda a unas ciertas páginas de Internet o que no acceda a ninguna. Con esta función es posible configurar una red local en la que existan usuarios a los que se les permita salir a Internet, otros a los que se les permita enviar correo, pero no salir a Internet y otros que no tengan acceso a Internet. Esta característica muchas veces hace que los proxies sean confundidos con un Firewall.

El Proxy y el Firewall son diferentes, pero no estaría mal que estuvieran combinados. El Proxy se usa para redirigir las peticiones que recibe de varios usuarios a Internet de forma transparente y se encarga de devolverles las respuestas (ejemplo: las páginas Web). Asimismo pueden ser utilizados para FTP, POP3, SMTP, IMAP, TELNET, etc.

El firewall sin embargo, es únicamente un método de protección de la red local (o de una PC personal), con el que es posible "cerrar" o "abrir" ciertos puertos, IPs, aplicaciones, etc.

6.2.4 Inspección de pleno estado (Stateful)

La Inspección de pleno estado (Stateful Inspection) es una técnica que trabaja en las 3 capas superiores del modelo TCP/IP, es decir: la Capa de Red, la Capa de Transporte y la Capa de Aplicación. Por otro lado los Firewalls que tienen implementado este mecanismo de seguridad se caracterizan por mantener una tabla denominada "stateful inspection" con las sesiones TCP y las "pseudo" sesiones UDP activas, en cada entrada de esta tabla se va almacenando la dirección IP de origen, de destino, los puertos de origen y destino y finalmente banderas y secuencia del paquete TCP, de esta forma el sistema sólo necesita comparar con las políticas de acceso el primer paquete que llega y el resto si continúa la secuencia de una misma comunicación lo deja pasar. Por otro lado gracias a la capacidad de recordar las sesiones anteriores y la posibilidad de analizar las capas de transporte y aplicación, hacen que el sistema pueda detectar una serie de ataques que hasta antes de la existencia de esta técnica no era posible hacerlo.

Además, los Firewalls basados en Stateful Inspection pueden autenticar los usuarios que establecen las conexiones, pueden determinar si un paquete que dice ser del tipo http realmente transporta este tipo de tráfico e inclusive pueden denegar una conexión en función del URL, como se puede ver tienen una mayor profundidad en sus características de filtrado a costa de un uso mayor de recursos.

6.3 ARQUITECTURAS DE IMPLEMENTACIÓN

De acuerdo al diseño de nuestra red y los elementos de seguridad que incorporemos, podemos definir las siguientes arquitecturas de Firewall:

- Gateway de doble conexión.
- Host protegido.
- Subred protegida.

Todas estas arquietecturas persiguen el mismo objetivo, controlar el acceso entre nuestra red interna y una red externa, asociada con un ambiente inseguro de cuyas amenazas nos queremos proteger. Antes de ver en detalle estos diseños, creemos conveniente definir el concepto de bastion host, debido a que se utilizará en varias oportunidades. Un bastion host, normalmente es un servidor donde se ejecutan procesos que son considerados críticos para la seguridad de la red, por este motivo su configuración se realiza pensando especialmente en la seguridad tanto lógica como física. En general posee una versión segurizada del sistema operativo, donde se han habilitado solamente los servicios esenciales, entre ellos el servicio de auditoría que debe ser revisado periódicamente por el administrador. Un ejemplo de su aplicación lo podemos encontrar en los proxies, quienes deberían implementarse siempre sobre bastion hosts.

6.3.1 Gateway de doble conexión

Una implementación de Firewall a través de un gateway de doble conexión (dual-homed gateway) se obtiene instalando un sistema segurizado entre la red privada e Internet, es altamente recomendable que este sistema tenga deshabilitado el ruteo IP. De esta manera, los hosts de la red interna e internet no se pueden comunicar directamente, sino que deben hacerlo a través del gateway La forma en que el administrador configura el acceso entre la red interna y la red externa y las capacidades de análisis y filtrado del gateway determinan las posibilidades de control y la facilidad de uso del sistema, por ejemplo podría instalar un sistema sofisticado con stateful inspection, complementado con un proxy para los servicios que desee habilitar. En general la política a implementar en este caso será "todo lo que no está permitido está prohibido", así los usuarios podrán solamente acceder a los servicios de Internet para los que exista un gateway configurado.

6.3.2 Host protegido

Una arquitectura del tipo "Screened Host" o host protegido, provee servicios a las estaciones a través de un sistema que está localizado en la red interna, que generalmente se denomina Bastion Host, donde se implementan proxies para las aplicaciones autorizadas. La arquitectura se completa agregando funciones de filtrado de paquetes al Firewall que nos conecta con la red exterior. Los paquetes filtrados por este Firewall son procesados de tal manera que el "Bastion Host" es la única máquina de la red interna con la que los host de la red externa pueden abrir conexiones, y además sólo cierto tipo de conexiones son permitidas. Por otro lado, el filtrado de paquetes, también debe permitirle al "Bastion Host" abrir conexiones con la red exterior. La configuración del filtrado de paquetes en el Firewall, debería combinarse con el o los servicios proxies implementados en el bastion host, de manera que se pueden brindar diferentes servicios: algunos pueden ser controlados con el filtrado paquetes, mientras que otros a través del proxy.

Existen algunas desventajas en una implementación de este tipo; la principal es que si un ataque vulnera el "Bastion Host", puede tener acceso a la red Interna o provocar una denegación de ciertos servicios.

6.3.3 Subred protegida (DMZ)

La arquitectura Screened Subnet, también conocida como red perimétrica, De-Militarized Zone o simplemente DMZ, añade un nivel de seguridad en las arquitecturas de Firewalls, situando una subred (la DMZ) entre las redes externa e interna, de forma que se consiguen reducir los efectos de un ataque exitoso al Bastion Host. En el diseño anterior, toda la seguridad se centra en el bastión de forma que si la seguridad del mismo se ve comprometida, la amenaza se podría extender automáticamente al resto de la red. Como el sistema bastión es un objetivo interesante para muchos piratas, la arquitectura DMZ intenta aislarlo en una red perimétrica, de forma tal que, si un intruso lograra acceder a este sistema, no consiga un acceso total a la red interna.

Screened subnet es la arquitectura más segura, pero también la más compleja. Se utilizan dos Firewalls denominados exterior e interior, conectados ambos a la red perimétrica. En esta red perimétrica se incluye el Bastion Host, pero también se podrían incluir otros sistemas que requieran un acceso controlado del exterior como por ejemplo el webserver o webmail, que serían los únicos elementos visibles desde fuera de nuestra red .

El Firewall exterior tiene como misión bloquear el tráfico no deseado en ambos sentidos (hacia la red perimétrica y hacia la red externa), mientras que el interior hace lo mismo pero con el tráfico entre la red interna y la perimétrica; de esta forma, un atacante habría de romper la seguridad de ambos dispositivos para acceder a la red protegida. Incluso es posible; si se desean mayores niveles de seguridad; definir varias redes perimétricas en serie, situando los servicios que requieran de menor fiabilidad en las redes más externas; así, el atacante habrá de saltar por todas y cada una de ellas para acceder a todos los sistemas de la empresa.

Un problema asociado con este diseño, es que la mayor parte de la seguridad reside en los Firewalls utilizados; como hemos dicho antes, las reglas de análisis y filtrado sobre estos elementos pueden ser complicadas de configurar y comprobar, lo que puede dar lugar a errores que abran importantes brechas de seguridad en toda la infraestructura de la empresa.

6.3 FIREWALLS PERSONALES

En las secciones siguientes analizaremos los Firewalls personales, se trata de una categoría relativamente nueva, que surgió como respuesta a las necesidades de seguridad de los usuarios de PC para entornos de banda ancha y navegación en Internet o en el entorno corporativo. En este último caso el Firewall personal es utilizado por los administradores en caso de necesitar un nivel de protección adicional para ciertas PC o servidores considerados muy importantes.

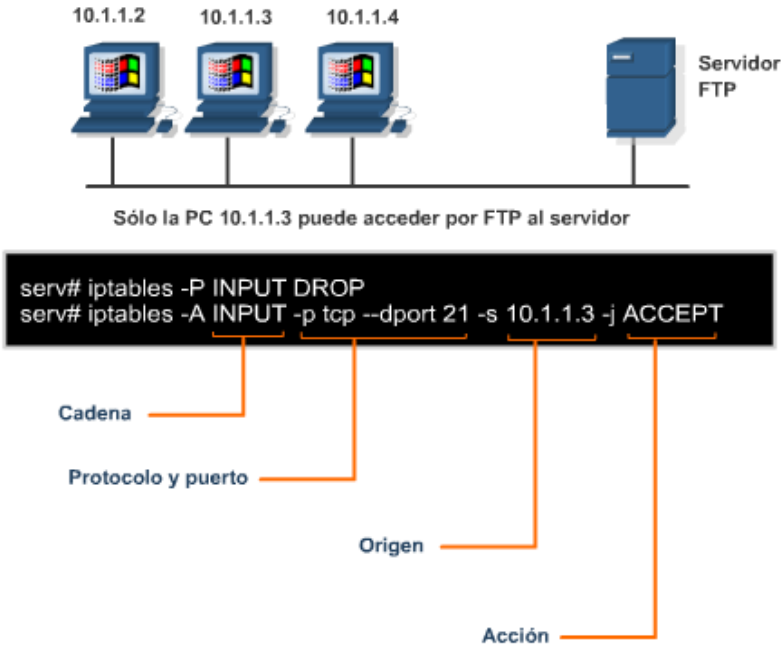
A pesar de que los Firewalls personales son muy sencillos de operar, hay muchas consideraciones a tener en cuenta según el escenario donde se utilicen. Quizás el escenario más simple sea el de un usuario con un único PC conectado a Internet, donde el Firewall protege ante cualquier intento de conexión proveniente de Internet que no haya sido pedido por el usuario. Pero la situación es más complicada cuando el usuario trabaja en una pequeña red y, además del acceso a Internet, debe conectarse a otros equipos, impresoras, etc. Estos casos exigen un determinado conocimiento de los programas y conexiones, muchas veces más allá del usuario promedio.

Si el usuario sin conocimiento avanza en la configuración se puede encontrar con dos escenarios, por un lado puede suceder que el Firewall este configurado en forma permisiva, dejando pasar más tráfico del que debería, con lo cual el Firewall no nos brindaría la protección que deseamos, y por otro lado podría denegar tráfico necesario para el funcionamiento normal de la PC con lo cual el Firewall estaría impidiendo que trabajemos correctamente.

Los Firewalls personales están diseñados para brindar la máxima seguridad posible, haciendo un balance entre el nivel de protección, facilidad de uso y mantenimiento. La mayoría tienen asistentes de configuración, así como también varias configuraciones predeterminadas que ayudan a mantener un alto nivel de seguridad sin perder funcionalidad. Muchos de ellos poseen servicios de actualización

automática y suman capacidades de detección de tráfico malicioso, y algunos incluso permiten bloquear los avisos pop-up tan comunes en muchos sitios de Internet.

Todavía los productos de Firewall personal están más avanzados en la plataforma Windows, aunque todas las distribuciones de Linux tienen la posibilidad de utilizar el Firewall propio del sistema operativo, denominado “ipchains“ o “iptables“ dependiendo las versiones.



6.3.1 Políticas de configuración

Una característica común a todos los productos es la capacidad que tienen de “ir aprendiendo“ las reglas necesarias junto con el usuario, de modo que cuando detectan un tipo de tráfico nuevo “preguntan“ lo que deben hacer. Las opciones siempre son “permitir“ o “prohibir“ un determinado intento de conexión. Esta capacidad es muy importante, porque permite al usuario estar al tanto de todo lo que está ocurriendo en su PC con respecto a la entrada y salida de datos de su equipo.

La política por defecto de estos productos es "todo lo que no está permitido está prohibido", entonces al comenzar existirá solamente una regla que denegará todas las conexiones y como comentamos anteriormente, debemos encargarnos de generar las reglas para permitir las conexiones autorizadas y denegar aquellas que no sean necesarias.

6.4 SISTEMA DE DETECCIÓN DE INTRUSIONES (IDS)

Los sistemas de detección de intrusiones (IDS) proporcionan seguridad a la empresa protegiendo la red de ataques y amenazas tanto internas como externas. Realizan un análisis on-line del tráfico y pueden tomar medidas sobre los paquetes y flujos que violan las normas de seguridad configuradas o representan una actividad malintencionada contra la red. Es decir, los IDS pueden responder en forma automática a las amenazas de hosts internos o externos. Veremos a continuación sus funciones principales, las tecnologías de análisis y detección de intrusiones utilizadas y las arquitecturas de implementación.

La filosofía de los sistemas de detección de intrusiones consiste en la protección basada en la vigilancia, con el objetivo de prevenir y reducir al máximo las posibles consecuencias de un ataque. Para ello es necesario cumplir los siguientes objetivos:

- Identificación y Detección precisa de las amenazas y situaciones susceptibles de constituir un ataque. Existen diversas técnicas, como las que se basan en patrones establecidos, las técnicas heurísticas, o técnicas basadas en análisis de anomalías.
- Investigación inteligente de las amenazas para filtrar y descartar las falsas alarmas o clasificarlas según el riesgo que conllevan las amenazas.
- Sistema de Gestión intuitivo, sencillo y flexible que informe de las amenazas más relevantes.

El Firewall es una herramienta de seguridad informática basada en la aplicación de un sistema de restricciones y excepciones. Es el equivalente a instalar una cerca alrededor de una propiedad con un custodio en la puerta de acceso. Logra mantener a la mayoría de las personas alejadas, pero no puede decir qué es lo que está pasando dentro del complejo. Los sistemas de detección de intrusiones son los equivalentes a los equipos de video y a los sistemas de alarma contra ladrones. Estos guardan la información que reciben y la analizan para detectar patrones de comportamiento sospechoso, retomando el ejemplo de seguridad física, operan de una forma parecida a un custodio que recorre los puestos y analiza las imágenes que vienen de las cámaras de seguridad

6.4.1 Funciones y ventajas

Las siguientes son algunas funciones y ventajas asociadas a los IDSs:

- **Monitorización**: cuentan con métodos para monitorizar y analizar, tanto los eventos del sistema como el comportamiento de los usuarios.
- **Claridad**: extraen los datos más relevantes de entre grandes cantidades de datos de eventos de auditoría, lo que facilita el trabajo del auditor de seguridad. Para ello suelen utilizar diversas técnicas de filtrado estadísticas.
- **Registro**: La mayoría de los IDSs proporciona no sólo métodos para registrar su propia actividad, sino que permiten emitir informes sobre los eventos más importantes ocurridos en un determinado período de tiempo.
- **Comprobación continua**: crean un modelo sobre el estado del sistema, y comparan los archivos y objetos para determinar si han habido cambios con respecto a ese modelo. Se utilizan para realizar los chequeos de integridad a través de un proceso por análisis estadístico.
- **Ataques conocidos**: los IDSs basados en la detección de usos indebidos pueden reconocer ataques que coinciden con patrones que se almacenan en su base de conocimientos (firmas).
- **Ataques no conocidos**: normalmente utilizan técnicas estadísticas para elaborar patrones de actividad y contrastarlas con la actividad normal, detectando situaciones desconocidas, que pueden estar asociadas con amenazas.
- **Tiempo real**: la mayoría de los productos de detección de intrusiones actuales utilizan mecanismos de análisis y registro en tiempo real.
- **Alarmas**: comunican alarmas a los responsables cuando se produce una situación anormal, como una intrusión. Las opciones para hacer esto son bastante variadas, por ejemplo, se puede registrar un evento de sistema, o enviar una notificación vía correo electrónico.
- **Seguridad básica**: proporcionan información sobre las políticas de seguridad por defecto, así como métodos para corregir los posibles errores de configuración de forma automática.
- **Actualización**: la mayoría de los productos de detección de intrusiones basados en patrones de ataques contemplan la posibilidad de actualizar con frecuencia sus bases de conocimiento. Muchos de ellos permiten programar este proceso, que suele realizarse periódicamente

mediante comunicación cifrada.

- **Autoconfiguración**: Los IDS no solamente permiten resetear conexiones, sino también modificar listas de control de acceso en routers o Firewalls a fin de bloquear tráfico malicioso.

6.4.2 Limitaciones e inconvenientes

Estas son algunas de las cosas que los IDSs no hacen, además de varios de sus inconvenientes:

- Solución definitiva: los problemas de seguridad pueden originarse por múltiples motivos. No existe ninguna solución única que los resuelva todos. Los sistemas de detección de intrusiones no son una excepción. No obstante, aportan una serie de características únicas que los convierten en herramientas de gran ayuda en muchos entornos.
- Falsos positivos: uno de los inconvenientes más populares en la detección de intrusiones es el de las falsas alarmas; falsos positivos y falsos negativos. Los primeros consisten en aquellas alarmas que tienen lugar cuando en realidad no se está produciendo ninguna intrusión. Por ejemplo, los detectores de anomalías pueden reconocer como hostil la aparición de un nuevo tipo de tráfico, provocado por la reciente instalación de un nuevo servicio, cuando en realidad la situación es normal. Lo negativo de esta cuestión es que la continua aparición de falsos positivos puede hacer que un administrador acabe ignorando las alarmas, que es igual de negativo que no recibirlas.
- Falsos negativos: se producen cuando no se emite el correspondiente aviso, ante un ataque o intrusión. Por ejemplo, cuando un atacante utiliza una técnica nueva, un ataque modificado basado en alguno ya existente, un ataque especializado contra este tipo de sistemas, o cuando un detector de anomalías es "entrenado" de forma progresiva por un intruso, para que interprete una acción hostil como normal, son algunos ejemplos en los que pueden ocurrir falsos negativos.
- Defensa ante nuevos ataques: en la mayoría de los casos, no pueden detectar ataques de reciente aparición, o variantes de ataques existentes. Esto ocurre con la mayoría de los productos que suelen utilizar detección de usos indebidos basada en reglas o patrones de ataques. La detección de anomalías, dada la naturaleza de su análisis, permite ampliar el rango de detección de este tipo de ataques, pero no los reconoce a todos.
- Defensa ante ataques sofisticados: estos sistemas aún no están preparados para identificar ataques demasiado sofisticados, realizados por atacantes expertos, que en algunas ocasiones utilizan técnicas de fragmentación de paquetes o incluso protocolos propios. En este punto, sigue siendo necesaria la intervención humana.
- Conocimiento de cada situación: estos sistemas no conocen de antemano las particularidades de cada entorno en que son implementados. Es el responsable de seguridad quien debe configurarlos, y adaptarlos a cada situación progresivamente.
- Entornos conmutados: los detectores de intrusiones basados en red no trabajan bien en entornos de red que utilicen switches. Estos dispositivos sólo les envían el tráfico de red que va destinado a ellos mismos, dificultando las tareas de monitorización del tráfico global de la red.

6.4.3 Tipos de análisis

Proceso por análisis de patrones: Algunos IDS pueden identificar usos indebidos o ataques conocidos utilizando firmas para detectar patrones de uso incorrecto en el tráfico de la red. El IDS actúa como un sensor de la detección de intrusiones en línea, observando paquetes y sesiones a medida que fluyen a través del Firewall, rastreando cada una de ellas y analizando si concuerdan con

cualquiera de las firmas IDS. Cuando detecta una actividad sospechosa, pueden responder antes de que se pueda poner en peligro la seguridad de la red. Además, el administrador de la red puede configurar el sistema IDS para que elija la respuesta apropiada ante diferentes amenazas, por ejemplo en algunos casos bastará con informar al responsable de seguridad la situación vía e-mail, pero en otros será conveniente que además bloquee la conexión asociada.

Proceso por análisis estadístico: Para detectar ataques no conocidos, normalmente se utilizan técnicas estadísticas que permiten elaborar patrones de actividad y contrastarlos con la actividad normal, detectando de esta manera posibles anomalías. Aunque poco desarrollado en la práctica, este enfoque tiene ilimitadas posibilidades. Los métodos basados en redes neuronales, algoritmos genéticos, minería de datos o los relacionados con el sistema inmune biológico, son tan sólo algunos de los utilizados en la detección de anomalías. Todos ellos han dado resultados satisfactorios.

Proceso por análisis de integridad: Permiten detectar cambios en los archivos u objetos, para esto crean un modelo sobre el estado del sistema, y comparan los cambios posteriores con respecto a ese modelo. Este es el método utilizado por las herramientas de chequeo de integridad de archivos, que utilizan mecanismos robustos de encriptación, como las funciones hash.

6.4.4 NIDS (Monitoreo basado en red)

Estos monitores actúan sobre un segmento de red capturando y analizando los paquetes que circulan, buscando patrones que supongan algún tipo de ataque. Actúan mediante la utilización de un dispositivo de red configurado en modo promiscuo (es decir, "ven" todos los paquetes que circulan por un segmento de red aunque estos no vayan dirigidos a él mismo).

La implementación del monitoreo basado en red o NIDS, implica la localización de dispositivos de sondeo o Sensores en determinados segmentos de la red, quienes se encargarán de capturar y analizar el tráfico en busca de actividades maliciosas o no autorizadas en tiempo real, y podrán tomar medidas preventivas cuando sea necesario.

Los sensores deben ser desplegados en puntos críticos de la red de manera que los administradores de seguridad puedan supervisar los eventos de toda la red mientras se está desarrollando, independientemente de la ubicación del objetivo del ataque.

El tipo de respuesta que el NIDS puede adoptar dependerá de su configuración, pero las mismas podrán pertenecer a dos categorías, respuestas pasivas o respuestas activas. Entre las aplicaciones más comunes usadas en esta área, se destaca ***Snort***

Snort es un sniffer de paquetes y un detector de intrusos basado en red (se monitoriza todo un dominio de colisión NIDS). Es un software muy flexible que ofrece capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas como lo es MySQL. Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida. Así mismo existen herramientas de terceros para mostrar informes en tiempo real (ACID) o para convertirlo en un Sistema Detector y Preventor de Intrusos.

Este IDS implementa un lenguaje de creación de reglas flexible, potente y sencillo. Durante su instalación ya nos provee de cientos de filtros o reglas para backdoor, DDoS, finger, FTP, ataques web, CGI, Nmap.

Puede funcionar como sniffer (podemos ver en consola y en tiempo real qué ocurre en nuestra red, todo nuestro tráfico), registro de paquetes (permite guardar en un archivo los logs para su posterior análisis, un análisis offline) o como un IDS normal (en este caso NIDS). Cuando un paquete coincide con algún patrón establecido en las reglas de configuración, se logea. Así se sabe cuando, de donde y

cómo se produjo el ataque.

Aún cuando tcpdump es considerada una herramienta de auditoría muy útil, no se considera un verdadero IDS puesto que no analiza ni señala paquetes por anomalías. tcpdump imprime toda la información de paquetes a la salida en pantalla o a un archivo de registro sin ningún tipo de análisis. Un verdadero IDS analiza los paquetes, marca las transmisiones que sean potencialmente maliciosas y las almacena en un registro formateado, así, Snort utiliza la librería estándar libcap y tcpdump como registro de paquetes en el fondo.

Snort está disponible bajo licencia GPL, gratuito y funciona bajo plataformas Windows y UNIX/Linux. Dispone de una gran cantidad de filtros o patrones ya predefinidos, así como actualizaciones constantes ante casos de ataques, barridos o vulnerabilidades que vayan siendo detectadas a través de los distintos boletines de seguridad.

La característica más apreciada de Snort, además de su funcionalidad, es su subsistema flexible de firmas de ataques. Snort tiene una base de datos de ataques que se está actualizando constantemente y a la cual se puede añadir o actualizar a través de la Internet. Los usuarios pueden crear 'firmas' basadas en las características de los nuevos ataques de red y enviarlas a la lista de correo de firmas de Snort, para que así todos los usuarios de Snort se puedan beneficiar. Esta ética de comunidad y compartir ha convertido a Snort en uno de los IDSes basados en red más populares, actualizados y robustos.

Respuestas Pasivas: Consiste en el tipo de respuesta más común a la mayoría de las intrusiones, siendo en general las más fáciles de implementar. Entre las respuestas más comunes, encontramos:

- *Registro de eventos (logging)*
- *Notificaciones*

Respuestas Activas: Involucra tomar una acción específica ante un ataque o amenaza determinada. El objetivo consiste en adoptar una acción o conjunto de acciones inmediatas que posibiliten minimizar el potencial impacto de un incidente. Este tipo de respuesta requiere una planificación minuciosa, que comprenda un análisis de la situación de cada evento en conjunto con políticas de seguridad claras y concretas. Entre las respuestas más comunes, encontramos:

- Descarte de paquetes
- Bloqueo de puertos
- Terminación de conexiones, procesos o sesiones
- Ejecución de cambios en la configuración de dispositivos de borde (Firewalls y Routers)

6.4.5 HIDS (Monitoreo basado en host)

Permite realizar la auditoría de los sistemas de archivos, recursos y logs de los hosts donde están instalados. Una ventaja del monitoreo basado en hosts es que puede supervisar los procesos del sistema operativo y proteger los recursos críticos. Por ejemplo, puede notificar a los administradores de red cuando algún proceso externo intenta modificar el sistema de archivos y este evento podría ser un intento de instalación de un troyano. Las implementaciones actuales de detección de intrusiones basadas en host, requieren que se instale un software agente en el host para supervisar las actividades y realizar los análisis de detección de intrusiones. Una de las características comunes de todo tipo de HIDS, es la verificación constante de la integridad de archivos claves para el sistema anfitrión, mediante la utilización de checksums de distintos tipos, incluyendo el uso de las conocidas Funciones de Hash. Estos archivos críticos, típicamente DLLs, son blancos comunes de todo tipo de ataque, en los cuales se busca corromper los mismos a fin de crear agujeros de seguridad, que

faciliten la ejecución de código arbitrario, la escalación de privilegios o bien la implantación de troyanos o backdors.

6.4.6 IPS

Los Sistemas de Prevención de Intrusiones (IPS) son dispositivos de hardware o software encargados de analizar el tráfico de red con el objetivo de detectar y responder a posibles ataques o intrusiones. La respuesta típica consiste en descartar los paquetes involucrados en el ataque o modificarlos para que se anule su propósito. Este comportamiento clasifica a los IPS como dispositivos proactivos, debido a su reacción automática ante situaciones anómalas. El comportamiento de los IPS se asemeja al de los Firewalls, ya que ambos toman decisiones con respecto a la aceptación de un paquete. Sin embargo, la diferencia radica en el hecho de que un Firewall basa sus decisiones en los encabezados del paquete entrante, particularmente los propios a la capa de red y transporte del modelo OSI, mientras que un IPS basa sus decisiones no solo en los encabezados del paquete, sino en el contenido del campo de datos. Mientras que un IDS tradicional se limita a detectar y notificar sobre una intrusión, el IPS intenta detener esa intrusión de algún modo. Aunque también existen los IDS con respuestas activas, típicamente un IDS monitorea una red, escuchando el tráfico y reaccionando ante una anormalidad, no siendo muy efectivo ante ataques atómicos, es decir, ataques de un solo paquete. Un IPS, al estar intercalado en la red de modo tal que el tráfico lo atraviesa, puede detectar y anular este tipo de ataque, disminuyendo el tiempo de reacción contra el mismo.

6.4.7 Honeypot (*Honeynet y Honeywall*)

Se llama **honeypot** (en ingles, tarro de miel) a una herramienta usada en el ámbito de la seguridad informática para atraer y analizar el comportamiento de los atacantes en Internet. Parece una contradicción, puesto que la función habitual de las herramientas de seguridad es exactamente la contraria: mantener alejados a los atacantes o impedir sus ataques. Sin embargo, desde hace unos años, se utilizan los honeypots para atraer a atacantes hacia un entorno controlado, e intentar conocer más detalles sobre cómo estos realizan sus ataques, e incluso descubrir nuevas vulnerabilidades.

Lance Spitzner, consultor y analista informático experto en seguridad, construyó a comienzos del año 2000 una red de seis ordenadores en su propia casa. Esta red la diseñó para estudiar el comportamiento y formas de actuación de los atacantes. Fue de los primeros investigadores en adoptar la idea, y hoy es uno de los mayores expertos en honeypots, precursor del proyecto honeynet (www.honeynet.org), en marcha desde 1999, y autor del libro "Honeypots: Tracking Hackers”.

Su sistema estuvo durante casi un año de prueba, desde abril del 2000 a febrero de 2001, guardando toda la información que se generaba. Los resultados hablaban por sí solos: en los momentos de mayor intensidad de los ataques, comprobaba que las vías de acceso más comunes a los equipos de su casa eran escaneadas, desde el exterior de su red, hasta 14 veces al día, utilizando herramientas de ataque automatizadas. Desde entonces, se ha creado toda una comunidad de desarrolladores aglutinados alrededor de honeynet.org que ofrecen todo tipo de herramientas y consejos para utilizar estas herramientas.

Un honeypot puede ser tan simple como un ordenador que ejecuta un programa, que analiza el tráfico que entra y sale de un ordenador hacia Internet, “escuchando” en cualquier número de puertos. El procedimiento consiste en mantener una debilidad o vulnerabilidad en un programa, en el sistema operativo, en el protocolo, o en cualquier otro elemento del equipo susceptible de ser atacado, que motive al atacante a usarlo, de manera que se muestre dispuesto a emplear todas sus habilidades para explotar dicha debilidad y obtener acceso al sistema.

Por otro lado, un honeypot puede ser tan complejo como una completa red de ordenadores completamente funcionales, funcionando bajo distintos sistemas operativos y ofreciendo gran cantidad

de servicios. Cuando algún sistema que está incluido en dicha red sea atacado de alguna forma, se advierte al administrador.

Otra opción muy utilizada es crear honeypots completamente virtuales: programas específicamente diseñados para simular una red, engañar al atacante con direcciones falsas, IP fingidas y ordenadores inexistentes, con el único fin de confundirlo o alimentar el ataque para analizar nuevos métodos. Si algo tienen en común los honeypots es que no guardan ninguna información relevante, y si lo parece, si se muestran contraseñas o datos de usuario, son completamente ficticios.

Los honeypots son clasificados según diferentes categorías:

Honeypots de alta interacción: Suelen ser usados por las compañías en sus redes internas . Estos honeypots están construidos con máquinas reales, o consisten en una sola máquina real con un sistema operativo “normal”, como el que podría utilizar cualquier usuario. Se colocan en la red interna en producción. Si están bien configurados, cualquier intento de acceso a ellos debe suponer una alerta a tener en cuenta. Puesto que no tienen ninguna utilidad más que la de ser atacados, el hecho de que de alguna forma se intente acceder a ese recurso significa por definición que algo no va bien.

Cada interacción con ese honeypot se considera sospechosa por definición. Todo este tráfico debe ser convenientemente monitorizado y almacenado en una zona segura de la red, y a la que un potencial atacante no tenga acceso. Esto es así porque, si se tratase de un ataque real, el intruso podría a su vez borrar todo el tráfico generado por él mismo, las señales que ha ido dejando, con lo que el ataque pasaría desapercibido y el honeypot no tendría utilidad real.

Las ventajas que ofrecen los honeypots de alta interacción es que pueden prevenir ataques de todo tipo. Tanto los conocidos como los desconocidos. Al tratarse de un sistema real, contiene todos los fallos de software conocidos y desconocidos que pueda albergar cualquier otro sistema. Si un atacante intenta aprovechar un fallo desconocido hasta el momento (llamados en el argot “0 day”), será la propia interacción con la máquina, para intentar explotar el fallo, lo que alerte del problema y ayude a descubrir ese nuevo fallo. En contraposición, por ejemplo un detector de intrusos (IDS) basado en firmas, podría alertar en la red de solo intentos de aprovechar fallos o ataques ya conocidos, para los que tiene firmas que le permiten reconocerlos. La ventaja del honeypot es que, sea el ataque nuevo o no, el intento de ataque alertará al administrador, y esto le permitirá estar alerta cuanto antes del potencial peligro.

En este sentido, los honeypots se usan para mitigar los riesgos de las compañías, en el sentido tradicional de uso de las conocidas herramientas defensivas. Lo que la diferencia de los tradicionales cortafuegos o detectores de intrusos es su naturaleza “activa” en vez de pasiva. De modo figurado un honeypot se muestra como un anzuelo, no como un muro de contención para evitar ataques, muy al contrario, busca dichos ataques y se encarga de “entretenerlos”. Muchas compañías lo usan como un valor añadido más a sus elementos de seguridad, como complemento a sus herramientas típicas. Se obtiene así una fácil detección y reconocimiento de los ataques, de forma que pueden elaborar con esos datos estadísticas que ayudan a configurar de manera más efectiva sus herramientas pasivas. Conociendo cuanto antes los problemas de seguridad a los que más se atacan o los nuevos objetivos, más eficazmente podrá defenderse una compañía concreta contra ellos.

Como toda herramienta destinada a mejorar la seguridad, los honeypots tienen sus ventajas e inconvenientes. Su mayor utilidad radica en su simpleza. Al ser un mecanismo cuyo único fin consiste en que intenten aprovechar sus debilidades, no realiza ningún servicio real, y el tráfico que transita a través de él va a ser muy pequeño. Si se detecta tráfico que va o viene hacia el sistema, casi con toda probabilidad va a ser una prueba, escaneo o ataque. El tráfico registrado en un sistema de este tipo es sospechoso por naturaleza, por lo que su gestión y estudio se simplifica en gran medida. Aunque, por supuesto, ocurran “falsos positivos”, expresión que, en este caso, invierte su significado. Si un falso positivo se produce normalmente cuando una actividad sospechosa tomada como ataque no resulta serlo, en el ambiente de los honeypots, el falso positivo sería el tráfico gestionado por la máquina que no representa una amenaza. En esta simpleza de uso de tráfico y recursos, radica su

mayor ventaja. En resumen, poca información, pero muy valiosa.

Entre los problemas que se pueden producir por el trabajo con honeypots, destaca la posibilidad de que se vuelva en contra del administrador. Si no se diseña de una manera absolutamente estudiada, si no se ata cada cabo, si no se aísla convenientemente, el atacante puede acabar comprometiendo un sistema real y llegar a datos valiosos conectados al honeypot.

Honeypots de baja interacción: Suelen ser creados y gestionados por organizaciones dedicadas a la investigación del fraude en Internet, o cualquier tipo de organización que necesite investigar sobre las nuevas amenazas en la red. Son mucho más complejos de administrar y mantener, y la información que reciben debe ser lo más extensa posible, ésta debe ser organizada y analizada para que sea de utilidad.

Se suelen tratar de sistemas específicos que emulan servicios, redes, pilas TCP o cualquier otro aspecto de un sistema real, pero sin serlo. Existe un "meta-sistema" detrás, invisible para el atacante, que está simulando ser cualquier cosa para la que esté programado ser. No tienen que implementar un comportamiento completo de un sistema o servicio. Normalmente simulan ser un servicio, y ofrecen respuesta a un subconjunto de respuestas simple. Por ejemplo, un honeypot que simule ser un servidor de correo, puede simular aceptar conexiones y permitir que se escriba en ellas un correo, aunque nunca llegará a enviarlo realmente.

Normalmente este tipo de honeypots no está destinado a "atrapar" atacantes reales, sino herramientas automatizadas. Un ser humano podría detectar rápidamente si se trata de un servidor real o no, bien por su experiencia o por otras características que le hagan sospechar que no se encuentra en un entorno real. Sin embargo, sistemas automatizados como programas de explotación automática, gusanos, virus, etc., programados específicamente para realizar una acción sobre un servicio, no detectarán nada extraño. Harán su trabajo intentando explotar alguna vulnerabilidad, el honeypot simulará ser explotado, y el administrador del honeypot obtendrá la información que desea.

Este tipo de honeypots, tienen el problema de que en ellos resulta más complejo descubrir nuevos tipos de ataques. Están preparados para simular ciertos servicios que se saben atacados, y a responder de cierta manera para que el ataque crea que ha conseguido su objetivo. Pero en ningún caso puede comportarse de formas para las que no está programado, por ejemplo para simular la explotación de nuevos tipos de amenazas.

Honeymonkeys: Un honeypot puede ser diseñado como un servidor en vez de cómo un equipo es decir, como un sistema (honeypot que hace de servidor) que espera ser contactado con un cliente (equipo). Desde el momento en el que uno de los objetivos de un honeypot es recavar información sobre ataques, surgió un concepto de un honeypot "cliente" que no espere a recibir ataques sino que los genere activamente. Se les llama honeymonkeys.

Desde hace varios años, el vector de ataque más utilizado en Internet es el navegador. Las medidas de seguridad han aumentado y cada vez resulta más difícil aprovechar vulnerabilidades en clientes –programas- de correo electrónico, que venía siendo el vector de ataque más usado. El uso popular de cortafuegos también hizo que cada vez fuese más complicado para atacantes aprovechar vulnerabilidades en el propio sistema operativo. Por tanto, con el traslado a la web de los servicios (foros, chats, etc.), el navegador se convirtió en el objetivo favorito de los atacantes. Con solo visitar una web, se intenta aprovechar todo tipo de vulnerabilidades en el navegador para ejecutar código en el cliente e infectarlo.

Tras este concepto surgen los honeymonkeys. Su función principal , al igual que la de los honeypots, es igualmente detectar nuevos tipos de ataques y fórmulas de infección e igual que los honeypots, están formados por un módulo de "exploración" y un módulo de recogida de datos. Sin embargo en el caso de los honeymonkeys, la exploración se hace activamente a través de navegadores. El honeymonkey funciona como un sistema automático de navegación que visita toda clase de páginas web con el fin de que alguna de ellas intente aprovechar vulnerabilidades en el navegador. Poseen una naturaleza mucho más activa que el honeypot, en el sentido en el que "patrullan" la red como si

fueran un usuario visitando enlaces compulsivamente.

Fue Microsoft quien los bautizó. “Monkey” (mono, en inglés) hace alusión a los saltos y el dinamismo del tipo de acción que realizan. Con este método, al igual que los honeypots, se pueden encontrar nuevos exploits, gusanos, etc., siempre que se analice y procese convenientemente toda la información recogida.

También existe el concepto de **Honeynet**, al que podemos considerar como un conjunto de Honeypots, siendo más tentador para el intruso y posibilitando obtener más información sobre el mismo. Incluso hace más fascinante el ataque al intruso, lo cual incrementa el número de ataques. La función principal, al margen de la de estudiar las herramientas y técnicas de ataque, es la de desviar la atención del atacante de la red real y la de capturar nuevos virus o gusanos para su posterior estudio. Una de las múltiples aplicaciones que tiene es la de poder determinar perfiles de atacantes y ataques.

Son sistemas que deliberadamente se exponen para ser atacados o comprometidos. Estos, no solucionan ningún problema de seguridad, mas bien consisten en una herramienta que nos sirve para conocer las estrategias que se emplean a la hora de vulnerar un sistema.

Constituyen una herramienta muy útil a la hora de conocer, de manera precisa, los ataques que se realizan contra la plataforma de trabajo que disponemos en nuestra red. Así mismo, nos permiten conocer nuevas vulnerabilidades y riesgos en los distintos sistemas operativos, entornos y programas, muchas de las cuales aún no se encuentran debidamente documentadas.

Una **honeywall** es un ordenador configurado para filtrar y observar el tráfico que generan uno o varios honeypots protegiendo al resto de la subred de los ataques de los mismos. Es una parte esencial de una honeynet y cuenta con varios mecanismos para controlar las acciones de los bots capturados. El equipo que hace este papel debe ser invisible para los honeypots con el fin de estudiar en profundidad y sin interferir qué hacen y cómo.

Dado el potencial peligro del uso de honeypots, y a su propia naturaleza, el uso de herramientas virtuales resulta muy conveniente y es ampliamente aceptado. Las ventajas de un sistema virtual sobre uno físico son evidentes:

- Permiten ser restauradas en cuestión de minutos en caso de accidente, desastre o compromiso: la mayoría de sistemas virtuales permiten almacenar un estado “ideal” y volver a él en cualquier momento de manera mucho más rápida que si hubiese que restaurar un sistema físico y devolverlo a un estado anterior.
- Permiten ser portadas a diferentes máquinas físicas que la alojan: los sistemas virtuales, por definición, se ejecutan por igual en cualquier máquina física, que emulan el entorno necesario a través de un programa para poder reproducir el sistema virtual.
- Permiten ahorrar costes: una misma máquina física puede alojar un número indeterminado de máquinas virtuales, tantas como le permitan sus recursos, y con tantos sistemas operativos como se desee.

Las principales herramientas virtuales usadas en honeypots son :

- VMware: se trata del sistema de virtualización más usado y famoso. Puede simular máquinas que ejecutan cualquier sistema operativo y a su vez hacerlo sobre cualquier sistema operativo. Muchas de las utilidades de virtualización que proporciona se ofrecen de forma gratuita, tales como VMWare Player.
- VirtualBox: es un proyecto de Sun, gratuito y de código abierto. Al igual que VMWare, puede

simular máquinas que ejecutan cualquier sistema operativo y a su vez hacerlo sobre cualquier sistema operativo.

- Qemu: proyecto de código abierto que puede usarse tanto como virtualizador como emulador. Disponible solo para entornos Linux. Resulta más complejo de usar que VMWare.
- User-Mode Linux: es una forma de simular un núcleo de Linux “virtual” como si se tratase de un proceso. Solo puede ser ejecutado desde un sistema Linux y sólo puede simular otro kernel, pero resulta muy útil para la puesta en marcha de honeypots.

6.4.8 Arquitecturas de implementación

En general los objetivos y recursos de cada organización indicarán la arquitectura de implementación, pero suele ser recomendable alcanzar una solución basada en el uso conjunto de herramientas de monitoreo basado en red y en hosts. Normalmente se empieza con la instalación de IDS basados en red, porque son más sencillos de instalar y gestionar. Posteriormente, se instalan los IDS basados en host en las máquinas críticas.

Será recomendable completar el esquema con el uso regular de analizadores de vulnerabilidades sobre los IDS y otros elementos de seguridad, de esta manera, se ayuda a mantener la estabilidad y confianza de estos mecanismos.

6.5 REGLAS DE DISEÑO

En esta unidad desarrollaremos los conceptos de diseño definidos en el modelo de seguridad Cisco SAFE. SAFE describe los requerimientos funcionales de las redes actuales. Las diferentes decisiones de diseño pueden variar, dependiendo de las funcionalidades que deseamos implementar en nuestra red. Sin embargo, los siguientes objetivos de diseño, listados de acuerdo a su prioridad, pueden ayudarlo en el proceso de la toma de decisiones:

- Seguridad y mitigación de ataques basada en políticas
- Implementación de seguridad en toda la infraestructura (no sólo en dispositivos de seguridad específicos)
- Instalación de bajo costo
- Administración y reportes seguros
- Autenticación y autorización de los usuarios y administradores a los recursos críticos
- Detección de intrusos en los recursos y subredes críticas

SAFE es ante todo, una arquitectura de seguridad. Debe prevenir que la mayoría de los ataques afecten los recursos más importantes de la red. Los ataques que logren tener éxito en penetrar la primer línea de defensa, o que sean originados desde la red interna, deben ser detectados y contenidos rápidamente para minimizar sus efectos en el resto de la red. Sin embargo, aún siendo segura, la red debe continuar proveyendo los servicios críticos esperados por los usuarios. Una seguridad apropiada y una buena funcionalidad pueden ser provistas al mismo tiempo. La arquitectura SAFE no es una forma revolucionaria de diseñar redes, sino que provee consejos para desarrollar redes seguras.

En muchos puntos del proceso de diseño de redes, es necesario decidir entre una funcionalidad integral de un dispositivo versus la utilización de un dispositivo especializado. La funcionalidad integral es muy atractiva porque se puede implementar en el equipamiento existente, o porque las características pueden interoperar con el resto de los dispositivos para proveer una mejor solución

funcional. Los dispositivos especializados son usados generalmente cuando la funcionalidad requerida es muy avanzada, o las necesidades de performance requieren el uso de un hardware particular. Tome sus decisiones basándose en la capacidad y funcionalidad del dispositivo versus las ventajas de integración del dispositivo. Por ejemplo, la elección entre un router con capacidades de Firewall, o un router más simple con un Firewall separado. A lo largo de esta arquitectura, ambos tipos de sistemas han sido usados. Cuando los requerimientos de diseño no apuntan a una decisión específica, se optó por la funcionalidad integral para reducir el costo global de la solución.

6.5.1 Verificación de accesos

En los sistemas Unix y Linux se tiene a disposición una herramienta que guarda los mensajes enviados por los diferentes servicios y a su vez, los generados por el mismo kernel, fundamental para una lectura de análisis. El mismo corre en forma de demonio (syslogd) el cual se encarga de capturar los mensajes que envía el sistema y guardarlos en diferentes archivos, según su procedencia, generalmente en el directorio /var/log. Para lograr mayor seguridad de estos archivos, el **syslog** puede ser configurado para que los mensajes se envíen a otro servidor y así tener un segundo respaldo de los archivos. **syslog** fue desarrollado por Eric Allman como parte del proyecto Sendmail en la década del 80, y al comprobarse que este era muy útil lo empezaron a utilizar otras aplicaciones hasta convertirse en el utilizado por defecto en casi todas las derivaciones de sistemas Unix y Linux y así estar a punto de lograr ser un estándar documentado en la RFC 3164.

Como protección de estos archivos necesarios para la obtención de información en un análisis de seguridad, se detallan algunos tips para considerar:

- No utilizar los directorios por defecto para guardar los logs ya que son muy conocidos por los atacantes.
- Asegurar que sólo el administrador de la máquina tenga permiso de acceso a estos directorios y archivos .
- Si se envían los mensajes a una máquina remota, tener en cuenta la posibilidad de intercepción de la información .

Como alternativa al ya mencionado syslog, existe una aplicación de características similares a éste, pero que implementa algunas mejoras. El **syslog-ng** es un sistema de logueo flexible y altamente escalable, ideal para crear soluciones de logueo centralizadas. Algunas de las mejores características se detallan a continuación:

- Transferencia de logs de manera fiable desde el host al servidor o servidores remotos, enviados mediante el protocolo TCP asegurando que no haya perdidas de mensajes.
- *Logueo seguro mediante SSL/TLS:* Los mensajes de logs pueden contener información sensible la cual no es conveniente que sea visualizada por terceros. Syslog-ng puede utilizar TLS para encriptar la comunicación. TLS también permite la autenticación mutua entre el cliente y el servidor mediante el uso de certificados X.509.
- *Buffering de mensajes en disco:* Si la conexión de red no se encuentra disponible durante el envío de mensajes, el syslog-ng almacena durante este tiempo los mismos en el disco local hasta que la conexión se reponga. De esta manera no existe pérdida de información ante una falla en la red.
- *Acceso directo a Base de datos:* Conservación de sus mensajes en una base de datos, lo que permite realizar búsquedas y consultas de los mensajes e interoperar con analizadores de logs. Esta aplicación puede interactuar con MySQL, Oracle, PostgreSQL y SQLite.
- *Entornos heterogéneos:* Syslog-ng permite recoger los registros de forma masiva en entornos heterogéneos utilizando diferentes sistemas operativos y plataformas de hardware, incluyendo

Linux, Unix, BSD, Sun Solaris, HP-UX y AIX. Además existe un agente el cual puede transferir registros de Microsoft Windows y almacenarlos en un servidor syslog-ng.

- *Filtrar y clasificar:* Syslog-ng puede ordenar los mensajes de registro basados en su contenido con diversos parámetros, como host de origen, aplicación y prioridad. Filtrados complejos utilizando expresiones regulares y operadores booleanos ofrecen la posibilidad de realizar envíos de los mensajes muy importantes a destinos específicos.
- *Soporte de Ipv4 e Ipv6*: Además, esta aplicación está preparada para trabajar en ambos entornos de red.

En sistemas operativos de Microsoft, existen algunas alternativas como WinSysLog, Syslog Watcher, SyslogIT, etc.

6.5.2 Concepto de modularización

A pesar de que muchas redes han evolucionado a medida que crecían sus requerimientos de IT, la arquitectura SAFE se basa en un diseño modular. El diseño modular tiene dos grandes ventajas: primero, permite que la arquitectura relacione la seguridad entre los diferentes bloques funcionales de la red. En segundo lugar, permite que los diseñadores evaluen e implementen seguridad por módulo, en lugar de intentar completar la arquitectura en un solo paso. El diseño de seguridad de cada módulo se describe de forma separada, pero es validada como una parte del diseño completo.

Muchas redes no se pueden dividir fácilmente en módulos bien definidos. Esta aproximación provee una guía para implementar diferentes funciones de seguridad en toda la red. Los autores no esperan que se diseñen las redes idénticas a los modelos definidos por la arquitectura SAFE, sino que se utilice una combinación de la arquitectura descripta integrada en la red existente.

El diseño SAFE consiste en tres módulos principales : el módulo internet corporativa, el módulo de red interna y el módulo WAN. El módulo de internet corporativa tiene la conexión a Internet y es el punto final de las VPN y servicios públicos (DNS, HTTP, FTP y SMTP). El tráfico dial-in también finaliza en este módulo. El módulo de red interna contiene la infraestructura de switcheado de capa 2 y 3 con los usuarios corporativos, servidores de administración y servidores de Intranet. Desde una perspectiva WAN, existen dos opciones para que los sitios remotos se conecten con la red. La primera es mediante una conexión WAN privada (Punto a punto digital, Frame Relay, etc.) provista por el módulo WAN. La segunda opción es mediante VPNs a través del módulo de internet corporativa.

6.5.3 Módulo WAN

El módulo WAN es incluido sólo cuando se requieren conexiones con sitios remotos a través de redes privadas. Este requerimiento puede suscitarse cuando las necesidades de QoS no pueden ser logradas mediante IPSec VPNs, o cuando se mantienen conexiones WAN antiguas que no han sido migradas a IPSec.

Dispositivos claves:

- Routers: Proveen enrutamiento, control de acceso y mecanismos de QoS.

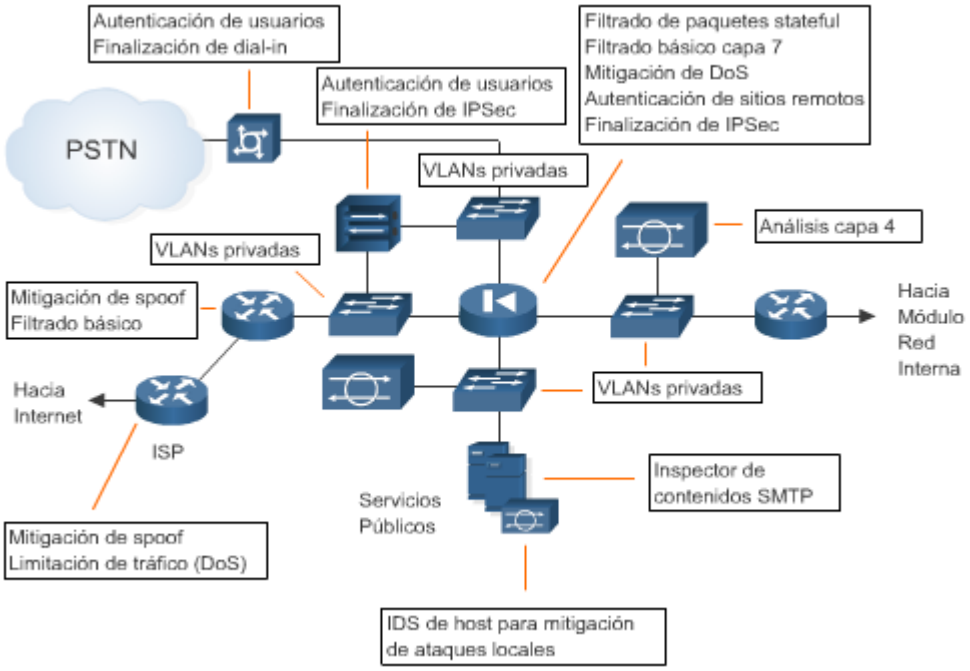
Mitigación de la amenazas:

- Spoofing de direcciones IP: La falsificación de direcciones IP puede ser mitigada a través de filtrado de capa 3. (RFC 19.18y RFC 2827)
- Accesos no autorizados: Un control de acceso simple puede limitar los tipos de protocolos que pueden acceder a cada sucursal.

- Guías de diseño: La cantidad de seguridad que se debe ubicar en el módulo WAN dependerá del nivel de confianza que se tenga de los sitios remotos y del proveedor de servicios. La seguridad es provista utilizando las características de seguridad de los routers. En este diseño se aplican listas de acceso entrantes en la interfaz serial (la conexión WAN). También pueden ser usadas listas de acceso entrantes en las interfaces Ethernet para realizar un mejor control del tráfico que pasa desde la red interna hacia los sitios remotos.

6.5.4 Módulo de Internet corporativa

El objetivo del módulo de Internet corporativa es proveer a los usuarios internos de conectividad con los servicios de Internet, y a los usuarios de Internet acceso a los servicios públicos (HTTP, FTP, SMTP y DNS). Adicionalmente, este módulo finaliza los túneles IPSec de los usuarios y sitios remotos, así como las conexiones dial-in



Dispositivos Claves:

- Servidor Dial-in: Autentica usuarios remotos individuales y finaliza sus conexiones analógicas.
- Servidores DNS: Dan servicio de DNS para los dominios propios a las consultas externas y resuelven todas las consultas internas.
- Servidores FTP/HTTP: Proveen información pública sobre la organización.
- Firewall: Provee protección de recursos y filtrado inteligente de tráfico. Provee seguridad diferenciada para los usuarios remotos. Autentica los sitios remotos de confianza y provee conectividad utilizando túneles IPSec.
- Switches de Capa 2: Proveen conectividad de capa 2.
- NIDS: Proveen monitores de capa 4-7 en los segmentos claves del módulo.
- Servidor SMTP: Actúa como relay entre Internet y los servidores de correo internos. Inspecciona el contenido de los correos (Spam, virus, contenidos).
- Concentrador VPN: Autentica usuarios remotos individuales y finaliza sus túneles IPSec.

- Router de borde: Provee filtrado básico y conectividad de capa 3 hacia Internet.

Mitigación de amenazas:

Los servidores de acceso público son potenciales objetivos de ataques. Las siguientes son las amenazas esperadas y la forma de mitigarlas:

- Acceso no autorizado: Mitigado por filtrado de paquetes en el router de borde y el Firewall corporativo.
- Ataques de capa de aplicación: Mitigado por los IDSs a nivel de host y red.
- Ataques de virus y troyanos: Mitigado por el filtrado de contenidos de e-mail, IDSs de host y antivirus de host.
- Ataques de Passwords: Limitar los servicios disponibles a ataques de fuerza bruta. Sistemas operativos e IDS pueden detectar esta amenaza.
- Denegación de Servicio: Control de tráfico en el router de borde.
- IP spoofing: Filtrado por RFC 2827 y 1918 en el router de borde y en el router de ingreso a la red.
- Packet sniffers: Infraestructura switcheada e IDS de host para limitar la exposición. Control de MACs por puerto para evitar el overflow de la tabla CAM en los switchs.
- Reconocimiento de la red: los IDSs detectan ataques de reconocimiento. Filtrado de protocolos para limitar la fuga de información.
- Explotación de confianza: Modelo de confianza restrictivo para limitar estos ataques

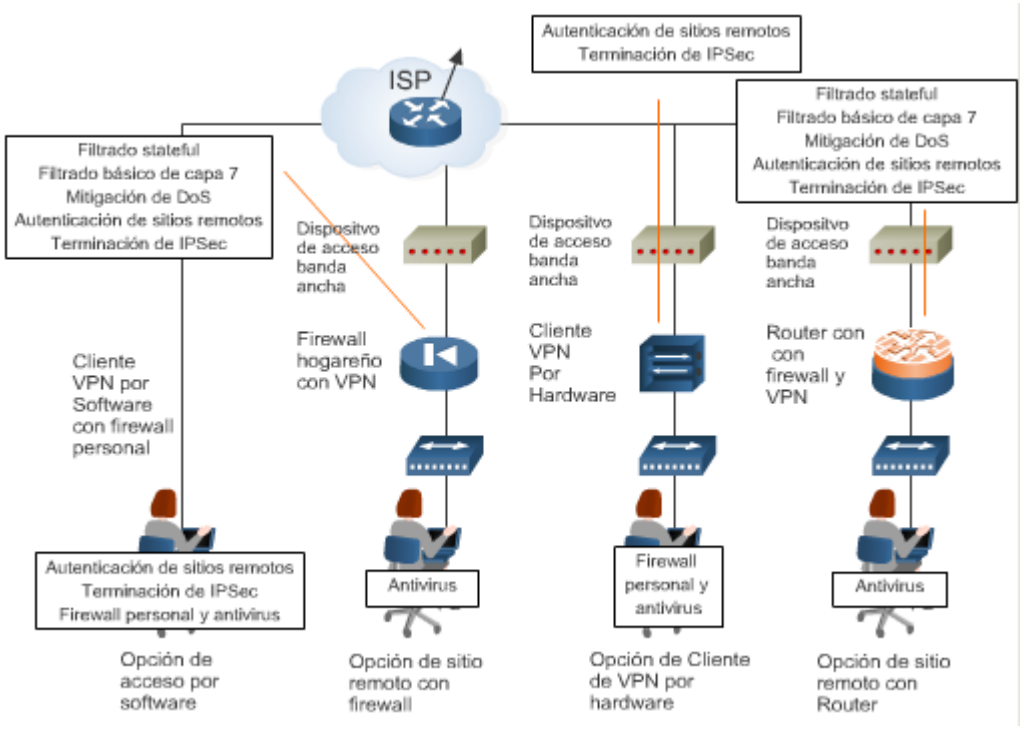
El servicio de acceso remoto y de VPNs también pueden ser objetivos de ataques. Las siguientes son las amenazas esperadas y la forma de mitigarlas:

- Descubrimiento de la topología de red: Listas de control de acceso en el router de ingreso limitan el acceso al concentrador de VPN y al Firewall (cuando finaliza túneles IPSec) sólo para tráfico IKE y ESP.
- Ataques de Password: Uso de One-time passwords (OTP) mitigarán los ataques de fuerza bruta.
- Accesos no autorizados: Servicios de Firewall luego de la desencripción de un paquete previenen tráfico a puertos no autorizados.
- Ataques Man-in-the-middle: Estos ataques son mitigados mediante la encriptación del tráfico remoto.
- Packet sniffers: Infraestructura switcheada para limitar la exposición. Control de MACs por puerto para evitar el overflow de la tabla CAM en los switchs.

6.5.5 Módulo de acceso remoto

Esta sección discute las diferentes opciones para proveer conectividad a los usuarios remotos dentro del diseño de SAFE. La conectividad remota se aplica tanto a los usuarios móviles como a los trabajadores hogareños. El enfoque principal de estos diseños es proveer conectividad desde el sitio remoto a la red central a través de Internet. Las cuatro siguientes opciones incluyen soluciones de sólo software, hardware y software o sólo hardware:

- Opción de acceso por software: Usuario remoto con un cliente de VPN por software y un Firewall personal en la PC.
- Opción de sitio remoto con Firewall: Sitio remoto protegido por un Firewall dedicado que también provee conectividad IPSec a la red central. La conexión a Internet es provista mediante un dispositivo de acceso banda ancha asignado por el ISP (P. Ej: DSL o CableModem).
- Opción de Cliente de VPN por hardware: Sitio remoto utilizando un cliente de VPN por hardware dedicado que provee conectividad IPSec a la red central. La conexión a Internet es provista mediante un dispositivo de acceso banda ancha asignado por el ISP
- Opción de sitio remoto con Router: Sitio remoto utilizando un router que provee servicios de Firewall y de conexiones IPSec. Este router puede conectarse directamente a Internet o utilizar un dispositivo de acceso banda ancha asignado por el ISP



Dispositivos Claves:

- Dispositivo de acceso banda ancha: Provee acceso a la red del proveedor (DSL, cable, etc.).
- Firewall con VPN: Provee túneles encriptados entre el sitio remoto y la red central. Provee protección a nivel de red de los recursos del sitio remoto y filtrado de tráfico stateful.
- Firewall personal: Provee protección a PCs individuales.
- Router con Firewall y VPN: Provee túneles encriptados entre el sitio remoto y la red central. Provee protección a nivel de red de los recursos del sitio remoto y filtrado de tráfico stateful. Puede proveer servicios avanzados como voz o QoS.
- Cliente de VPN por software: Provee túneles encriptados entre PCs individuales y la red central.
- Cliente de VPN por hardware: Provee túneles encriptados entre el sitio remoto y la red central.

Mitigación de amenazas:

- Acceso no autorizado: Mitigado por filtrado e inspección stateful en el router o Firewall remoto, o a través del control de acceso a las aplicaciones via Firewalls personales.
- Reconocimiento de la red: Filtrado de protocolos en el dispositivo del sitio remoto para limitar su efectividad.
- Ataques de virus y troyanos: Mitigado por el filtrado de contenidos de e-mail, IDSs de host y antivirus de host.
- IP spoofing: Filtrado por RFC 2827 y 1918 en el router de borde y en el router del sitio remoto.
- Ataques Man-in-the-middle: Estos ataques son mitigados mediante la encriptación del tráfico remoto.

Las conexiones RAS y VPN contra el concentrador deben pasar por el Firewall antes de permitir su acceso a dispositivos de la red interna, por tal motivo se recomienda colocarlos en interfaces del Firewall de menor seguridad y filtrar el uso de los protocolos permitidos.

6.5.6 Módulo de red interna

El módulo de red interna contiene las estaciones de trabajo, servidores corporativos servidores de administración, y su infraestructura de capa 2 y 3 asociada.

Dispositivos Clave:

- Switch de capa 3: Provee conmutación y enrutamiento en la red interna. Soporta servicios de filtrado de tráfico.
- Switch de capa 2: Provee servicios de capa 2 a las estaciones de trabajo.
- Servidores corporativos: Proveen correo electrónico (SMTP y POP3) a los usuarios internos, así como servicios de archivo, impresión y DNS.
- Estaciones de trabajo: Proveen servicios de datos a los usuarios autorizados.
- Estación de administración SNMP: Provee administración de dispositivos y manejo de alarmas.
- Estación de IDSs de red: Provee resúmen de las alarmas de los IDS de toda la red.
- Estaciones Syslog: Recopila la información de log de los dispositivos.
- Servidor de control de acceso: Provee servicios de autenticación a los dispositivos de red
- Servidor de One-time Password (OTP): Autoriza el paso de la información de OTP del Servidor de control de acceso.
- Dispositivos IDS de red: Proveen monitoreo de Capa 4-7 de los segmentos claves.

Mitigación de amenazas:

- Packet sniffers: Infraestructura switcheada e IDS de host para limitar la exposición. Control de MACs por puerto para evitar el overflow de la tabla CAM en los switchs.
- Ataques de virus y troyanos: Mitigado por el filtrado de contenidos de e-mail, IDSs de host y antivirus de host.
- Acceso no autorizado: Mitigado por el uso de IDS de host.

- Ataques de Passwords: El servidor de control de acceso permite el uso de autenticación fuerte para las aplicaciones claves.
- Ataques a capa de aplicación: Sistemas operativos, dispositivos y aplicaciones deben mantenerse con sus actualizaciones al día. Mitigados por IDS de Host.
- IP spoofing: Filtrado por RFC 2827 previene spoofing.
- Explotación de confianza: Las relaciones de confianza deben ser explícitos.

6.5 DISEÑO DE UN SERVIDOR DE SEGURIDAD

Las instrucciones de diseño que se presentan en este capítulo sirven de ayuda para seleccionar las características necesarias para el servidor de seguridad, teniendo en cuenta consideraciones importantes como el crecimiento y el costo. Este capítulo define también las distintas clases de servidores de seguridad y, mediante el uso de las instrucciones de diseño, debe poder seleccionar la clase que se ajuste mejor a sus necesidades. A partir de los conocimientos y la terminología técnica proporcionados en este capítulo, podrá analizar con los fabricantes del servidor de seguridad los productos que pueden ofrecerle y evaluar si se adecúan a sus necesidades.

Este capítulo considera los requisitos de un servidor de seguridad interno de una red empresarial, los tipos de dispositivos que pueden cumplir esos requisitos y las opciones disponibles para su implantación. Desafortunadamente, las intrusiones en redes por parte de usuarios externos e internos se han convertido en un suceso habitual, lo que significa que las organizaciones deben instalar alguna protección contra las mismas. Un servidor de seguridad cuesta dinero y supone un impedimento para el flujo de tráfico. Por lo tanto, debe asegurarse de que el servidor de seguridad esté diseñado para ser tan rentable y eficaz como sea posible.

En una arquitectura de red empresarial, generalmente, existen tres zonas:

- ***Red de borde***: Esta red se conecta directamente a Internet a través de un enrutador que proporciona una capa de protección inicial en forma de filtro básico de tráfico de red. Envía datos a la red perimetral a través de un servidor de seguridad perimetral.
- ***Red perimetral:*** Esta red, a menudo denominada DMZ (red desmilitarizada) o red de extremo, vincula los usuarios entrantes a los servidores Web u otros servicios. A continuación, los servidores Web se vinculan a las redes internas a través de un servidor de seguridad interno.
- ***Redes internas:*** Las redes internas se vinculan a los servidores internos, como el servidor SQL y los usuarios internos.

En una organización empresarial, a menudo habrá dos servidores de seguridad distintos: el servidor de seguridad perimetral y el servidor de seguridad interno. Aunque las tareas de estos servidores de seguridad son similares, también tienen prioridades distintas, ya que el servidor de seguridad perimetral se centra en proporcionar límites a los usuarios externos no confiables, mientras que el servidor de seguridad interno se centra en evitar que los usuarios externos obtengan acceso a la red interna y en limitar las acciones que pueden realizar los usuarios internos. Un servidor de seguridad comprueba los paquetes IP y bloquea los que reconoce como intrusos. Se puede realizar el bloqueo si se reconoce de forma predeterminada que ciertos paquetes son ilegales. También es posible configurar el servidor de seguridad para que bloquee ciertos paquetes. El protocolo TCP/IP se diseñó hace muchos años sin tener en cuenta la piratería informática ni las intrusiones y, por lo tanto, presenta muchos puntos débiles. Por ejemplo, el protocolo ICMP se diseñó como un mecanismo de señales dentro de TCP/IP, pero está expuesto al abuso y puede provocar problemas como ataques de denegación de servicio. Un servidor de seguridad interno tiene requisitos más exactos que un servidor de seguridad perimetral. Esto sucede porque el tráfico interno resulta más difícil de controlar, ya que

su destino legítimo puede ser cualquier servidor de la red interna.

¿Cuál es el presupuesto disponible? Todos los servidores de seguridad del entorno deben proporcionar el mayor nivel de servicio posible y ser, además, rentables. Se deben tener en cuenta los daños que podría sufrir el negocio si el servidor está demasiado restringido por el costo. Tenga en cuenta cuáles serían los costos del tiempo de inactividad de la organización si un ataque de denegación de servicio suspendiese el servicio.

¿La organización requiere que el servidor de seguridad esté activo en todo momento? Si ofrece un servicio de servidor Web público con disponibilidad constante, necesita un tiempo de actividad de casi el 100%. Todos los servidores de seguridad tienen probabilidades de error, ¿cómo se pueden reducir? La disponibilidad de un servidor de seguridad se puede mejorar mediante dos métodos:

- *Componentes redundantes*: Al duplicar algunos de los componentes con más posibilidades de error, como el sistema de alimentación, la resistencia del servidor mejora, ya que el primer componente puede dar error sin que ello tenga efectos sobre el funcionamiento general. Normalmente, los servidores de seguridad más económicos no tienen opciones redundantes, ya que resulta costoso agregar resistencia, en particular, porque no aumenta la potencia de procesamiento.
- *Dispositivos duplicados:* La duplicación del dispositivo del servidor de seguridad proporciona un sistema completamente resistente, aunque a un costo considerable, ya que también requiere un cableado de red duplicado y una conectividad duplicada en los enrutadores o conmutadores a los que se conecta el servidor de seguridad. Sin embargo, en función de los servidores de seguridad, es posible que también se doble el rendimiento como compensación. En teoría, todos los servidores de seguridad, desde el más pequeño al más grande, pueden duplicarse, pero en la práctica también se necesita un mecanismo de cambio de conexión de software que los servidores de seguridad más pequeños pueden no tener.

¿Cuáles son los requisitos de rendimiento de los servidores de seguridad? El rendimiento se puede considerar en términos de bits por segundo o de paquetes transferidos por segundo. Si se trata de una operación nueva, es posible que no conozca las velocidades de rendimiento y, si esta operación se lleva a cabo de forma satisfactoria, el rendimiento de Internet podría aumentar rápidamente. ¿Cómo se puede controlar un aumento? Debe seleccionar una solución de servidor de seguridad que pueda escalar a medida que aumenta el rendimiento. ¿El servidor de seguridad puede crecer agregando más componentes o se podría instalar otro servidor de seguridad en paralelo?

A menudo, personas que desean perjudicar a organizaciones o robar secretos comerciales para obtener una ventaja competitiva utilizan Internet como herramienta. Si instala un servidor de seguridad perimetral y observa el registro de intrusiones, el volumen de las mismas le sorprenderá. La mayoría de estas intrusiones sólo son pruebas para ver si la máquina responde y averiguar los servicios que utiliza. Puede parecer inofensivo, pero si el atacante descubre la máquina que utiliza, podría atacar sus servicios, una vez conocidos sus puntos débiles. No todos los ataques se basan en Internet. También debe proteger la información importante de los usuarios internos de la red empresarial. La mayoría de las organizaciones dispone de información importante que debe protegerse de ciertos usuarios de la red interna, incluidos empleados, proveedores y clientes.

Un servidor de seguridad es un mecanismo que sirve para controlar el flujo de tráfico IP entre dos redes. Los dispositivos de servidor de seguridad funcionan habitualmente en L3 (nivel 3) del modelo OSI, aunque algunos modelos también pueden funcionar a niveles superiores.

Generalmente, un servidor de seguridad interno proporciona las ventajas siguientes:

- Defensa de servidores internos contra ataques de red.

- Aplicación de directivas de uso y acceso a la red.
- Supervisión de tráfico y generación de alertas en caso de detección de patrones sospechosos.

Es importante destacar que los servidores de seguridad mitigan sólo algunos tipos de peligros. Generalmente, un servidor de seguridad no evita el daño que se puede infligir a un servidor con un problema de seguridad de software. Los servidores de seguridad se deben implementar como parte de una arquitectura de seguridad completa de la organización. En función de las características que admita un servidor de seguridad, el tráfico se permite o bloquea mediante varias técnicas. Dichas técnicas ofrecen grados distintos de protección, según las capacidades del servidor de seguridad. Las características siguientes del servidor de seguridad se enumeran de menor a mayor complejidad:

- Filtros de entrada del adaptador de red
- Filtros de paquetes estáticos
- Traducción de direcciones de red (NAT)
- Inspección con estado
- Inspección de circuitos
- Filtrado de aplicaciones

En general, los servidores de seguridad que proporcionan características complejas también incluyen características más simples. Sin embargo, debe leer la información del proveedor con atención antes de elegir un servidor de seguridad, ya que pueden existir diferencias sutiles entre su funcionalidad implícita y su funcionalidad real. Normalmente, la selección de un servidor de seguridad implica la consulta de sus características y su prueba, para comprobar que funciona de acuerdo con las especificaciones.

Filtros de entrada del adaptador de red: El filtrado de entrada del adaptador de red examina las direcciones de origen o destino y otra información del paquete entrante y lo bloquea o lo deja pasar. Se aplica sólo al tráfico entrante y no puede controlar el tráfico de salida. Relaciona direcciones IP y números de puerto para UDP y TCP, así como para el protocolo de tráfico, TCP, UDP y encapsulación de ruta genérica (GRE). El filtrado de entrada del adaptador de red permite una denegación rápida y eficiente de los paquetes entrantes estándar que cumplan los criterios de las reglas configurados en el servidor de seguridad. Sin embargo, puede eludirse fácilmente, ya que sólo relaciona encabezados del tráfico IP y asume que el tráfico que se filtra sigue los estándares IP y no ha sido fabricado para eludir el filtrado.

Filtros de paquetes estáticos: Los filtros de paquetes estáticos son similares a los filtros de entrada del adaptador de red en cuanto a que simplemente comparan los encabezados IP para determinar si debe o no permitir que el tráfico pase por la interfaz. Sin embargo, los filtros de paquetes estáticos permiten el control sobre las comunicaciones entrantes y salientes de una interfaz. Además, los filtros de paquetes estáticos suelen permitir una función adicional sobre el filtrado del adaptador de red, que consiste en comprobar si se incluye el bit de reconocimiento en el encabezado IP. El bit ACK proporciona información acerca de si el paquete es una solicitud nueva o una solicitud devuelta de otra original. No verifica si el paquete se envió en un principio por la interfaz que lo recibe, sólo comprueba si el tráfico que entra en la interfaz parece tráfico de respuesta en función de las convenciones de los encabezados IP. Esta técnica sólo se aplica al protocolo TCP y no al protocolo UDP. Al igual que el filtrado de entrada del adaptador de red, el filtrado de paquetes estático es muy rápido, pero sus capacidades son limitadas y el tráfico manipulado para eludirlo, lo consigue.

Traducción de direcciones de red: En el intervalo de direcciones IP de todo el mundo, algunos intervalos se designan como direcciones privadas. Estos intervalos se han creado para su utilización en la organización y no tienen ningún sentido en Internet. El tráfico con destino a estas direcciones IP no se puede enrutar a través de Internet, por lo que asignar una dirección privada a sus dispositivos internos puede proporcionarles cierta protección frente a los intrusos. Sin embargo, a menudo estos dispositivos internos necesitan tener acceso a Internet y la Traducción de direcciones de red (NAT) convierte la dirección privada en una dirección de Internet. Aunque NAT no es estrictamente una tecnología de servidor de seguridad, al ocultar la dirección IP real de un servidor, se evita que algún atacante pueda obtener información valiosa sobre el servidor.

Inspección con estado: En la inspección con estado, todo el tráfico de salida se registra en una tabla de estado. Cuando el tráfico de conexión vuelve a la interfaz, se comprueba la tabla de estado para garantizar que el tráfico se ha originado en ésta. La inspección con estado es ligeramente más lenta que el filtrado de paquetes estático. Sin embargo, garantiza que el tráfico sólo pasa si coincide con las solicitudes de tráfico salientes. La tabla de estado contiene elementos como la dirección IP de destino, el paquete IP de origen, el puerto al que se llama y el host de origen. Algunos servidores de seguridad almacenan más información (como los fragmentos IP enviados y recibidos) en la tabla de estado, mientras que otros almacenan menos. El servidor de seguridad puede comprobar que el tráfico se procesa cuando vuelve toda la información fragmentada o una parte de ésta. Los servidores de seguridad de distintos proveedores implantan la característica de inspección con estado de forma distinta, por lo que debe leer con atención la documentación del servidor de seguridad. La característica de inspección con estado ayuda a mitigar el peligro que supone el reconocimiento de redes y la suplantación de IP.

Inspección de circuitos: El filtrado de circuitos permite inspeccionar sesiones, en lugar de conexiones o paquetes. Una sesión puede incluir varias conexiones. Al igual que el filtrado de paquetes dinámico, las sesiones sólo se establecen como respuesta a la solicitud de un usuario. El filtrado de circuitos proporciona compatibilidad integrada para protocolos con conexiones secundarias, como FTP y multimedia de transmisión por secuencias. Normalmente, ayuda a mitigar el riesgo que suponen los ataques de reconocimiento de redes, DoS e imitación de IP.

Filtrado de aplicaciones: El nivel más sofisticado de inspección de tráfico del servidor de seguridad es el filtro de aplicaciones. Los buenos filtros de aplicación permiten analizar una secuencia de datos para una aplicación particular y proporcionan un procesamiento específico de aplicación. Este procesamiento incluye la inspección, el filtrado, el bloqueo, la redirección y la modificación de los datos a medida que pasan por el servidor de seguridad. Este mecanismo se utiliza para protegerse de comandos SMTP no seguros o ataques contra el sistema de nombres de dominio (DNS) interno, entre otros problemas. Normalmente, es posible agregar al servidor de seguridad herramientas de terceros para el filtrado de contenido, como detección de virus, análisis léxico y categorización de sitios.

Un servidor de seguridad de aplicaciones puede inspeccionar protocolos distintos en función del tráfico que pase por el mismo. Al contrario de lo que sucede con un servidor de seguridad proxy, que normalmente inspecciona el tráfico de Internet, como HTTP, descargas FTP y SSL, el servidor de seguridad de aplicaciones tiene un control mucho mayor sobre el tráfico que pasa por el mismo. Por ejemplo, un servidor de seguridad de aplicaciones sólo puede permitir el paso al tráfico UDP que se origina dentro de sus límites. Si un host de Internet examinase los puertos de un servidor de seguridad con estado para comprobar si permite el tráfico DNS en el entorno, probablemente el examen mostraría que el puerto conocido asociado con el DNS está abierto, pero una vez iniciado el ataque, el servidor de seguridad con estado rechazaría las solicitudes por no haberse originado internamente. Un servidor de seguridad de aplicaciones puede abrir puertos dinámicamente en función del origen del tráfico.

La característica de servidor de seguridad de aplicaciones ayuda a mitigar el riesgo que suponen los ataques de imitación de IP, DoS, ataques de aplicaciones, reconocimiento de redes y ataques de virus

o caballos de Troya. Los inconvenientes de un servidor de seguridad de aplicaciones se refieren a que requiere mucha más potencia de procesamiento y, normalmente, es mucho más lento al pasar el tráfico que los servidores de seguridad con estado o filtrado estático. La consideración más importante a la hora de utilizar servidores de seguridad de aplicaciones consiste en determinar qué puede hacer.

El filtrado de aplicaciones se utiliza de forma generalizada para proteger servicios expuestos públicamente. Si su organización dispone de una tienda en línea que recopila números de tarjetas de crédito y otra información personal sobre los clientes, resulta prudente tomar el máximo nivel de precaución para proteger esta información. La característica de aplicaciones garantiza que el tráfico que pasa por un puerto es el apropiado. Al contrario de lo que sucede con los servidores de seguridad con filtros de paquetes o inspección con estado, que simplemente miran el puerto y la dirección IP de origen y destino, los servidores de seguridad que admiten la característica de filtrado de aplicaciones pueden inspeccionar los datos y comandos que entran y salen.

La mayoría de los servidores de seguridad que admite la característica de aplicaciones sólo dispone de filtrado de aplicaciones para tráfico de texto no cifrado, como un servicio de mensajería compatible con proxy, HTTP y FTP. Es importante tener en cuenta que un servidor de seguridad compatible con esta característica puede regir el tráfico que entra y sale del entorno. Otra ventaja de esta característica es la capacidad de inspeccionar el tráfico DNS para buscar comandos específicos de DNS a medida que pasan por el servidor de seguridad. Este nivel adicional de protección garantiza que usuarios o atacantes no podrán ocultar información en los tipos de tráfico admitidos.

6.5.1 Clases de servidor de seguridad

En la sección siguiente se presentan varias clases de servidores de seguridad, con sus correspondientes características. Las clases de servidor de seguridad específicas pueden utilizarse para responder a requisitos específicos del diseño de una arquitectura de TI.

La agrupación de servidores de seguridad en clases permite la abstracción del hardware de los requisitos del servicio. A continuación, pueden hacerse coincidir los requisitos del servicio con las características de la clase. Siempre que un servidor de seguridad encaje en una clase específica, éste puede admitir todos los servicios que se requiere que admita la clase.

Las clases son las siguientes:

Clase 1: Servidores de seguridad personales: Un servidor de seguridad personal se define como un servicio de software que se ejecuta en un sistema operativo que proporciona una sencilla funcionalidad de servidor de seguridad para un equipo personal. Al crecer el número de conexiones permanentes a Internet (al contrario que las conexiones de acceso telefónico), ha aumentado el uso de servidores de seguridad personales.

Aunque se ha diseñado para proteger a un único equipo personal, un servidor de seguridad personal también puede proteger a una red pequeña si el equipo en el que se ha instalado comparte su conexión a Internet con otros equipos de la red interna. Sin embargo, un servidor de seguridad personal tiene un rendimiento limitado y reduce el rendimiento del equipo personal en el que está instalado. Los mecanismos de protección suelen ser menos efectivos que una solución de servidor de seguridad dedicada porque suelen estar restringidos al bloqueo de direcciones IP y de puertos aunque, en general, un equipo personal necesita un nivel de protección inferior.

Los servidores de seguridad personales pueden incluirse sin costo alguno con un sistema operativo o adquirirse a un precio muy bajo. Son adecuados para el fin con el que se han diseñado, pero no deben utilizarse en empresas, ni siquiera en pequeñas oficinas satélite, ya que su rendimiento y funcionalidad están muy limitados. Sin embargo, son particularmente adecuados para los usuarios móviles que utilizan equipos portátiles.

Las ventajas de los servidores de seguridad personales incluyen:

- Económicos: Cuando se necesita sólo un número limitado de licencias, los servidores de seguridad personales son una opción económica. Las distintas versiones de Windows XP incluyen un servidor de seguridad personal. Encontrará productos adicionales disponibles que funcionan con otras versiones de Windows u otros sistemas operativos de forma gratuita o por un costo limitado.
- Fáciles de configurar: Los productos de servidores de seguridad personales suelen tener configuraciones básicas que funcionan tal cual con opciones de configuración directas.

Entre los inconvenientes de los servidores de seguridad personales se incluyen:

- Difíciles de administrar de forma centralizada: Los servidores de seguridad personales se deben configurar en cada cliente, lo que aumenta la carga de administración.
- Sólo control básico: La configuración suele ser sólo una combinación de filtrado de paquetes estático y bloqueo de aplicaciones basado en permisos.
- Limitaciones de rendimiento: Los servidores de seguridad personales están diseñados para proteger equipos personales individuales. Al utilizarlos en un equipo personal que funciona como enrutador para una pequeña red, el rendimiento se reduce.

Clase 2: Servidores de seguridad de enrutador: Habitualmente, los enrutadores son compatibles con una o varias de las características de servidor de seguridad tratadas anteriormente, y se pueden subdividir en dispositivos inferiores diseñados para conexiones a Internet y enrutadores tradicionales superiores. Los enrutadores inferiores proporcionan características de servidor de seguridad básicas para bloquear y permitir direcciones IP y números de puerto específicos y utilizar NAT para ocultar direcciones IP internas. Suelen proporcionar la característica de servidor de seguridad como estándar, optimizada para bloquear intrusiones de Internet, y aunque no es necesario configurarlos, se pueden delimitar mejor con una configuración adicional.

Los enrutadores superiores se pueden configurar para restringir el acceso al impedir las intrusiones más obvias, por ejemplo pings, e implementar otras restricciones de direcciones IP y puertos a través del uso de listas ACL. Es posible adquirir características de servidor de seguridad adicionales que proporcionen filtrado de paquetes con estado en algunos enrutadores. En los enrutadores superiores, la funcionalidad del servidor de seguridad es similar a la de un dispositivo de hardware de servidor de seguridad, a un costo más bajo pero también con un rendimiento inferior.

Entre las ventajas de los servidores de seguridad de enrutador se incluyen:

- Solución de bajo costo: Puede que la activación de un servidor de seguridad de enrutador existente no agregue ningún costo al precio del enrutador y, además, no requiere hardware adicional.
- La configuración se puede consolidar: La configuración del servidor de seguridad de enrutador se puede llevar a cabo cuando se configura el enrutador para su funcionamiento normal, por lo que reduce el trabajo de administración. Esta solución es particularmente adecuada para oficinas de sucursales satélite, puesto que se simplifica el hardware y la administración de la red.
- Protección de la inversión: El personal de operaciones está familiarizado con la configuración y administración del servidor de seguridad del enrutador, por lo que no se necesita formación adicional alguna. El cableado de red es más simple, ya que no se instala hardware adicional, lo que también simplifica la administración de la red.

Entre los inconvenientes de los servidores de seguridad del enrutador se incluyen:

- Funcionalidad limitada: En general, los enrutadores inferiores ofrecen sólo características

básicas de servidor de seguridad. Por su parte, los enrutadores superiores suelen ofrecer características de servidor de seguridad de alto nivel, pero pueden requerir una configuración considerable. Gran parte de esta configuración se realiza mediante la incorporación de controles que se olvidan fácilmente, lo que dificulta una correcta configuración.

- Sólo control básico: La configuración suele ser sólo una combinación de filtrado de paquetes estático y bloqueo de aplicaciones basado en permisos.
- Impacto de rendimiento: Utilizar un enrutador como servidor de seguridad empeora el rendimiento del enrutador y ralentiza su función de enrutamiento, que es su tarea principal.
- Rendimiento del archivo de registro: La utilización de un archivo de registro para descubrir actividades inusuales puede reducir drásticamente el rendimiento del enrutador, especialmente cuando ya ha sido atacado.

Clase 3: Servidores de seguridad de hardware inferiores: En el mercado de servidores de seguridad de hardware inferiores existen unidades Plug and Play que requieren muy poca o ninguna configuración. A menudo, estos dispositivos incluyen la funcionalidad de conmutador y/o VPN. Los servidores de seguridad de hardware inferiores son adecuados para empresas pequeñas y para su uso interno en organizaciones más grandes. Generalmente, ofrecen capacidades de filtrado estático y funcionalidad de administración remota básica. Es posible que los dispositivos de los mayores fabricantes ejecuten el mismo software que sus homólogos superiores y dispongan de una revisión de actualización.

Entre las ventajas de los servidores de seguridad de hardware inferiores se incluyen:

- Bajo costo: Los servidores de seguridad inferiores se pueden adquirir a un precio económico.
- Configuración sencilla: Casi no se necesita configuración alguna.

Entre los inconvenientes de los servidores de seguridad de hardware inferiores se incluyen:

- Funcionalidad limitada: En general, los servidores de seguridad de hardware inferiores ofrecen sólo funcionalidad básica de servidor de seguridad. No se pueden ejecutar en paralelo para la redundancia.
- Rendimiento bajo: Los servidores de seguridad de hardware inferiores no se han diseñado para administrar conexiones de alto rendimiento, lo que puede provocar cuellos de botella.
- Soporte técnico limitado del fabricante: Puesto que se trata de productos de bajo costo, el soporte técnico del fabricante se limita, habitualmente, al correo electrónico o a un sitio Web.
- Capacidad de actualización limitada: No suelen existir actualizaciones de hardware aunque, a menudo, hay actualizaciones de firmware periódicas disponibles.

Clase 4: Servidores de seguridad de hardware superiores: En el mercado de servidores de seguridad de hardware superiores existen productos de alto rendimiento y resistentes adecuados para las empresas o los proveedores de servicios. Normalmente, estos servidores de seguridad ofrecen la mejor protección sin reducir el rendimiento de la red.

La resistencia puede conseguirse agregando un segundo servidor de seguridad que se ejecute como unidad de espera activa que mantenga la tabla de conexiones actual mediante sincronización automática con estado.

Deben usarse servidores de seguridad en todas las redes conectadas a Internet, ya que se producen intrusiones constantemente, como los ataques DoS, los robos y la corrupción de datos. Las oficinas centrales o principales de una empresa deben considerar la implantación de unidades de servidor de seguridad de hardware superiores.

Entre las ventajas de los servidores de seguridad de hardware superiores se incluyen:

- Alto rendimiento: Los productos de servidor de seguridad de hardware se han diseñado para un solo objetivo y proporcionan altos niveles de bloqueo de intrusiones junto con el menor grado de degradación del rendimiento.
- Gran disponibilidad: Los servidores de seguridad de hardware superiores pueden estar conectados entre ellos para conseguir una disponibilidad óptima y equilibrio de carga.
- Sistemas modulares: Tanto el hardware como el software se pueden actualizar para cumplir con los requisitos nuevos. Las actualizaciones de hardware pueden incluir puertos Ethernet adicionales, mientras que las actualizaciones de software pueden incluir la detección de nuevos métodos de intrusión.
- Administración remota: Los servidores de seguridad de hardware superiores ofrecen una mejor funcionalidad de administración remota que sus equivalentes inferiores.
- Resistencia: Los servidores de seguridad de hardware superiores pueden tener características de disponibilidad y resistencia, como la espera activa mediante una segunda unidad.
- Filtrado de aplicaciones: A diferencia de sus homólogos inferiores, que normalmente sólo filtran en el nivel 3 y tal vez 4 del modelo OSI, los servidores de seguridad de hardware superiores proporcionan filtrado en los niveles del 5 al 7 de aplicaciones conocidas.

Entre los inconvenientes de los servidores de seguridad de hardware superiores se incluyen:

- Costo elevado: Los servidores de seguridad de hardware superiores suelen ser caros. Aunque pueden adquirirse por tan poco como 100 dólares USA, el costo es mucho mayor para un servidor de seguridad empresarial y con frecuencia se basa en los requisitos de número de sesiones simultáneas, rendimiento y disponibilidad.
- Configuración y administración complejas: Dado que esta clase de servidores de seguridad tiene una funcionalidad mayor que la de los servidores de seguridad inferiores, también resultan más difíciles de configurar y administrar.

Clase 5: Servidores de seguridad de servidor superiores: Los servidores de seguridad de servidor proporcionan la funcionalidad de servidor de seguridad a servidores superiores, ofreciendo una protección sólida y rápida para sus sistemas estándar de hardware y software. La ventaja de este enfoque es el uso de hardware o software conocido. Esto proporciona un número reducido de artículos de inventario, una formación y administración simplificadas, así como confiabilidad y capacidad de expansión. Muchos de los productos de servidor de seguridad de hardware superiores se implantan en plataformas de hardware estándar con sistemas operativos estándar (pero ocultos a la vista) y, por lo tanto, se diferencian poco, a nivel de técnica y rendimiento, de un servidor de seguridad de servidor. Sin embargo, puesto que el sistema operativo sigue siendo visible, la característica de servidor de seguridad de servidor se puede actualizar y hacer más resistente mediante técnicas como el servicio de clúster.

Dado que el servidor de seguridad de servidor es un servidor que ejecuta un sistema operativo común, es posible agregarle software, características y funcionalidades adicionales de varios proveedores (y no de uno solo, como sucede con el servidor de seguridad de hardware). El hecho de estar familiarizado con el sistema operativo también puede llevar a una protección más eficaz, ya que algunas de las demás clases necesitan unos conocimientos técnicos considerables para una configuración completa y correcta.

Esta clase resulta adecuada en casos de una gran inversión en una plataforma de hardware o software particular, ya que la utilización de la misma plataforma para el servidor de seguridad facilita las tareas de administración. La capacidad de almacenamiento en caché de esta clase también puede ser muy eficaz.

Entre las ventajas de los servidores de seguridad de servidor se incluyen:

- Alto rendimiento: Cuando se ejecutan en un servidor de tamaño adecuado, estos servidores de seguridad pueden ofrecer altos niveles de rendimiento.
- Integración y consolidación de servicios: Los servidores de seguridad de servidor pueden utilizar características del sistema operativo en el que se ejecutan. Por ejemplo, el software de un servidor de seguridad que se ejecute en el sistema operativo Windows Server™ 2003 puede aprovechar la funcionalidad de equilibrio de carga de red integrada en dicho sistema operativo. Además, el servidor de seguridad también puede utilizarse como servidor VPN, de nuevo gracias a la funcionalidad del sistema operativo Windows Server 2003.
- Disponibilidad, resistencia y escalabilidad: Puesto que este servidor de seguridad se ejecuta en el hardware estándar de un equipo, tiene todas las características de disponibilidad, resistencia y escalabilidad de la plataforma en la que se ejecuta.

Entre los inconvenientes de los servidores de seguridad de servidor se incluyen:

- Requiere hardware superior: Para un óptimo rendimiento, la mayoría de los productos de servidor de seguridad de servidor requiere hardware superior en cuanto a unidad central de procesamiento (CPU), memoria e interfaces de red.
- Susceptible a problemas de seguridad: Puesto que los productos de servidor de seguridad de servidor se ejecutan en sistemas operativos conocidos, son susceptibles a los problemas de seguridad presentes en el sistema operativo y en otro software que se ejecute en el servidor. Aunque se trata del mismo caso que en los servidores de seguridad de hardware, los sistemas operativos de estos no resultan tan familiares a los atacantes como la mayoría de los sistemas operativos de servidor.

Es importante comprender que algunas de estas clases se solapan. Esto se debe a su diseño, ya que la solapación permite a un tipo de solución de servidor de seguridad abarcar varias clases. También es posible que más de un modelo de hardware del mismo proveedor proporcione varias clases, lo que permite a la organización seleccionar un modelo que se adapte a sus requisitos presentes y futuros. Aparte del conjunto de precio y características, los servidores de seguridad se pueden clasificar según su rendimiento. Sin embargo, en la mayoría de los casos, los fabricantes no proporcionan cifras sobre el rendimiento. Cuando se proporcionan (normalmente, para dispositivos de sistemas de seguridad de hardware) no se sigue el proceso de medida estándar, lo que dificulta las comparaciones entre distintos fabricantes. Por ejemplo, una medida es el número de bits por segundo (bps), pero puesto que, en realidad, el servidor de seguridad transmite paquetes IP, esta medida no tiene sentido si no se incluye el tamaño del paquete utilizado al medir la velocidad.

6.5.2 Reglas de un Servidor de Seguridad Interno

Los servidores de seguridad internos supervisan el tráfico entre la zona perimetral y las zonas internas de confianza. Los requisitos técnicos para los servidores de seguridad internos son considerablemente más complejos que los de los servidores de seguridad perimetrales, a causa de la complejidad de los flujos y tipos de tráfico entre estas redes.

En esta sección, se hace referencia a "hosts de bastión". Los hosts de bastión son servidores ubicados en la red perimetral que proporcionan servicios a usuarios internos y externos. Algunos ejemplos de hosts de bastión son los servidores Web y los servidores VPN. Normalmente, el servidor de seguridad interno necesitará tener implantadas las normas siguientes, de forma predeterminada o configuradas:

- Bloquear todos los paquetes de forma predeterminada.

- En la interfaz perimetral, bloquear paquetes entrantes que parezcan haberse originado desde una dirección IP interna para evitar la imitación de IP.
- En la interfaz interna, bloquear paquetes salientes que parezcan haberse originado desde una dirección IP externa para restringir un ataque interno.
- Permitir consultas basadas en UDP y respuestas de los servidores DNS al host de bastión de resolución de DNS.
- Permitir consultas basadas en UDP y respuestas del host de bastión de resolución de DNS a los servidores DNS internos.
- Permitir consultas basadas en TCP de los servidores DNS internos al host de bastión de resolución de DNS, incluidas las respuestas a las consultas.
- Permitir consultas basadas en TCP del host de bastión de resolución de DNS a los servidores DNS internos, incluidas las respuestas a las consultas.
- Permitir transferencias de zona entre el host de bastión de anuncio de DNS y los hosts servidores DNS internos.
- Permitir correo saliente del servidor de correo SMTP interno al host de bastión SMTP de salida.
- Permitir correo entrante del host de bastión SMTP de entrada al servidor de correo SMTP interno.
- Permitir que el tráfico originado desde el servidor en servidores VPN llegue a los hosts internos y que las respuestas se devuelvan a los servidores VPN.
- Permitir el tráfico de autenticación con servidores RADIUS en la red interna y la devolución de respuestas a los servidores VPN.
- Todo el acceso Web de salida de los clientes internos pasa por un servidor proxy y las respuestas se les devuelven.
- Admitir el tráfico de autenticación de dominios de Microsoft Windows 2000/2003 entre segmentos de red para el dominio perimetral y el dominio interno.
- Admitir al menos cinco segmentos de red.
- Realizar una inspección con estado de paquetes entre todos los segmentos de red que se unan (servidor de seguridad de circuitos, nivel 3 y nivel 4).
- Admitir características de alta disponibilidad como conmutación por error con estado.
- Enrutar el tráfico entre todos los segmentos de red conectados sin utilizar la Traducción de direcciones de red.

6.5.3 Requisitos de Hardware

Los requisitos de hardware para un servidor de seguridad son distintos para servidores de seguridad basados en software y servidores de seguridad basados en hardware, como se describe a continuación:

- *Servidor de seguridad basado en hardware*: Estos dispositivos ejecutan, habitualmente, código especializado en una plataforma de hardware personalizada. Los servidores de seguridad suelen ajustarse (y valorarse económicamente) en función del número de conexiones que puedan admitir y la complejidad del software que se ejecutará.
- Servidores de seguridad basados en software: Se configuran también según el número de conexiones simultáneas y la complejidad del software del servidor de seguridad. Existen

calculadoras capaces de calcular la velocidad de procesador, el tamaño de la memoria y el espacio en disco que necesita un servidor en función del número de conexiones admitidas. También se debe tener en cuenta cualquier otro software que pueda ejecutarse en el servidor del servidor de seguridad, como software de equilibrio de carga y VPN. Asimismo, deberá tener en cuenta los métodos para escalar el servidor de seguridad de forma vertical u horizontal. Estos métodos incluyen el aumento de la potencia del sistema mediante procesadores, memoria y tarjetas de red adicionales, así como la utilización de varios sistemas de equilibrio de carga para repartir entre ellos las tareas del servidor de seguridad. Algunos productos aprovechan el multiprocesamiento simétrico (SMP) para aumentar el rendimiento. El servicio de equilibrio de carga de red de Windows Server 2003 puede ofrecer tolerancia a errores, alta disponibilidad, eficacia y mejoras de rendimiento para algunos productos de servidor de seguridad de software.

Para aumentar la disponibilidad del servidor de seguridad, puede implantarse como un único dispositivo con o sin componentes redundantes o como un par de servidores de seguridad redundantes con algún tipo de mecanismo de equilibrio de carga y/o conmutación por error.

La seguridad de los productos de servidor de seguridad tiene una importancia capital. Aunque no hay estándares en la industria para la seguridad del servidor de seguridad, la asociación independiente de proveedores International Computer Security Association (ICSA) utiliza un programa de certificación destinado a comprobar la seguridad de los productos de este tipo disponibles en el mercado. ICSA somete a sus pruebas a un número significativo de los productos de servidor de seguridad disponibles actualmente en el mercado.

Se debe prestar atención para asegurar que un servidor de seguridad cumple los estándares de seguridad requeridos, y una forma de hacerlo consiste en seleccionar un servidor de seguridad con la certificación ICSA. Además, debe existir un registro de seguimiento para el servidor de seguridad que se elija. Existen varias bases de datos de problemas de seguridad en Internet. Resulta interesante consultarlas para obtener información sobre los problemas de seguridad del producto que tiene pensado adquirir. Desafortunadamente, todos los productos (basados en hardware y software) presentan problemas. Además de determinar el número y la gravedad de los errores que han afectado al producto que desea comprar, también es importante evaluar la respuesta del proveedor a los problemas de seguridad expuestos.

La mayoría de los protocolos de Internet que utiliza la versión 4 del Protocolo de Internet (IPv4) puede protegerse con un servidor de seguridad. Esto incluye protocolos de bajo nivel, como TCP y UDP, y protocolos de alto nivel como HTTP, SMTP y FTP. Revise cualquier producto de servidor de seguridad que se pueda considerar para asegurar de que admite el tipo de tráfico necesario. Algunos servidores de seguridad también pueden interpretar el protocolo GRE, que es el de encapsulación para el protocolo de túnel punto a punto (PPTP) utilizado en algunas implementaciones de VPN.

Algunos servidores de seguridad han integrado filtros de aplicaciones para protocolos como HTTP, SSL, DNS, FTP, SOCKS v4, RPC, SMTP, H. 323 y el protocolo de oficina de correo (POP).

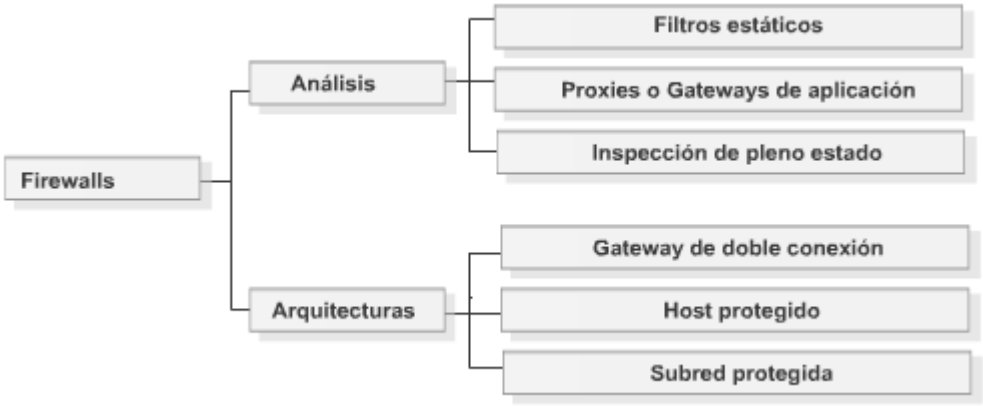
También debe considerar el futuro del protocolo TCP/IP e IPv6, y si éste debe ser un requisito obligatorio para cualquier servidor de seguridad, incluso si actualmente utiliza Ipv4.

6.6 *SÍNTESIS*

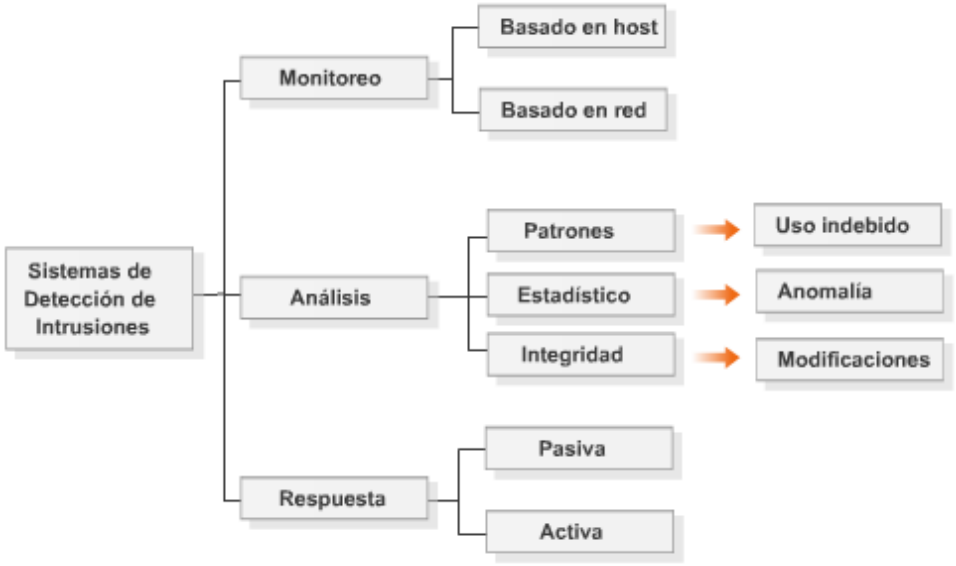
Muchos de los servicios que las personas demandan son, por naturaleza, inseguros. Los Firewalls son como los agentes de tránsito para estos servicios. Refuerzan las políticas de seguridad del sitio, permitiendo que pasen sólo los servicios aprobados y aquellos que cumplen con las reglas establecidas para ello.

Su implementación física varía de un sitio a otro. Con mayor frecuencia un Firewall es un conjunto de componentes de hardware (un equipo dedicado, un router o un host, con el software apropiado).

Existen varias formas de configurar estos equipos, dependiendo de la política de seguridad, del presupuesto y de las operaciones generales de un sitio específico.



Los Firewalls ofrecen una excelente protección contra las amenazas a la red, pero no son una solución de seguridad total. Ciertas amenazas están fuera del control del Firewall. Debe encontrar otras formas de protegerse contra ellas incorporando seguridad física, seguridad a nivel de los hosts y educación para el usuario en su plan de seguridad.



Los Sistemas de detección de intrusiones complementan las medidas de seguridad, y nos protegerán en caso que el atacante ya esté dentro de la red interna, en este caso el Firewall no puede hacer casi nada por resistir un ataque. Los usuarios internos pueden robar datos, dañar el hardware y el software y modificar programas de manera sutil. Las amenazas desde adentro requieren medidas de seguridad internas, como los sistemas de detección de intrusiones.

En general podremos implementar IDSs basados en red y en hosts, los primeros escuchan las comunicaciones que circulan por el segmento donde están instalados y los basados en hosts se instalan en hosts determinados, por ejemplo los servidores, y permiten auditar los eventos que suceden en el mismo. Ambos IDSs recogen información, la analizan y pueden frenar en forma activa aquellos eventos que interpreten como un ataque, además deben enviar reportes a una consola central donde el administrador puede observar el comportamiento de la red.

6.7 PREGUNTAS Y TIPS

- **¿Cuál es el objetivo de un proceso de análisis de patrones?** Identificar usos indebidos o ataques conocidos
- **¿Dónde podemos encontrar implementaciones de Firewall?** Como una funcionalidad adicional de un router, Como un dispositivo independiente y dedicado
- **¿Cuál política de un Firewall es la más recomendable?** Prohibir todo lo que no está expresamente permitido
- **¿Por qué decimos que NAT contribuye a la seguridad de la red?** Utiliza un mecanismo inequívoco para controlar los paquetes que pueden ingresar a la red interna, Impide que los dispositivos externos accedan directamente a las estaciones de la red interna
- **¿Para qué se utiliza la tabla de traslaciones en NAT y PAT?** Para controlar los paquetes que pueden ingresar a la red interna
- **¿Cuál es una ventaja del uso de PAT?** Impide que los dispositivos externos accedan directamente a las estaciones de la red interna
- **¿Cuál es uno de los datos que almacena PAT en la tabla de traslaciones?** El número de puerto TCP/IP con el cual se reemplazó el número de puerto de origen
- **¿En qué capa del modelo OSI operan los filtros estáticos de paquetes?** Red y Transporte
- **¿En qué capa del modelo OSI operan los Proxies?** Aplicación
- **¿En qué capas opera la Inspección de pleno estado (Stateful Inspection)?** Red, Transporte, Aplicación
- **¿Cuáles son arquitecturas de Firewall?** Subred protegida, Host protegido, Gateway de doble conexión.
- **¿Cuál arquitectura de Firewall es la más segura?** Subred segurizada
- **¿Cuáles son objetivos de los IDS?** Identificación y detección de las amenazas
- **¿Cuáles dispositivos nos puede proteger de los abusos cometidos por los usuarios internos?** Los sistemas de detección de intrusiones
- **¿Cuáles son funciones de un IDS?** Monitorizar y analizar los eventos del sistema y el comportamiento de los usuarios, Comunican alarmas cuando se produce una situación anormal
- **¿Cuáles son limitaciones o desventajas de un IDS?** Falsos positivos, Defensa ante nuevos ataques, Defensa ante ataques sofisticados
- **¿Cómo se denomina el caso en el cual existe un ataque pero el IDS no lo detecta?** Se denomina Verdadero negativo

CAPÍTULO 7

7.1 HARDENING (Endurecimiento)

Todo especialista en seguridad necesita conocer los fundamentos del hardening de sistemas. Este capítulo tiene como objetivo presentar las técnicas y métodos del hardening, orientados principalmente a sistemas operativos, redes y aplicaciones.

Es bien sabido que al instalar cualquier sistema operativo o aplicación, las opciones y características por defecto suelen ser genéricas, no adecuadas a necesidades en particular. Esto no tiene una razón de ser caprichosa, sino que responde a que lo que se instala sea funcional a la mayoría de las personas. Mucho software también brinda la posibilidad de seleccionar entre distintos tipos de instalación, en la cual se hace foco en ciertas cosas, como minimización de lo instalado, maximización de recursos disponibles, y otras opciones típicas.

Así es como nace el concepto de Hardening, del inglés “endurecimiento”, que refiere al proceso de segurizar un sistema o aplicación en función de su protección contra eventos determinados. Normalmente esto incluye habilitar o deshabilitar funciones, cerrar accesos y puertos no utilizados, y eliminar lo que no es necesario para el funcionamiento normal.

Para poder mantener un sistema en un estado de funcionamiento seguro es necesario conocer primero los aspectos que lo podrían transformar en inseguro. El conocimiento en profundidad de las características de los sistemas servirá para tomar conciencia del impacto que puede provocar el uso incorrecto del mismo o la existencia de una vulnerabilidad.

Es por esto que se requiere ante todo estar informado. Claro que en un mundo donde la información circula a altísima velocidad, cuesta demasiado estar constantemente actualizado en lo que a tecnología se refiere, pero tratándose de la seguridad, será una tarea crítica para poder obtener resultados positivos.

Existe una gran cantidad de recursos en la web que nos pueden mantener al tanto de las noticias de seguridad. Tal vez una de las más reconocidas de habla hispana sea Hispasec (http://www.hispasec.com/). También en la sección de noticias del sitio “Delitos Informáticos” podemos hallar datos actualizados (http://www.delitosinformaticos.com).

Es recomendable contar con distintas fuentes, ya que las noticias suelen ser encaradas para en distintos niveles de usuario, desde lo meramente informativo hasta lo más técnico.

Los **Hotfixes** son componentes diseñados para reparar problemas que ocurren en un número de servidores o equipos de trabajo relativamente pequeño. Son creados en general por el proveedor del software cuando aparecen ciertos problemas de compatibilidad o funcionalidad con un producto de un fabricante utilizado en una plataforma de hardware específica. En español se encuentra traducido muchas veces a la palabra "revisión" al referirse a un hotfix.

Por lo general suelen contener uno o más archivos, y tienen como fin resolver problemas de reciente aparición, como son los agujeros de seguridad. Pueden instalarse manual o automáticamente a través de un sistema de gestión de paquetes como puede ser Windows Update para el sistema operativo Windows, YUM o APT para el sistema operativo Linux.

Muchas veces un hotfix no es sometido a rigurosas pruebas antes de ser lanzado, pues soluciona problemas críticos que fueron descubiertos recientemente. Por lo tanto, los hotfixs simplemente sirven para solucionar un problema específico, y se recomienda al igual que con los updates, instalarlos sólo si es necesario, para el caso sería cuando se manifieste ese error o problema en la aplicación o sistema operativo.

En lo posible, se deberían probar en un ambiente que no sea de producción, y solo luego de una etapa de prueba debería considerarse la aplicación en producción. También es bueno tener en cuenta una metodología de vuelta atrás, en el caso de querer eliminarlos luego de ser aplicados.

En el caso de Microsoft, dispone del “Microsoft Network Security Hotfix Checker” (HfNetChk), una herramienta que puede ser descargada y utilizada en los sistemas Windows y sirve para detectar faltas de parches en el sistema. También existen herramientas de otras compañías para la misma tarea.

Los **Service Packs** son grupos de parches que se utilizan para actualizar, corregir y mejorar aplicaciones y sistemas operativos. Son testeados sobre una gran cantidad de hardware y aplicaciones, a fin de asegurar compatibilidad con otros parches y actualizaciones existentes, y para cubrir mucha más área funcional que un conjunto de hotfixes. También se recomienda que sean testeados antes de ser aplicados en entornos de producción, esto es porque más allá de los testeos que pueda realizar el proveedor del software, sería imposible probar todas las combinaciones de sistemas que podemos encontrar en el mercado, con lo cual dependerá del administrador el testeo propio.

La denominación “Service Pack” fue popularizada por Microsoft cuando comenzó a agrupar conjuntos de parches que actualizaban su sistema operativo Windows. Son de dos tipos:

- Incremental: en la cual cada SP no contiene las actualizaciones anteriores, por lo que debe instalarse el SP anterior antes de instalar el SP siguiente.
- Acumulativo: que es el caso contrario, cada SP contiene el SP anterior, lo que hace mucho más fácil y rápida la actualización. Microsoft Windows posee esta técnica. Por lo general es altamente recomendable la instalación de un SP actualizado (especialmente los de sistemas operativos) para mejorar el rendimiento, reparar errores y solucionar agujeros de seguridad. De hecho es común que para poder ejecutar nuevas aplicaciones se deba obligatoriamente instalar determinados SP.

Un **parche** es una actualización de un programa usado para solucionar problemas o mejorar la usabilidad de una versión previa de la aplicación. Normalmente están relacionados con la seguridad. El proveedor del parche suele ser el mismo que el del software relacionado, que puede ser cualquier programa desde un procesador de texto o juego hasta un sistema operativo.

El término se origina probablemente en el nombre de una antigua utilidad de Unix llamada patch. El parche se puede aplicar a un binario ejecutable o al código fuente de un programa. Para el caso del archivo binario, puede ser modificado realizándole cambios o bien reemplazarlo por completo. Los tamaños de los parches varían, algunos parches solamente modifican un binario de la aplicación pero otros alteran mucho más contenido. Si el parche solo modifica el ejecutable, puede llegar a ser muy pequeño.

Para el caso de los parches de código, se aplican directamente al código fuente de las aplicaciones en lugar de a la versión compilada, por lo tanto un programador podrá saber que nuevas características añade el parche.

Por ejemplo, en el desarrollo del sistema operativo Linux, que publica todo su código libremente, Linus Torvalds (su autor original) recibe cientos de miles de parches desde muchos programadores para que los aplique en su versión. En estos proyectos de software libre, es común que los autores reciban parches o que mucha gente publique parches de forma autónoma que arreglan problemas o agregan funcionalidades.

Como dato curioso, podemos mencionar al servidor web más usado en la actualidad, Apache, que evolucionó como un conjunto de parches que un grupo de encargados de páginas web creaban para añadir funcionalidades. Además, su nombre deriva del hecho de que sea un conjunto de parches (en inglés, a patchy server o un servidor parcheado).

Existe una categoría de parches que tiene como fin el de alterar el comportamiento del software para fines específicos, no considerados por el proveedor, por ejemplo el de no pagar por un software pago, lógicamente que estos últimos son ilegales y no se recomienda su utilización.

La creciente industria del software y sus continuo ciclo de actualizaciones hace que sea necesario organizar de manera clara y segura la aplicación de parches y demás componentes orientados al mantenimiento del software, ya sean aplicativos o sistemas operativos.

De esta manera, muchos fabricantes de software diseñaron sistemas automáticos para la aplicación de parches, a fin de resolver los posibles problemas derivados de la gran cantidad de software existente para ser administrado y mantenido.

Para los sistemas operativos más utilizados, como la serie Windows, de Microsoft, existen también aplicaciones de terceras partes, que también pueden gestionar parches de dicha plataforma. Un claro ejemplo de un completo sistema de aplicación de parches es el "Windows Server Update Services" (WSUS) de Microsoft, que provee actualizaciones de seguridad para los sistemas operativos Microsoft Windows y otras aplicaciones. WSUS es una alternativa centralizada de otros sistemas como Microsoft Update. Mediante WSUS los administradores pueden manejar centralmente la distribución de parches a través de Actualizaciones automáticas a todas las computadoras de una red corporativa.

WSUS se desarrolló a partir de Software Update Services (SUS), el que solo podía actualizar parches del sistema operativo. WSUS supera a SUS en que expande el rango de aplicaciones que puede actualizar. La infraestructura de WSUS permite que desde un servidor central se descarguen automáticamente los parches y actualizaciones para los clientes en la organización, en vez de hacerlo del sitio web Microsoft Windows Update. Esto ahorra ancho de banda, tiempo y espacio de almacenamiento debido a que las computadoras individualmente no necesitan conectarse a servidores externos a la organización, sino que se conectan a servidores locales.

7.1.1 Seguridad en capas

Podemos considerar que una estrategia de seguridad para una organización es más efectiva cuando los datos están protegidos por más de un nivel de acciones. La estrategia de seguridad de defensa en capas utiliza varios niveles de protección. Si un nivel se ve comprometido, no pondrá en peligro a toda la organización. Una estrategia de defensa en capas aumenta la probabilidad de detectar un intruso y disminuye su oportunidad de éxito.

Para reducir al mínimo la posibilidad de que un ataque alcance su objetivo, debemos implementar el grado apropiado de defensa en cada nivel. Además, debe utilizar herramientas, tecnologías y directivas, y aplicar las recomendaciones con el fin de proteger cada nivel.

Entre los niveles a tener en cuenta, podemos discretizar algunos del los más importantes:

- Seguridad administrativa: políticas, normas y procedimientos
- Seguridad física: guardias de seguridad, bloqueos y dispositivos de seguimiento
- Perímetro de red: de seguridad de hardware y software, redes privadas virtuales
- Red interna: segmentación de red, IPSec, IDS de red
- Host: autenticación, IDS de host
- Aplicación: software antivirus
- Datos: listas de control de acceso (ACL) y cifrado

Un correcto trabajo en cada uno de los niveles supone un mayor nivel de seguridad que crece exponencialmente con la conjunción de los mismos.

7.1.2 Menor Privilegio

Muchas organizaciones dan a los usuarios privilegios de administración para sus equipos. Esta medida es particularmente común en el caso de los equipos portátiles. En ciertas ocasiones se intenta

justificar aduciendo que algunos programas sólo pueden ejecutarse con derechos administrativos, o para permitir que los usuarios móviles instalen hardware o software relacionado con el trabajo. A pesar de que pueden existir algunas razones, esta medida aumenta considerablemente el riesgo de compromiso de equipos.

Así llegamos a la necesidad de uno de los principios más importantes de la seguridad informática, que es el del menor (o mínimo) privilegio. El mismo está contemplado en el documento “Criterios de Evaluación de Sistemas Informáticos de Confianza” del Departamento de Defensa de los Estados Unidos (TCSEC DOD-5200.28-STD), también conocido como el Libro Naranja. Esta publicación, que fue un estándar aceptado para la seguridad de equipos por muchos años, define el privilegio mínimo como un principio que “requiere que a cada sujeto de un sistema se le otorgue el conjunto de privilegios más restrictivo (o la autorización más baja) necesario para el desempeño de sus tareas autorizadas. La aplicación de este principio limita el daño que puede generar un accidente, error o uso no autorizado”.

De una manera muy simple, podemos complementar lo antedicho, considerando que si un usuario no requiere de un recurso específico para realizar sus tareas, entonces no debería tener acceso a dicho recurso, ya que esto permitiría que sea utilizado (intencionalmente o no) para ocasionar una brecha de seguridad.

El correcto uso y aplicación de los principios fundamentales de la seguridad ayuda a mantener una organización estable basada en conceptos ampliamente aceptados, los cuales se combinan para lograr mejores resultados con el tiempo y el aprendizaje.

7.1.3 Control de cambios

Son muchos los negocios que dependen fuertemente de la integridad de sus datos y se sabe que determinados cambios pueden corromper un eficiente modelo de seguridad. Dado que la modificación de los sistemas puede afectar su garantía, es que surge la necesidad del control de cambios. El control de cambios en un entorno tecnológico particularmente, cobra vital importancia debido a que cada parte constituyente del sistema puede debilitar al sistema completo. Podemos definirlo como aquel proceso que tiene como objetivo introducir cambios en el ambiente de tecnología informática de manera rápida y con mínima interrupción del servicio. Como caso general de control, hablaremos de “Administración de Cambios”.

Los cambios se refieren tanto a tecnología, sistemas, aplicaciones, hardware, documentación, procesos, roles y responsabilidades. Esta administración de cambios tiene a su cargo proveer el manejo rápido y eficiente de cualquier requerimiento de cambios que se haya realizado.

El control efectivo de cambios nos permite descubrir distintos problemas, desde la violación de políticas internas hasta posibles fallas de hardware. Por esto es necesario el desarrollo de procesos formales que aseguren que solo las modificaciones autorizadas son realizadas y que estas se efectúan en los tiempos establecidos utilizando procedimientos admitidos.

Tomando en cuenta los ítems anteriores, es recomendable también detenerse en la creación de procedimientos de roll-back a versiones anteriores de software, o quitado de parches y hotfixes para los casos en que una modificación genere problemas.

7.1.4 Control de Integridad

Desde el punto de vista de la seguridad informática, podemos definir la integridad como aquella característica que determina que toda modificación a datos o información es realizada por personas autorizadas utilizando procedimientos autorizados. También es posible aplicar la definición a procesos. Los controles de integridad son aquellos que tienen como objetivo el cumplimiento de la definición, contando con mecanismos y métodos que permitan establecer parámetros para conseguirlo. Existen diversas herramientas que pueden ayudar a gestionar la integridad de los componentes de un

sistema. Tomando como ejemplo la integridad de los datos, una herramienta deberá realizar comprobaciones periódicas del mismo, de manera tal que pueda detectar posibles cambios. Particularmente para este caso, si se tratara de datos binarios almacenados en un disco rígido, podemos utilizar procedimientos matemáticos y técnicas criptográficas. La forma más sencilla de ejemplificar esto sería mediante la aplicación de una función unidireccional de hash, que producirá un resumen (digest) que actuará a modo de firma para dicho dato, y que será la contrastada sucesivamente en las etapas de comprobación periódica. Un cambio en un solo bit del dato produce una firma diferente, que determina que el dato fue alterado. Para que pueda ser modificado por métodos autorizados, deberíamos poder realizar nuevas firmas cada vez que se realiza una modificación, y el sistema de control de integridad tendrá en cuenta esto, lo cual genera también la necesidad de protección de la base de datos de las firmas.

7.1.5 Firewalling

El hecho de contar con un dispositivo de firewalling en el perímetro de una red, nos obliga a analizarlo como parte del hardening del sistema informático. Esto puede parecer redundante, ya que los Firewalls se configuran exclusivamente para brindar seguridad, pero dicha tarea no implica un funcionamiento inherentemente efectivo. Puede continuar pareciendo una obviedad, pero una verdadera configuración segura de un dispositivo perimetral como lo es un Firewall, requiere un estricto control y verificación, tanto antes de ser puesto en marcha como periódicamente, o bien cuando exista un requerimiento que lo amerite.

La regla de oro a seguir será la siguiente: “todo aquello que no fue explícitamente permitido, debe ser prohibido”. Esto implica mucho trabajo de configuración, ya que frente a cada requisito de entrada o salida de la red, se debe contemplar una regla de filtrado, y si consideramos la gran cantidad de puertos y accesos que utiliza el software en los sistemas actuales, es fácil notar la complejidad que se asume al cumplir esta regla.

De todas maneras, al instalar un Firewall puede ser preferible priorizar la incomodidad inicial frente a la exposición inicial, ya que la primera se mitiga con el tiempo y un cuidadoso seguimiento y la segunda podría conducir a incidentes. Así podemos comenzar a realizar los chequeos correspondientes dependiendo del tipo de Firewall con el que contemos. No olvidemos que no es lo mismo un filtrado de capa 3 (por dirección) que un filtrado de capa 4 (por puerto), así como tampoco será lo mismo el filtrado en capa 7 (aplicaciones). Para cada instancia de revisión, debemos comprobar que el uso de cada recurso es indispensable para quien lo solicita.

Se debe tener sumo cuidado al intentar modificar reglas o directivas previamente definidas, ya que el procesamiento ordenado y secuencial de las mismas, tiene un efecto específico para cada petición de acceso. Es decir, se debe comprender el funcionamiento completo del Firewall y sus reglas para poder considerar modificaciones.

Por otra parte, un Firewall no nos protegerá de ataques internos ni sustituirá otras medidas de seguridad, por lo tanto deben considerarse como un elemento más (aunque indispensable) de la seguridad de un sistema. En cuanto a los parches y actualizaciones de seguridad, deben tenerse en cuenta, tanto para los Firewalls por software como por hardware (firmware upgrade).

Los sistemas operativo Windows poseen un sistema de Firewall reducido que provee características de filtrado. Los sistemas del tipo GNU/Linux basan su filtrado de paquetes en el esquema de netfilter, implementado mediante la herramienta iptables. Está considerado uno de los sistemas de filtrado más potentes que existen.

7.1.6 HIDS

Los sistemas de detección de intrusos (IDS) pueden estar basados en Host o ser de Red. Esta principal clasificación determina el uso que se le dará y su ámbito de aplicación. En este caso nos

referimos a los Host IDS (HIDS) y las consideraciones en cuanto al hardening de los mismos.

Primeramente, será necesario tener en cuenta el sistema operativo sobre el cual se quiere realizar la detección, ya que de este dependerá el software utilizado y diversas medidas basadas en su funcionamiento interno. Una vez definido el SO, podemos definir algunos criterios de selección y optimización

Uno de los principales podría ser la carga de la CPU, esto es debido a que tendremos que establecer una buena relación entre detección y rendimiento. De nada servirá un sistema muy ajustado que no permita trabajar a las aplicaciones y usuarios, pero tampoco servirá un sistema que no consuma tantos recursos y a la vez sea ineficiente.

Otro de los aspectos será el uso en el disco rígido. Esto es relativo al tamaño que la aplicación utiliza para sí mismo, tanto en su estado fundamental recién instalado, como a través del tiempo con los nuevos archivos generados (firmas, logs, etc.)

Continuando con los criterios, podemos tomar en cuenta la usabilidad, ya que nos permitirá el mejor acceso a la configuración, y finalmente, estudiaremos la calidad en la detección, ya sea para ataques conocidos como desconocidos.

Una buena optimización de seguridad en cuanto a HIDS consistirá en la verificación de la detección y posterior ajuste (realimentación) dentro del sistema. Es necesario que los patrones y firmas estén actualizados, y que se haya contado con suficiente tiempo de entrenamiento, el cual dependerá del tamaño, carga y tráfico del equipo en cuestión (por lo general servidores).

La optimización también constará en asegurarse de que los patrones de comportamiento considerados por nosotros como intrusivos, son efectivamente detectados, y que frente a cada nivel de alerta se origine el aviso correspondiente, ya sea en la consola local, o mediante mensajes al administrador (e-mail, sms, etc.).

7.1.7 Listas de comprobación (Checklist)

Las listas de comprobación son una serie de guías metodológicas que se utilizan para controlar que una tarea es realizada por completo (muchas veces en un determinado orden) y sin olvidar los ítems fundamentales de la misma. Estas checklists se utilizan tanto en procesos de auditoria informática como en tareas cotidianas de mantenimiento y también para realizar procedimientos definidos y repetibles.

En la práctica son una herramienta que intenta apuntalar la dificultad de las personas para recordar demasiadas tareas, y por otro lado, asegura un estándar en el relevamiento de datos realizado, a fin de ser procesado posteriormente de manera más fácil y rápida.

Las listas de comprobación deben ser confeccionadas por personas idóneas para tener la plena certeza de que se contemplara todo lo necesario para completar la tarea en cuestión. Muchas veces es bueno que estén sujetas a revisión antes de ser puestas en uso.

No debe olvidarse que es bueno tomar como parámetro otras listas de comprobación relacionadas, ya que de esa manera se pueden ajustar a nuestras necesidades sin tener que crearlas desde cero, con un consecuente ahorro de tiempo y esfuerzo. Para ayudarnos en esta tarea, existen aplicaciones para crear listas de comprobación, pero bien puede utilizarse un simple procesador de texto.

7.1.8 Hardening en SO

Las listas de comprobación son una serie de guías metodológicas que se utilizan para controlar que una tarea es realizada por completo (muchas veces en un determinado orden) y sin olvidar los ítems fundamentales de la misma. Estas checklists se utilizan tanto en procesos de auditoria informática como en tareas cotidianas de mantenimiento y también para realizar procedimientos definidos y

repetibles.

En la práctica son una herramienta que intenta apuntalar la dificultad de las personas para recordar demasiadas tareas, y por otro lado, asegura un estándar en el relevamiento de datos realizado, a fin de ser procesado posteriormente de manera más fácil y rápida.

Las listas de comprobación deben ser confeccionadas por personas idóneas para tener la plena certeza de que se contemplara todo lo necesario para completar la tarea en cuestión. Muchas veces es bueno que estén sujetas a revisión antes de ser puestas en uso.

No debe olvidarse que es bueno tomar como parámetro otras listas de comprobación relacionadas, ya que de esa manera se pueden ajustar a nuestras necesidades sin tener que crearlas desde cero, con un consecuente ahorro de tiempo y esfuerzo. Para ayudarnos en esta tarea, existen aplicaciones para crear listas de comprobación, pero bien puede utilizarse un simple procesador de texto.

La seguridad de los sistemas operativos es la base del nivel de seguridad esperable para todo lo que dependa del mismo, empezando por las aplicaciones. Es por esta simple razón que debe dedicarse un tiempo razonable a la segurización inicial del mismo, ajustando sus configuraciones e intentando que no queden opciones por defecto sin analizar.

Comenzaremos estudiando el proceso de inicialización del sistema, pasando por la selección del sistema de archivos y su integridad, hasta el ajuste de políticas y logs de auditoria. Luego estudiaremos la configuración de los protocolos relacionados con el uso de las redes e Internet, y veremos algunas herramientas útiles a la hora de realizar hardening.

Debemos tener en cuenta que con el concepto de hardening siempre intentará segurizar la plataforma con las herramientas que la misma cuenta, y mediante el ajuste de configuraciones existentes. El agregado de aplicaciones externas escapa al concepto ortodoxo de hardening, aunque por supuesto que sirve a los fines de la seguridad.

Es importante conocer el estado en el que se encuentran los sistemas operativos “out of the box” para poder reforzarlos a partir de dicho estado. En el caso de sistemas Windows, es bien conocido el estado recién instalado, ya que será único para toda instalación. Para el caso de sistemas GNU/Linux, la gran variedad de distribuciones y opciones de instalación existentes hace que se torne más complejo el hecho de saber a priori el estado en el que queda el sistema out of the box.

Como normal general, empezaremos por dejar en los sistemas solamente las aplicaciones y características que se utilizarán específicamente.

7.1.9 OS y NOS

A la hora de reforzar los sistemas, es bueno tener en cuenta para empezar, las recomendaciones que da el proveedor del mismo. En cuanto a los sistemas instalados en equipos cliente, tendrán configuraciones especiales que los harán dependientes en gran medida de los servidores contra los cuales realicen sus tareas. Por su parte, los servidores pueden diferir en sus aplicaciones instaladas y los servicios que proveen.

Se debe tener especial cuidado de no desactivar servicios y funciones importantes del sistema, tomando en cuenta que algunos SO permiten deshabilitar incluso las funciones críticas. Una práctica recomendable es documentar todos los cambios que se realizan, a fin de poder construir una metodología replicable en el futuro, y también para poder volver hacia atrás las modificaciones en caso de necesitarlo.

El sistemas operativo más utilizados hoy en día en equipos de escritorio es sin duda Windows XP de Microsoft, que poco a poco reemplazó a las versiones anteriores (Windows 95, 98 y ME). En menor medida se pueden encontrar equipos con sistemas GNU/Linux, cada vez más cerca del usuario final, y Mac OS X en equipos Apple.

En cuanto a sistemas de red, también Microsoft tiene gran presencia con su serie comenzada por los clásicos Windows NT y 2000, hoy evolucionados hacia Windows 2003/2008. Pero en el ámbito de los

servidores también encontramos una amplia difusión de sistemas derivados de UNIX, como ser Sun Solaris, HP-UX, AIX, BSD, y por supuesto, GNU/Linux. Por otro lado tenemos Novell Netware, que implementó su propio protocolo y basa su seguridad en lo que se denominó NDS (Network Directory Service) hoy conocido como eDirectory.

7.1.10 Seguridad desde el inicio

Si bien la seguridad del sistema en sí mismo la podemos evaluar una vez que lo tengamos funcionando en un estado estable de operación, todo sistema operativo atraviesa una serie de estados previos a la operación por parte del usuario.

Es entonces en este punto que tomaremos en cuenta los procesos previos a la carga total del sistema. Por empezar, los estados internos de operación pueden no depender de las configuraciones que pueda realizar un administrador, exceptuando los sistemas libres, como ser GNU/Linux, donde root tiene la posibilidad de indicarle al sistema operativo absolutamente todas las operaciones que se deseen realizar, en un orden específico y con niveles de seguridad asociados.

Para el caso de plataformas Windows, es fundamental analizar el comportamiento y la carga de los servicios y programas al inicio. Esto normalmente se puede acceder mediante herramientas propias, como msconfig.exe o bien de terceros, como autoruns.exe de Sysinternals (aunque hoy perteneciente a Microsoft). Asimismo, es posible acceder manualmente a la ubicación de cada aplicación mediante la ruta correspondiente del registro de Windows, que puede manipularse con la herramienta regedit.exe, incluida en el sistema operativo.

Como norma de seguridad, debemos eliminar todos aquellos programas que se ejecuten al inicio y no sean obligatorios, así como también aquellos que si bien se cargan en el inicio, bien podrían ejecutarse manualmente cuando se los desee utilizar. Con los servicios ocurre lo mismo, por lo cual se debe prestar especial atención a la funcionalidad de cada uno y sus dependencias asociadas, a fin de que no se desactiven masivamente características necesarias pero a la vez no se reduzca la performance del sistema.

Otra barrera de seguridad que podemos tener en cuenta si hablamos de la inicialización de un sistema son los passwords de usuario, que pueden definirse en distintos niveles:

- Acceso al equipo: mediante una contraseña de BIOS
- Acceso a un SO en particular: mediante una contraseña en el gestor de arranque
- Acceso al SO: mediante el control de acceso correspondiente a la plataforma

Una buena combinación de líneas de defensa en el inicio brindará una barrera cada vez mas difícil de atravesar para los atacantes locales.

7.1.11 Sistemas de archivos

Los sistemas de archivos estructuran la información que será representada para su uso. Pueden ser clasificados en sistemas de archivos de disco, de red y de propósito especial. Un sistema de archivo de disco está diseñado para el almacenamiento de archivos en una unidad de disco, en tanto que uno de red es un sistema que accede a sus archivos a través de una red. Dentro de esta clasificación encontramos dos tipos: los archivos distribuidos y los paralelos. Por otra parte, los de propósito especial son aquellos que no caen en ninguna de las dos clasificaciones anteriores. Es necesario conocer sistemas de archivos más comunes a fin de poder seleccionarlos en función de sus características. Algunos de los más representativos son:

- **File Allocation Table (FAT):** Original de Microsoft. Se utiliza a veces como mecanismo de

intercambio de datos entre sistemas operativos distintos que coexisten en el mismo equipo. También se utiliza en tarjetas de memoria. Tiene baja tolerancia a la fragmentación (suelen fragmentarse mucho). No fue diseñado para ser redundante ante fallos. Carece de permisos de seguridad. Específicamente FAT 32 tiene un tamaño máximo de archivo de 4 Gb.

- **NTFS (New Technology File System):** Diseñado originalmente para Windows NT con el objetivo de crear un sistema robusto y con seguridad incorporada. Admite compresión nativa, cifrado y transacciones a partir de Windows Vista. Soporta permisos y journaling. Es adecuado para particiones de gran tamaño, puede manejar volúmenes de hasta aproximadamente 16 Terabytes usando clústeres de 4KB.
- **EXT3:** Es un sistema de archivos con journaling., el más usado en distribuciones GNU/Linux. Puede ser montado y usado como ext2, su predecesor. Utiliza un árbol binario balanceado e incorpora un avanzado asignador de bloques de disco. Su velocidad y escalabilidad es menor que sus competidores, como JFS2, ReiserFS o XFS, y tiene alta tolerancia a la fragmentación.
- **NFS:** Desarrollado por Sun Microsystems con el objetivo de ser independiente de la máquina, el SO y el protocolo de transporte. Los datos pueden ser accedidos y modificados por varios usuarios de tal forma que no es necesario replicar la información. Todas las operaciones se realizan de manera sincronica (la operación sólo retorna cuando el servidor ha completado todo el trabajo para la misma). En caso de una solicitud de escritura, el servidor escribirá físicamente los datos en el disco, y si es necesario, actualizará la estructura de directorios antes de devolver una respuesta al cliente. Esto garantiza la integridad de los archivos.

7.1.12 Políticas de cuentas

Las políticas de cuentas son parte de las configuraciones de seguridad, y determinan los privilegios y vigencia de las cuentas de los usuarios en un sistema. En general, se tendrán en cuenta las siguientes características:

- Política de contraseñas de acceso: longitud mínima, duración máxima, claves complejas, no repetición de claves, filtrado por patrones típicos.
- Política de bloqueo de cuentas: tras un número determinado de intentos de inicio de sesión fallidos. Se puede especificar un período de inhabilitación.
- Política de autenticación: ya sea mediante Kerberos o cualquier otro sistema. Las políticas de cuentas se aplican a nivel de dominio y afectan a todas las cuentas del mismo. De existir un grupo de usuarios que necesiten una política separada se recomienda segmentarlos en otro dominio.

Se debe tener cuidado de no contar con políticas demasiado estrictas para las cuentas, ya que pueden impactar negativamente en los usuarios, por ejemplo, al obligar a u usuario a recordar contraseñas nuevas y largas lo único que conseguimos en el mediano plazo es que las anote en un papel o en un archivo de texto plano en su escritorio.

7.1.13 Auditoría

En general, se define como un proceso sistemático que consiste en obtener y evaluar objetivamente evidencias sobre las afirmaciones relativas a actos y eventos, con el fin de determinar el grado de correspondencia entre esas afirmaciones y los criterios establecidos, para luego comunicar los resultados a las personas interesadas.

En el entorno de los sistemas operativos, un registro de auditoria (log) es un registro permanente de acontecimientos importantes ocurridos en el sistema. La escritura del mismo se realiza

automáticamente cada vez que ocurre un evento, se almacena en un área protegida del sistema, y es un mecanismo importante de detección. El registro de auditoria debe ser revisado cuidadosamente y con la frecuencia adecuada. Las capacidades de auditoria que proveen un sistema o aplicación son las que van a permitir determinar qué elementos acceden a qué partes del mismo en sus distintos niveles.

Para los fines del hardening, es necesario ajustar al máximo las capacidades propias de los SO y combinarlas adecuadamente con las de las aplicaciones, a fin de poder contar con los registros más completos para cada área de operación. Debe tenerse cuidado de proteger el propio mecanismo de auditoría, ya que si se desactiva, de nada servirán tantos ajustes.

En el caso de que un sistema quede comprometido, los logs ya no serán de utilidad debido a que carecen de confiabilidad por el solo hecho de haber sido vulnerada la seguridad del sistema. Es posible considerar un sistema de log que solo permita escribir los archivos al final de los mismos (modo append) para que no puedan ser modificados en cualquier ubicación del mismo una vez escritos. Una vez alcanzado un determinado tamaño o pasado un tiempo predefinido, los logs pueden almacenarse, y deben hacerlo en un lugar seguro, que cuente con la posibilidad de accederlos si se requieren para futuros análisis. También podemos contar con un log server (servidor de logs) que podría centralizar los registros de auditoria de los distintos servidores de una red, para que puedan ser analizados y protegidos de manera más controlada. Por último, existe la posibilidad de utilizar registros físicos para casos muy especiales o críticos.

7.1.14 Seteos de Seguridad

Las configuraciones de seguridad de los sistemas serán las herramientas propias de estos que nos permitirán contemplar aspectos relativos a la seguridad. En el caso de los sistemas de escritorio orientados a usuario final, como Windows XP, las configuraciones principales se realizan desde una ventana especial ubicada en el panel de control, llamada “Centro de Seguridad”

Dentro de esta ventana se encuentran centralizados los controles de Firewall de Windows (Internet Conection Firewall), opciones de internet, y actualizaciones automáticas, incluyendo el chequeo de existencia de un software antivirus.

A nivel de servidor Windows las configuraciones de seguridad se manejan mediante la consola MMC correspondiente en las Herramientas Administrativas y provee acceso al a modificación en las directivas de cuentas, directivas locales y registros de sucesos.

También a nivel de Windows Server, para implementar una directiva de seguridad, se puede optar por varias formas:

- Ejecutando el archivo msi en el equipo en que desea implementar la directiva, desde el disco local o desde un recurso compartido
- Con el uso de la Directiva de grupo
- Mediante el uso de Microsoft Systems Management Server (SMS)

7.1.15 Configuración de Servicios y protocolos

Entre los protocolos asociados a distintos servicios de red, encontramos principalmente: NetBEUI, IPX/SPX y TCP/IP. En el caso de utilizar un sistema operativo de Microsoft, estos encapsularán a NetBIOS para el trabajo en red. El proceso de asociación de un protocolo a otro se denomina “binding”. NetBIOS significa "Network Basic Input/Output System" y es una especificación para acceso a servicios de red, es decir, una capa de software desarrollado para enlazar un sistema operativo de red con hardware específico. Fue originalmente desarrollado por IBM y Sytek como API para el software cliente de recursos de una red LAN.

NetBEUI significa “NetBIOS Extended User Interface”, y es un protocolo de nivel de red no enrutable utilizado desde las primeras redes Microsoft. Implementa los servicios de nombres, para registro y resolución de nombres, servicios de sesión para comunicaciones y servicio de distribución de datagramas.

TCP/IP está diseñado para enrutar, es fiable y adecuado para distintos tamaños de redes. Se utiliza a nivel mundial para conectarse a Internet, y es blanco de innumerables ataques de implementación y diseño, dada su amplia difusión y aceptación. No incluye características de seguridad, por lo tanto deben tomarse medidas externas para su uso como protocolo seguro.

IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange) es utilizado por los sistemas Novell Netware. IPX y SPX derivan de los protocolos IDP y SPP de los servicios de red de Xerox. El uso de IPX está disminuyendo desde el boom de Internet. Hoy es posible utilizar productos Novell sin IPX.

Para cada uno de estos protocolos, debemos realizar las configuraciones necesarias en los sistemas operativos, a fin de evitar posibles ataques. Un intruso podría cambiar la configuración de red en un equipo para que el comportamiento de las comunicaciones se modifique, por ejemplo, podría redireccionarse el tráfico, cambiarse el servidor de resolución de nombres, o bien utilizar nuestro sistema para lanzar ataques de denegación de servicios.

7.1.16 Estructura de directorios y datos

La estructura de directorios es la forma en que se definen los distintos directorios a lo largo de un sistema de archivos en un determinado SO. Cada SO tendrá su estructura estándar predeterminada, muchas veces obedeciendo a cuestiones históricas.

Para el caso de los sistemas basados en UNIX, la estructura se denomina Filesystem Hierarchy Standard (FHS) y coloca todos los archivos y directorios bajo el directorio raíz (“/”) aunque se encuentren en distintos dispositivos físicos. De esta manera, habrá directorios asociados a las carpetas de usuarios (/home), un directorio que contiene binarios ejecutables del sistema (/sbin), un directorio especial para el administrador (/root), uno para archivos de configuración (/etc), uno para bibliotecas (/lib) y varios más, cada uno considerando las funciones específicas que se requieren para el uso de las aplicaciones en un SO. En el caso de los sistemas Windows, tendremos la carpeta llamada de la misma forma, que se considera el directorio principal del sistema operativo. Además, en las versiones de Windows XP por ejemplo, aparece la carpeta “Documents and Settings”, donde se almacena la información y archivos de los usuarios. También tenemos por ejemplo la carpeta “Archivos de Programa”, ya disponible en sistemas Windows anteriores, que guarda los archivos de las aplicaciones que se van instalando. Las consideraciones de seguridad referentes a la estructura de directorios serán analizadas desde el punto de vista de su posible aprovechamiento, por ejemplo, podemos recorrer los directorios conocidos en busca de archivos y carpetas que sabemos que no deberían estar en ese lugar (un atacante podría utilizar estos lugares para esconder ejecutables de código malicioso). En cuanto al hardening, solo debemos asegurarnos de que la estructura se mantenga íntegra y familiarizarnos con la misma a fin de poder detectar problemas mientras permanezca instalado el sistema operativo.

7.1.17 Herramientas para el aseguramiento de sistemas

Si bien el hardening puede realizarse manualmente, cuando se realiza en numerosos equipos puede transformarse en una tarea tediosa. Para completar entonces un correcto y rápido hardening del sistema pueden utilizarse herramientas automatizadas

Estas utilidades permitan reforzar aspectos específicos del sistema o bien aquellas que contemplen toda la plataforma. Dichas herramientas dependen exclusivamente del sistema operativo a tratar.

En plataformas GNU/Linux suelen ser grupos de scripts que actúan directamente sobre archivos de

configuración, en tanto que en sistemas Windows suelen tener menus gráficos con selección de opciones para las diferentes posibilidades de segurización. Algunos programas freeware o libres para realizar hardening son:

- Syhunt: refuerza Apache/PHP
- Windows Worms Doors Cleaner: controla algunos puertos de servicios específicos
- XPantispy: refuerza diversos aspectos de Windows
- harden-tools: paquete para Debian Linux

Para completar la lista, no podemos dejar de mencionar a Microsoft Baseline Security Analyzer (MBSA) que es una herramienta fácil de utilizar que ayuda a determinar el estado de seguridad en función de las recomendaciones de seguridad de Microsoft y ofrece guías para corregir los fallos.

- **Bastille Linux:** Bastille es un programa para hardening de SO GNU/Linux que actúa mediante el bloqueo de características habituales, configurándolo para que se comporte de manera proactiva frente a la seguridad, y disminuya la susceptibilidad de ser comprometido. Bastille también puede evaluar el estado actual de seguridad de un sistema, reportando los seteos con los que trabaja, e incluso considera la funcionalidad de deshacer y revertir. Bastille hace foco en dejar que el administrador elija como quiere segurizar el sistema. En su modo por defecto hace preguntas interactivas, explicando los temas y creando una política basada en las respuestas del usuario o administrador (root). Luego aplica las políticas al sistema. En su modo de valuación, crea un reporte orientado a explicarle al usuario los tópicos relativos a las opciones disponibles mientras le indica cuales son las que están vigentes en el sistema en ese momento. Otro de los objetivos de Bastille es educar al administrador respecto a la seguridad, ayudándolo a realizar elecciones concretas y bien pensadas.
- **Grsecurity:** ofrece una serie de parches al núcleo de Linux para mejorar la seguridad del sistema. No es un servicio adicional de seguridad ni un módulo de kernel. Toma prestados algunos conceptos de LIDS (Linux Intrusion Detection System). Provee protecciones para distintos tipos de ataques a nivel de software e incluye auditoria adicional del kernel. (figura 3.3.10) Toma el modelo de “detección, prevención y contención”. Para cada una de estas instancias se vale de diferentes mecanismos. El proyecto nos ofrece prevención contra Buffer Overflows mediante el sistema PaX, control de Acceso basado en Roles (RBAC), aleatoriedad en los ID de los procesos y la pila TCP/IP y vistas restringidas de los procesos, entre otras cosas. Los parches se distribuyen en un único parche que se aplica al kernel, el cual pesa menos de un megabyte actualmente, y habilita las características antes mencionadas, muchas de las cuales son independientes entre sí. Cada funcionalidad opera como un pequeño parche del kernel y algunas pueden resultar en una sensible baja de la performance.

7.1.18 Plantillas de seguridad

Las plantillas de seguridad son conjuntos preconfigurados de opciones que se aplican a los sistemas operativos o aplicaciones con el fin de ajustar su nivel de seguridad. La plantilla en sí misma es un archivo de texto que representa una configuración. Se pueden aplicar a un equipo local, importar a un objeto de directiva de grupo o utilizar para analizar la seguridad. Normalmente están asociadas a la plataforma Windows y se manejan mediante el complemento de Plantillas de seguridad para Microsoft Management Console (MMC). Se pueden usar tal como se suministran o se pueden crear plantillas personalizadas, para lo que hay que modificar la configuración de las plantillas de seguridad integradas. Después de hacer los cambios en la plantilla, pueden aplicarse al sistema. Las plantillas se pueden aplicar a un equipo local, un dominio o una unidad organizativa. En sistemas Windows existen cuatro categorías de plantillas de seguridad pregeneradas: Básica, Segura, Alta seguridad y

Variada. Las plantillas de seguridad básica, segura y de alta seguridad representan niveles de seguridad crecientes. Las plantillas variadas incluyen las de compatibilidad, componentes opcionales, y de configuración original. Es importante utilizarlas adecuadamente. Esto implica por ejemplo, no aplicarlas sin haberlas probado, no modificar una original sin guardarla y conocer bien la implicancia de todas las opciones disponibles.

7.1.19 Web Servers

Los web servers (servidores web) se han transformado en uno de los elementos indispensables para la interacción entre usuarios e información. Esto se debió al crecimiento de los lenguajes y tecnologías web desarrolladas en nuestros días, mediante los cuales es posible crear complejos sitios dinámicos, relacionarse con bases de datos, o bien manejar aplicaciones.

La seguridad en los web servers estará distribuida entre todos sus componentes, no solamente en la aplicación que maneja las páginas. De esta manera, será necesario asegurar el sistema operativo, el motor de bases de datos y el código fuente que se incorpore. Además, se deben considerar las medidas externas como ser el perímetro de red o DMZ en la cual esté colocado el servidor. Los servidores web pueden dar servicios internos o externos, lo cual también hace que tengan que restringirse de manera especial las solicitudes dependiendo de su origen.

Es importante utilizar protocolos seguros (HTTPS, SSL, etc.) además de los tradicionales, a fin de poder manejar transacciones seguras mediante sistemas criptográficos, con los correspondientes certificados digitales.

Los software's de servidores más utilizados en la actualidad son:

- Apache: un software libre de código abierto para plataformas basadas en Unix y también con versiones para Windows. Se desarrolla dentro del proyecto HTTP Server de la Apache Software Foundation.
- Internet Information Server: una serie de servicios para Windows. Originalmente era parte del Option Pack para Windows NT, luego fue integrado en otros sistemas de Microsoft. Los servicios que ofrece son: FTP, SMTP, NNTP y HTTP/HTTPS.

7.1.20 Control de acceso

Muchas veces se nos presenta la necesidad de restringir el acceso en ciertas áreas de los web servers. Esto puede controlarse modificando los permisos de los usuarios en el servidor o bien por la creación de listas de control de acceso. Pero a veces no se dispone de privilegios para modificar los permisos ni crear listas, por lo que debe haber alternativas, como basarse en el secreto de la ubicación (URL) de lo que se desea proteger. Este tipo de protección está basada en el cliente y no puede considerarse del todo seguro.

Si queremos proporcionar una interfaz más flexible será necesario tener una pequeña aplicación en algún lenguaje como Java, JavaScript, CGI, ASP, o PHP, por ejemplo. Esta aplicación debería presentar una ventana donde se solicite un nombre de usuario y contraseña (pueden también utilizar cookies para almacenarlas). Una primera limitación utilizando JavaScript es que se puede examinar editando el código fuente de la página, por lo que no debería definirse ninguna clave allí dentro, sino utilizar otros métodos de control.

En Java se puede elaborar un método similar que consistente en solicitar una clave a través de un applet. El código comprobará si existe la página para luego abrirla en la misma ventana desde la que se lanzó la applet. Tampoco conviene incluir la clave dentro del código ya que hay técnicas para obtenerla a partir de los archivos compilados “.class”. Sin embargo, Java provee métodos más seguros que JavaScript. ASP resulta útil cuando se desea acceder a bases de datos y páginas generadas al vuelo.

Normalmente se presenta una página de autenticación para solicitar el usuario y la clave. No es necesario preocuparse por el código VBScript al descubierto ya que en ASP el código se ejecuta en el servidor y no en el cliente. De esta manera acceder directamente a la página de login no ofrece pistas acerca de otros contenidos. Hay que tener cuidado con el uso de la función de autocompletar. En cuanto a CGI, una aplicación debe alojarse en servidor para realizar la validación, pero en este caso el programa se compila.

7.1.21 Estructura de directorios y datos

En la estructura de directorios del web server deberemos asegurar que cada lugar se acceda solamente en las condiciones esperadas, es decir, solo usuarios autorizados por medio de métodos autorizados.

Muchas veces al introducir una URL apuntando a un directorio pueden aparecer listados todos los contenidos, lo cual invalidaría algunos métodos de protección, es por esto que deberían deshabilitarse los listados en el server.

Otro tema delicado es que una vez que se accede a una página protegida (es decir una vez que conoce su URL) nada impide que se guarde en los marcadores para futuro acceso sin pasar por el proceso de autenticación, incluso mediante un enlace desde otro sitio. Para resolverlo, es necesario cambiar con cierta frecuencia los datos de acceso del archivo a proteger. En ASP no aparece este problema ya que el proceso de autenticación se incluye en la página a proteger. Utilizando CGI también se evita este problema. Es una buena práctica el hecho de no utilizar opciones y nombres por defecto en archivos y directorios. Por otro lado, debe tenerse sumo cuidado en cuanto a la ubicación de los logs de auditoria, con su consecuente protección.

7.1.22 Logging

El sistema de logs en un webserver es la herramienta fundamental en la que se basa el análisis y posterior interpretación de la información obtenida de la navegación realizada en las páginas contenidas en el mismo.

En los logs de un webserver interesan principalmente los datos de los navegantes, es decir, la dirección de origen, navegador utilizado, hora de acceso, tiempo total de conexión, y operaciones realizadas contra el sitio. El consorcio W3C determina un formato standard para logs de servidores web, pero existen distintos formatos propietarios.

Es de esperarse que la cantidad de información obtenida por los registros de un webserver pueda ser mucha, por lo cual puede ser necesario contar con aplicaciones externas para su análisis. Así nacen las herramientas de análisis de logs, que tienen la capacidad de correlacionar eventos y datos a fin de obtener información procesada que sirva para el administrador. Normalmente los logs solo deben ser accedidos por el administrador, nunca por los usuarios del sistema. El análisis estadístico de los logs puede usarse para definir patrones de tráfico, comportamiento o similares.

Como todo sistema de logs, debe tenerse en cuenta el almacenamiento de los logs antiguos (incluyendo su compresión y seguridad) y los ciclos de rotación definidos.

7.1.23 Ejecución de Backups

Así como ocurre con la información utilizada dentro de la empresa, es necesario hacer copias de respaldo en los servidores web, de forma tal que puedan restaurar un sistema después de una potencial perdida de datos. El backup es útil tanto para restaurar por completo un equipo a un estado operativo como para restaurar un pequeño número de archivos después de haberlos borrados o dañado accidentalmente. La copia de respaldo puede realizarse sobre los datos, el sistema operativo,

o ambos, pero claro que será considerada como un último recurso a utilizar. Es importante realizar copias específicas de las bases de datos relacionadas con los servidores web, además de la estructura funcional del sitio o las páginas.

Deben definirse claramente y de manera efectiva los métodos de realización de las copias. Así, se estudiará la necesidad de backups completos y diferenciales, dependiendo del nivel de actualización de los contenidos.

Por otro lado, se definirán los medios de almacenamiento, tanto locales como remotos, así como también la consideración de un sistema de servidores replicados en tiempo real en el caso de que sea necesario.

Como el servidor suele estar en uso mientras está realizándose su copia de seguridad, es posible que existan archivos abiertos. Esto representaría un reto al copiar un archivo en constante modificación. Existen diversas aproximaciones técnicas para resolver esto, algunas simplemente comprueban que no estén en uso los archivos, otros los cierran forzosamente antes de realizar la copia, y finalmente algunos utilizan algoritmos especiales para soportar el manejo de datos en caliente.

7.1.24 Manteniendo la integridad de los archivos

El tema de la integridad de los archivos y la información es uno de los pilares de la seguridad informática. No servirá que la información esté en condiciones operativas si está incompleta o alterada. Para que resulte inútil la información no necesariamente debe ser destruida, sino que con una sutil alteración puede quedar en estado de inutilización. En los servidores web, tenemos diferentes archivos que deben ser protegidos contra alteraciones no autorizadas. Por empezar están los archivos de código fuente de los sitios web, además de los propios del sistema operativo y la aplicación web en sí misma, pero también tenemos que cuidar los logs del sistema, que no pueden ser firmados de manera tan simple debido a su constante modificación.

La integridad de una página puede ser dañada por fallas de software o bien por ataques de intrusos que toman el control sobre algún sector y modifican su contenido (web defacing). Es responsabilidad del dueño que la información de la página esté en condiciones de integridad, y responsabilidad del prestador del servicio asegurar la integridad de la información a partir de que se encuentre en el servidor correspondiente. Se recomienda entonces utilizar software de chequeo de integridad para los archivos estáticos, y manejarse con políticas correctas para evitar la alteración no autorizada de los archivos que realmente deben cambiar (utilizar procedimientos autorizados).

7.1.25 Detección de Web Servers clandestinos

Los servidores fraudulentos y clandestinos son un tipo de fraude muy difundido en la actualidad. Algunos se basan en la imitación de un sitio para conseguir que los usuarios coloquen sus datos, especialmente en instituciones bancarias (phishing). Otros simplemente ofrecen servicios ilegales, protegidos por la ubicación geográfica o leyes locales.

Un sitio fraudulento suele adoptar un nombre y dirección muy similar al original, incluso tomando elementos directamente del mismo. También puede incluir links a distintos sitios oficiales legítimos para denotar confiabilidad. Una de las recomendaciones más importantes es ingresar directamente tipeando las direcciones en el navegador y no a través de links, que puedan derivar en una página fraudulenta.

Otros servidores contienen material ilegal, como ser software, música, películas y demás. Es por eso que muchos fabricantes de software solo proveen descargas desde su propio sitio y unos pocos autorizados genuinamente. Estos servidores suelen contener diversas formas de malware y software espía (spyware), además de continuas ventanas y pop-ups que tienen como fin hacer llegar al usuario información publicitaria sobre otros productos o servicios. Las descargas desde estos sitios suele

venir acompañada de la aceptación de varias condiciones, como bien podría ser la instalación de software. Finalmente se encuentran los servidores de pornografía infantil y demás delitos asociados, que se caracterizan por ofrecer dicho material a los usuarios registrados. Desde el punto de vista de la navegación es muy difícil saber si un sitio es original más allá de leer su verdadera dirección URL y posterior comprobación de su dirección IP mediante consultas de DNS, por lo tanto se debe hacer uso y comprobación de los certificados digitales para el caso de querer comprobarlos sin lugar a dudas.

7.2 PROGRAMACIÓN SEGURA

La industria del software en su creciente y decidida penetración en todos los aspectos de los negocios y procesos de las organizaciones modernas, es una de las realidades tangibles que la sociedad, particularmente del siglo XXI, observa con inquietante y curioso análisis. Si bien, la necesidad de generar mejores soluciones sistematizadas, que aumenten la efectividad de las acciones corporativas y den mayor valor agregado a sus clientes, se contrasta con las presiones e implicaciones que esto lleva en el desarrollo mismo de dichas soluciones. En este sentido, el balancear la necesidad de obtener un producto de software de óptima calidad que permita a la organización adelantar con oportunidad y alto contenido estratégico sus directrices de negocio, enfrenta un doble desafío para los dedicados a la programación y construcción de los sistemas de información de las organizaciones, así como para los clientes de los mencionados sistemas. Por un lado, todas las variables asociadas con la administración del proyecto en sí mismo, las cuales imprimen una importante complejidad al desarrollo de soluciones informáticas, y en segundo lugar, los altos estándares de aseguramiento de la calidad del desarrollo de software.

En esta encrucijada de formalidad administrativa y técnica, la construcción de sistemas de información ofrece un desafío práctico para las nuevas generaciones de programadores y administradores de proyectos informáticos, y una especial atención de los experimentados ingenieros de software para contextualizar sus aprendizajes en elementos conceptuales y formales que alimenten la práctica de la creación de software.

Por tanto y, considerando el gran reto de la construcción de software, la necesidad de soluciones de software intercomunicadas (orientadas al uso de redes de computadores), la utilización de modernos lenguajes de programación (JAVA, PYTHON, PERL, PHP, entre otros), la necesidad de soluciones eficientes y de alta portabilidad, el uso de metodologías de aseguramiento de calidad, se hace necesario revisar elementos relacionados con las prácticas y principios de programación segura como aspecto complementario del proceso de desarrollo de software.

7.2.1 Principios de un diseño seguro

Si bien las metodologías y estándares relacionados con el desarrollo y construcción de software buscan mantener altos niveles de confiabilidad y control de la solución informática, la seguridad informática y sus principios de diseño seguro no son parte formal de dichos estándares. En este sentido, la formalidad en la evaluación del diseño de la solución desde el punto de vista seguridad podría verse comprometida, dado que no se encuentran claros criterios de análisis en este sentido. En este sentido, muchos investigadores a nivel internacional han adelantado estudios interesantes sobre este particular, buscando elementos comunes que permitan orientar a los programadores en estrategias y principios que disminuyan potenciales problemas de seguridad asociado con el desarrollo del software.

Considerando éstos esfuerzos internacionales y tratando de establecer elementos básicos que orienten criterios en la programación segura de aplicaciones, se sugieren algunos principios del diseño seguro de aplicaciones que se enumeran y comentan a continuación:

1. ***Menor Privilegio:*** Este principio establece que un sujeto sólo debe dar a un objeto los privilegios que necesita para completar sus tareas asignadas.

2. ***Economía y simplificación de mecanismos de seguridad:*** Este principio establece que los mecanismos de seguridad que se establezcan deben ser tan sencillos como sea posible.
3. **Configuraciones por defecto seguras:** Este principio comenta que a menos que un sujeto haya otorgado acceso explícito a un objeto, éste no debería tenerlo. Es decir, todo lo que no está estrictamente permitido es prohibido.
4. **Mediación completa:** Este principio afirma que todos los accesos a un objeto(s) deben ser verificados para asegurarse de que cuentan con el permiso para hacerlo.
5. **Diseño Abierto:** Este principio establece que la seguridad de un mecanismo no debería depender del secreto o confidencialidad de su diseño o implementación.
6. **Privilegios Condicionados:** Este principio dice que se deben mantener los privilegios necesarios en diferentes momentos, en diferentes rutinas o programas. Es decir, los privilegios no deben ser estáticos para los programas o rutinas en el tiempo y en ejecución.
7. **Menor mecanismo común:** Este principio comenta que deben existir el menor número de recursos compartidos entre sujetos u objetos.
8. **Aceptación psicológica:** Este principio comenta que el mecanismo de seguridad que se establezca para un objeto no debe sugerir mayor dificultad a la que si el mecanismo no estuviese presente. En otras palabras, el mecanismo de seguridad deber ser fácil de usar.

Estos principios básicos enunciados, más que sugerir elementos novedosos a la programación de aplicaciones, nos recuerda que son prácticas generales que intuitivamente manejamos, pero que en el momento de la construcción de aplicaciones generalmente se dejan marginados. Por tanto, los principios de un diseño seguro, son directrices generales que deben materializarse en prácticas de programación que deberían ser parte de las formalidades del desarrollo del software mismo, donde la industria y la academia hacen parte fundamental de la misma disciplina.

Cuando estas mínimas sugerencias de diseño seguro no se consideran en la construcción de aplicaciones, la probabilidad de que surjan problemas de seguridad en el futuro es alta, dado que se compromete no solamente la funcionalidad misma de la aplicación sino las condiciones de su elaboración y ambiente de ejecución que puede socavar la confianza de los clientes frente a fallas donde se comprometa la integridad de la información de la organización.

7.2.2 Fuentes de vulnerabilidades en el Software

Complementario a los elementos establecidos alrededor de los principios de diseño seguro, es importante considerar e identificar elementos prácticos al buscar y establecer vulnerabilidades o fallas de seguridad en el software. Los elementos presentados a continuación responden a experiencias en el desarrollo de software que de alguna manera materializan la ausencia de uso de estándares de desarrollo de software y de adecuadas prácticas de programación, las cuales se encuentran directamente relacionadas con los escenarios de pruebas requeridos para verificar las condiciones y confiabilidad del software:

1. **Cambios en el ambiente de ejecución:** Los parches, los cambios en la configuración y variables de entorno alrededor de las aplicaciones son elementos críticos para mantener una ejecución adecuada y controlada de las rutinas y acciones previstas en el software. Al descuidar este aspecto, es probable involucrar efectos de borde o condiciones de excepción no previstas que comprometan no solamente un módulo de la aplicación sino el sistema de información mismo.
2. **Desbordamientos y chequeos de sintaxis:** Dos elementos importantes en la revisión y evaluación de software. Por un lado la evaluación de los desbordamientos bien sea de memoria o de variables específicas dentro de un programa y por otro lado, la verificación de buen uso de los comandos o palabras reservadas en el lenguaje de programación, que

permitan al programador un uso adecuado y eficiente de las estructuras. Si este aspecto no se considera con el rigor necesario, se estará comprometiendo la integridad del ambiente de ejecución de la aplicación.

3. **Convenientes pero peligrosas características del diseño del software:** Esta fuente de vulnerabilidad nos presenta funcionalidades que son deseables en el software para aumentar la versatilidad de uso de las aplicaciones. Entre estas tenemos herramientas de depuración o debugging, conexiones remotas en puertos especiales, entre otras, las cuales ofrecen importante elementos a los programadores y usuarios, pero que generalmente abren posibilidades de ingresos no autorizados que comprometen la integridad de sistemas y socavan la confianza del usuario frente a la aplicación
4. **Invocaciones no controladas:** En este aparte hacemos referencia a un inadecuado manejo de errores o excepciones en las aplicaciones o exceso de privilegios de ejecución, los cuales se manifiestan en comportamientos inesperados del software que generalmente ofrecen mayores privilegios o accesos adicionales a la información del sistema. En este sentido, el control adecuado de interrupciones, mensajes de error y entorno de ejecución de los programas se vuelve crítico al ser éstos elementos los que definen la interacción del software con el usuario final y su relación con el entorno de ejecución.
5. **Bypass a bajo nivel:** Las implicaciones de esta fuente de vulnerabilidades hace referencia al aseguramiento que la aplicación debe tener al ser invocada o ejecutada en un ambiente computacional seguro. El programador debe fortalecer y asegurar una manera autorizada de ingreso a la aplicación por parte del usuario, estableciendo mecanismos de monitoreo y control que velen porque esto se cumpla. El sobrepasar un control de acceso a un objeto, bien sea a través de permisos deficientemente otorgados, artificios que interrumpan la normal ejecución (contraseñas de BIOS) o por la manipulación de la memoria de ejecución de la aplicación constituye un atentado directo contra la confiabilidad e integridad del software.
6. **Fallas en la implementación de protocolos:** Los elementos de seguridad mencionados en este apartado, hacen referencia a las medidas de seguridad en redes. Si bien, los protocolos utilizados para transmisión y control de datos, presentan múltiples fallas, éstas con frecuencia no son consideradas dentro del proceso de implementación de una aplicación. En este sentido, sabemos que las aplicaciones que se ejecutan sobre TCP/IP tienen inherentes las fallas de éste conjunto de protocolos, por tanto es menester del programador establecer junto con el encargado de la seguridad informática, analizar los posibles requerimientos de seguridad necesarios para que la aplicación funcione sobre un ambiente de red que brinde mayores niveles de seguridad y control de tráfico.
7. **Fallas en software de base:** Todas las aplicaciones finalmente se ejecutan bajo la supervisión de un software de base o sistema operacional. Generalmente cuando se desarrollan aplicaciones, las condiciones o aseguramiento del software de base, no es condición para la adecuada ejecución de aplicaciones. Nada ganamos con aplicar y efectuar un amplio espectro de pruebas y controles, cuando el ambiente de ejecución o el software base no ha pasado por una valoración y afinamiento necesario para asegurar un ambiente de ejecución estable y seguro. En este punto, se llama la atención tanto a proveedores como a programadores, donde el trabajo conjunto debe ser una constante para incrementar los niveles de seguridad y disminuir las vulnerabilidades frecuentes inherentes al arte y la ciencia de programar.

En esta sección no se pretende estudiar de forma más profunda los aspectos relacionados con la programación segura, solo dar un resumen completo de sus principales características. La Metodología, o estándar de programación segura de ISECOM (Institute for Security and Open Methodologies) ahonda más en e tema, proponiendo prácticas seguras en el desarrollo de software y aplicaciones para la Web.

7.2.3 Vulnerabilidades de Scripting

Los lenguajes de scripting son aquellos que están diseñados para ser ejecutados por medio de un intérprete, a diferencia de los compilados. Muchos rechazan la clasificación de lenguajes interpretados y compilados, considerando que el modo de ejecución es independiente del mismo. Como ejemplo podemos nombrar los ya conocidos Perl, Python, Bash, Ruby y muchos más.

Particularmente en las plataformas GNU/Linux, el scripting es un componente fundamental de la administración, que se realiza en lenguajes como el anteriormente mencionado Bash, u otros intérpretes similares, como ser csh, tcsh, ksh y otros. La potencia y simpleza de esta clase de lenguajes aplicados a los sistemas Linux consigue una combinación muy poderosa para realizar todo tipo de tareas administrativas. Existe un tipo de ataque basado en la explotación de vulnerabilidades del sistema de validación de HTML incrustado que se denomina XSS por Cross Site Scripting (se lo llamó así para no confundirlo con la tecnología CSS). Originalmente abarcaba cualquier ataque que permitiera ejecutar código de scripting en el contexto de otro dominio. Estos errores se pueden encontrar en cualquier aplicación web, no solo sitios.

El problema radica en que normalmente no se validan correctamente los datos de entrada usados en las aplicaciones. Puede estar presente de forma directa, por medio de foros, mensajes de error o comentarios, o bien indirecta, por redirecciones o framesets, etc. En cuanto a los lenguajes de scripting, el intérprete puede considerar parte de la seguridad del mismo, pero la lógica será responsabilidad del programador.

7.2.4 CGIs

CGI, o Common Gateway Interface es una tecnología que permite a un cliente con un explorador web, solicitar datos de un programa ejecutado del lado del servidor web. CGI especifica un estándar para transferencia de datos entre cliente y programa. El resultado final de la ejecución son objetos MIME. Las aplicaciones que se ejecutan en el servidor se denominan CGIs.

Cuando un usuario invoca un CGI se le está permitiendo ejecutar remotamente un programa en el servidor, de manera que podría intentarse la introducción de parámetros manipulados para que funcionase de manera maliciosa. Como condición de seguridad, los programas solamente deberían ejecutar las acciones para las que fueron concebido. No se debe dar al cliente más información que la que se desee suministrar. Tampoco se debe confiar en la información de los datos introducidos por el cliente. En caso de éxito en un ataque, se debe minimizar el daño potencial al sistema.

Para distinguir si un CGI es seguro, debemos analizar primero su complejidad (es preferible que sean sencillos). Por otra parte, debemos chequear si actúa sobre archivos del sistema o interactúa con otros programas. Siempre es necesario validar las entradas procedentes de los formularios. Debe tenerse especial cuidado con los campos ocultos, ya que no se visualizan en el navegador pero sí en el código HTML. Es importante recordar que no se ejecutan necesariamente desde un formulario, sino que también pueden hacerlo directamente a través de la ventana de URL.

7.2.5 Java

Java es un lenguaje orientado a objetos desarrollado por Sun Microsystems a principios de los 90.

Las aplicaciones se compilan normalmente en un bytecode que se interpreta en tiempo de ejecución. El lenguaje toma mucha de su sintaxis de C y C++ pero su modelo de objetos es más simple. Para trabajar con el lenguaje, el fabricante proporciona un compilador y una máquina virtual. Utiliza el modelo de seguridad de Sandbox, el cual se implementa con distintas técnicas:

- Las características del lenguaje y el compilador

- La verificación del bytecode
- El cargador de clases
- El gestor de Seguridad Desde este punto de vista podemos considerar seguro el uso de este lenguaje, aunque de todas formas siempre es posible desactivar su ejecución desde las "Opciones de Internet" si nos encontramos en un entorno Windows con Internet Explorer.

Es una buena práctica el hecho de contar con la versión más actualizada de la máquina virtual provista por Sun para ejecutar las aplicaciones en este lenguaje, llamadas comúnmente "applets".

7.2.6 Javascript

Javascript es un lenguaje interpretado (no requiere compilación) que se utiliza principalmente en páginas web. Posee una sintaxis semejante a la de Java y el lenguaje C. Por el contrario que Java, no es un lenguaje orientado a objetos propiamente dicho (no dispone de herencia) sino que está basado en prototipos (las clases se generan clonando clases base). Los navegadores por su parte, interpretan su código, que está integrado en las páginas web. Fue diseñado para cumplir ciertas normas de seguridad para proteger el sistema del usuario. Tras cargar una página HTML, el navegador ejecuta su código sin que el usuario tenga que saberlo. Una norma de sus creadores fue la imposibilidad de acceder a elementos externos a la página web. No puede acceder a archivos de usuario ni ejecutar programas. Tampoco se pueden realizar conexiones con otros servidores desde el lado del usuario. El Internet Explorer de Microsoft puede eludir estas restricciones mediante controles ActiveX, por lo cual debe tenerse sumo cuidado al combinar las tecnologías.

7.2.7 ActiveX

ActiveX es una tecnología de Microsoft que se utiliza para desarrollar componentes de software orientados a objetos reutilizables. Es aprovechada en el desarrollo de páginas dinámicas. Se presenta tanto del lado del servidor como del cliente, aunque existan diferencias en el uso en cada caso. En el cliente, funcionan como pequeños programas que se pueden incluir en de páginas web y sirven para realizar diversas acciones. Son parecidos a los Applets de Java en su funcionamiento, aunque difieren en la seguridad, ya que un Applet de Java no podrá tomar privilegios más allá de la máquina virtual y los controles ActiveX sí. Los scripts de ActiveX son particulares del navegador Internet Explorer, y funcionan como "controles", similares al uso de plugins. En el servidor también existen controles ActiveX, y están presentes en la creación de sitios en ASP.

En cuanto a las consideraciones de seguridad referidas a esta tecnología, debemos tener en cuenta su alta interactividad con el sistema operativo, lo cual puede convertirlo en un eslabón débil de la cadena de seguridad. Desde el navegador Internet Explorer es posible ajustar las configuraciones predeterminadas para aceptar o no los controles ActiveX. Esto se realiza mediante el ajuste de "Nivel Personalizado" en la solapa "Seguridad" del cuadro de "Opciones de Internet" (en la barra del programa aparece luego de un click en "Herramientas"). En cuanto al lado del servidor, debemos asegurarnos de cumplir con los requerimientos de seguridad al realizar la programación de los sitios dinámicos.

7.2.8 Programación segura de Scripts

Para conseguir scripts seguros se debe tener muy en cuenta el correcto armado de los algoritmos, a fin de que no se produzca el consumo excesivo de recursos o el descontrol interno de la lógica de programación. Como consideración de seguridad asociada a estos lenguajes podemos decir que debe tenerse sumo cuidado respecto al lugar y la forma de almacenamiento, debido a que es posible acceder a su código en texto claro y modificarlo muy fácilmente, a diferencia de los binarios

ejecutables, que requieren de la recompilación. Es buena práctica la validación adecuada de parámetros, buffers y variables utilizadas, así como también el buen uso de la sintaxis correspondiente, sin omitir el concepto del mínimo privilegio en la creación de funciones. Se deben comprobar todo tipo de accesos de los scripts, y la forma predeterminada de funcionamiento debe ser la de no permitir nada. También se debe minimizar el acceso a recursos. Todo esto no debe interferir con la usabilidad de la aplicación. Por su parte, cada lenguaje de scripting posee sus propias singularidades y características a tener en cuenta a la hora de programar, por lo que es indispensable consultar la documentación oficial

7.2.9 Code Signing

El Code Signing, o firma de código, es el proceso de firmar digitalmente archivos ejecutables y scripts para confirmar la autoría del software y garantizar que el código no ha sido alterado ni está corrupto desde que fue firmado.

Las firmas se realizan en unos pocos pasos:

- Se aplica una función hash al archivo y se obtiene un resumen
- El resumen es encriptado con una llave privada del creador
- El archivo y la firma se distribuyen juntos
- El que recibe los archivos le aplica la misma función hash al ejecutable
- Luego desencripta el resumen recibido con la llave pública del creador
- Finalmente lo compara con el que obtuvo él mismo
- Si ambos resúmenes coinciden, el archivo en cuestión conserva su integridad

De esta manera es posible asegurar que un archivo o documento que emite un creador a muchos usuarios, conserva su integridad y no es modificado en el camino. Es decir, el archivo es exactamente el mismo que el provisto por el creador. Ampliando el concepto, podemos obtener certificados que permitan confirmar además los datos del creador de código que es entregado para su instalación. Es muy recomendable que empresas y desarrolladores que pretendan distribuir programas o contenido, los aseguren a través de los mecanismos de firma digital, para así generar confianza en sus receptores. Para hacerlo de manera válida oficialmente, debe obtenerse un certificado de una autoridad certificante. En pocas palabras, una manera muy útil de fortalecer un sistema es mediante la comprobación de las firmas de los archivos, especialmente una vez descargados de la web del proveedor.

7.2.10 Protegiendo el Web Browser

Un navegador o explorador web es la aplicación que nos permite visualizar documentos de hipertexto desde servidores web. Los principales navegadores que se utilizan son el Internet Explorer de Microsoft y el Mozilla Firefox, los cuales trabajan de formas diferentes. Los navegadores se pueden complementar con plugins que agregan funcionalidades, pero se debe tener en cuenta que los mismos no provoquen una reducción en el nivel de seguridad.

Los navegadores pueden interpretar distintos protocolos y códigos, lo cual los hace vulnerables a muchos tipos de ataque. El caso más peligroso es cuando puede conseguirse que un navegador ejecute comandos del sistema operativo. Una de las técnicas utilizadas por los atacantes es la manipulación de cookies, ya sea para interpretarlas y extraer de ellas información de navegación, o bien para escribirlas especialmente a fin de que afecten al usuario. Los navegadores nos permiten el acceso a distintos servicios, incluyendo webmail y correo electrónico, por lo cual se utilizan muy

frecuentemente sistemas de recordatorio de usuarios y passwords. Estos sistemas dependen de la seguridad interna del navegador y su forma de almacenamiento, pero se recomienda dentro de lo posible, no permitir que se recuerde información de cuentas de usuario.

Otra aplicación puede ser la de acceso a sitios de homebanking, contra el cual se intercambiará información privada. El navegador gestionará las transacciones con estos sitios, por lo tanto debe tener la posibilidad de utilizar diversos algoritmos criptográficos, que se podrán negociar en tiempo real. Las funciones de autocompletar también pueden derivar en una brecha de seguridad al revelar información que atravesó el navegador en distintas ocasiones. También debemos poner atención a los agregados y plugins que se relaciona con sitios no confiables, ya que los programas espía y demás software malicioso están a la orden del día. Finalmente, debe tenerse en cuenta que un error en la información presentada por el navegador podría ocasionar el pasaje involuntario por un sitio de phishing, que solo tiene como objetivo el robo de información del usuario. Para el caso particular del Internet Explorer, las características de seguridad se configuran desde las “Opciones de Internet”. En el Firefox, las encontramos en la pestaña de “Seguridad” del cuadro de “Opciones”.

7.2.11 Mail Servers

Los servidores de correo electrónico, la mayoría de las veces, son el eje central del negocio de una organización. Por lo general, el servidor de correo trabaja como una aplicación adicional dentro de un servidor que brinda más servicios, aunque también puede hacerlo de manera dedicada l mismo, siendo esta la opción más recomendable siempre y cuando sea posible.

Técnicamente, si bien nos referimos al servidor de correo electrónico como un único componente, es necesario dividir en dos sus funcionalidades. Por un lado tenemos el MTA (Mail Transfer Agent) y por el otro el servidor de correo entrante (POP3 o IMAP). Si bien los servidores de correo electrónico tienen las vulnerabilidades respectivas a cada aplicación que funcione como servidor, también todos ellos están sujetos a las vulnerabilidades propias del sistema operativo sobre el cual se están ejecutando. Más específicamente aún, también son vulnerables a los ataques de Denegación de Servicio (DoS), ataques de software malicioso y de Open Relay y Spoofing.

Para proteger a los servidores de correo de este tipo de ataques, el mismo debe ser Hardenizado. Del mismo modo, también las aplicaciones de correo electrónico que corran sobre él. Las mismas, tienen varias deficiencias en lo que respecta a seguridad, independientemente del sistema operativo sobre el cual esté corriendo, tales como Sendmail para sistemas Linux y Unix o Exchange/Outlook para entornos Microsoft. Como normas generales, no debería haber aplicaciones extrañas o desconocidas instaladas en el servidor de correo electrónico. Los permisos y accesos al mismo deben ser estrictamente controlados para bloquear la instalación o ejecución de programas no autorizados. Para esto siempre es conveniente que quién esté a cargo de la administración del servidor de correo electrónico esté familiarizado con el mismo, con el objetivo de poder detectar anomalías en el funcionamiento del mismo por simple inspección.

Arquitectura: La arquitectura de los servidores de correo electrónico es del tipo cliente/servidor. Donde los clientes se conectan al servidor para descargar o enviar los mensajes. En el caso de la recepción, el cliente se autentica contra el servidor, y una vez autorizado descarga los mensajes. En el caso del envío, en un principio no se requería autenticación para establecer la conexión, pero considerando los problemas relativos a la seguridad que fueron apareciendo, se agregaron extensiones a los protocolos de envío de mensajes para que soporten esta característica. De todas formas, la mayoría de los protocolos no encriptan la información de autenticación, si no que esta viaja en texto plano a través de Internet. Como se analizará en cada uno de los protocolos a continuación, es altamente recomendado utilizar mecanismos seguros para llevar a cabo la autenticación al servidor de correo.

SMTP: El SMTP (Simple Mail Transfer Protocol) es un protocolo de red, basado en texto plano que se

utiliza para el intercambio de correo electrónico entre distintos equipos. Una limitación del protocolo SMTP, es el hecho que no soporta autenticación en forma nativa. A partir de una extensión realizada a este protocolo, el SMTP-AUTH, se obtuvo una mejora en el hecho que los usuarios emisores deben autenticarse para poder enviar sus correos. También se puede fortalecer el nivel de seguridad de las conexiones por SMTP, configurándolo para que soporte encriptación por Secure Socket Layer (SSL). Para esto por defecto se suele utilizar el puerto TCP 587.

POP3: El POP3 (Post Office Protocol versión 3) es un protocolo que se utiliza para obtener mensajes de correo electrónico alojados en un servidor. Algunas versiones no tan conocidas de POP3 son:

- APOP — POP3 con autenticación MDS. En este protocolo, el cliente de correo envía un hash codificado de la contraseña al servidor en lugar una contraseña encriptada
- KPOP — POP3 con autenticación Kerberos
- RPOP — POP3 con autenticación RPOP, que utiliza un identificador de usuario similar a una contraseña para autenticar las peticiones POP Para añadirle seguridad a la conexión por protocolo POP3, una buena práctica es utilizar la encriptación Secure Socket Layer (SSL) para la autenticación del cliente y las sesiones de transferencias de datos. El puerto por defecto para este tipo de conexión es el TCP 995.

IMAP: El IMAP (Internet Message Access Protocol) es un protocolo de red para acceder a mensajes de correo electrónico que se encuentren almacenados en un servidor. Mediante este protocolo se puede tener acceso al correo desde cualquier equipo con conexión a Internet, ya que los mensajes permanecen en el servidor. Los usuarios una vez que acceden a su correo pueden borrarlos. IMAP también permite a las aplicaciones cliente crear, modificar y borrar carpetas del lado del servidor, facilitando la gestión de los correos electrónicos. Es especialmente recomendado para usuarios que acceden a su correo desde diversos equipos. De manera análoga a POP3, se puede agregar un nivel de seguridad a la conexión por IMAP utilizando la encriptación Secure Socket Layer (SSL) para la autenticación del cliente y las sesiones de transferencias de datos.

MIME: El formato MIME (Multipurpose Internet Mail Extensions) son una serie de especificaciones dirigidas al intercambio de todo tipo de archivos a través de Internet y que este sea transparente para el usuario. De todas las especificaciones, una parte importante está orientada a mejorar la transferencia de texto en distintos idiomas. Hoy por hoy, se puede afirmar que ningún cliente de correo electrónico o navegador web puede considerarse como tal si no soporta el formato MIME.

S/MIME: El formato S/MIME (Secure / Multipurpose Internet Mail Extensions) es un estándar criptográfico de clave pública y firmado de correo electrónico encapsulado en MIME desarrollado por RSA. S/MIME provee los servicios de seguridad criptográfica para distintas aplicaciones de mensajería electrónica:

- Autenticidad
- Integridad
- No repudio
- Privacidad
- Seguridad de los datos

En la actualidad la mayoría de los clientes de correo electrónico soportan el formato S/MIME. Al tratarse de un sistema de clave pública, antes de poder usarse en algunos de los clientes de correo,

es necesario obtener e instalar una clave o certificado individual, tanto de la autoridad certificante interna como de una externa. Como buena práctica relativa a la seguridad informática se recomienda usar claves privadas separadas (y sus respectivos certificados) para firma y para cifrado.

7.2.12 Nuevos vectores de ataque

Con el avance continuo de los sistemas de mensajería instantánea, fundamentalmente a nivel corporativo, los ataques a estos sistemas continuarán aumentando, particularmente los que estén relacionados con el robo de información (passwords, cuentas, información financiera, etc) y aquellos que brinden un medio al atacante para tomar control del equipo víctima, convirtiéndolo en un equipo zombie (y así poder utilizar dicho equipo para lanzar otro tipo de ataques). Por otro lado también están proliferando casos de phishing que utilizan como medio los sistemas de mensajería instantánea, aprovechando la falta de toma de conciencia de parte de los usuarios sobre los riesgos que esto conlleva.

7.2.13 Servidores DNS

Un servidor de DNS (Domain Name Services) resuelve hostnames con direcciones IP. Este servicio permite a un sitio llamado por ejemplo, http://www.misitio.com, resolver a la dirección IP correspondiente a ese sitio dado. Estos servidores se pueden usar internamente, para brindar servicios y funcionalidades privadas, o bien externamente para “lookups” públicos. Los ataques directamente relacionados con sistemas DNS no son muy comunes, pero cuando aparecen, lo suelen hacer en alguno de estos 3 (tres) tipos:

- Ataque de DoS a un DNS: Los ataques de denegación de servicio fueron concebidos en un principio para servidores DNS. En este caso, el objetivo es interrumpir las operaciones normales del servidor, volviendo al sistema inutilizable. Para minimizar este tipo de ataques es altamente recomendado asegurarse estar al día con las actualizaciones de seguridad del sistema.
- Footprinting de la red: Una gran cantidad de información relativa a las redes se almacena en los servidores DNS. Mediante el uso de algunas aplicaciones sencillas de DNS lookup, un atacante puede tomar conocimiento de varias de las configuraciones de la red. Típicamente hay información disponible relativa a los nombres de dominio, correo electrónico, web y mucho más. Lo que conviene hacer respecto a este tipo de ataque es mantener la mayor cantidad de información posible almacenada dentro de la red interna, solamente lo mínimo indispensable que esté expuesto a un servidor DNS externo.
- Delegación de dominios: Los DNS lookup por lo general requieren de dos servidores

DNS primarios, o bien uno primario y uno secundario. Si se realiza algún cambio en un servidor primario o secundario, el cambio se propagará hacia otros servidores DNS de confianza. Si se inserta un registro falso dentro de los servidores DNS, este registro apuntará a la ubicación del atacante, convirtiéndola en una ubicación legítima. Imaginen la situación donde un determinado sitio, fue redireccionado maliciosamente a otro de la competencia, o peor aún, a algún sitio ilegal. Para evitar este tipo de ataques, se debe estar seguro que los servidores DNS requieran autenticación antes que se haga cualquier tipo de propagación. En entornos Linux y Unix, y prácticamente la mayor parte de los servidores DNS, están montados sobre BIND.

7.2.14 Servidores DHCP

DHCP (Dynamic Host Configuration Protocol) es el protocolo que permite a los distintos nodos de una red IP obtener sus parámetros de configuración automáticamente, como ser dirección IP, máscara de subred, Gateway, etc. En lo que respecta a la seguridad, los servidores DHCP agregan un nivel de complejidad más a la estructura de seguridad, pero bien configurados también ofrecen la posibilidad de acotar y controlar la asignación de direcciones y parámetros de red a los equipos cliente. Para poder lograr esto los administradores deben definir estrictas ACL (Access Control Lists) para limitar a los usuarios la posibilidad de modificar las configuraciones de red. Del mismo modo que en todas las aplicaciones de servidores anteriores, los administradores también deben aplicar los parches de seguridad, updates, service packs y hotfixes necesarios para que el DHCP quede correctamente configurado y protegido. Como consideración adicional relativa a la seguridad, es importante controlar la generación de servidores DHCP falsos, ya que estos pueden enviar direcciones distintas a los diversos clientes, violando las configuraciones y los controles de seguridad. Para evitar esto, es necesario que los administradores tengan herramientas de control de tráfico de red y así detectar cualquier tipo de anomalía. En la mayoría de las plataformas existen distintos controles de acceso y autenticación para este tipo de servidores, como administrador es una buena práctica estar familiarizados con las mismas.

7.2.15 Servidores NNTP

El NNTP (Network News Transfer Protocol) es un protocolo que se utiliza para la lectura y publicación de artículos de noticias en Usenet. Por defecto, este servicio utiliza el puerto 119 TCP, pero para que los clientes se conecten al servidor mediante SSL la conexión se suele realizar en el puerto TCP 563. Básicamente, el sistema funciona de la siguiente manera, los clientes, se conectan a un servidor conectado a Internet donde se alojan las noticias. Esta conexión entre cliente y servidor se realiza interactivamente, logrando que el número de artículos duplicados en el servidor sea muy reducido. Por otro lado, los servidores NNTP son vulnerables a diversos tipos de ataques, ya que suelen ser una fuente de recursos para la red interna. Estos servidores a menudo realizan transmisiones de información en grandes cantidades, por lo que son blancos de ataques de DoS en momentos de altos niveles de tráfico. Otros tipos de ataques frecuente en los servidores NNTP son los ataques de SPAM o mensajes no solicitados. Para evitar este tipo de ataques usualmente los mensajes son evaluados por un moderador antes de llegar a las listas, con el objetivo de asegurarse que los mismos correspondan a usuarios válidos. En el caso que se manejen grandes cantidades de mensajes, se suele complementar la tarea del moderador con Bots, unas herramientas automatizadas que pueden detectar mensajes SPAM y eliminarlos.

Como ocurre con el caso del SPAM, los servidores NNTP también pueden llegar a tener problemas relativos a la seguridad similares a las de los servidores de correo electrónico. Esto se debe a que por defecto, no siempre están configurados en forma correcta las limitaciones de los parámetros de almacenamiento de información o limitados los archivos adjuntos. También es importante tomar conciencia de la problemática que puede ocasionar el hecho que software malicioso adjunto a los mensajes pueda aceptarse en el servidor y ser almacenado en el mismo.

Por lo tanto, los servidores NNTP deben estar restringidos solamente a entidades válidas, las cuales requieren por parte del administrador una correcta configuración de los límites de acceso y el tipo de adjuntos que se pueden almacenar. También es importante tener en cuenta cual es la plataforma sobre la cual está montado el servidor, a fin de ajustar las medidas relativas a la dicha plataforma.

7.2.16 File Servers

La función de un servidor de archivos desde un principio, es brindar el acceso remoto a archivos

almacenados en dicho equipo, haciendo que para el cliente de dicho servidor, la ubicación de los archivos compartidos es transparente. Algunos protocolos para compartir archivos utilizados en este tipo de servidores son SMB (Unix/Linux y Windows) y NFS (Unix/Linux). Desde el punto de vista de la seguridad informática, los servidores de archivos usualmente ofrecen diversas formas para limitar el acceso a los recursos a usuarios específicos o a grupos, mediante distintos métodos de autenticación. Ejemplo de esto es el Active Directory de Microsoft. Si bien, como se dijo anteriormente, la principal función y beneficio de un servidor de archivos es compartir archivos con los usuarios específicos de una red; esto también tiene su contrapartida, sobre todo cuando los usuarios no son consientes de las implicancias de seguridad que conlleva compartir los recursos. Si un usuario válido puede obtener acceso a cierto recurso, entonces existe la posibilidad que un usuario malicioso también lo pueda obtener. Ampliando más el espectro, si existen conexiones de banda ancha que unan dos puntos distantes, es probable que existan usuarios maliciosos que estén intentando conectarse a los recursos compartidos para tratar de explotarlos. Para ajustar los niveles de seguridad de un servidor de archivos, como primera medida es necesario utilizar sistemas de autenticación confiables. Por otro lado, todos los servicios relativos a los recursos compartidos deberían deshabilitarse o bloquearse de la interfaz externa de la red. Otra solución, o complemento, sería utilizar protocolos distintos en la red interna.

7.2.17 Print Servers

Un servidor de impresión o servidor de impresoras es una computadora o equipo discreto que puede aceptar y administrar distintos trabajos de impresión de computadoras cliente conectadas a dicho servidor a través de la red. Cada uno de estos puede tener conectada una o varias impresoras. Una vez recibido el trabajo de impresión, lo gestiona y envía a una impresora según una serie de criterios. Estos servidores funcionan de manera análoga a los servidores de archivos. Comparten uno o varios recursos (en este caso las impresoras) en la red. Por lo que las vulnerabilidades y problemas relativos a la seguridad, aplican de igual manera para estos. Son susceptibles fundamentalmente a los ataques de DoS. Una de las diferencias quizás más notables respecto a los servidores de archivos, es que puede variar el protocolo por el cual se establece la comunicación. Por ejemplo, el sistema CUPS (Common Unix Printing System) para Unix/Linux trabaja sobre el protocolo IPP (Internet Printing Protocol), agregando a las vulnerabilidades mencionadas en el servidor de archivos, las relativas a este protocolo. Para tener en cuenta al asegurar un servidor de impresión, del mismo modo que con el servidor de archivos, es indispensable contar con métodos de autenticación que impidan a usuarios no válidos hacer uso de los recursos de este servidor. También es recomendable bloquear estos servicios de la interfaz externa, o bien, utilizar protocolos distintos.

7.2.18 Repositorio de datos

Los repositorios de datos incluyen una gran cantidad de variantes de sistemas de almacenamiento interconectados para el mantenimiento y protección de los datos. Por ende es absolutamente necesaria la protección de estos sistemas. Estos pueden ser distintas combinaciones de dispositivos de almacenamiento, métodos de acceso a la información, consideraciones de las implicancias de dicho acceso y las configuraciones, mantenimiento y chequeo de la integridad de esos datos.

Como es de imaginarse, el hecho de aumentar el nivel de seguridad de los repositorios de datos, está íntimamente relacionado con los servidores de archivos por un lado, y por otro, con las distintas arquitecturas de almacenamiento como NAS (Network Attached Storage) y SAN (Storage Area Network). Particularmente, las arquitecturas SAN y NAS pueden presentar diversos desafíos a la hora de fortalecer la seguridad. Un caso típico es el hecho que normalmente las configuraciones NAS utilizadas en una LAN hacen uso de distintos sistemas de archivos o protecciones de acceso que suelen no ser compatibles con los sistemas operativos. Con lo cual, el sistema operativo deja de tener el control sobre los permisos asignados para el acceso a los datos, haciendo mucho más compleja la generación de reglas de acceso. Por otro lado las configuraciones SAN permiten la

intercomunicación que están siendo utilizados por el SAN, dando de esta manera cierta libertad a la comunicación entre equipos y acelerando los accesos. Como contrapartida, se necesita una mayor dedicación inicial para crear los controles de acceso en forma adecuada para limitar los contactos no autorizados con el procesamiento de los datos.

7.3 PREGUNTAS Y TIPS

- El proceso para segurizar un sistema o aplicación en función de su protección contra eventos determinados se denomina Hardening
- El sistema centralizado de aplicación de parches de Microsoft que provee actualizaciones de seguridad para los sistemas operativos Windows y otras aplicaciones se llama *Windows Server Update Services* (WSUS).
- Un proceso de "*Vulnerability Assessment*" tiene un carácter menos intrusivo que un *"Penetration test"*
- Los servicios de "*Penetration test*" y *"Vulnerability Assessment"* incluyen la utilización de vulnerabilidades o *exploits* de día cero

CAPÍTULO 8

8.1 ANÁLISIS DE VULNERABILIDADES

¿Qué tareas realizaría si tuviera que hacer un análisis de vulnerabilidades en una red?

- Reunir información
- Test interior
- Test exterior
- Documentar e informar

¿Cómo puede detectar una vulnerabilidad? Mediante herramientas de detección de vulnerabilidades. Realizan un escaneo de puertos, y para los puertos que detecten abiertos intentan obtener información sobre el servicio que se encuentre corriendo. Con esta información buscan las vulnerabilidades asociadas a los servicios asociados.

¿Qué métodos se pueden usar para obtener información?

- Información de dominio a través de consultas tipo WHOIS
- Consultas NSLOOKUP para saber cuales son los servidores que tiene la empresa
- Identificación de la plataforma mediante OS fingerprinting
- Identificación de los servicios mediante port-scanners

Las vulnerabilidades de seguridad informática han existido desde siempre. Hasta 1990 la gran mayoría de los intrusos ingresaba a los sistemas informáticos utilizando técnicas de scanning, ataques de fuerza bruta, probando usuarios y diferentes passwords, ingeniería social, etc. A partir de principios de los 90 los intrusos comenzaron a ingresar a los sistemas informáticos a través de la explotación de vulnerabilidades, que eran conocidas primariamente dentro de los ambientes *underground* y posteriormente, con el uso masivo de Internet comienza a surgir los primeros Web Sites de vulnerabilidades. A medida que se hacían conocidas diferentes vulnerabilidades, también se publicaban herramientas de seguridad y parches con el objetivo de ayudar a los administradores. Actualmente, Internet representa una gran fuente de información donde existe mucha más cantidad de información sobre cómo ingresar a sistemas que sobre cómo protegerlos.

8.1.1 ¿Qué comprende la seguridad de una red?

La seguridad de la red, comprende tanto la protección física de los dispositivos al daño, robo o manipulación como también la integridad, confidencialidad y autenticidad de las transmisiones de datos que circulen por ésta . La siguiente lista resume los puntos que comprende la seguridad de una red:

- La información debe estar protegida de una posible destrucción o modificación accidental o intencional (integridad).
- Los datos no deben estar disponibles a los accesos no autorizados (privacidad).
- Las transacciones no deben ser modificadas en su trayecto desde un host a otro y se debe asegurar que quien las generó es quien dice ser (integridad, autenticidad y no repudio).

- Se mantenga la integridad física de los dispositivos de red como servidores, switches, etc.
- El uso de la red no debe ser con fines maliciosos o fines que no estén contemplados por las políticas de utilización.
- La red debe estar disponible siempre y con la eficiencia necesaria, aún ante fallas inesperadas (disponibilidad).

8.1.2 ¿Para qué sirve un análisis de vulnerabilidad?

A través de un análisis de vulnerabilidades, un analista en seguridad puede analizar exhaustivamente la robustez y seguridad de cada uno de los sistemas y dispositivos ante ataques y obtener la información necesaria para analizar cuáles son las contramedidas que se pueden aplicar con el fin de minimizar el impacto de un ataque.

El análisis de vulnerabilidades debe realizarse:

- Cuando ocurran cambios en el diseño de la red o los sistemas: Un cambio de topología, de direccionamiento o de ubicación de dispositivos representa un escenario totalmente diferente para segurizar. Con cada cambio de diseño que se realice es imprescindible volver a revisar si se cumplen todos los requisitos de seguridad y los sistemas no quedan expuestos a posibles ataques.
- Cuando se realicen actualizaciones de los dispositivos: El reemplazo de un dispositivo por otro o simplemente la actualización del software de algún dispositivo puede incorporar alguna vulnerabilidad que antes no estaba presente.
- Periódicamente: Existen numerosas entidades (las estudiará en secciones siguientes) que se ocupan de realizar estudios de seguridad sobre productos e implementaciones. Como resultado de estos estudios o por un ataque de algún usuario, salen a la luz vulnerabilidades en las implementaciones y se buscan mecanismos para evitar su explotación. Un análisis periódico le indicará si sus sistemas continúan siendo seguros o no.

El principal objetivo de un análisis de vulnerabilidades es anticiparse al agresor

8.1.3 Métodos: caja negra versus caja blanca

Caja negra y caja blanca son dos conceptos aplicables a la forma en que el analista de seguridad realiza el análisis de vulnerabilidad en una red y la información que dispone para realizarlo:

- Caja Negra: Al analista se le proporciona sólo la información de acceso a la red o al sistema (podría ser sólo una dirección IP). A partir de esta información, el analista debe realizar toda la exploración y obtener toda la información posible desde dicha IP y del resto de los equipos que se encuentren en el rango asociado. No se realiza ninguna intrusión, tan solo se detecta y se documenta.
- Caja Blanca: El analista de seguridad tiene una visión total de la red a analizar, así como acceso a todos los equipos como súperusuario. Se realiza un análisis de la configuración del S.O, de los servicios instalados, de las comunicaciones entre equipos. Este tipo de análisis tiene la ventaja de ser más completo y exhaustivo, el resultado suele ser mucho más específico y muestra una visión más exacta del estado actual de un sistema.

8.1.4 Test de penetración o Hacking Ético

Durante el test de penetración el analista de seguridad simula ser un atacante. Así, desde esta

posición, se realizan varios intentos de ataques a la red, buscando debilidades y vulnerabilidades:

- Estudio de la red externa.
- Análisis de servicios disponibles
- Estudio de debilidades.
- Análisis de vulnerabilidades en dispositivos red.
- Análisis de vulnerabilidades de implementaciones y configuraciones.
- Denegación de servicio

El test de penetración o Hacking ético implica, entonces, al conjunto de actividades que permiten comprometer un equipo con el fin de determinar que tan seguro es ante los ataques realizados.

El resultado del test de penetración mostrará una idea general del estado de la seguridad de los sistemas frente a los ataques. Si se encontraran una o más vulnerabilidades, no se realiza su explotación. Como conclusión de este paso, se debe obtener un informe que indique:

- Pruebas de seguridad realizadas en el test.
- Lista de vulnerabilidades y debilidades encontradas.
- Referencia técnica a estas vulnerabilidades y sus contramedidas.
- Recomendaciones.

Es muy importante tener en cuenta que si un test de penetración no reporta la existencia de vulnerabilidades no significa que el sistema sea seguro, sino que es inmune a los ataques que le fueron realizados.

8.2 VULNERABILIDADES DE LAS REDES

A lo largo de esta unidad estudiaremos el origen de las vulnerabilidades. Este estudio nos ayudará en la realización de un análisis de vulnerabilidades y una vez encontradas las vulnerabilidades a buscar sus soluciones.

Las vulnerabilidades provienen de diferentes ámbitos, y las podemos clasificar en:

- Vulnerabilidades de implementación
- Vulnerabilidades de configuración
- Vulnerabilidades de dispositivo
- Vulnerabilidades de protocolo

Muchas vulnerabilidades existentes provienen de errores de implementaciones de estándares. Recordemos que los estándares se encuentran definidos por entidades, y son publicados mediante documentos. Estos documentos son luego desarrollados por diferentes empresas para generar implementaciones particulares a su plataforma conformes a los estándares.

Si al momento de codificar o programar el código se cometen errores o se omiten ciertas normas de seguridad, se generará una implementación con vulnerabilidades de seguridad que podrán ser detectadas y explotadas por atacantes. La forma de detectar estas vulnerabilidades es mediante el estudio del código (en caso de ser código abierto) o mediante pruebas directas contra el software para ver si su comportamiento es conforme a las especificaciones. En general, las vulnerabilidades de

implementación pueden ser aprovechadas utilizando software específico, denominado "exploits". La forma de solucionar alguna vulnerabilidad de implementación encontrada es mediante una actualización del software en problemas. Si no existiera una actualización por parte de los desarrolladores, habría que buscar una solución alternativa, como crear filtros para detener el tráfico que puede explotar la vulnerabilidad, reemplazar el software por otro, o directamente recodificar en caso que se tenga el código fuente.

8.2.1 Vulnerabilidades de configuración

Quizás la vulnerabilidad más común y la más fácil de solucionar son las vulnerabilidades generadas por errores de configuración. Estos errores pueden provenir de falta de conocimiento por parte del personal dedicado a la instalación y configuración de los servicios. En general, la facilidad de configuración va en contra de la seguridad. Es por esto que muchos desarrolladores optan por simplificar la instalación, configuración y puesta en funcionamiento, a costa de dejar opciones por defecto inseguras. Por otra parte, existen productos que requieren un mayor tiempo y conocimiento para su instalación y configuración, pero una vez en funcionamiento, se encuentran configurados con la seguridad deseada. Para detectar estas vulnerabilidades es necesario conocer de manera exhaustiva el software a analizar. De esta forma se pueden generar pruebas específicas para conocer cuáles han sido las opciones configuradas. La forma de protegernos de este tipo de vulnerabilidades es clara: conocimiento. Se debe conocer el software a instalar y se deben investigar las diferentes opciones de configuración para conocer cuál es la seguridad que permite habilitar y cuál es la seguridad que necesitamos. Si lo que necesitamos no se encuentra dentro de las capacidades del software, tenderemos que agregar algún control auxiliar para no quedar desprotegidos.

8.2.2 Vulnerabilidades de dispositivo

Los dispositivos de red contienen software que puede generar vulnerabilidades. Un error de programación en el sistema operativo del dispositivo podría estar abriendo una puerta de acceso a nuestra red o proveyendo herramientas para avanzar en un ataque por denegación de servicios.

Un ejemplo de este tipo de vulnerabilidades que tuvo una gran difusión fue la vulnerabilidad en los sistemas operativos de Cisco que con sólo enviar un paquete IP con ciertas características (para más detalle puede ver el vínculo) el dispositivo deja de reenviar paquetes. Esto puede permitir realizar de manera muy sencilla un ataque por denegación de servicios.

La solución a este tipo de vulnerabilidades debe ser provista por los fabricantes o desarrolladores del dispositivo. En caso de no contar con una solución, se deberán utilizar medidas alternativas, como filtrado de paquetes, reemplazo del dispositivo afectado, etc.

8.2.3 Vulnerabilidades de protocolo

Existen múltiples protocolos que fueron definidos sin tener en cuenta la seguridad. Muchas veces no se tuvo en cuenta la seguridad porque cuando se creó el protocolo no existía una difusión tan grande de Internet, y otras veces no se agregó seguridad porque son protocolos simples que no soportarían la complejidad o el procesamiento de la seguridad. En el caso de estos protocolos, ya conocemos desde su definición que no proveen herramientas de seguridad.

Un ejemplo de esto puede ser HTTP. HTTP no es un protocolo seguro, dado que no realiza autenticación ni encriptación de los datos que intercambia . Esto puede no ser necesario en algunos ambientes (por ejemplo en las páginas visitadas por los usuarios), pero cuando se realizan transacciones económicas, es necesario ofrecer privacidad de la información transmitida. Esto se puede lograr mediante protocolos adicionales: SSL o TSL.

El mayor problema es cuando se define un marco de seguridad que tiene fallas, como sucedió en la definición de WEP del estándar IEEE 802.11, que ya hemos estudiado.

Es necesario conocer los protocolos utilizados y sus aspectos de seguridad, a fin de realizar el análisis de vulnerabilidades correcto.

8.3 HERRAMIENTAS PARA EL ANÁLISIS DE VULNERABILIDADES

En esta sección estudiaremos las herramientas que se pueden utilizar para realizar un análisis de vulnerabilidades. Existen diversas herramientas, y hemos intentado realizar una clasificación de ellas. Posiblemente, muchas herramientas quedarán fuera de estas categorías, pero esto servirá para conocer las más utilizadas:

- Escaneo de puertos
- Detección de vulnerabilidades
- Analizador de protocolos
- Passwords crackers
- Ingeniería social
- Trashing

Como parte del análisis de vulnerabilidades, es necesario conocer cuándo se debe aplicar cada herramienta, y los resultados que podemos esperar de ellas.

8.3.1 Escaneo de puertos

Quizás una de las primeras herramientas utilizadas una vez que se conoce el objetivo son los escaneos de puertos. Los escaneos de puertos se realizan utilizando herramientas automáticas denominadas "escaneadores de puertos" o "port-scanners".

El objetivo de estas herramientas es informar qué puertos se encuentran activos (abiertos) y cuáles no. Existen diversas forma de obtener esta información. La forma más clásica es intentar establecer una conexión con cada uno de los puertos, denominada Connect scanning. Se envía un SYN al puerto deseado, se espera por un SYN-ACK y se responde un ACK . Si el acuerdo de tres vías finaliza correctamente, significa que el host se encuentra aceptando conexiones a ese puerto. Este método es fácilmente detectable por los sistemas de detección de intrusos (IDS).

Existen otras técnicas para realizar escaneos de puertos, donde no se establece una conexión completa:

- *TCP SYN scanning:* Esta técnica no establece una conexión completa. Envía un SYN y espera la respuesta. Si recibe como respuesta un segmento RST, significa que el puerto no se encuentra activo. Si la respuesta es SYN-ACK, significa que el puerto se encuentra abierto [3], inmediatamente se envía un RST para evitar que se establezca la conexión. Esta técnica al no establecer una conexión, no es logueada por los sistemas estándares.
- *TCP FIN scanning (Stealth scanning):* Esta técnica se basa en un bug en las implementaciones TCP, por lo que no es 100% confiable. Este bug hace que si se envía un segmento FIN hacia un puerto abierto, el puerto lo descarta, y si el puerto se encuentra cerrado, envía como respuesta el RST apropiado.
- *Fragmentation scanning:* ésta no es una técnica nueva, sino que es una modificación a otras técnicas para evitar ser detectadas por Firewalls o IDS. Antes de enviar directamente el

segmento apropiado, se fragmenta en pequeños paquetes IP. De esta forma, los dispositivos de control que no realicen un reensamblado de los paquetes, no podrán detectar el escaneo en curso.

- *UDP ICMP port unreachable scanning*: este tipo de escaneo realiza prueba a puertos UDP. Como no se establecen conexiones se vuelve más complicado realizar el escaneo. Pero en general, las implementaciones UDP devuelven un paquete ICMP_PORT_UNREACH cuando se envía un segmento a un puerto UDP que no se encuentra activo. De esta forma se puede detectar los puertos cerrados, y por exclusión, obtener los puertos abiertos. Dado que ni los segmentos UDP ni los paquetes ICMP tienen la seguridad de llegar a destino, el escaneo de puertos UDP puede ser inexacto.

La manera más común de que un atacante obtenga información, es realizar un barrido de puertos mediante algún programa dedicado, como por ejemplo Nmap. Nmap es una herramienta de escaneo de puertos creado para analizar grandes redes a una velocidad relativamente rápida para obtener, entre otras cosas, las IPs de los equipos que se encuentran conectados en la red, los servicios, versiones, nombres de programas, sistemas operativos, filtros de paquetes de Firewalls, y otras muchas características más.

Los puertos se pueden encontrar en diferentes estados que se describen a continuación:

- Puerto Abierto: Un puerto se encuentra abierto cuando al enviar un SYN para intentar establecer una conexión, el destino responde exitosamente con un SYN+ACK. Es este estado el que generalmente los atacantes buscan para explotar vulnerabilidades, ya que se sabe que un servicio se encuentra detrás esperando conexiones.
- Puerto Cerrado: De manera inversa, un puerto se encuentra cerrado cuando como respuesta al SYN se recibe un RST (o destino inalcanzable en el caso de un test UDP), lo que significa que no existe servicio esperando conexión por este puerto.
- Puerto Filtrado: En el caso de los puertos filtrados o bloqueados, a cualquier envío de SYN (o intento de establecer una conexión), no se recibe nada. Muy probablemente se deba a que el destino tiene un firewall que elimina el flujo normal de los paquetes.

La detección de un barrido de puertos es muy fácil: Se generan muchas conexiones simultáneas a una gran cantidad de puertos, originadas por la misma dirección IP, según las respuestas de dichas conexiones se imprime el resultado del test de barrido. Con el correr de los años, la técnica que utilizan los escáner ha ido evolucionando mediante el cambio de estrategias (aumentando los tiempos entre pruebas, hasta desarrollar un barrido silencioso con SYN, FIN, Xmas, Null, UDP, paquetes fragmentados y barridos paralelos de diferentes tipos) pero siempre bajo el mismo principio.

Ahora que se conocen las posibilidades de los escáner de redes, y como contrarrestar los intentos de ataques, se va a describir una de las herramientas más utilizadas para este fin. **Portsentry** es una aplicación desarrollada por Psionic que permite detectar escaneos de puertos, incluidos de semiconexión, y actuar en consecuencia. Su misión radica en escuchar los puertos que según el administrador deberían permanecer inactivos, y en caso de encontrar una conexión entrante a uno de ellos, se procederá marcando este evento en el log del sistema y alternativamente bloqueando la comunicación con la dirección IP identificada o hacer correr algún comando externo.

Existen herramientas para detectar vulnerabilidades. Estas herramientas realizan un escaneo de puertos, y para los puertos que detectan abiertos, intentan obtener información sobre el servicio que se encuentra corriendo. La información del servicio incluye: plataforma, software, versión y release. Con esta información, buscan las vulnerabilidades asociadas a los servicios encontrados. Para poder detectar las vulnerabilidades, necesitan tener una base de datos donde guardan cada servicio y sus vulnerabilidades. Obviamente, estas herramientas sólo pueden detectar vulnerabilidades que hayan

sido publicadas, no pueden detectar vulnerabilidades nuevas. Por esto se recomienda una actualización periódica de la base de datos. Las herramientas de detección de vulnerabilidades más conocidas son Nessus , LANguard Network Security Scanner de GFI y Retina de Eeye.

8.3.2 Analizador de protocolos

Los analizadores de protocolo son herramientas que realizan capturas de tráfico en redes de difusión (como Ethernet, Wireless LANs, Token Ring o FDDI) y permiten realizar una interpretación de la captura. Este tipo de herramientas son utilizadas para obtener información mediante eavesdropping, como ya hemos estudiado.

Cuando un test de penetración no se realiza desde la red local, probablemente no podremos utilizar directamente estas herramientas, pero en caso de conseguir acceso a algún host de la red, se podrá instalar un analizador de protocolos para comenzar con la captura de datos y realizar la interpretación en búsqueda de información crítica. Tenga en cuenta que existen en utilización muchos protocolos que no encriptan información, con lo que pueden brindar datos críticos para seguir avanzando en nuestro análisis. Existen muchos analizadores de protocolos, algunos son: Ethereal (gratis) y Etherpeek (comercial)

8.3.3 Passwords Crackers

Cuando debemos lograr un acceso a un host, servidor o dispositivo, lo ideal es obtener algún nombre de usuario y contraseña. Esta información es muy compleja de obtener por adivinación o por prueba y error. Existen herramientas automáticas para realizar múltiples intentos de acceso que pueden facilitar el análisis de la fortaleza de las contraseñas. Estas herramientas hacen intentos repetidos con diferentes contraseñas, algunas veces tomándolas de un diccionario, o generándolas mediante combinaciones de un conjunto de caracteres (esta técnica se denomina "fuerza bruta"). Existen otras herramientas que primero necesitan obtener la base de datos de contraseñas y luego realizan los ataques mediante criptoanálisis. Para lograr esto, primero se debe comprometer un host o servidor de la red, y conseguir la copia de la base de datos o, mediante eavesdropping , tomar la información de algún inicio de sesión. Una herramienta muy utilizada para realizar auditorías de contraseñas en los ambientes Microsoft es L0pht Crack

8.3.4 Ingeniería social

El término "Ingeniería social" incluye a un conjunto de técnicas y habilidades sociales realizadas por el atacante para obtener información de terceros.

Estas técnicas o habilidades, incluyen generalmente un engaño o parcialización de la verdad con el objetivo de obtener la confianza de la persona con los conocimientos a obtener. Una vez que se ha obtenido la confianza de la persona, se procede a obtener la información considerada importante. La ingeniería social se da muchas veces vía telefónica o a través de sesiones de chat, donde la verdadera personalidad del atacante queda oculta.

Una técnica de Ingeniería social que muchas veces no se tiene en cuenta es la denominada "trashing" que consiste en la revisión sistemática de los desechos de las oficinas. Muchas veces se puede encontrar información importante dentro de cestos de residuos, como por ejemplo: listados, diskettes, cds, etc. que han sido desechados por algún motivo.

Un ejemplo típico de Ingeniería social, es cuando el atacante llama a un usuario de la red, simulando ser del departamento de informática, y le exige que le informe de su nombre de usuario y contraseña. Si el usuario que está siendo víctima del engaño, no conoce la estructura de la organización, es muy probable que le pase al atacante la información solicitada. De esta forma, el atacante, con sólo

conocer el número telefónico de la víctima, y sin realizar ninguna acción sospechosa sobre la red, podrá tener acceso con los privilegios de un usuario interno.

La ingeniería social termina cuando se obtiene la información buscada. Las actividades que se realicen con la información obtenida ya no entran en el marco de la Ingeniería social.

Aquí, la mejor contramedida es la educación de los usuarios de la red. En la política que firman los usuarios, se debe especificar que el nombre de usuario y contraseña no pueden ser transmitidos mediante otro medio que no sea persona a persona. De esta forma se evitará también que posibles escuchas de la red intercepten la información.

8.3.5 Trashing

Aunque parezca desagradable, la búsqueda de datos dentro de la basura puede proveer información importante para comenzar un análisis. Tomar objetos de la basura es completamente legal, por lo que no existe una forma de evitarlo. Quizás la información obtenida no sea la necesaria para realizar un ataque, pero, por ejemplo, puede ofrecer información para realizar Ingeniería Social. Datos tales como agendas con números de teléfono, memos, organigramas, resúmenes de ventas, planificaciones de reuniones, hardware fuera de uso, manuales de uso, etc. pueden ser un muy buen paso para comenzar la investigación. Las planificaciones de vacaciones, pueden decirnos qué usuarios se encuentran fuera de la organización, los manuales o políticas nos pueden informar sobre la estructura de seguridad y permisos que tienen los usuarios, el hardware en desuso, se puede utilizar para poder recuperar la información que tenía. Quizás dentro del disco obtengamos nombres de usuarios, contraseñas, etc.

8.4 METODOLOGÍA

En esta sección desarrollaremos los pasos a seguir para llevar a cabo un análisis de vulnerabilidades. Estos pasos comprenden:

- Acuerdo de confidencialidad entre las partes
- Estableciendo las reglas del juego
- Reuniendo información
- Test interior
- Test exterior
- Documentación e informe

Es importante conocer los pasos a seguir durante el análisis. Generalmente, el análisis de vulnerabilidades forma parte de un desarrollo de seguridad más general, donde el objetivo sea conocer el estado actual de la red y los riesgos que ésta tiene.

8.4.1 Acuerdo de confidencialidad entre las partes

Es importante realizar un acuerdo de confidencialidad entre todas las partes involucradas en el análisis. Recuerde que a lo largo del desarrollo del análisis de vulnerabilidades se puede obtener información crítica para la organización analizada. Nombres de usuarios y contraseñas, agujeros de seguridad, documentos expuestos, etc. Toda la información obtenida a través del análisis debe ser utilizada sólo para fines informativos y de mejora de servicios y seguridad, y no podrá ser divulgada a terceras partes no involucradas. Desde el punto de vista de la organización, debe existir confianza

absoluta con la parte analizadora. Recuerde que si se está realizando un test de caja blanca, deberán abrirle todas las puertas a la red y ofrecerle toda la información que solicite.

Desde el punto de vista del analizador, el acuerdo de confidencialidad le ofrece un marco legal sobre el cual trabajar. Es un respaldo formal a su labor.

8.4.2 Estableciendo las reglas del juego

Antes de comenzar con el análisis de vulnerabilidades es necesario definir cuáles van a ser las tareas a realizar, y cuáles serán los límites, permisos y obligaciones que se deberán respetar.

Es probable que la entidad analizada no esté interesada en que sus servicios se suspendan por un ataque de Denegación de Servicio exitoso por parte del analista. En caso de que esto sea así, el analista deberá ser capaz de determinar las vulnerabilidades sin hacerlas efectivas.

Durante el análisis, deben estar informadas la menor cantidad de personas, de forma que la utilización de la red por parte del personal sea normal, se deben evitar cambios en la forma de trabajo. Si los usuarios de la red son informados que se realizará el análisis, muy probablemente modificarán algunas prácticas inseguras por miedo a ser reprendidos. Si esto sucede, el análisis no resultará valedero.

8.4.3 Reuniendo información

Así como hemos estudiado anteriormente en las fases de un ataque, un análisis de vulnerabilidades comienza con la obtención de información del objetivo. Recuerde que si se ha seleccionado realizar un test por caja negra, el proceso del análisis será muy similar al proceso seguido por un atacante. Si se utiliza un método de caja blanca, éste es el momento para recopilar la información de acceso a servicios, hosts y dispositivos, información de direccionamiento, y todo lo que considere necesario.

- Si está realizando un tes de caja blanca obtenga: Direcciones de los servidores, Nombres de usuario y contraseñas, Servicios que se brindan, Esquema de direccionamiento, Topología física de la rede, Niveles de privilegios.
- Si está realizando un test de caja negra obtenga: Dirección o nombre de dominio a testear

8.4.4 Test interior

El test interior trata de demostrar hasta dónde se puede llegar con los privilegios de un usuario típico dentro de la organización. Para realizarlo se requiere que la organización provea una computadora típica, un nombre de usuario y una clave de acceso de un usuario común. Se compone de numerosas pruebas, entre las que podemos citar:

- **Revisión de Privacidad:** La revisión de privacidad se centra en cómo se gestiona, desde un punto de vista ético y legal, el almacenamiento, transmisión y control de datos de información privada perteneciente a empleados y clientes.
- **Testeo de Aplicaciones de Internet:** Un test de Aplicaciones de Internet emplea diferentes Técnicas de testeo de Software para encontrar fallos de seguridad en aplicaciones cliente/servidor de un sistema desde Internet. Como se está realizando un análisis interno, se deben probar las aplicaciones accesibles por un usuario de la red.
- **Testeo de Sistema de Detección de Intrusos:** Este test está enfocado al rendimiento y susceptibilidad de un IDS. La mayor parte de este test no puede ser llevada a cabo adecuadamente sin acceder a los registros del IDS.

- **Testeo de Medidas de Contingencia:** Se debe medir el mínimo de recursos necesarios que se necesitan en el subsistema para realizar las tareas y verificar la detección de medidas presentes para la detección de intentos de acceso a los recursos protegidos.
- **Descifrado de Contraseñas:** Descifrar las contraseñas es el proceso de validar la robustez de una contraseña a través del uso de herramientas de recuperación de contraseñas automatizadas, que dejan al descubierto la aplicación de algoritmos criptográficos débiles, implementaciones incorrectas de algoritmos criptográficos, o contraseñas débiles debido a factores humanos.
- **Testeo de Denegación de Servicios:** La Denegación de Servicios (DoS) es una situación donde una circunstancia, sea intencionada o accidental, previene el sistema de tal funcionalidad como sea destinada. En ciertos casos, el sistema debe funcionar exactamente como se diseñó, nunca fue destinado para manejar la carga, alcance, o parámetros que abusen de ellos. Es muy importante que los tests de DoS reciban ayuda adicional de la organización y sean monitorizados a nivel privado.
- **Evaluación de Políticas de Seguridad:** la reducción de riesgos en una organización con la utilización de tipos específicos de tecnologías. Existen dos funciones a llevar a cabo: primero, el testeo de lo escrito contra el estado actual de las conexiones ; y segundo, asegurar que la política este incluida dentro de las justificaciones de negocio de la organización, de los estatutos legales locales, federales e internacionales, en especial en lo que hace referencia a los derechos y responsabilidades tanto del empleador como de los empleados. Además de estas pruebas se pueden incorporar las pruebas que se listan en el test exterior (en la siguiente sección), pero tomando como punto de inicio del test a un usuario interno.

8.4.5 Test exterior

El principal objetivo del test exterior es acceder en forma remota a los servidores de la organización y obtener privilegios o permisos que no deberían estar disponibles.

El test exterior puede comenzar con técnicas de Ingeniería Social, para obtener información que luego se utilizará en el intento de acceso.

Los pasos del estudio previo de la organización deben incluir:

1. Revisión de la Inteligencia Competitiva: información recolectada a partir de la presencia en Internet de la organización.
2. Revisión de Privacidad: La revisión de privacidad es el punto de vista legal y ético del almacenamiento, transmisión y control de los datos basados en la privacidad del cliente.
3. Testeo de Solicitud: Este es un método de obtener privilegios de acceso a una organización y sus activos preguntando al personal de entrada usando las comunicaciones como un teléfono, e-mail, chat, boletines, etc desde una posición "privilegiada" fraudulenta.
4. Testeo de Sugerencia Dirigida: En este método se intenta lograr que un integrante de la organización ingrese a un sitio o reciba un correo electrónico, en este sitio o correo se podrían agregar herramientas que luego serán utilizadas en el intento de acceso.

Una vez que se recopiló esta información, se procede a realizar las siguientes pruebas:

- **Sondeo de Red:** El sondeo de red sirve como introducción a los sistemas a ser analizados. Se analizan Nombres de Dominio, Nombres de Servidores, Direcciones IP, Mapa de Red, Información del ISP, Propietarios del Sistema y del Servicio.
- **Identificación de los Servicios de Sistemas:** En esta prueba se deben enumerar los servicios de Internet activos o accesibles así como traspasar el Firewall con el objetivo de

encontrar más máquinas activas. Luego es necesario llevar adelante un análisis de la aplicación que escucha tras dicho servicio. Tras la identificación de los servicios, el siguiente paso es identificar el sistema mediante las pruebas sobre el sistema con el fin de obtener respuestas que puedan distinguir su sistema operativo y su versión (fingerprinting).

- **Búsqueda y Verificación de Vulnerabilidades:** La finalidad de esta prueba es la identificación, comprensión y verificación de debilidades, errores de configuración y vulnerabilidades en un servidor o en una red. La búsqueda de vulnerabilidades utilizando herramientas automáticas es una forma eficiente de determinar agujeros de seguridad existentes y niveles de parcheado de los sistemas, pero no se debe menospreciar la información de nuevas vulnerabilidades que se publican en sitios underground, todavía no incluidas en las herramientas automáticas.
- **Testeo de Aplicaciones de Internet:** Un test de Aplicaciones de Internet emplea diferentes técnicas de testeo de Software para encontrar fallos de seguridad en aplicaciones cliente/servidor de un sistema desde Internet. Como se está realizando un análisis externo, pueden ser utilizados en este módulo los tests de "Caja Negra".
- **Enrutamiento:** Este módulo está diseñado para asegurar que sólo aquello que debe ser expresamente permitido, puede ser aceptado en la red; todo lo demás debe ser denegado.
- **Testeo de Relaciones de Confianza:** El propósito es verificar los controles de acceso desde Internet planteándose como una entidad confiada de la red interna.
- **Verificación de Radiación Electromagnética (EMR):** Este es un método para verificar la Seguridad de las Emisiones electromagnéticas emitidas por diferentes dispositivos. Se puede capturar la radiación electromagnética de los dispositivos tales como CRTs, LCDs, impresoras, módems, teléfonos móviles, entre otros y utilizarse para reconstruir los datos mostrados en la pantalla, impresos, transmitidos.
- **Verificación de Redes Inalámbricas [802.11]:** Este es un método para la verificación del acceso a redes WLAN 802.11, estudiando la cobertura de la red y el acceso a los access points o redes ad-hoc.

8.4.6 Documentación e informe

Como finalización del análisis de vulnerabilidades se debe presentar un informe donde se detalle cada uno de los tests realizados y los resultados.

En este informe se debe especificar:

- Lista de vulnerabilidades probadas
- Lista de vulnerabilidades detectadas
- Lista de servicios y dispositivos vulnerables
- El nivel de riesgo que involucra cada vulnerabilidad encontrada en cada servicio y dispositivo.

Como anexo, se deben incluir los resultados de los programas utilizados

8.5 PREGUNTAS Y TIPS

- **¿Cuándo es recomendable realizar un análisis de vulnerabilidades en una red?** Cuando cambia el diseño de la red, Cuando se implementan actualizaciones de software, Cuando se realizan actualizaciones de dispositivos
- **Suponga que Ud. quiere realizar un análisis de vulnerabilidades de toda una red y el único dato que tiene para realizar el análisis es la dirección IP de un host ¿Qué tipo de análisis sería?** Caja Negra
- **¿En qué circunstancias utilizaría el Hacking ético?** Si quiere analizar el comportamiento y la seguridad de sus sistemas frente a los ataques
- **¿Cómo podemos detectar las vulnerabilidades de configuración?** Conociendo exhaustivamente el software analizado
- **¿Cómo puede solucionar una vulnerabilidad de un dispositivo?** Mediante actualización del software del dispositivo, Mediante el reemplazo del dispositivo vulnerable, Mediante filtros específicos
- **¿Por qué existen protocolos inseguros?** Porque cuando se definieron no existía una difusión tan grande de Internet, Porque algunos protocolos simples se volverían muy complejos agregando características de seguridad, Porque se cometieron errores al definir los protocolos
- **¿Cuáles son técnicas de escaneo de puertos?** TCP SYN scanning, TCP FIN scanning, Connect scanning
- **¿Qué tipo de información pueden proveer los detectores de vulnerabilidades?** Vulnerabilidades conocidas de los servicios detectados
- **¿Para qué pueden ser utilizados los analizadores de protocolos?** Para capturar contraseñas de Telnet, Para capturar contraseñas de FTP
- **¿Cómo se puede automatizar un intento de acceso a un host o servicio?** Mediante password crackers
- **¿Cuál es el principal objetivo de un test interior?** Acceder a los servidores desde la red interna de la empresa como un usuario típico con el fin de obtener privilegios y/o accesos no autorizados
- **¿Cuál es el principal objetivo de un test exterior?** Acceder en forma remota a los servidores de la empresa obteniendo accesos y/o privilegios no autorizados
- **¿Qué diferencia existe entre un test interior y un test exterior?** Para realizar el test interior el analista en seguridad se ubica en la red interna y para el otro caso en la red externa
- **¿Qué información NO se debe incluir en la documentación de un Análisis de Vulnerabilidades realizado?** Solución a las vulnerabilidades detectadas
- **¿Cuáles son los pasos a seguir para realizar un análisis de vulnerabilidades?** Acuerdo de confidencialidad entre las partes, Establecimiento de las reglas, Reuniendo información, Test interior, Test exterior, Documentación e informe

CAPÍTULO 9

9.1 CÓDIGO MALICIOSO

Sin duda, una de las amenazas de seguridad con más prensa entre los usuarios de computadores y público en general, sea aquella referida a los ataques de Virus informáticos. Desde hace algunos años y especialmente a partir de la explosión de Internet como medio de comunicación global, se han sucedido una serie de episodios que han hecho del Código Malicioso en general y de los virus en particular, una de las principales causas de pérdida de dinero por incidentes de seguridad. A lo largo de esta unidad, definiremos conceptualmente el término “Código Malicioso” así como cada uno de los componentes de software que integran esta categoría, la forma en la que se presentan, los daños que son capaces de causar y las medidas de protección que se encuentran a nuestra disposición a fin de minimizar el riesgo de su amenaza.

¿Qué es el código malicioso? Todo programa o fragmento de código generado para que su accionar produzca algún problema en un equipo o sistema de cómputo, interfiriendo en su normal funcionamiento.

Ya sea que usted administre una red corporativa de computadoras, o bien su propio sistema hogareño, probablemente haya sido víctima de algún tipo de virus informático, al menos una vez. Desde la introducción conceptual de estos últimos en los años sesenta, hasta nuestros días, el software catalogado como “Código Malicioso”, ha sido parte responsable, de algunos de los más importantes incidentes de seguridad a nivel mundial, acarreando en la mayoría de los casos, pérdidas económicas contadas en millones de dólares, a las compañías y usuarios damnificados.

Pero los virus informáticos, no son la única manifestación de código malicioso, de la misma forma en que los perjuicios económicos, no siempre se encuentran relacionados con la “pérdida” de un bien tangible. Ataques a la privacidad, productividad, disponibilidad e integridad suelen ser también, producidos por este tipo de amenazas.

Como profesional en seguridad de la información, deberá estar preparado para poder identificar los aspectos claves respecto de cada una de las variantes conocidas de “Código Malicioso”, así como también su alcance y la contramedida asociada.

El enunciado de métodos, políticas, procedimientos y el empleo de herramientas relacionadas con la seguridad de la información frente a este tipo de amenazas, así como la concientización respecto del alcance global de las mismas, son el eje principal del presente capítulo.

Comenzaremos esta sección definiendo el término “Código Malicioso”, como “Todo programa o fragmento de código, que genera en su accionar, algún tipo de problema en el sistema de cómputo en el cual se ejecuta, interfiriendo de esta forma con el normal funcionamiento del mismo”.

Si bien es cierto que los distintos tipos de “Código Malicioso” poseen características particulares, que los distinguen entre sí y ayudan a su catalogación, también lo es el hecho de que comparten algunos aspectos en común:

- Generalmente se trata de componentes de software, desarrollados con un fin específico.
- En algún punto interfieren con la operación normal del sistema de cómputo.
- Suelen instalarse y ejecutarse sin el consentimiento “expreso” del usuario.
- Requieren de un sistema de cómputo anfitrión para cumplir su cometido.

Si bien es cierto, que el verdadero origen de lo que hoy se conoce como “Código Malicioso”, es incierto, existen una serie de hitos históricos que suelen servir como referencia al momento de establecer una línea de tiempo al respecto.

La historia nos indica que ya en 1949, el matemático John Von Neumann describió conceptualmente, programas que se reproducían a sí mismos y que podrían asemejarse a los que hoy conocemos como virus informáticos. Los finales de la década del 50 por su parte, fueron testigo del desarrollo por parte de un grupo de programadores de los laboratorios Bell, de un juego denominado “Core Wars”, el cual tenía la capacidad de reproducirse cada vez que se ejecutaba y podía llegar a saturar la memoria del equipo del otro jugador. Al mismo tiempo, los propios creadores del curioso juego, inventaron también lo que hoy día, a la distancia, podría denominarse el primer antivirus, al escribir una aplicación llamada “Reeper” que básicamente se encargaba de destruir las copias hechas por “Core Wars”.

De todas formas, no sería hasta 1986, año en el cual haría su aparición “Brain”, un virus para DOS de origen Pakistaní, que se comenzaría a hablar de “virus dañinos”, probablemente uno de los primeros “Códigos Maliciosos” de la historia.

Muchas cosas han cambiado desde la aparición de las primeras formas de “Código Malicioso”, aunque sin lugar a dudas la capacidad de distribución que estos han logrado es el factor de mayor evolución. Atrás han quedado los días en los que se apelaba al uso de disquetes como medio predilecto para el despliegue de virus informáticos. La explosión de Internet ha transformado las antiguas infecciones locales, en epidemias mundiales.

Antiguamente, los creadores de “Código Malicioso” apelaban a técnicas de programación que les permitiera distribuir su producto a través de la memoria compartida de un mainframe, más tarde llegaría el turno de aquellos que haciendo uso del sector de boteo de los discos anfitriones, esperaban ansiosos la llegada de un ente portador que los trasladara hasta su próxima víctima. Las primeras conexiones LAN fueron testigo de alguna de las primeras infecciones a través de recursos compartidos. Finalmente Internet, se ha transformado en el medio de distribución por excelencia, contribuyendo incluso al desarrollo de nuevas formas de “Código Malicioso” como los cookies y el spyware. Si ha estado atento a lo leído hasta el momento, probablemente este de acuerdo con nosotros respecto de que las perspectivas actuales no parecen ser muy buenas. Espere a conocer las futuras.

Como veremos en las próximas secciones, el “Código Malicioso” se ha vuelto más sofisticado especialmente respecto de las formas en las que se presenta y los medios que utiliza a la hora de infectar nuevas víctimas. Este último tiempo han visto la luz una serie de gusanos de características singulares, las cuales los hacen sumamente letales.
Pero no sólo los programadores expertos en desarrollo de virus representan una amenaza. Hoy día puede resultar sumamente sencillo conseguir a través de Internet, herramientas que permiten a una persona sin muchos recursos intelectuales generar su propio virus con tan solo unos clicks del ratón. Si bien estos últimos no suelen llegar a provocar los daños de sus hermanos mayores, no dejan de ser preocupantes.

Es cierto que generalmente se suele asociar a los virus con el término de “Código Malicioso”, aunque como ya hemos manifestado anteriormente, no son la única amenaza. Empresas encargadas, por ejemplo, de realizar el seguimiento de los hábitos de compra o uso, de Internet por parte de los usuarios haciendo uso de cookies o código activo descargable imperceptiblemente, en nuestra rutina diaria de exploración de Internet, se están convirtiendo cada vez más en una amenaza común, al dispensar componentes no autorizados en nuestros equipos.

Entre las novedades, algunos grupos del underground informático, ya se encuentran trabajando en pruebas de concepto respecto del desarrollo de “Código Malicioso” capaz de distribuirse a través de dispositivos móviles tales como asistentes personales o teléfonos celulares, abriendo de esta forma nuevas posibilidades para la distribución de este tipo de componentes de software.
En resumen, epidemias mundiales, ataques a la privacidad a gran escala y una comunidad de

creadores de virus a la orden del día, componen junto a la explosión de Internet como medio de distribución un cuadro al que debe prestarse la debida atención.
¿Pero cuál es la buena noticia detrás de estos datos? La buena noticia, es precisamente que a pesar de los malos augurios existen una serie de buenas prácticas y herramientas de software con un alto grado de eficacia a la hora de hacer frente a esta amenaza minimizando el impacto de su accionar.
Hoy día, es muy común observar que la mayoría de los usuarios promedio, posee “al menos” su software antivirus. Por otra parte, generalmente los equipos que se comercializan para el uso corporativo u hogareño suelen despacharse con alguno de estos programas como parte del paquete de software incluido. Lo cierto es que a pesar de ello, cada vez con más frecuencia nos encontramos con software antivirus o sistemas operativos que carecen de las actualizaciones que los hacen inmunes a las amenazas conocidas, y este es “una vez más” el punto débil que seguirá haciendo del “Código Malicioso” un verdadero dolor de cabeza.

Al margen de las características comunes que comparten los distintos tipos de “Código Malicioso”, existen diferencias fundamentales que hacen necesaria su clasificación de acuerdo a su origen, forma, daños que provocan y función para la cual han sido desarrollados.

Siguiendo este criterio y a los efectos de su estudio en el presente capítulo, revisaremos en detalle las siguientes cinco categorías principales, las cuales a su vez podrán contener su propia estructura interna:

- Virus
- Troyanos
- Cookies
- Keyloggers
- Spyware

9.2 VIRUS

Sin temor a equivocarnos, estamos en condiciones de afirmar que los virus informáticos, son quizás el tipo de “Código Malicioso” más extendido. Su historia y evolución han hecho de ellos una de las amenazas más temidas para los administradores de sistemas de información y usuarios en general.

Como veremos a lo largo de esta sección la variedad de virus conocidos va desde aquellos sumamente inofensivos hasta algunos de los más destructivos. En algunos casos, hasta se torna complicado encuadrar algunos de ellos en alguna de las categorías que presentaremos a continuación, puesto que los últimos especímenes conocidos hacen uso de diversas técnicas para lograr su objetivo, las cuales a su vez incluyen aprovechamientos de vulnerabilidades en los sistemas operativos más frecuentemente utilizados, carga de códigos exploits y sus propios servidores de correo SMTP incorporados tendientes a hacer más efectiva su distribución.

9.2.1 ¿Qué es un virus?

Un virus es una pieza de software diseñada para infectar un sistema de cómputo. En esencia, los diferentes tipos de virus, al igual que el resto del “Código Malicioso” sobre los que trataremos en este capítulo, no son más que pequeños componentes de software, desarrollados generalmente en lenguajes de alto nivel, bajo nivel e híbridos (C, C++, Assembler, etc.) con el objeto de concretar algún tipo de acción maliciosa, no deseada por el propietario del equipo anfitrión.

A pesar de que un virus puede estar construido tan solo con el objeto de infectar una PC y permanecer en ella el mayor tiempo posible, lo cierto es que generalmente suelen acarrear problemas mayores que van desde la simple eliminación de archivos claves del sistema operativo, pasando por la completa destrucción de particiones de discos duros, hasta llegar incluso en algunos casos, a dañar el

firmware del equipo de la víctima.

Pero esto no es todo, la mayoría de ellos suelen contar con las habilidades necesarias como para atacar nuevos sistemas y distribuirse tanto como les sea posible, causando frecuentemente ataques de denegación de servicio, algunas veces fríamente calculados y dirigidos a objetivos previamente estipulados

En resumen, podríamos concluir que algunas de las características más importantes de los virus, son la posibilidad de replicarse y de poseer rutinas de daño. Aquellos virus que no poseen una rutina de daño, pueden igualmente causar distintos tipos de inconvenientes, al consumir espacio de almacenamiento, memoria y degradar completamente el desempeño de los equipos de cómputo infectados.

9.2.2 Tipos de virus

Una de las particularidades de los virus informáticos, en relación al resto del "Código Malicioso" estudiado en el presente capítulo es su diversidad. Debido a ello, suele ser necesario establecer diferentes grupos respecto de su tipo, a fin de realizar en cada caso su correcta identificación.

Generalmente, suelen clasificarse en función de múltiples características y criterios: según su origen, las técnicas que utilizan para infectar, los tipos de ficheros que infectan, los lugares donde se esconden, los daños que causan, el sistema operativo, la plataforma tecnológica que atacan, etc. Todas estas clasificaciones tienen muchos puntos en común, por lo que un mismo virus puede pertenecer a varias categorías al mismo tiempo. A continuación se presenta una breve descripción de los tipos de virus más importantes.

Macro Virus: De acuerdo a un estudio de la ICSA (International Computer Security Association), los denominados "Macro Virus", suman alrededor del 80 por ciento del total de virus conocidos, al tiempo que ostentan el título de ser uno de los tipos de más amplia explotación hoy día.

A diferencia de otros virus, estos no son específicos de un sistema operativo en particular, pero sí del grupo de aplicaciones para las que fueron creados.

Los "Macro Virus", suelen estar construidos con código tendiente a explotar algunas de las características avanzadas, implementadas en las aplicaciones de oficina más ampliamente utilizadas. Las capacidades integradas de programación o creación de macros que éstas poseen, suelen incluir un set de instrucciones lo suficientemente potente, como para que los creadores de este tipo de virus elaboren su código malicioso basado en él. Algunos macro virus crean réplicas de sí mismos, mientras que otros infectan documentos. Ejemplos: Relax, Melissa.A, Bablas, 097M/Y2K.

Virus Polimorfos: El término de Polimorfo, de múltiples formas, suele ser el apropiado para nombrar a aquellos virus que tienen la capacidad de mutar alguna de sus formas (cambiar las características de su código cuando se replica), haciendo más difícil su detección por parte del software antivirus que utiliza métodos de análisis de cadenas simples. Funcionalidades tales como la encriptación de determinadas partes de su código original suelen servir también a este propósito, evitando en algunos casos, la detección por firmas. Ejemplos: Elkern, Marburg, Satan Bug, Tuareg.

Bombas Lógica: Las bombas lógicas, son un tipo de "Código Malicioso" muy particular. Si bien pueden encontrarse como un programa independiente, generalmente suele asociarse el término de "Bomba Lógica" con pequeños fragmentos de código, incluidos dentro de otros programas preparados específicamente para activarse al cumplirse ciertos eventos definidos como parte de su lógica interna.

Una de las particularidades de este tipo de amenazas, es que mientras que ninguno de estos eventos predefinidos suceda, pueden llegar a pasar totalmente desapercibidas.

Hoaxes o Engaños: De la mayoría de los códigos maliciosos existentes, los Hoax quizás sean los más simpáticos, aunque no por eso, del todo inofensivos. En rigor de verdad, un Hoax es un falso virus y no realiza por sí mismo ninguna acción. Generalmente consiste en un mensaje de correo electrónico en el que se alerta sobre la supuesta existencia de un nuevo virus que ningún antivirus detecta. Este tipo de mensaje generalmente apela a técnicas de ingeniería social, mediante las que se insta a los usuarios a eliminar en forma manual, los supuestos archivos infectados por este virus inexistente, generando de esta forma que el propietario del sistema sea quien se auto-inflija el daño.

Caballos de Troya o Troyanos: Un troyano o Caballo de Troya, es un programa que se diferencia de los virus tradicionales en que no se reproduce infectando otros ficheros. Tampoco se propaga haciendo copias de sí mismo. Por el contrario, suelen llegar al sistema objetivo como parte de programas aparentemente inofensivos, a la espera de poder ser ejecutados a fin de instalar el verdadero código troyano escondido detrás de esta cortina de humo. (Debido a la amenaza que representan los troyanos para los sistemas de información, se ha dispuesto una sección exclusiva para su tratamiento, más adelante en este mismo capítulo). Ejemplos: IRC.Sx2, Trifor.

Worms o Gusanos: Antiguamente, solía utilizarse el término de “Worm” o “Gusano”, para referirse a un tipo de código malicioso en particular con el poder de auto-replicarse realizando copia de sí mismo o de alguna de sus partes. Los primeros gusanos, tenían como única finalidad, la de ir consumiendo memoria del sistema atacado hasta desbordar la RAM, siendo ésta su única acción maligna.
Los “Worm” o “Gusanos” no son considerados virus en el estricto sentido de la palabra, pues básicamente no necesitan infectar otros archivos para poder multiplicarse, de hecho, la multiplicación es una característica inherente a su construcción.

Si bien es cierto que la esencia detrás de la creación de “Worms” o “Gusanos” no ha variado, muy lejos han quedado ya, los tiempos en los que su accionar apuntaba “*tan solo”* a consumir memoria de los mainframe atacados. Hoy día, los gusanos suelen estar dotados de la capacidad necesaria como para:

- Instalar troyanos y keyloggers en nuestro sistema.
- Configurar los equipos atacados para que actúen como un servidor Proxy.
- Hacer uso de los recursos de procesamiento y ancho de banda del sistema víctima para lanzar ataques dirigidos de denegación de servicio.
- Hacer uso de los recursos de almacenamiento del sistema víctima para albergar material considerado como ilegal en algunos países.

Los últimos gusanos conocidos, han causado estragos alrededor del mundo. Sus nuevas capacidades, incluyen la explotación de vulnerabilidades conocidas en algunos de los sistemas operativos más utilizados, característica que ha contribuido a transformar este tipo de “Código Malicioso” en una de las amenazas más serias en materia de seguridad de la información. Ejemplos: PSWBugbear.B, Lovgate.F, Trile.C, Sobig.D, Mapson.

Retrovirus: Los denominados Retrovirus, son aquellos que actúan directamente sobre el software antivirus instalado en su sistema, intentando de esta forma anular su accionar. Algunos de estos especímenes utilizan vulnerabilidades del propio software antivirus o intentan eliminar las definiciones de las cuales estos se valen para realizar su tarea.

Stealth Virus o Virus indetectable: La particularidad de los virus Stealth o Indetectables, reside en la capacidad de ocultamiento que éstos poseen. Una de las técnicas básicas en tal sentido, suele estar dada por acciones tendientes a engañar al sistema operativo, de forma tal que éste reporte un tamaño para el archivo infectado igual que el original. Esta acción podría hacer que en ciertas circunstancias el software antivirus, no se percate de su presencia.

Multipartite Virus o Virus Multi-parte: Suele denominarse Virus Multi-parte, a aquellos que tienen la capacidad de atacar un sistema en múltiples formas. Los virus incluidos en esta categoría, suelen ser sumamente dañinos y pueden comenzar infectando el sector de boteo para luego continuar con los archivos ejecutables y documentos de Word, para finalmente volver el disco inutilizable. Ejemplo: Ywinz.

Armored Virus o Virus Blindado/ Encriptado: El término blindado proviene de las características de diseño de algunos virus, tendientes a dificultar su análisis o detección. Por lo general, suelen incorporar funciones de protección, especialmente contra los debuggers o des-ensambladores utilizados por los expertos. Otras veces, incluyen aspectos en su programación, tendientes a desviar la atención del código verdaderamente responsable por la actividad maliciosa. Ejemplos: Elvira, Trile.

Companion Virus o Virus Acompañante: Un virus acompañante, suele unirse a programas legítimos para luego crear un programa con una extensión diferente, que se albergará en algún directorio temporal de su sistema. Al momento en que el usuario ejecute el programa legítimo, el programa compañero se ejecutará en su lugar, logrando de esta forma, que el programa infectado, realice el trabajo sucio, para finalmente dejar actuar al programa verdadero. Ejemplos: Stator, Asimos.1539, Terrax.1069.

Phage Virus o Virus Parásito: Este tipo de virus, actúa modificando otros programas. Debido a su accionar, la re-instalación de los programas infectados, suele ser la única forma de quitarlo del sistema víctima. Si una vez reinstalados los programas atacados, por algún motivo, quedara vestigio del parásito en cualquiera de los archivos del sistema, no tardaría en lanzarse un nuevo proceso de infección. Ejemplos: Jerusalem, CIH (Chernobyl), WNT/RemEXp.

9.2.3 Historia y presente: Virus famosos

Melissa: Se trata de uno de los primeros macro virus. Como parte de su funcionamiento, infectaba los módulos Class de Word, a partir de lo cual se enviaba a las primeras 50 cuentas de correo, de cada una de las libretas de direcciones a las que Outlook tuviera acceso. El asunto del mensaje resultante era: 'Important Message From <nombre de usuario>' (donde <nombre de usuario> era tomado de la configuración del sistema) y en el cuerpo podía leerse la leyenda 'Here is that document you asked for... don't show anyone else ;-)'. Además se incluía un archivo adjunto, conteniendo una copia del documento con el virus. En su momento, a Melissa le tomo tan solo un día para distribuirse alrededor del mundo.

CIH (Chernobyl): Hacia Junio de 1998, unos cuantos virus habían sorprendido al mundo, pero la aparición de CIH marcó un hito al convertirse en el primer virus con la capacidad de dañar el hardware de una computadora. La acción destructiva se lanzaba, en su versión original, el 26 de Abril, y consistía en sobre-escribir la BIOS de cierto tipo de computadores. Una vez logrado su objetivo, el chip conteniendo la BIOS dañada, debía ser remplazado para volver a poner el equipo atacado en funcionamiento.

Love Bug (I Love You): Love Bug, es probablemente uno de los virus más conocidos de la historia. Este original gusano de origen Filipino, programado en Visual Basic Script, se presentaba ante el usuario pretendiendo ser una carta de amor, utilizando como asunto, la frase “I LOVE YOU”, mientras que en su cuerpo podía leerse el mensaje: “kindly check the attached love letter coming from me”. Finalmente, el abrir el archivo adjunto, ejecutaba el código malicioso, el cual en caso de detectar un cliente Outlook instalado en el sistema, realizaba el reenvío del virus a todas las cuentas de correo contenidas en la libreta de direcciones del sistema infectado, y sobrescribía ciertos archivos. Love Bug, fue uno de los primeros gusanos en demorar tan solo algunas horas, en dar la vuelta alrededor del mundo.

Sircam: Sircam es básicamente un gusano que llega oculto dentro de un mensaje de correo electrónico. La primera línea del contenido del mensaje incluye el texto: Hola cómo estás? mientras que el cuerpo del mismo invita al usuario infectado, a dar su "punto de vista" respecto de un archivo adjunto, el cual contiene la carga maliciosa. Sircam es altamente infeccioso motivo por el cual consigue propagarse muy rápidamente enviándose automáticamente a todos los contactos que encuentra en la libreta de direcciones existente en las computadoras infectadas y a su vez esparciéndose en las redes internas bajo plataformas Microsoft, en las cuales se utilicen unidades de disco como recursos compartidos. Dos consecuencias conocidas de este gusano son: la obtención de datos privados de los usuarios que infecta y una posible denegación de servicio al consumir el espacio total del disco duro y la eliminación de datos contenidos en el mismo.

Nimda: Originario de China, Nimda es un peligroso gusano. El mismo se propaga extremadamente rápido valiéndose de dos vulnerabilidades. La primera, afecta servidores Windows corriendo IIS ("Web Directory Traversal Exploit") y la segunda a las versiones 4.0 y 5.0 de "Microsoft Internet Explorer". A su vez, Nimda es capaz de forzar la creación de los recursos compartidos en redes Windows, para luego utilizarlas también como medio de propagación. Su objetivo es propagarse al mayor número de equipos, infectando todos los ficheros con extensión EXE que encuentra y activándose cuando el usuario abre los programas Word y Wordpad. Nimda apareció cuatro meses después de que se anunciara la vulnerabilidad de la que hace uso.

Código Rojo: Código Rojo o Red Code es otro gusano que se propaga a través de redes, aprovechándose de una vulnerabilidad existente en los servidores Index Server 2.0, Indexing Service e IIS 4.0 y 5.0 consistente en un desbordamiento de buffer. Adicionalmente, es capaz de reiniciar o bloquear los equipos, causando una DoS al crear numerosos hilos (procesos) de ejecución en memoria, las cuales se comportan como copias del propio gusano (600 hilos en el caso de ordenadores con el sistema operativo en chino y 300 en los demás casos). Por otra parte, para encontrar otros equipos a los que infectar, Red Code genera máscaras y direcciones IP. Cuatro de estas direcciones se encuentran dentro de la red de clase A, tres de ellas están en la red de clase B y otra se genera de manera totalmente aleatoria.

SQL Slammer: *Este gusano cuenta con la particularidad de que sus* ataques, afectan exclusivamente a servidores que ejecuten Microsoft SQL. Se aprovecha de una vulnerabilidad de tipo desbordamiento de buffer encontrada en servidores SQL que no tengan instalado el SP 3. Las consecuencias de su ataque pasan por la denegación de servicio causada por el tráfico generado por el código del gusano dirigido al puerto 1434 UDP (*SQL Server Resolution Service Port*). *Slammer* apareció seis meses después de que se hubiera anunciado la vulnerabilidad de la que hace uso.

Blaster: También conocido como Lovsan, *Blaster* es un gusano que sólo afecta a ordenadores con sistemas operativos Windows 2003/XP/2000/NT. Se aprovecha de una vulnerabilidad conocida como "Desbordamiento de Buffer RPC" para propagarse al mayor número de ordenadores posible. Una de las particularidades de este virus es la lógica incluida en él, mediante la cual se planifica en el tiempo, un ataque DoS contra el sitio web de Microsoft: windowsupdate.com. Para ello, *Blaster* envía un paquete de tamaño 40 *Bytes* a dicho sitio web cada 20 milisegundos, a través del puerto 80.

Blaster se propaga atacando direcciones IP generadas aleatoriamente y explotando los servicios RPC vulnerables, luego de lo cual intenta descargar en el ordenador atacado una copia de sí mismo, vía su propio servidor TFTP. Este gusano, apareció sólo tres semanas después de que se diera a conocer la vulnerabilidad de la que hace uso.

Klez: *Klez*, probablemente se encuentre entre los gusanos más exitosos de la historia de Internet. Un año después de hacer su aparición, continuaba siendo uno de los códigos maliciosos más extendido.

Klez se aprovecha de una vulnerabilidad de Outlook Express, logrando de esta forma activarse con sólo hacer una vista previa del mensaje (característica que suele ser utilizada por un sin número de usuarios de este tipo de software). Como en la mayoría de los casos, existía el parche correspondiente para esta vulnerabilidad, antes de que se lanzara el gusano. Así y todo, *Klez* logró una penetración pocas veces vistas. Como parte de su actividad maliciosa, éste instalaba un nuevo virus conocido como *Elkern,* el cual se encargaba de desactivar Firewalls personales y aplicaciones antivirus, no sin antes eliminar archivos del sistema infectado.

Nicehello: Se trata de un gusano sin efectos destructivos que se propaga a través del correo electrónico. De este modo, una vez infectado el ordenador, manda una copia de sí mismo a todas las direcciones de correo que encuentra en la *Lista de contactos* del programa de mensajería instantánea *MSN Messenger.* Además, *NiceHello* envía un correo electrónico al autor del virus, en el que incluye el nombre de usuario y contraseña de *MSN Messenger* del usuario del ordenador afectado. Si bien es cierto que este virus no posee en principio implicancias destructivas, suele tomarse como prueba de concepto respecto de las posibilidades que representa la obtención de claves de uno de los mensajeros instantáneos más ampliamente utilizados, con la invasión a la privacidad que ello significa.

Bugbear: A pesar de que este código malicioso, comparte algunas características con *Klez* (Aprovecha la misma vulnerabilidad de Outlook Express) es mucho más peligroso, debido a que entre sus acciones, se cuenta la apertura de una puerta trasera a la escucha en el puerto 1080, más un keylogger capaz de registrar lo tipiado por el usuario víctima. Como si esto fuera poco, *Bugbear* poseía una lista de 1300 direcciones de entidades bancarias que utilizadas en conjunto con los registros de teclado, le permitía activar el mismo al detectar el acceso a alguno de los bancos incluidos en su carga útil, por parte del usuario.

Sobig: La versión original de este virus, se propagaba a un ritmo estremecedor, en parte gracias a que poseía su propio motor SMTP. Si bien como en el resto de los casos, las sucesivas versiones mutaban su presentación, en sus inicios solía llegar al usuario desde el remitente big@boss.com y el contenido: Attached file: a la vez que adjuntaba un archivo con extensión .PIF o .MPEG. *Sobig* hacía uso de otro método de dispersión el cual le permitía atravesar redes internas a través de los recursos compartidos. Una vez producida la infección, *Sobig* enviaba un mensaje a la dirección: pagers.icq.com y a continuación, se conectaba a una página Web para descargarse un virus de tipo troyano.

Sasser: El accionar de *Sasser* no difiere mucho del resto de los gusanos comentados, desde el punto de vista que también se propaga explotando una vulnerabilidad, en aquellos sistemas Windows 2000, 2003 y XP que no han sido convenientemente actualizados. En este caso se trata de un desbordamiento de buffer en el subsistema LSASS (Local Security Authority Subsystem Service). Cuando *Sasser* explota la vulnerabilidad LSASS, provoca un desbordamiento de *buffer* en el programa LSASS.EXE, lo cual desencadena el reinicio del ordenador.

9.2.4 Síntomas de un ataque

Suelen existir diferentes síntomas de un ataque o infección de acuerdo al tipo de virus que actúe en cada caso. Muchos virus han hecho historia, encargándose de presentarse por sí solos, anunciando el comienzo de su actividad infecciosa, muchos otros por el contrario intentan pasar desapercibidos.

Como regla general, usted debería sospechar de su instalación de software si observara al menos alguno de los siguientes síntomas:

- Su sistema muestra un mensaje indicándole que usted ha sido infectado con un virus.

- Los programas en su sistema tardan en cargar o lo hacen muy lentamente.
- Archivos desconocidos aparecen en su disco rígido.
- Archivos necesarios para la ejecución de uno de sus programas o del sistema operativo desaparecen de su disco rígido.
- Escrituras inesperadas en una unidad de disco.
- Actividad de pantalla no estándar o extraña.
- El tamaño de sus archivos de programa cambia súbitamente respecto de su tamaño original.
- Su software de aplicación cambia su aspecto o se comporta de forma extraña.
- Su sistema repentinamente no inicia o exhibe algún mensaje de error inesperado.
- Su sistema se reinicia en forma inesperada o manifiesta un uso intensivo de sus recursos sin motivo aparente.
- Misteriosamente su disco se vuelve inutilizable.
- Su sistema muestra signos de estar siendo víctima de un ataque DoS.
- Su servidor de correo presenta una carga de trabajo fuera de lo común.
- Su red o dispositivos de Networking ostentan una carga de trabajo fuera de lo normal.
- El ancho de banda contratado a su proveedor parece estar sobrecargado.

9.2.5 Etapas de contaminación

Hace algunos años, los especialistas se referían a los ataques de virus informáticos situándose en el marco de tres etapas principales respecto de la infección o contaminación:

1. Etapa de Infección: El virus infecta el sistema que es su blanco.
2. Etapa de Contaminación: El virus se conforma con propagarse e infectar otros blancos o tan solo se conserva estático.
3. Etapa destructiva: El virus entra en actividad y produce los efectos para los que fue programado.

Si bien esta primer enumeración sigue estando vigente, en la actualidad, solemos más bien, referirnos al “Ciclo de Vida de un Virus”, haciendo un paralelismo con su contrapartida biológica. Dicho ciclo empieza cuando es creado y termina cuando es completamente erradicado. El siguiente esquema describe cada etapa:

- **Creación:** Hasta hace poco tiempo, crear un virus requería el conocimiento de un lenguaje de programación. Hoy en día cualquier persona con un conocimiento básico de programación puede crear un virus. Típicamente, las personas que desean causar un daño extenso y aleatorio a las computadoras crean un virus.
- **Replicación:** Los virus típicamente se replican por un largo período antes de que estos se activen, permitiendo un basto tiempo para su esparcimiento.
- **Activación:** Los virus con rutinas de daño se activarán cuando ciertas condiciones sean cubiertas, por ejemplo, en cierta fecha o cuando los usuarios infectados realicen una acción en particular. Los virus sin rutinas de daños no se activan, sin embargo causan daño al robar espacio de almacenamiento.
- **Descubrimiento:** Esta fase no siempre sigue a la activación, pero típicamente lo hace. Cuando un virus es detectado y aislado, este es enviado al ICSA en Washington, DC., para ser

documentado y distribuido a los desarrolladores de software antivirus.

- **Asimilación:** En este punto, los desarrolladores de software antivirus modifican su software para que este pueda detectar el nuevo virus. Esto puede tomar desde un día hasta seis meses, dependiendo del desarrollador y el tipo de virus.
- **Erradicación:** Si suficientes usuarios instalan software de actualización para la protección antivirus, cualquier virus puede ser limpiado. No todos los virus han desaparecido completamente, pero muchos han dejado de ser una amenaza mayor.

9.2.6 ¿Quiénes son los blancos?

El creciente avance tecnológico en materia de comunicaciones, la interconexión de redes a gran escala y el acceso masivo a Internet junto con el empleo del correo electrónico, han puesto de manifiesto la problemática de los virus informáticos y sus cortos tiempos de propagación.

En un principio la distribución de virus sólo se producía a través del intercambio de discos, afectando en mayor medida a aquellos usuarios de software ilegal. Con el acelerado desarrollo de las redes mundiales, la amplia difusión de las aplicaciones de intercambio de archivos y la gran cantidad de conexiones domiciliarias, han hecho de este tipo de código malicioso un dolor de cabeza no sólo para las redes empresariales, sino también para el usuario hogareño.

En la actualidad, la gran mayoría de los sistemas de cómputo, son susceptibles a sufrir el ataque de algún tipo de virus informático . Sin lugar a dudas, existen sistemas operativos o aplicativos con mayor riesgo, principalmente debido a su gran penetración en el mercado, lo cual los convierte en un objetivo atractivo para los desarrolladores de este tipo de amenazas.

La peligrosidad de un virus se establece en base a dos criterios principales: su capacidad de hacer daño y la posibilidad de propagación o difusión del código malicioso. De acuerdo a este principio, deberá considerarse más peligroso un virus que elimine información y esté propagándose por toda la Red que otro que también elimine información, pero que no pueda propagarse.

Entre los daños más importantes que producen los virus informáticos, se encuentran:

1. Daños a determinado tipo de hardware.
2. Alteración o pérdida de datos.
3. Denegación de Servicio.
4. Manipulación de Datos.
5. Pérdida de Productividad.
6. Pérdida de Credibilidad.
7. Pérdida de Ganancias.
8. Vergüenza.

9.2.7 Aspectos legales

Los ataques producidos por virus, suelen estar ligados legalmente a lo que se conoce como “Leyes de Delitos Informáticos”. Si bien a nivel mundial, la constitución de leyes precisas al respecto, es en general muy reciente, muchos países han legislado en tal sentido intentando llenar el vacío legal existente hasta ese momento.

9.2.8 Medidas de protección

Antiguamente, las medidas de protección en general contra los virus informáticos, pasaban únicamente por la instalación de software antivirus. Hoy día, a la luz de las nuevas amenazas, la mayoría de las cuales se aprovecha de vulnerabilidades del software de base o aplicación para realizar su actividad maliciosa, debe trabajarse fuertemente sobre el modelo de "Prevención por Capas":

1. Instalación de actualizaciones de seguridad liberadas para sistemas operativos y de aplicación.
2. Implementación de software antivirus en estaciones de trabajo.
3. Implementación de software antivirus en servidores de archivos.
4. Implementación de software antivirus en servidores de correo corporativo.
5. Implementación de software antivirus sobre la navegación corporativa (proxies).
6. Implementación de software de administración de contenidos.
7. Implementación de políticas de filtrado en el perímetro externo.
8. Implementación de sistemas de búsqueda y actualización de vulnerabilidades.
9. Implementación de una política de control de instalación de software legal.

Acompañando esta estrategia, existen en el mercado diferentes proveedores, con productos orientados a brindar la solución necesaria en cada una de las capas mencionadas. Al margen de ello, desde el punto de vista de la seguridad, debería recomendarse siempre que sea posible, la implementación de productos de diferentes proveedores en las diferentes capas. Si esto no fuera así, podría suceder que un virus nuevo, no incluido en el archivo de definiciones del proveedor seleccionado, probablemente no fuera detectado por "ninguna" de las capas en las que se encuentren instalados productos de un mismo proveedor (Por lo general, diferentes productos de un mismo proveedor, suelen compartir su "engine" y "archivo de definiciones de virus").

Un buen software de control antivirus debería cumplir mínimamente con los siguientes requisitos que a continuación se detallan:

- Debe estar certificado por la ICSA (International Computer Security Association).
- Debe tener exploración en tiempo real o programado.
- Debe contar con una consola de administración y reportes central.
- Debe contar con las herramientas para proteger los diferentes focos de infección (discos, mail, web, etc.).
- Debe cubrir la actualización de nuevas firmas antivirus en forma automática y desatendida en servidores y clientes.
- No debe degradar la performance del dispositivo resguardado.
- Debe integrarse con el sistema de respaldo sin afectar la performance, garantizando un backup libre de virus.
- Debe contar con herramientas de logueo de eventos, estadísticas y reportes para el seguimiento de incidentes.
- Debe implementar un sistema de alarmas (e-mail, traps SNMP, pager, etc.).

Independientemente del sistema antivirus a emplear, es fundamental acompañar su implementación con una política antivirus a nivel empresarial correctamente diseñada, que defina cómo debe establecerse y mantenerse el sistema antivirus. Para ello son necesarios los siguientes elementos:

- Calidad del software antivirus.
- Equipos de respuesta ante incidentes.
- Prevención automática (tiempo real).
- Actualización y modificaciones automatizadas.
- Respaldo de la información.
- Protección de los servidores de archivos.
- Identificación de los usuarios que ponen en peligro el sistema.
- Eliminación las fuentes de software no controlado.

9.2.9 Soluciones por Hardware

La creciente demanda respecto de la detección y eliminación de virus informáticos, sumada a la diversidad de ataques perpetrados por el accionar del código malicioso moderno, ha llevado a que el software antivirus realice chequeos que hasta hace algunos años no eran necesarios, convirtiendo a éstos en complejas aplicaciones. Dicha complejidad, se ve reflejada muchas veces en los recursos de hardware necesarios para mantener una solución en forma efectiva.

Precisamente pensando en los entornos corporativos donde suele ser necesaria por ejemplo, la examinación de entre 20000 y 30000 mensajes por hora, algunos de los más importantes proveedores de software antivirus, han lanzado equipos denominados “Appliance” , los cuales suelen consistir en una solución de alto rendimiento, compuesta de hardware y software, que protege las comunicaciones de la empresa ante posibles virus informáticos.

Entre algunas de las características más importantes de estos dispositivos, se encuentran:

- Sencillez de instalación.
- Alta escalabilidad.
- Balanceo de carga.
- Protección de los protocolos de comunicación más utilizados.
- Filtrado de contenidos.
- Administración remota.
- Actualizaciones diarias y automáticas.
- Informes de detección de virus.
- Filtrado de contenidos y monitorización del sistema en tiempo real.

9.2.10 Soluciones On-Line y Gratuitas

En la actualidad, se encuentran a nuestra disposición una serie de alternativas gratuitas al momento de escanear nuestros equipos en busca de virus, sin necesidad de instalar un completo software antivirus. Se trata de una interesante opción On-Line, de la cual disponen la gran mayoría de las compañías importantes del sector a través de la Web

También existe una serie de alternativas gratuitas para instalar y mantener la PC libre de virus, si bien en algunos casos se trata de soluciones que no tienen una interfaz tan completa como sus competidores pagos, en todos los casos su nivel de confiabilidad y de detección es bastante alto y pueden ser una buena opción en ámbitos hogareños.

9.3 TROYANOS

Dentro de los denominados “Códigos Maliciosos”, los troyanos han sabido ganarse un lugar privilegiado. A través del tiempo, este tipo de amenaza ha ido creciendo no solo en número, sino también respecto del potencial daño que son capaces de producir. Integridad y Privacidad son dos principios que suelen ser fácilmente vulnerados, una vez que un troyano ingresa exitosamente a nuestro sistema.

9.3.1 ¿Qué es un troyano?

En su definición más amplia, solemos referirnos a los Troyanos como todo programa que lleva oculta una funcionalidad determinada que será usada con fines maliciosos y en contra del usuario que lo instala. Un Troyano, tomado de la mitología griega del Caballo de Troya, el cual se entregó como un regalo de buena fe y en cuyo interior se escondían los soldados enemigos, típicamente viene en un correcto empaquetamiento, pero al igual que su par mitológico, tiene intenciones ocultas dentro de su código.

Una de las principales diferencias entre un virus y un troyano, es la inhabilidad de estos últimos para replicarse. En teoría, si éste se replica entonces se debe de clasificar como un virus. Otra de las grandes diferencias, es que generalmente, el Troyano forma parte del código fuente del programa instalado y se compila junto con él, mientras que el virus simplemente se añade o suplanta el programa original. Cabe aclarar, que si bien un troyano, no necesariamente debe funcionar como “Backdoor” o “Puerta Trasera”, lo cierto es que la mayoría de ellos sí lo hace, por lo tanto, cuando en este capítulo nos refiramos a “Troyanos”, lo haremos teniendo en mente su aplicación como herramienta de administración remota subrepticia. Los Troyanos, suelen llegar a nuestro sistema, como un programa aparentemente inofensivo, pretendiendo “ser algo que no son” o “hacer algo que no hacen”. Algunas veces, se envían como adjuntos de correo, fingiendo ser una utilidad de sistema , otras como parte integral de una aplicación lícita previamente “troyanizada”, aunque desde el punto de vista específico de su difusión, son capaces de aprovechar cualquiera de los métodos utilizados por los virus informáticos, de hecho, algunos de los tipos de Virus y Gusanos más peligrosos, poseen la capacidad de introducir y ejecutar troyanos y keyloggers, como parte de su accionar malicioso. Ciertas herramientas disponibles en la actualidad, permiten ocultar un troyano, en casi cualquier tipo de archivo o aplicación, lo que genera para el atacante, un sin número de posibilidades a la hora de planear su introducción en el sistema objetivo.

9.3.2 Troyanos famosos

A través del tiempo, gran cantidad de troyanos fueron liberados al público en general. Como gran parte de las herramientas que utilizamos frecuentemente, la mayoría de los troyanos, tienen su origen en grupos de Hackers. Tiempo más tarde, algunos de ellos seguirían evolucionado, hasta convertirse en verdaderas aplicaciones de administración remota de sistemas, mientras que otros darían paso a transformaciones con fines menos nobles. Sin lugar a dudas Netbus, Back Orifice, Subseven y Optix, ostentan hasta el momento, el título de ser los troyanos más famosos, útiles y dañinos a la vez. Si bien es cierto que entre ellos existen diferencias, la gran mayoría cuentan con algunas de las siguientes características principales:

- Edición remota del registro.

- Archivos compartidos.
- Apagado/Reinicio del sistema.
- Recupero de contraseñas almacenadas en cache.
- Captura de pantallas.
- Keylogger.
- Monitoreo del tráfico de red.
- Funcionalidades de Proxy.
- Redirección de puertos y aplicaciones.
- Funciones "*Fun"* o divertidas (Apertura y cierre del CD-DRIVE, intercambio de botones del mouse, ejecución de archivos .WAV, Grabar sonidos desde un micrófono, etc.)
- Presentación de imágenes (BMP/JPEG) y mensajes en pantalla.
- Ejecución de aplicaciones.
- Manipulación del sistema de archivos.
- Notificaciones del éxito del ataque a través de aplicaciones tales como ICQ, IRC o correo electrónico.

Magic Lantern: Para la fecha, 2010 y según una fuente mencionada por el servicio de noticias MSNBC, el FBI estaría desarrollando su propio troyano, para combatir al terrorismo. La idea del programa, es robar las contraseñas de todo aquel (en principio sospechoso), que use correo electrónico cifrado para sus comunicaciones.

Este troyano, conocido como Magic Lantern (Linterna Mágica), podría enviarse a cualquier sospechoso, como un adjunto a un mensaje aparentemente inocente.

Aprovechándose de algunas vulnerabilidades, podría incluso instalarse sin el conocimiento del destinatario, y a partir de allí capturaría las contraseñas usadas por el supuesto terrorista, enviándolas a las oficinas del FBI.

Linterna Mágica sería parte de un programa más complejo de vigilancia, llamado Cyber Knight (Caballero cibernético), el cuál incluiría una base de datos que permitiría al FBI cruzar información proveniente de e-mails, salas de chat, mensajeros instantáneos tipo ICQ y llamadas telefónicas por Internet.

Algunas fuentes consultadas del FBI, ni negaron ni admitieron la noticia, pero declararon que no es nada nuevo que la organización ha estado trabajando con especialistas de la industria de la seguridad, para crear una herramienta que fuera eficaz en combatir tanto al terrorismo, como a otros actos delictivos. Y aunque no debería ser una sorpresa, tampoco es apropiado que se revelen las tecnologías que específicamente se usarán, explicó un portavoz.

Por otro lado, está el gran tema que involucra a nuestras libertades individuales. Organizaciones norteamericanas que defienden los derechos civiles de los ciudadanos, ya han reaccionado ante lo que consideran un claro abuso a estos principios.

Mientras algunos discuten si el uso de este software por parte del FBI debería limitarse a casos especiales, otros están seguros que este tipo de tecnología no va a impedir los actos criminales serios, aunque si va a comprometer la privacidad de usuarios inocentes en todo el mundo.

Back Orifice: El 3 de Agosto de 1998 el grupo de Hackers conocidos como "*The Culto of the Dead Cow"* (el Culto a la Vaca Muerta) sorprendió al mundo con el lanzamiento de su popular y temido *Back Orifice*, uno de los troyanos más importantes de la historia, el cual incluso fue distribuido con su código fuente y plug-ins, además de sus componentes compilados. Unos años más tarde, el mismo grupo liberaba su nueva versión "*Back Orifice 2000"* mejor conocida como "*BO2K"*, la cual contaba con grandes modificaciones, entre ellas la posibilidad de poder ser ejecutado sobre Windows NT/2000. De la misma forma que en su primera versión, "*BO2K"* puede conseguirse junto a su kit de desarrollo, lo cual hace que cualquier programador pueda variar su fisonomía o agregar características que lo hagan más potente y menos detectable. "*BO2k"* posee características que le

permiten conectarse con canales de Chat específicos e informar la dirección IP de la PC en donde se está ejecutando. A su vez, permite ser instalado en modo “Stealth”. Al igual que el resto de los troyanos analizados en esta sección, permite a un usuario remoto, controlar la mayoría de las funciones principales del equipo víctima, incluyendo: Sistema de archivos, Registro, Passwords, Networking y Procesos en ejecución.

Netbus: Netbus fue desarrollado por el programador sueco Carl Frederik Neikter en Marzo de 1998, quien alguna vez dijo: "NetBus fue creado para que la gente tenga algo de diversión con sus amigos. Yo espero que NetBus y programas similares como Back Orifice harán que la gente sea más consciente de los riesgos de seguridad de sus sistemas". Desafortunadamente, ambos programas fueron más allá de ser aparentes simples travesuras. Netbus dispone de una interfaz más práctica y sencilla que Back Orifice. Es muy versátil en su configuración y hay varias versiones circulando por Internet. Por defecto el servidor ejecutable se llama patch.exe (aunque obviamente puede llamarse de cualquier otra forma).

Netbus 2.0 Profesional: Esta versión, posee algunas características que lo alejarían de la categoría de troyano y lo acercarían a su calidad de herramienta de administración remota. La más importante de ellas, es que su activación en la parte servidor, requiere (a diferencia de su antecesor) la interacción con el usuario para ser instalado.

SubSeven: Desarrollado en Alemania por el grupo de Hackers S7G (Sub 7 Germany), este troyano es más fácil de usar y ofrece más funciones que las primeras versiones de Back Orifice y NetBus. Al margen de aquellas que comparte con el resto del grupo, Subseven posee un sin número de utilidades que lograrían irritar al más tranquilo de los usuarios una vez dentro de su sistema. Cambio de los seteos gráficos de Windows, utilización remota de su webcam, efectos del tipo “Flip Screen” y lograr que la PC atacada pronuncie palabras gracias a los plugins de “Text-2-Speech”, son funcionalidades incluidas dentro de esta “suite”.

Optix: Siendo uno de los troyanos más nuevos, Optix desarrollado por el grupo de Hackers alemán “EvilEye”, es sin lugar a dudas uno de los más potentes de su grupo. Desde su liberación el 22 de Abril del 2003, representa uno de los códigos maliciosos más peligrosos. Quizás una de sus características más temidas, es aquella que le permite actuar como “retrovirus” y deshabilitar 75 de los software antivirus más populares (Anti-Trojan, AVG, Cheyenne, eTrust Antivirus, Norton Antivirus, F-Prot, Kaspersky, McAfee, NOD32, Panda, TrendMicro, etc.). Lo mismo sucede con los procesos de 32 de los Firewalls personales frecuentemente utilizados en estaciones de trabajo (Agnitum Outpost, eTrust Firewall, Kaspersky AntiHacker, Kerio, BlackIce, Norton Firewall, Zonealarm, etc) Algunas de las mejoras introducidas en Optix, incluyen nuevos canales de notificación al lograr un ataque exitoso (CGI, MSN y PHP), autodestrucción de su componente de “server” en caso de ser atacado, etc.

9.3.3 Funcionamiento

Al margen de su definición formal, solemos referirnos a los troyanos, básicamente como un programa de administración remota que suele instalarse y actuar en forma oculta para poder funcionar, sin ser percibido por el usuario atacado. Como tal, desde el punto de vista de su funcionamiento requiere al menos de tres componentes fundamentales:

1. Una parte “Servidor”, a ser instalada en forma subrepticia en la máquina del usuario objetivo, de forma tal que pueda ejecutarse en cada reinicio de Windows, abriendo (en la mayoría de los casos) una puerta trasera en el sistema a través de un puerto de comunicación.
2. Una parte “Cliente”, a ser instalada en el equipo del atacante, encargada de comunicarse con

la máquina infectada y llevar a cabo acciones contra ella.

3. Un protocolo de comunicación compartido entre ambos extremos, a fin de asegurar la comunicación. Generalmente TCP/UDP.

Más allá de sus componentes básicos, la mayoría de los troyanos conocidos, suelen incluir una serie de herramientas tendientes a configurar la forma en la que se deberá comportar este código malicioso, de cara a su distribución y funcionamiento en general una vez dentro del sistema objetivo.

Existen al menos tres fases claramente identificadas respecto del funcionamiento de un troyano:

1. Arribo al Sistema Víctima: Aunque existen determinados virus que como parte de su accionar instalan troyanos, a diferencia de éstos, los troyanos no tienen capacidad para reproducirse por su cuenta y la infección ha de pasar generalmente por manos del usuario incauto que, mediante engaños, ejecuta el fichero con el troyano.
2. Consolidación de Posición: En el momento que el troyano es ejecutado intentará modificar el sistema a fin de garantizar su ejecución cada vez que nuestro equipo sea arrancado. A tal efecto deberá modificar los archivos y registros del sistema que crea necesarios para que Windows lo ejecute automáticamente.
3. Comunicación con el atacante: Si su ejecución es exitosa, intentará establecer un vínculo de comunicación con el atacante, a través de alguna de las formas disponibles (MSN, ICQ, CGI, etc.)

Los daños producidos a través de la ejecución de troyanos en nuestro sistema, pueden ser tan importantes como el atacante lo haya planeado. A diferencia de otras amenazas, la posibilidad de tomar control remoto de un equipo, pone al intruso en posición de “decidir” sobre el destino de los datos. Acciones tales como, el registro de pulsaciones de teclado, la obtención de contraseñas del equipo atacado, la utilización del mismo como plataforma de nuevos ataques, la copia o eliminación de archivos privados, la obtención de instantáneas mediante el uso de la webcam de la victima y tantas otras acciones que atentan contra la privacidad e integridad, suelen contarse entre algunas de las posibilidades brindadas por este tipo de amenaza.

9.3.4 Medidas de protección

Uno de los primeros aspectos que debemos conocer de los troyanos, es que probablemente la mejor defensa sea evitar su ingreso al sistema. Una vez en nuestros equipos, probablemente parte de su objetivo haya sido cumplido. De todas formas, existen algunas medidas de protección a adoptar, al momento de minimizar el riesgo de esta amenaza:

- **Implementación de Software antivirus:** Gran parte de los antivirus suelen detectar la actividad de los troyanos más utilizados. Por tanto, la instalación del mismo en las estaciones de trabajo y su permanente actualización, es una primera medida a tomar.
- **Implementación de filtros de contenido (Content Manager):** Los antivirus en general y el software de administración de contenidos en particular, suelen brindarnos la posibilidad de bloquear el ingreso de archivos a la red o a los clientes de correo tradicionales, de acuerdo a sus características (tipo, extensión, tamaño, origen, etc.)
- **Implementación de Firewalls:** Correctas políticas de filtrado configuradas en los “Firewalls” o “Border Router”, pueden prevenir accesos, entrantes a los puertos de escucha por defecto de estos programas, como salientes (¿Debería su servidor de correo permitir una conexión saliente al puerto 23400?). Respecto a lo último, si bien es cierto que un atacante avezado, podría configurar sus servidores para comunicarse a través de los puertos 80 y 25 (generalmente habilitados para el tráfico saliente), de todas formas el filtrado saliente es algo

que debería considerar a la hora de configurar su Firewall.

- **Implementación de IDS:** Algunos de los sistemas IDS o NIDS más conocidos ("Snort" por ejemplo) poseen reglas preconstruidas, tendientes a detectar actividad de troyanos en nuestra red.
- **Implementación de controles de distribución e instalación de software:** Regular y restringir la instalación de software no licenciado en las estaciones de trabajo de su compañía por usuarios no autorizados, constituye otra fuerte medida para impedir la instalación de software "troyanizado". Esto puede ser complementado con el filtrado de sitios web donde se ofrecen cracks o software gratuito.
- **Implementación de Software Anti-Troyanos:** También existen algunas herramientas específicas de detección de troyanos, que nos permiten fortalecer la seguridad de la PC y la red en la que se encuentra.

9.4 COOKIES

Las "*Cookies"*, constituyen un importante método utilizado al momento de mantener el "estado" en la web, interpretando como "estado" a la habilidad que poseen determinadas aplicaciones, de trabajar en forma interactiva con el usuario.

Originalmente, fueron diseñadas para ayudar a que un sitio web, reconociera el navegador de un usuario que repite su visita al mismo, y de esta forma ser capaz de guardar y recordar las preferencias que el usuario hubiera escogido durante su visita anterior.

Con el correr del tiempo, las cookies se fueron transformando, en potentes herramientas de marketing, o visto de otra forma, en un nuevo tipo de "*Código Malicioso"* que atenta contra la privacidad.

En esencia, una cookie no es más que un archivo de texto con el que algunos servidores piden a nuestro navegador que escriba en nuestro disco duro información relacionada con lo que hemos estado haciendo en sus páginas o con algún tipo de codificación que permite identificar en forma inequívoca al equipo/usuario que ha realizado el requerimiento al servidor web.

Las cookies fueron inventadas por Netscape en 1995 e introducidos en el Navegator 2.0 al siguiente año. Hoy en día lo soportan todos los browsers de uso público.

Si bien es cierto que las "*Cookies"* no son consideradas una amenaza a su computador, o a los datos que éste alberga, sí lo es respecto de su privacidad y confidencialidad, puesto que habilitan a un Website a recordar detalles y mantener registros de su visita.

Las cookies suelen introducirse en nuestra computadora cada vez que visitamos un Website programado para hacer uso de éstas. Los diferentes lenguajes de programación utilizados por los desarrolladores web (JavaScript, ASP, PHP, etc), incluyen instrucciones específicas respecto de la manipulación de estas características.

Por ejemplo, algunos de los más importantes sitios de venta en Internet, utilizan el concepto de "Carro Electrónico" para referirse a la selección de productos que va realizando el usuario al recorrer sus páginas en busca de ofertas. En muchas implementaciones de este tipo, suele grabarse la información referente a los productos seleccionados en "Cookies", de forma tal que si usted decide abandonar el sitio y regresar tiempo más tarde, el servidor web pueda detectar no solo que usted ya estuvo allí con anterioridad, sino también los productos que usted había seleccionado previamente

Mucho se ha hablado respecto de las cookies. Si bien es cierto que gran parte de la funcionalidad que disfrutamos hoy día al navegar en la Web, está relacionada con sus buenos usos, lo cierto es que suelen encontrarse con frecuencia, implementaciones para nada aceptables.

Usos tales como la personalización de páginas, la selección de idiomas y los carritos de compras, sin

duda ofrecen ventajas para todos. No obstante, el seguimiento de visitas a una web, carteles publicitarios, marketing personalizado, almacenamiento de contraseñas o números de tarjetas de crédito y otro tipo de información sensible, deberían ser tenidas en cuenta como verdaderas amenazas a la privacidad y confidencialidad.

DoubleClick es una de las más célebres compañías de marketing en Internet que con sus tracking cookies monitorea la navegación de los usuarios en decenas de millones de computadoras en todo el mundo. Dicha información luego es comercializada entre sus clientes para definir tendencias, gustos y hábitos de esos usuarios que puedan definir estrategias de publicidad y marketing.

Las cookies son enviadas desde el servidor al cliente (navegador) y almacenadas en éste, luego el navegador envía estas cookies al servidor permitiendo así la identificación del cliente en el servidor.

Un dato importante, es que en todos los caso, no es el servidor quien escribe en nuestro disco duro, sino nuestro explorador. Esto es, el servidor donde se encuentra alojado el Website, solicita a nuestro explorador de Internet que lea o escriba las “Cookies”, pero en ningún caso tiene acceso a nuestro disco duro a través de ellas.

Desde el punto de vista de la construcción de una “Cookie”, existen básicamente seis parámetros que pueden ser pasados a éstas.

1. Nombre: Nombre de la “Cookie”.
2. Value: Valor de la “Cookie”.
3. Expire: Indica la hora en que se eliminará la cookie
4. Path: Subdirectorio en donde tiene valor la cookie.
5. Dominio: Dominio en donde tiene valor la cookie.
6. Secure: Indica que la cookie sólo se transmitirá a través de una conexión segura HTTPS.

De acuerdo a sus necesidades, los desarrolladores web, suelen hacer uso de estas variables, a fin de obtener la interactividad requerida.

9.4.1 Medidas de protección

En principio, protegerse de las “Cookies” no debería representar un problema en sí mismo. Tanto “Nestcape” como “Microsoft Internet Explorer” y Firefox, permiten ser configurados para rechazar los diferentes tipos de “Cookies”, en relación a las preferencias del usuario. Por otra parte, existen aplicaciones de terceros, muchas veces referidas como “Cookie Monsters” o “Cookie Managers”, aunque su funcionalidad final no deja de ser extensiva a la proporcionada por la configuración de nuestro explorador. Básicamente, los productos anti-cookies trabajan filtrándolas en tiempo real, incluso de sitios determinados y/o limpiándolas en cada oportunidad de los archivos generados en el disco, algunos ejemplos son NSClean32 y Cookie Monster.

Otros mecanismos trabajan filtrando cookies en un intermediario o proxy entre la PC del usuario y el sitio web. En estos casos no hay posibilidad por parte del sitio web de identificar los usuarios, pero en contrapartida se impide cualquier tipo de personalización. Los ejemplos más conocidos son The Anonymizer y el Internet Junkbuster Proxy.

9.5 KEYLOGGERS

Pocas aplicaciones atentan contra la privacidad, como es capaz de hacerlo el uso de un “Keylogger”. Sin embargo, hace ya unos años, se ha instalado en la sociedad, una gran polémica en torno a ellos, debido a que en algunos casos, su utilización podría encontrarse circunscripta a actividades lícitas. En

esta sección definiremos el término “Keylogger”, a la vez que revisaremos su funcionamiento, uso, contramedidas y aspectos legales relacionados.

Un “**Keylogger**” no es ni más ni menos que una aplicación destinada a registrar en forma remota, el comportamiento de un usuario en una PC. Su función principal, es la de grabar todo aquello que sea escrito por intermedio del teclado (aunque la mayoría no sólo se remite a esto) para que luego, esta información sea enviada al atacante, o almacenada en algún sitio del disco rígido del equipo víctima, esperando a ser recuperada. En concordancia con su origen como herramienta espía, una de las características básicas de todo “Keylogger” es la de pasar desapercibido tanto al momento de la instalación como de su uso y reporte, para lo que cuentan con características de las denominadas “Stealth”. Generalmente, su introducción depende del propósito para el cual se haya planeado su utilización. En el caso de los atacantes, probablemente sea a través de la construcción de un troyano que los incluya. Por otro lado, si se tratara de un administrador de sistemas corporativo con instrucciones precisas acerca de vigilar el accionar de los empleados, seguramente utilizará alguna otra técnica de instalación remota.

De todas formas, la introducción de “Keyloggers” a los sistemas informáticos, no siempre se refieren a instalaciones dirigidas. En la actualidad, existen una gran cantidad de “virus, gusanos y troyanos” que los incluyen como parte de su carga maliciosa

Un ejemplo claro de esta metodología, es la utilizada por un gusano de nombre “Bugbear”. Una de sus variantes, introducida en Junio del 2003, no sólo se propagaba rápidamente a través del correo electrónico y recursos compartidos, sino que a su vez incluía una puerta trasera y un “Keylogger” de características un tanto especiales.

“Bugbear” incorporaba en su codificación referencias a un millar de instituciones bancarias, en caso de que el usuario del equipo infectado utilizara el servicio on-line de alguna de las instituciones bancarias incluidas en su lista interna, el “Keylogger” era lanzado, con el propósito de registrar cuentas, usuarios, contraseñas y demás información que enviaba a un conjunto de 10 direcciones de correo propiedad del creador del virus.

Básicamente, el funcionamiento de un “Keylogger” depende específicamente, de la configuración previa que se haya realizado sobre él y de la plataforma para la que haya sido desarrollado (Unix, Windows, etc.). La mayoría de los “Keylogger” más utilizados, suelen permitir embeber el software espía dentro de una aplicación legítima, para así distribuirlo en forma sencilla. Por otra parte, estos programas pueden ser configurados para interceptar todo contenido escrito después de que sean digitadas ciertas frases como “porno”, “sexo”, “fraude” o “¿tu esposa está durmiendo?”, en el equipo auditado.

En líneas generales, la secuencia lógica al momento de trabajar con un “Keylogger”, consta de tres pasos principales:

- **Configuración de los aspectos del “Keylogger”:** Este es probablemente, uno de los pasos más importantes, pues es la instancia en donde se decide cuáles son los eventos que “despertarán” al keylogger (una hora en particular, el tipeo de una palabra especial, etc.), la forma en la que se espera recibir o almacenar la información obtenida y las características del “Log” (sólo texto, snapshot del escritorio, sitios web más visitados, mensajes escritos en MSN o ICQ, etc.). El punto final de este primer paso, consiste en la obtención del ejecutable a ser instalado.
- **Instalación:** Este es el paso en el cual se realiza la distribución del archivo generado en instancias anteriores. Generalmente, se tratará de una instalación silenciosa a efectos de evitar detecciones. La mayoría de los “Keyloggers” brindan su colaboración en esta instancia al dotar a su ejecutable de características tales como las de no mostrar iconos o botones en pantalla, a la vez que resultan invisibles desde el “Task Manager” de Windows.
- **Obtención de la Información Registrada:** Finalmente, y de acuerdo a la configuración realizada en el primer paso, el atacante recibirá la información recolectada a una cuenta de

correo de su propiedad, o en su defecto, en caso de haber instalado una puerta trasera, procederá a su retiro en forma remota.

Tal como mencionáramos en un principio, el uso de “Keyloggers” ha desencadenado una gran polémica en la comunidad en general, de la cual los profesionales en seguridad informática deben tomar nota a la hora de evaluar las circunstancias en las que estas herramientas pueden o deben ser implementadas. Hay quienes alegan que al atentar contra la privacidad y la confidencialidad, el uso de este tipo de aplicaciones, no sólo es ilegal, sino que también inconstitucional. Al mismo tiempo, el mercado parecería demostrar que existe una gran demanda, considerada lícita, respecto de la compra y utilización de este tipo de herramientas.

Entre los usuarios legales de “Keyloggers” se encuentran aquellos padres que quieren vigilar a sus hijos menores de edad, o empresas que quieren saber exactamente que es lo que hacen los empleados cuando se encuentran conectados a Internet. Con respecto a este último caso, vale aclarar que en algunos países se considera “lícito” este accionar, siempre y cuando los empleados hayan sido notificados previamente y subscripto la política interna de la compañía al respecto. Como un dato adicional, un estudio realizado al respecto en EEUU, por la “Society for Human Resource Management (SHRM)” a principios del 2001 y publicado en cnn.com, revelaba entre otros datos, que sobre una encuesta realizada a 722 compañías, el 74% decía monitorear el uso de Internet en el trabajo.

Ahora bien, de la misma forma, existe por supuesto, la posibilidad de utilizar este tipo de herramientas de manera ilegal. Obtención de contraseñas en lugares públicos de acceso a Internet, es tan solo un ejemplo. Administradores maliciosos serían capaces de generar un gran caos al hacer uso fraudulento de este tipo de aplicaciones en su red. Por su parte, intrusos y Hackers suelen hacer uso de herramientas similares incluidas en sus troyanos favoritos, a fin de consolidar su posición una vez dentro del sistema objetivo.

Si bien es cierto que existen en el mercado, aplicaciones específicamente pensadas para hacer frente a esta amenaza (tal es el caso de “Advanced Ant-Keylogger” de “Spydex, Inc.” y “Privacy Keyboard” de “Raytown Corp.”), al día de hoy, ninguna suele ser lo suficientemente efectiva como para ser considerada una solución seria. De todas formas, la combinación de estas últimas con el software antivirus, debería conformar una contramedida aceptable.

Al igual que con los troyanos, la mejor protección contra los “Keyloggers” debería pasar por no permitir su ingreso a la red.

9.6 MALWARE

A medida que Internet se convertía en un medio de comunicación global, millones de programadores veían en ella una gran vidriera a la hora de hacer conocer sus aplicaciones, sea cual fuere el propósito de las mismas. Lo cierto, es que el distribuir sus desarrollos en forma gratuita, en algunos casos, podía dar como resultado una falta de soporte al momento de intentar dotar a estas aplicaciones de mayor funcionalidad o servicios asociados. En parte, como una alternativa de solución ante esta problemática, nace el spyware como soporte financiero de la gran mayoría del software disponible como “freeware” en Internet. Puesto que el accionar del “Spyware” y sus derivados, suele ser considerado en muchos casos como una herramienta de invasión a la privacidad, a lo largo de esta sección intentaremos abordar esta problemática, definiendo algunos términos, revisando los fundamentos de las partes, los aspectos legales de su utilización y las contramedidas asociadas con esta amenaza.

Según la Wikipedia, el **Malware** (Malicious Software – Software malicioso) “*es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario. El*

término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto. El término virus informático es utilizado en muchas ocasiones para referirse a todos los tipos de malware, incluyendo los verdaderos virus."

9.6.1 ¿Qué es un spyware?

En el sentido más amplio de su definición, el término "Spyware" se utiliza para describir toda tecnología que asista a la obtención de información acerca de una persona u organización sin su conocimiento. En la jerga de Internet sin embargo, se conoce como "Spyware" a pequeños programas dedicados a llevar un control del comportamiento de los usuarios, con la intención de vender esta información a terceras partes interesadas, generalmente empresas relacionadas con las áreas de marketing y publicidad.

Desde todo punto de vista, el "Spyware" ostenta claramente un amplio sentido comercial. Muchas empresas se relacionan comercialmente a través de estos programas espías obteniendo algún rédito de su accionar que, de una u otra forma, termina significando un ingreso monetario.

Esta "Cadena Comercial" se encuentra formada principalmente por:

- Programadores independientes que incluyen "Spyware" en sus aplicaciones, a cambio de unos centavos por cada versión que sea descargada de Internet.
- Empresas dedicadas a la implementación de productos de medición de audiencia (tal es el caso de "Red Sheriff") del lado del servidor, que si bien no distribuyen spyware utilizan técnicas similares para obtener información del perfil del consumidor, obtienen dinero a cambio de la implementación de su software.
- Compañías dedicadas al marketing y la publicidad, quienes consumen la información proporcionada por el "Spyware", y brindan servicios a terceros por los que cobran dinero (Estudios de mercado, Penetración de productos, Perfil del consumidor, Información demográfica, etc.).

9.6.2 Tipos de Spyware

Si bien es cierto que el "Spyware" , generalmente, tiene como propósito obtener información del uso de Internet por parte de los usuarios, existen algunas diferencias entre ellos que hacen necesaria su identificación y catalogación. A continuación presentamos una lista conteniendo los tipos más importantes:

Adware: Su nombre proviene de "Advertising Supported Software" y es probablemente el tipo de "Spyware" más conocido, puesto que a su vez es una de sus representaciones más antiguas. Por lo general se trata de aplicaciones que incluyen como parte de su interfaz de usuario, ventanas de publicidad. Generalmente, estas aplicaciones se aprovechan de algún tipo de información básica obtenida de la PC en donde se instala la aplicación anfitrión, tal como el país, el idioma, el sistema operativo utilizado, etc. El "Adware" representa una posibilidad para los desarrolladores de aplicaciones, de distribuir su software sin aparente costo adicional para el usuario final, mientras ellos perciben ingresos tendientes a financiar las mejoras de su producto, gracias al importe que pagan las empresas que colocan el "Advertising" en dicho software, por cada descarga de Internet.

Scumware: En esencia, solemos referirnos a "Scumware" como el tipo de "Spyware" con la habilidad de personalizar la publicidad mostrada en nuestro explorador (generalmente en formato de "PopUp's"), haciendo uso para ello de la información obtenida como parte del accionar de estos programas. Algunos, como "FlashTrack", cuentan incluso con la posibilidad de registrar el tipo de

búsquedas que como usuarios solemos realizar en los motores del tipo de Google o Yahoo y relacionarlo con su base de datos de anunciantes a fin de mostrar publicidades relacionadas con nuestras búsquedas.

Browser Hijackers: Este tipo de "Spyware" es probablemente uno de los más intrusivos, teniendo en cuenta que como parte de su accionar suelen interactuar, generalmente, con el registro de Windows modificándolo con el objeto de alterar algunas características de nuestro Explorador. Cuestiones tales como el re-direccionamiento de la página de inicio o el agregado de nuevos botones a la barra de tareas de nuestro explorador, suelen formar parte de su accionar.

Server Side Spyware: Este tipo de "Spyware", se diferencia del resto debido a que los componentes "espías", se encuentran implementados del "lado del servidor". Al igual que sus colegas que hacen lo propio del "lado del cliente", se encuentran programados para recolectar información de los usuarios, que luego es comercializada.

Por lo general, el "Spyware" suele introducirse en nuestras PC como parte de la instalación de algún tipo de software gratuito (freeware) o con la ejecución de cracks para software licenciado. Frecuentemente sin el consentimiento del usuario. Uno de los ejemplos más significativos, lo constituye sin lugar a dudas, el de las aplicaciones de intercambio de archivo tales como: KaZaa, Bearshare e iMesh, debido a que, producto de su enorme penetración entre los usuarios de todo el mundo, se han transformado en una posibilidad de negocio tanto para sus propios desarrolladores, como para las empresas que utilizan sus aplicaciones como transporte del software espía. El "Spyware" se instala en nuestra PC, de la misma forma que lo hace cualquier aplicación tradicional. Si bien muchas veces se encuentran contenidos en sus propios archivos ejecutables, suele ser muy común, encontrarlos como .DLL's adjuntas al software anfitrión. De la misma manera, el registro de Windows, suele ser utilizado por estas aplicaciones para almacenar información relativa a su configuración inicial.

En líneas generales, la mayoría del software "Spyware", basa su funcionamiento en los siguientes pasos principales:

- **Ingreso al sistema:** Generalmente en forma subrepticia y como parte de alguna de las aplicaciones "Freeware" de mayor distribución.
- **Obtención de información local:** Aprovechando toda la información provista por el propio sistema operativo (Configuración Regional, Tipo del sistema operativo, etc.)
- **Monitoreo del Sistema:** Programas residentes, análisis de los archivos del explorador (historia de los sitios visitados) y detección preactiva de las conexiones a Internet, son acciones llevadas a cabo en este punto.
- **Registro:** Grabación en disco de la información recolectada.
- **Acción:** En este punto, el "Spyware" puede realizar una o varias de las siguientes acciones: envío de la información obtenida al centro de recolección de datos vía Internet; obtención de mensajes personalizados por parte del centro de recolección, tendientes a ser mostrados al usuario; modificación de determinados aspectos de las páginas Web visualizadas mediante el explorador; reemplazo de banners estándares por banners personalizados; etc.

Un aspecto sumamente importante al referirnos a la supuesta legalidad o ilegalidad, en relación al "Spyware", radica en que muchos de los productos que suelen ser cuestionados ética o moralmente por incluir software "Espía" como parte de su instalación, suelen advertir en forma "expresa" a sus usuarios, del accionar de estos como parte de su licencia. Claro está, el hecho de que por lo general, muy pocas personas se detengan a leerlas alguna vez.

Algunos ejemplos de programas espía conocidos son Gator, o Bonzi Buddy.

- **Gator** uno de los spywares más conocidos, hecho por Claria Corporation, se instala en los equipos de los usuarios habitualmente como parte de alguna aplicación que lo incorpora por ejemplo Kazaa o bien como sistema independiente. Sin embargo, su poder va mucho más allá y además de espiar la actividad de estos, modifica las páginas web que se muestran en los ordenadores donde se encuentra instalado, cambiando los banners de publicidad por propios. Gator es detectado por la mayoría de los anti-spyware. Si mientras navega le aparecen ventanas emergentes con publicidad, puede que su equipo forme parte de la red de varios millones de sistemas que se estiman están infectados con el adware de Claria. Además de haberse infiltrado en su equipo de forma oculta al instalar cualquier otra aplicación, y de molestarle continuamente con la aparición de ventanas publicitarias, debe saber que sus hábitos de navegación pueden estar siendo recogidos por Claria en su base de datos de más de 12 Terabytes y expuestos al mejor postor.
- **Bonzi Buddy:** Se trata de un simio de color violeta que aparece en un pop-up (mensaje emergente) y dice en inglés : "Estoy solo. ¿No quieres ser mi amigo?". Al aceptar la instalación se instala un software gratuito en la computadora que hará que el gorila cante, baile, ayude en las descargas y de paso registre el comportamiento en Internet de aquel que instaló BonziBuddy. También cambia la página de inicio del navegador a la de Bonzi. Los niños y personas con poco conocimiento técnico sobre Internet suelen descargar este programa por su interfaz divertida, sin percatarse de su naturaleza publicitaria.

  El programa es en realidad un paquete de aplicaciones que incluye un cliente de correo, un gestor de downloads y un calendario, entre otras cosas. Varios programas instalan enlaces en nuestro Escritorio y en el menú Inicio: entre los más conocidos, están AudioGalaxy y WebAccelerator. En el caso de que los hayan bajado, desinstalar el programa es muy sencillo: sólo basta con seleccionar su entrada en Agregar o quitar programas del Panel de control de Windows, aunque cada aplicación extra que instala requiere ser desinstalada por separado.

Badware Alcalinos: Este es un tipo de Malware mitad spyware, mitad backdoor, suele residir en las ventanas del sistema observando incesantemente hasta que se lanza al acecho de un usuario.

Dialers: son programas que llaman a un número telefónico de larga distancia, o de tarifas especiales, para, a través del módem, entrar de forma automática y oculta para el usuario y sin su consentimiento, principalmente a páginas de juegos, adivinación o pornográficas, que van a redituar en beneficio económico a los creadores del malware, pero que además al usuario le crean la obligación de pagar grandes tarifas por el servicio telefónico. Existen en Internet páginas preparadas para descargar, instalar y ejecutar dialers de conexión y virus informáticos capaces de llevar a cabo todo lo anterior, con la desventaja de su rápida propagación. Actualmente las conexiones por medio de banda ancha, han evitado estos problemas.

Así que, habiendo aclarado un poco las terminologías de Malware y Virus Informático, podemos comenzar a ver con mayor claridad que a pesar de que ambos términos formen parte de un “mismo entorno” tienen algunas diferencias, es como comparar a un mamífero con un elefante, el mamífero es un conjunto pero el elefante es una “entidad” que forma parte del conjunto “mamífero” Las diferencias entre unos y otros existen, al igual que existen diferencias entre los diferentes métodos para prevenir y limpiar un computador infectado, decir que un Antivirus muchas veces no reconoce todos los tipos de malware, y los antimalware o antispyware no tienen la capacidad de reconocer virus y menos eliminarlos.

9.6.3 Principales síntomas de infección

- Cambio de la página de inicio, error en búsqueda del navegador web.

- Aparición de ventanas "pop-ups", incluso sin estar conectados y sin tener el navegador abierto, la mayoría son temas pornográficos y comerciales (por ejemplo, la salida al mercado de un nuevo producto).
- Barras de búsquedas de sitios como la de Alexa, Hotbar, MyWebSearch, FunWeb, etc.. que no se pueden eliminar.
- Creación de carpetas tanto en el directorio raíz, como en "Archivos de programas", "Documents and Settings" y "WINDOWS".
- Modificación de valores de registro.
- La navegación por la red se hace cada día más lenta, y con más problemas.
- Aumento notable en el tiempo que toma el computador en iniciar, debido a la carga requerida por el spyware que se ejecuta en ese momento, alterando el registro con el fin de que el spyware se active a cada inicio.
- Al hacer click en un vínculo el usuario retorna de nuevo a la misma página que el software espía hace aparecer.
- Botones que aparecen en la barra de herramientas del navegador y no se pueden quitar.
- Aparición de un mensaje de infección no propio del sistema, así como un enlace web para descargar un supuesto antispyware.
- Al acceder a determinados sitios sobre el escritorio se oculta o bloquea tanto el panel de control como los iconos de programas.
- Denegación de servicios de correo y mensajería instantánea.

9.6.4 Medidas de protección

En la actualidad, existen varios productos tendientes a lidiar con el “Spyware”. La mayoría, incluyen bases de datos actualizables a través de Internet conteniendo los detalles o “firmas” correspondientes a cada uno de ellos, lo que permite que puedan ser identificados mediante un “escaneo” similar al que suelen realizar los software antivirus, y eliminados en caso de que la concordancia sea positiva. “Spyware Blaster” de “Javacool Software”, “Spyhunter” de “Enigma Software” y “Ad-Ware” de “Lavasoft Sweden”, representan tan solo algunas de las herramientas de este tipo. Al mismo tiempo, suele ser útil como medida de protección el monitoreo frecuente de los aspectos claves de los sistemas o redes que tengamos a nuestro cuidado. Debido al funcionamiento propio de gran parte del “Spyware”, actividad inusual en cuanto a la utilización de memoria o ancho de banda de nuestras conexiones a Internet, podría encontrarse relacionado con la actividad de este tipo de programas espías. Una vez más, la aplicación de una correcta política de filtrado en nuestros “Firewalls” y “Border Router”, especialmente en los filtros de salida, dificultará el accionar por parte de este tipo de software que eventualmente podrían requerir el establecimiento de una conexión no esperada. Por último, entornos corporativos con políticas y procedimientos claros respecto de la instalación de software autorizado, no deberían ver el “Spyware” como una amenaza seria.

9.6.5 Algunos de los más conocidos Anti-Spyware

- **Malwarebytes' Anti-Malware**: Una excelente utilidad gratuita que busca, detecta y elimina todo tipo de Malware, desarrollado por la gente de MalwareBytes (creadores de About:Buster, FileASSASSIN y otros tantos buenos programas).
- **SuperAntiSpyware** analiza tu sistema en busca de cualquier tipo de amenaza que pueda colarse en tu PC.: spyware, troyanos, dialers, rootkits, gusanos, adware, malware y cualquier

otro tipo de elemento de software malintencionado.

- **SpywareBlaster**: Una herramienta fundamental y gratuita para la prevención de ataques de spywares, no los elimina simplemente deshabilita los controles ActiveX de los mas conocidos spywares. bloquea, de la computadora del usuario, la capacidad de instalación y ejecución de la mayoría de spyware, adware, secuestradores de navegadores, dialers y otros programas maliciosos basados en ActiveX. SpywareBlaster trabaja al poner en la "lista negra" (Activando el "Killbit") de los Clsid de los programas malware conocidos, evitando efectivamente que puedan infectar el computador protegido. Este enfoque se diferencia de muchos otros programas anti-spyware, que típicamente ofrecen al usuario una posibilidad para explorar el disco duro y la memoria del computador para eliminar el software indeseado, después de que éste se haya instalado. SpywareBlaster también permite al usuario prevenir riesgos de privacidad como las cookies de seguimiento. Otra característica es la capacidad de restringir las acciones de sitios web conocidos como distribuidores de adware y spyware. Soporta varios navegadores web, incluyendo el Internet Explorer, Netscape, Mozilla y Mozilla Firefox.

9.6.6 Malware en Linux

El sistema operativo GNU/Linux, Unix y otros derivados generalmente son calificados como bien protegidos contra los virus de ordenador. No se conoce la existencia de ninguna amenaza del denominado software malicioso, malware, en Linux que se haya expandido a un nivel siquiera similar a las amenazas existentes en el sistema operativo Microsoft Windows. Esto se atribuye en gran parte a que el malware carece usualmente de permisos para realizar actividades nocivas dentro del sistema y a las rápidas actualizaciones frente a vulnerabilidades que se eliminan a diario en Linux, propias del modelo de software de código abierto. Algunos factores adicionales, para el refuerzo de la seguridad en Linux, son la mayor cultura informática difundida entre los usuarios de sistemas GNU/Linux y la falta de incentivos para un programador a la hora de escribir malware para Linux, debido a su relativamente baja cuota de mercado. Además, un sistema con Linux instalado, por lo general, no se parece a otro: Diferentes versiones de núcleo Linux, diferente software instalado, opciones de configuración y características de seguridad estrictas, etcétera. Lo cual dificulta en gran medida la labor de un atacante. La cantidad de software malicioso disponible en Linux, incluyendo virus, troyanos y otro software escrito específicamente para Linux, se ha incrementado en los últimos años.

Al igual que otros sistemas Unix, Linux implementa un entorno multiusuario donde los usuarios reciben una serie de privilegios o permisos específicos y donde existe un control de acceso dedicado. Para obtener el control de un sistema Linux o provocar alguna consecuencia seria al propio sistema, el malware debería obtener acceso root en dicho sistema. Una de las vulnerabilidades de Linux es que multitud de usuarios piensan que no es vulnerable a los virus. Tom Ferris, un investigador de Security Protocols en Mission Viejo, California, dijo en 2006: "*En la mente de la gente, si no es Windows, es seguro, y ese no es el caso. Piensan que nadie escribe malware para Linux o Mac OS X. Pero eso no es necesariamente cierto...*". Shane Coursen, un consultor técnico senior de Kaspersky Lab señaló que "*el crecimiento del malware en Linux se debe simplemente a su creciente popularidad, particularmente como sistema operativo de escritorio...* La utilización de un sistema operativo es directamente relacionada con el interés de los programadores de malware a la hora de desarrollar software malicioso para ese sistema operativo". Los virus presentan una potencial, aunque mínima, amenaza a los sistemas Linux. Si un binario infectado contiene uno de esos virus al ser ejecutado, el sistema se infectaría. El nivel de infección dependería de los privilegios del usuario que ejecutó el binario. Un binario ejecutado bajo una cuenta de superusuario podría llegar a infectar el sistema entero. Por otro lado, las vulnerabilidades de escalada de privilegios pueden permitir que malware ejecutándose bajo una cuenta de acceso limitado también se propague por todo el sistema. El uso de repositorios oficiales de software reduce las amenazas de instalación de software malicioso, al ser comprobados por los administradores, los cuales intentan asegurar que no se cuele ningún malware en sus repositorios. Por ello, para asegurar la distribución segura de software, están disponibles sistemas como los checksum MD5. El uso adecuado de estas firmas digitales supone una línea

adicional de defensa, que previene la violación de las comunicaciones a través de ataques man-in-the-middle o ataques de redirección como ARP Spoofing o DNS Poisoning. Todo esto limita el alcance de los ataques, reduciendo los potenciales usuarios malignos a los autores originales y a aquellos con acceso administrativo al propio repositorio.

Una nueva área de sospecha descubierta en 2007 es el de los virus multiplataforma, a raíz del incremento de la popularidad de las aplicaciones multiplataforma. Este tema apareció en el frente debido a la distribución de un virus de OpenOffice.org llamado Bad Bunny.

Stuart Smith, de Symantec, escribió lo siguiente: "*Lo que hace a este virus merecedor de mención es que ilustra lo fácil que puede abusarse de las plataformas de scripting, extensiones, plug-ins, ActiveX, etc. [...] La habilidad del malware de sobrevivir en un entorno multiplataforma o multiaplicación tiene especial relevancia según más y más malware se lanza a través de sitios web. Cuánto falta para que alguien use algo como esto para poder infectar a través de JavaScript, sin importar la plataforma del usuario?"*

Scott Granneman, de SecurityFocus, declaró que: "*algunas máquinas Linux definitivamente necesitan software antivirus. Servidores Samba o NFS, por ejemplo, pueden almacenar documentos en formatos vulnerables e indocumentados de Microsoft, como Word o Excel, que contengan y propaguen virus. Los servidores de correo de Linux deberían ejecutar software AV para neutralizar los virus antes de que aparezcan en las bandejas de entrada de usuarios de Outlook o Outlook Express*".

9.7 ANTIVIRUS

Los antivirus nacieron como una herramienta simple cuyo objetivo fuera detectar y eliminar virus informáticos, durante la década de 1980. Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, los antivirus han evolucionado hacia programas más avanzados que no sólo buscan detectar un Virus informáticos, sino bloquearlo para prevenir una infección por los mismos, así como actualmente ya son capaces de reconocer otros tipos de malware, como spyware, rootkits, etc. El funcionamiento de un antivirus varía de uno a otro, aunque su comportamiento normal se basa en contar con una lista de virus conocidos y su formas de reconocerlos (las llamadas firmas o vacunas), y analizar contra esa lista los archivos almacenados o transmitidos desde y hacia un ordenador. Adicionalmente, muchos de los antivirus actuales han incorporado funciones de detección proactiva, que no se basan en una lista de malware conocido, sino que analizan el comportamiento de los archivos o comunicaciones para detectar cuales son potencialmente dañinas para el ordenador, con técnicas como Heurística, HIPS, etc. Usualmente, un antivirus tiene un (o varios) componente residente en memoria que se encarga de analizar y verificar todos los archivos abiertos, creados, modificados, ejecutados y transmitidos en tiempo real, es decir, mientras el ordenador está en uso. Asimismo, cuentan con un componente de análisis bajo demando (los conocidos scanners, exploradores, etc), y módulos de protección de correo electrónico, Internet, etc.

El objetivo primordial de cualquier antivirus actual es detectar la mayor cantidad de amenazas informáticas que puedan afectar un ordenador y bloquearlas antes de que la misma pueda infectar un equipo, o poder eliminarla tras la infección. Dado que una característica de los virus es el consumo de recursos, los virus ocasionan problemas tales como pérdida de productividad, baja en el rendimiento del equipo, cortes en los sistemas de información o daños a nivel de datos. Otra de las características es la posibilidad que tienen de ir replicándose en otras partes del sistema de información. Las redes en la actualidad ayudan a dicha propagación.

Los daños que los virus dan a los sistemas informáticos son:

- Pérdida de información (evaluable y actuable segun el caso)
- Horas de contención (Técnicos de SI, Horas de paradas productivas, perdida productiva, tiempos de contención o reinstalación, cuantificables según el caso+horas de asesoría

externa)

- Pérdida de imagen (Valor no cuantificable)

También es importante tener en cuenta que existen algunos malware que tienen la capacidad de ocultar carpetas. Hay que tener en cuenta que cada virus es una situación nueva, por lo que es difícil cuantificar a priori lo que puede costar una intervención. Tenemos que encontrar métodos de realizar planificación en caso de que se produzcan estas contingencias. Existen dos grandes grupos de contaminaciones, los virus donde el usuario en un momento dado ejecuta o acepta de forma inadvertida la instalación del virus, o los gusanos donde el programa malicioso actúa replicándose a través de las redes. En cualquiera de los dos casos, el sistema operativo infectado comienza a sufrir una serie de comportamientos anómalos o no previstos. Dichos comportamientos son los que nos dan la traza del problema y tienen que permitir la recuperación del mismo.

Dentro de las contaminaciones más frecuentes por interacción del usuario están las siguientes:

- Mensajes que ejecutan automáticamente programas (como el programa de correo que abre directamente un archivo adjunto)
- Ingeniería social, mensajes como ejecute este programa y gane un premio.
- Instalación de software que pueda contener junto con éste uno o varios programas maliciosos.

Existen múltiples medios de intentar combatir el problema. Sin embargo debemos ser realistas. Conforme nuevos programas y sistemas operativos se introduzcan en el mercado más difícil va a ser tener controlados a todos y más sencillo va a ser que a alguien se le ocurran nuevas formas de infectar el sistema. Ante este tipo de problemas están los softwares llamados antivirus. Estos antivirus tratan de descubrir las trazas que ha dejado un software malicioso, para eliminarlo o detectarlo, y en algunos casos contener o parar la contaminación. Los métodos para contener o reducir los riesgos asociados a los virus pueden ser los denominados activos o pasivos.

Antivirus (activo): Estos programas como se ha mencionado tratan de encontrar la traza de los programas maliciosos mientras el sistema este funcionando. Tratan de tener controlado el sistema mientras funciona parando las vías conocidas de infección y notificando al usuario de posibles incidencias de seguridad. Como programa que esté continuamente funcionando, el antivirus tiene un efecto adverso sobre el sistema en funcionamiento. Una parte importante de los recursos se destinan al funcionamiento del mismo. Además dado que están continuamente comprobando la memoria de la maquina, dar más memoria al sistema no mejora las prestaciones del mismo. Otro efecto adverso son los falsos positivos, es decir al notificar al usuario de posibles incidencias en la seguridad, éste que normalmente no es un experto de seguridad se acostumbra a dar al botón de autorizar a todas las acciones que le notifica el sistema. De esta forma el antivirus funcionando da una sensación de falsa seguridad.

Tipos de vacunas:

- CA:Sólo detección: Son vacunas que solo detectan archivos infectados sin embargo no pueden eliminarlos o desinfectarlos.
- CA:Detección y desinfección: son vacunas que detectan archivos infectados y que pueden desinfectarlos.
- CA:Detección y aborto de la acción: son vacunas que detectan archivos infectados y detienen las acciones que causa el virus.

- CA:Detección y eliminación de archivo/objeto: son vacunas que detectan archivos infectados y eliminan el archivo u objeto que tenga infección.
- CB:Comparación directa: son vacunas que comparan directamente los archivos para revisar si alguno esta infectado
- CB:Comparación por firmas: son vacunas que comparan las firmas de archivos sospechosos para saber si están infectados.
- CB:Comparación de signature de archivo: son vacunas que comparan las signaturas de los atributos guardados en tu equipo.
- CB:Por métodos heurísticos: son vacunas que usan métodos heurísticos para comparar archivos.
- CC:Invocado por el usuario: son vacunas que se activan instantáneamente con el usuario.
- CC:Invocado por la actividad del sistema: son vacunas que se activan instantáneamente por la actividad del sistema

Filtros de ficheros (activos): Otra aproximación es la de generar filtros dentro de la red que proporcionen un filtrado más selectivo. Desde el sistema de correos, hasta el empleo de técnicas de firewall, proporcionan un método *activo* y eficaz de eliminar estos contenidos.

En general este sistema proporciona una seguridad donde el usuario no requiere de intervención, puede ser más tajante, y permitir emplear únicamente recursos de forma más selectiva. Cuando el número de puestos a filtrar crece puede ser conveniente.

Copias de seguridad (pasivo): Mantener una política de copias de seguridad garantiza la recuperación de los datos y la respuesta cuando nada de lo anterior ha funcionado.

Asimismo las empresas deberían disponer de un plan y detalle de todo el software instalado para tener un plan de contingencia en caso de problemas.

Consideraciones de software: El software es otro de los elementos clave en la parte de planificación. Se debería tener en cuenta la siguiente lista de comprobaciones:

1. Tener el software imprescindible para el funcionamiento de la actividad, nunca menos pero tampoco más. Tener controlado al personal en cuanto a la instalación de software es una medida que va implícita. Así mismo tener controlado el software asegura la calidad de la procedencia del mismo (no debería permitirse software pirata o sin garantías). En todo caso un inventario de software proporciona un método correcto de asegurar la reinstalación en caso de desastre.
2. Disponer del software de seguridad adecuado. Cada actividad forma de trabajo métodos de conexión a Internet requieren una medida diferente de aproximación al problema. En general, las soluciones domésticas, donde únicamente hay un equipo expuesto, no son las mismas que las soluciones empresariales.
3. Métodos de instalación rápidos. Para permitir la reinstalación rápida en caso de contingencia.
4. Asegurar licencias. Determinados softwares imponen métodos de instalación de una vez, que dificultan la reinstalación rápida de la red. Dichos programas no siempre tienen alternativas pero ha de buscarse con el fabricante métodos rápidos de instalación.
5. Buscar alternativas más seguras. Existe software que es famoso por la cantidad de agujeros de seguridad que introduce. Es imprescindible conocer si se puede encontrar una alternativa que proporcione iguales funcionalidades pero permitiendo una seguridad extra.

Consideraciones de red: Disponer de una visión clara del funcionamiento de la red permite poner

puntos de verificación filtrado y detección ahí donde la incidencia es más claramente identificable. Sin perder de vista otros puntos de acción es conveniente:

1. Mantener al máximo el número de recursos de red en modo de sólo lectura. De esta forma se impide que computadoras infectadas los propaguen.
2. Centralizar los datos. De forma que detectores de virus en modo batch puedan trabajar durante la noche.
3. Realizar filtrados de firewall de red. Eliminar los programas de compartición de datos, como pueden ser los P2P; Mantener esta política de forma rigurosa, y con el consentimiento de la gerencia.
4. Reducir los permisos de los usuarios al mínimo, de modo que sólo permitan el trabajo diario.
5. Controlar y monitorizar el acceso a Internet. Para poder detectar en fases de recuperación cómo se ha introducido el virus, y así determinar los pasos a seguir.

9.7.1 Heurística

En los productos antivirus se conoce como Heurística a las técnicas que emplean para reconocer códigos maliciosos (virus, gusanos, troyanos, etc.) que no se encuentren en su base de datos (ya sea porque son nuevos, o por no ser muy divulgados). El término general implica funcionalidades como detección a través de firmas genéricas, reconocimiento del código compilado, desensamblado, desempaquetamiento, entre otros. Su importancia radica en el hecho de ser la única defensa automática posible frente a la aparición de nuevos códigos maliciosos de los que no se posea firmas:

- **Firmas Genéricas**: Hay muchos códigos maliciosos que son modificados por sus autores para crear nuevas versiones. Usualmente, estas variantes contienen similitudes con los originales, por lo que se catalogan como una familia de virus. Gracias a las similitudes dentro del código del virus, los antivirus pueden llegar a reconocer a todos los miembros de la misma familia a través de una única firma o vacuna genérica. Esto permite que al momento de aparecer una nueva versión de un virus ya conocido, aquellos antivirus que implementan esta técnica puedan detectarlo sin la necesidad de una actualización. sistema para realizar las operaciones necesarias. Las implementaciones de heurística de algunos antivirus utilizan técnicas para reconocer instrucciones comúnmente aplicadas por los códigos maliciosos, y así poder identificar si un archivo ejecutable puede llegar a ser un código malicioso.
- **Desensamblado:** La heurística de algunos antivirus es capaz de analizar el código fuente de los programas sospechosos. De esta forma puede reconocer un posible código malicioso si encuentra técnicas de desarrollo que suelen usarse para programar virus, sin la necesidad de una actualización.
- **Desempaquetamiento:** Los programadores de códigos maliciosos suelen usar empaquetadores de archivos ejecutables como UPX con el fin de modificar la "apariencia" del virus a los ojos del análisis antivirus. Para evitar ser engañados por un código malicioso antiguo y luego reempaquetado, los antivirus incluyen en sus técnicas heurísticas métodos de desempaquetamiento. De esta forma pueden analizar el código real del programa, y no el empaquetado.

¿Qué son las evaluaciones retrospectivas?: Para poder analizar correctamente el funcionamiento de las capacidades heurísticas o *proactivas* de un antivirus, lo que se hace es detener la actualización de firmas del producto durante un período de tiempo **X**. En ese lapso, se acumulan muestras de códigos maliciosos nuevos, para que una vez recolectada una cantidad suficiente, se analice si los antivirus las reconocen o no. Al no haber sido actualizados para detectar esas muestras, el antivirus solo podrá reconocer si están infectadas o no a través de sus capacidades heurísticas.

Gracias a estas evaluaciones se puede conocer en detalle el rendimiento de los productos antivirus frente a virus nuevos o desconocidos.

La prueba **EICAR** consiste en un archivo que sirve para comprobar la eficacia de los programas antivirus. La ventaja que tiene sobre otras comprobaciones es que el equipo queda libre de riesgos. Se trata de un inofensivo archivo de texto. Consiste en copiar la siguiente cadena de caracteres:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

En el bloc de notas, y guardarlo con una extensión .com Un antivirus con protección en tiempo real debería detectarlo inmediatamente. Un escaneo en busca de virus también debería detectarlo. Esta prueba ya no es demasiado eficaz, es antigua y muy conocida por todos los fabricantes de software.

9.8 PREGUNTAS Y TIPS

- **¿Cómo se conoce la técnica para redirigir a los usuarios a sitios Web clandestinos, a través de DNS infectadas o creadas intencionalmente para el fraude?** Pharming
- **¿Cómo se denomina al tipo de spyware que tiene la habilidad de personalizar la publicidad mostrada en nuestro explorador?** Scumware
- **¿Cuáles son componentes fundamentales de los troyanos?** Protocolo de comunicación, Cliente, Servidor
- **¿Cómo se denomina al tipo de virus que tiene la capacidad de mutar alguna de sus formas, haciendo más difícil su detección?** Polimorfo
- **¿Cuál era la única finalidad de los primeros gusanos?** Consumir memoria del sistema atacado hasta desbordar la RAM
- **¿Cómo se denomina el tipo de virus que actúa directamente sobre el software antivirus instalado en un sistema, intentando anular su accionar?** Retrovirus

CAPÍTULO 10

10.1 SEGURIDAD DE LOS DATOS: CRIPTOGRAFÍA

¿Qué es la criptografía? Es la técnica o conjunto de de técnicas empleadas para proteger los datos almacenados o en tránsito de manera que no sean legibles frente a observadores no autorizados. Según el diccionario de la Real Academia, la palabra Criptografía proviene del Griego “Kriptos” que significa oculto, y “Graphein” que significa escritura, y su definición es: *“Arte de escribir con clave secreta o de un modo enigmático”*

¿Qué tipo de claves utilizan los algoritmos simétricos y asimétricos? Un algoritmo simétrico utiliza una única clave o secreto compartido para encriptar y desencriptar, en cambio, un algoritmo asimétrico utiliza una clave pública para encriptar y una clave privada para desencriptar.

¿Cuál es la desventaja de un sistema asimétrico para procesos de encriptación de datos? Los sistemas asimétricos utilizan altos niveles de recursos de procesamiento para la encriptación de grandes bloques de datos, dado que emplean claves de mayor tamaño para ofrecer una seguridad comparable a los sistemas simétricos.

¿Qué es una función de Hash? Es una operación matemática que, aplicada sobre un conjunto de datos de cualquier tamaño otorga como resultado un conjunto de caracteres de tamaño fijo (hash) e independiente del original, con la propiedad de ser inequívocamente asociado a los datos iniciales y prácticamente imposible obtener a partir de dicho resultado o hash, el mensaje o conjunto de datos originales.

Desde tiempos inmemorables, la humanidad ha recurrido a diversas artimañas al momento de ocultar de algún modo, cualquier tipo de elemento que resultara vital para su supervivencia. La información o los datos, transmitidos de hombre a hombre en aquellas primeras comunicaciones gestuales, probablemente hayan incluido algún tipo de método, que permitiera a los involucrados, sentirse seguros respecto de la confidencialidad de sus acciones.

En la actualidad, una sociedad altamente dependiente de la tecnología en general y de la administración de la información por medios electrónicos en particular, requiere de métodos cada vez más sofisticados como prácticos, al momento de asegurar cuestiones tales como: la confidencialidad, integridad , autenticidad y no-repudio de los datos envueltos en un sistema de información. Las siguientes secciones, nos permitirán introducir el término Criptografía, así como los aspectos referentes a su funcionamiento y aplicación.

En su acepción general, suele utilizarse el término Criptografía, para referirse al “Arte de ocultar información”. A pesar de ello, la Criptografía como la conocemos hoy día, ha dejado de ser un arte para convertirse en una técnica o conglomerado de técnicas, tendientes a la protección u ocultación de algún tipo de información frente a observadores no autorizados.

Uno de los aspectos determinantes en el ámbito de la Criptografía, se encuentra dado por los códigos criptográficos que en él se utilizan. Las personas relacionadas con la investigación y el desarrollo de los diferentes códigos criptográficos, suelen ser referidos como Criptógrafos.

Evidentemente, el requerimiento de comunicaciones secretas se encuentra directamente relacionado con la existencia de algún tipo de peligro o desconfianza respecto de que un mensaje transmitido sea interceptado por un potencial atacante.

Es de esperar, que de existir este potencial atacante, utilizará todos los medios a su alcance para

descifrar esos mensajes secretos mediante un conjunto de técnicas y métodos que constituyen una ciencia conocida como criptoanálisis. El grupo de personas capaces de analizar, interpretar y finalmente romper dichos códigos, invalidando su utilización como mecanismo efectivo de protección de datos, se denominan Criptoanalistas. La estrategia que utiliza un Criptoanalista depende de la naturaleza del esquema de cifrado y la información de que éste disponga.

Por lo general, tanto los Criptógrafos como los Criptoanalistas, suelen ser eminentes profesionales, provenientes del ámbito de estudio de las matemáticas y las ciencias de la computación.

10.1.1 Historia

La Criptografía, es un campo casi tan antiguo como la humanidad misma. A lo largo de la historia, los mensajes cifrados han jugado un rol preponderante en el desarrollo de grandes acontecimientos.

Alguno de los primeros registros de esfuerzos criptográficos, datan del año 2000 antes de Cristo. Los antiguos egipcios usaron métodos criptográficos, mientras el pueblo utilizaba la lengua demótica, los sacerdotes usaban la escritura hierática (jeroglífica) incomprensible para el resto.

Esclavos con textos grabados en su cuero cabelludo y alfabetos de extraños símbolos parecen haber estado relacionados de algún modo con los inicios de su aplicación.

Parecería ser que el primer caso claro de uso de métodos criptográficos, tuvo lugar durante la guerra de Atenas y Esparta. En este caso, el cifrado se basaba en la alteración del mensaje original, mediante la inclusión de símbolos innecesarios que desaparecían al enrollar la lista en un rodillo llamado escitala. El mensaje quedaba claro cuando se enrollaba la tira de papel alrededor de éste, el cual estaba diseñado con la longitud y el grosor adecuados.

Pero existe un punto en la historia que suele ser considerado como el primer antecedente claramente documentado de un sistema de cifrado. El mismo, tiene como protagonista a Julio César, quien habría ideado un método consistente en sustituir cada letra de un mensaje, por su tercera siguiente en el alfabeto. La mayoría de las fuentes indican también que, hacia la misma época, existieron muchas otras civilizaciones que utilizaron métodos similares.

Pero el ingenio humano se seguiría aplicando en pro de la confidencialidad. Hacia finales del siglo XVI, el Italiano Girolamo Cardano, utilizó el método de la tarjeta perforada, la cual se debía colocar sobre un texto, para poder leer el mensaje cifrado.

En el siglo XVII Carlos I, hizo uso de los códigos de sustitución silábica, mientras que Napoleón en sus campañas militares y escritos diplomáticos, usó los llamados métodos Richelieu y Rossignol.

El siglo XIX por su parte, dejaría su huella en la historia de la Criptografía. El criptógrafo holandés Auguste Kerckhoffs, escribía un libro fundamental bajo el título “La Criptografía Militar”, en el que se expresaban claramente una serie de reglas, que debían ser cumplidas por un buen sistema criptográfico.

Si bien es cierto que el desarrollo de la Criptografía habría mostrado hasta este momento un crecimiento interesante, el comienzo de la Segunda Guerra Mundial marca sin lugar a dudas el inicio de la Criptografía Moderna, coincidente con el nacimiento de las computadoras. Alemania construía su máquina Enigma, mientras que en un lugar llamado Bletchley Park, un grupo de científicos, entre los que se encontraba Alan Turing, trabajaba en el proyecto ULTRA tratando de descifrar los mensajes enviados por el ejército alemán, con su nueva máquina. Este grupo de científicos diseñó y utilizó el primer computador de la Historia, denominado Colossus, aunque esta información permaneció en secreto hasta mediados de los 70.

10.1.2 Panorama actual

Como hemos podido observar, en sus inicios, la Criptografía ha sido utilizada casi exclusivamente con

fines militares. De hecho, hasta hace algún tiempo, la mayoría de las investigaciones en este aspecto, eran financiadas (y lo siguen siendo) por agencias dependientes de los diferentes gobiernos nacionales, como por ejemplo la NSA (Agencia Nacional de Seguridad de los EE.UU) y guardadas celosamente como secretos militares.

Sin embargo, en los últimos años, investigaciones serias llevadas a cabo en universidades de todo el mundo, han logrado que la Criptografía sea una ciencia al alcance de todos, convirtiéndola de esta forma, en parte fundamental de algunos de los avances tecnológicos más significativos de nuestra época.

Cuestiones tales como el comercio electrónico, la telefonía móvil, o las nuevas plataformas de distribución de contenidos multimedia, se encuentran sin lugar a dudas entre los más beneficiados, al igual que los usuarios comunes, que gracias a las bases teóricas de los algoritmos de clave pública desarrollada por los expertos, contamos con las aplicaciones prácticas necesarias para ejercer nuestro derecho a la privacidad, a la hora de enviar correo electrónico o almacenar información en nuestros equipos de escritorio.

Una premisa fundamental en la criptografía moderna es la suposición de **Kerckhoffs**, que establece que los algoritmos deben ser conocidos públicamente y su seguridad solo depende de la clave. En lugar de intentar ocultar el funcionamiento de los algoritmos, es mucho más seguro y efectivo mantener en secreto solamente las claves.

A lo largo de la historia ha habido casos que han demostrado la peligrosidad de basar la protección en mantener los algoritmos en secreto (lo que se conoce como “seguridad por ocultismo”). Si el algoritmo es conocido por muchos, es más fácil que se detecten debilidades o vulnerabilidades y se puedan corregir rápidamente. Si no, un experto podría deducir el algoritmo por ingeniería inversa, y terminar descubriendo que tiene puntos débiles por donde se puede ataca, como sucedió con el algoritmo A5/1 de la telefonía móvil GSM.

Un algoritmo se considera seguro si a un adversario le es imposible obtener el texto en claro *M* aun conociendo el algoritmo *e* y el texto cifrado *C*. Es decir, es imposible descifrar el mensaje sin saber cuál es la clave de descifrado. La palabra “imposible”, debe tormarse en consideración con distintos matices. Un algoritmo criptográfico es computacionalmente seguro si, aplicando el mejor método conocido, la cantidad de recursos necesarios (tiempo de cálculo, número de procesadores, etc.) para descifrar el mensaje sin conocer la clave es mucho más grande (unos cuantos órdenes de magnitud) de lo que está al alcance de cualquier persona. En el límite, un algoritmo es incondicionalmente seguro si no se puede invertir ni con recursos infinitos. Los algoritmos que se utilizan en la práctica son (o intentan ser) computacionalmente seguros.

La acción de intentar descifrar mensajes sin conocer la clave de descifrado se conoce como “ataque”. Si el ataque tiene éxito, se suele decir coloquialmente que se ha conseguido “romper” el algoritmo.

Existen dos formas de llevar a cabo un ataque:

- Mediante el **criptoanálisis**, es decir, estudiando matemáticamente la forma de deducir el texto en claro a partir del texto cifrado.
- Aplicando la **fuerza bruta**, es decir, probando uno a uno todos los valores posibles de la clave de descifrado *x* hasta encontrar uno que produzca un texto en claro con sentido.

10.1.3 Criptología

La criptología es el estudio de los criptosistemas, sistemas que ofrecen medios seguros de comunicación en los que un emisor oculta o cifra un mensaje antes de transmitirlo para que sólo un receptor autorizado pueda descifrarlo. Sus áreas principales de estudio son la criptografía y el *criptoanálisis*, pero también se incluye la *esteganografía* como parte de esta ciencia aplicada. En tiempos recientes, el interés por la criptología se ha extendido asimismo a otras aplicaciones aparte

de la comunicación segura de información y, actualmente, una de los más extendidos usos de las técnicas y métodos estudiados por la criptología es la autentificación de información digital (también llamada firma digital).

En ocasiones se emplean los verbos encriptar y cifrar como sinónimos, al igual que sus respectivas contrapartes, desencriptar y descifrar. No obstante, lo correcto es utilizar el término cifrar en lugar de encriptar, ya que se trata de un anglicismo sin reconocimiento académico, proveniente del término encrypt. Por otra parte, tampoco debe emplearse codificar en lugar de cifrar, puesto que el primero designa la emisión de un mensaje mediante algún código, mas no necesariamente oculto, secreto o ininteligible. Escribir en cualquier idioma, por ejemplo, implica el uso de un código, que será comprensible para los receptores que conozcan dicho código, pero no para otros individuos.

10.1.4 Criptoanálisis

Criptoanálisis (del griego *kryptós*, "escondido" y *analýein*, "desatar") es el estudio de los métodos para obtener el sentido de una información cifrada, sin acceso a la información secreta requerida para obtener este sentido normalmente. Típicamente, esto se traduce en conseguir la clave secreta. En el lenguaje no técnico, se conoce esta práctica como romper o forzar el código, aunque esta expresión tiene un significado específico dentro del argot técnico.

"Criptoanálisis" también se utiliza para referirse a cualquier intento de sortear la seguridad de otros tipos de algoritmos y protocolos criptográficos en general, y no solamente el cifrado. Sin embargo, el criptoanálisis suele excluir ataques que no tengan como objetivo primario los puntos débiles de la criptografía utilizada; por ejemplo, ataques a la seguridad que se basen en el soborno, la coerción física, el robo, el keylogging y demás, aunque estos tipos de ataques son un riesgo creciente para la seguridad informática, y se están haciendo gradualmente más efectivos que el criptoanálisis tradicional.

Aunque el objetivo ha sido siempre el mismo, los métodos y técnicas del criptoanálisis han cambiado drásticamente a través de la historia de la criptografía, adaptándose a una creciente complejidad criptográfica, que abarca desde los métodos de lápiz y papel del pasado, pasando por máquinas como Enigma -utilizada por los nazis durante la Segunda Guerra Mundial-, hasta llegar a los sistemas basados en computadoras del presente.

Los resultados del criptoanálisis han cambiado también: ya no es posible tener un éxito ilimitado al romper un código, y existe una clasificación jerárquica de lo que constituye un ataque en la práctica. A mediados de los años 70 se inventó una nueva clase de criptografía: la criptografía asimétrica. Los métodos utilizados para romper estos sistemas son por lo general radicalmente diferentes de los anteriores, y usualmente implican resolver un problema cuidadosamente construido en el dominio de la matemática pura. El ejemplo más conocido es la factorización de enteros.

El criptoanálisis ha evolucionado conjuntamente con la criptografía, y la competición entre ambos puede ser rastreada a lo largo de toda la historia de la criptografía. Las claves nuevas se diseñaban para reemplazar los esquemas ya rotos, y nuevas técnicas de criptoanálisis se desarrollaban para abrir las claves mejoradas. En la práctica, se considera a ambas como las dos caras de la misma moneda: para crear un sistema criptográfico seguro, es necesario tener en cuenta los descubrimientos del criptoanálisis. De hecho, hoy en día se suele invitar a la comunidad científica a que trate de romper las nuevas claves criptográficas, antes de considerar que un sistema es lo suficientemente seguro para su uso.

Aunque la expresión criptoanálisis es relativamente reciente (fue acuñada por William F. Friedman en 1920), los métodos para romper códigos y cifrados son mucho más antiguos. La primera explicación conocida del criptoanálisis se debe al sabio árabe del siglo IX, Yusuf Yaqub ibn Ishaq al-Sabbah Al-Kindi, en su Manuscrito para Descifrar Mensajes Criptográficos. Este tratado incluye una descripción del método de análisis de frecuencias (Ibraham, 1992).

El análisis de frecuencias es la herramienta básica para romper los cifrados clásicos. En todas las lenguas conocidas, ciertas letras del alfabeto aparecen más frecuentemente que otras; por ejemplo, en español, las vocales son muy frecuentes, ocupando alrededor del 45% del texto, siendo la E y la A las que aparecen en más ocasiones, mientras que la frecuencia sumada de F, Z, J, X, W y K no alcanza el 2%. Igualmente, se pueden reunir estadísticas de aparición de pares o tríos de letras. El análisis de frecuencias revelará el contenido original si el cifrado utilizado no es capaz de ocultar estas estadísticas. Por ejemplo, en un cifrado de substitución simple (en el que cada letra es simplemente substituida por otra), la letra más frecuente en el texto cifrado sería un candidato probable para representar la letra "E".

El análisis de frecuencias se basa tanto en el conocimiento lingüístico como en las estadísticas, pero al volverse cada vez más complicados los cifrados, las matemáticas se convirtieron gradualmente en el enfoque predominante en el criptoanálisis. Este cambio fue particularmente evidente durante la Segunda Guerra Mundial, cuando los esfuerzos para romper los códigos del Eje requirieron nuevos niveles de sofisticación matemática. Más aún, la automatización fue aplicada por primera vez en la Historia al criptoanálisis, bajo la forma de los dispositivos Bomba y Colossus, una de las primeras computadoras.

Aunque la computación fue utilizada con gran éxito durante la Segunda Guerra Mundial, también hizo posible nuevos métodos criptográficos que eran órdenes de magnitud más complejos que los empleados hasta la fecha. Tomada como un todo, la criptografía moderna se ha vuelto mucho más impenetrable al criptoanalista que los métodos de pluma y papel del pasado, y parece que en la actualidad llevan ventaja sobre los métodos del puro criptoanálisis. El historiador David Kahn escribió: "*Son muchos los criptosistemas en venta hoy por parte de cientos de compañías comerciales que no pueden ser rotos por ningún método conocido de criptoanálisis. De hecho, en ciertos sistemas incluso un ataque de texto plano escogido, en el que un fragmento de texto plano seleccionado es comparado con su versión cifrada, no permite conocer el código para romper otros mensajes. En cierto sentido, entonces, el criptoanálisis está muerto. Pero éste no es el final de la historia. El criptoanálisis puede estar muerto, pero, mezclando mis metáforas, hay más de un modo de desollar un gato.*"

10.1.5 Esteganografía

Del griego *steganos* (oculto) y *graphos* (escritura), la esteganografía se puede definir como la ocultación de información en un canal encubierto con el propósito de prevenir la detección de un mensaje oculto.

La esteganografía estudia el conjunto de técnicas cuyo fin es insertar información sensible dentro de otro fichero. A este fichero se le denomina fichero contenedor (gráficos, documentos, programas ejecutables, etc.). De esta forma, se consigue que la información pase inadvertida a terceros, de tal forma que sólo sea recuperada por un usuario legítimo que conozca un determinado algoritmo de extracción de la misma.

Esta ciencia ha suscitado mucho interés en los últimos años debido a que ha sido utilizada por organizaciones criminales y terroristas. No obstante, no se trata de ningún nuevo ingenio, se lleva empleando desde la más remota antigüedad. Este artículo pretende introducir al lector en el campo de la esteganografía, clarificando sus diferencias con la criptografía y mostrando ejemplos de software para hacer uso de esta técnica.

Más de 400 años antes de Cristo, Herodoto ya reflejó en su libro Las Historias el uso de la esteganografía en la antigua Grecia. En dicho libro describe como un personaje toma un cuadernillo de dos hojas o tablillas; raya bien la cera que las cubre y en la madera misma graba un mensaje y lo vuelve a cubrir con cera.

De manera similar, durante la Segunda Guerra Mundial se hacen pequeñas perforaciones sobre las letras de interés de un periódico de tal forma que al sostenerlo a la luz se pueden observar todas aquellas letras seleccionadas e interpretarlas en forma de mensaje.

Bastante más familiar para el lector resulta el ejemplo de la tinta invisible. Son muchos los niños que juegan a enviarse mensajes escritos con zumo de limón o substancias similares (con alto contenido en carbono), de tal forma que al calentar la superficie sobre la que se escribe el mensaje, éste aparece en un tono color café. Esta técnica se puede hacer más compleja si se involucran reacciones químicas.

Queda patente que la esteganografía ha estado presente en nuestra civilización desde tiempos inmemoriales y ha sido tradicionalmente empleada por las agencias militares y de inteligencia, los criminales y la policía, así como por civiles que desean saltarse restricciones gubernamentales. Ahora bien, mientras la esteganografía clásica se basaba únicamente en el desconocimiento del canal encubierto bajo uso, en la era moderna se emplean canales digitales (imagen, video, audio, protocolos de comunicaciones, etc.) para alcanzar el objetivo. En muchos casos el objeto contenedor es conocido, lo que se ignora es el algoritmo de inserción de la información en dicho objeto.

Se pueden observar distintos actores implicados en el campo de la esteganografía:

- **Objeto contenedor:** se trata de la entidad que se emplea para portar el mensaje oculto.
- **Estego-objeto:** se trata del objeto contenedor más el mensaje encubierto.
- **Adversario:** son todos aquellos entes a los que se trata de ocultar la información encubierta.
- **Estegoanálisis:** ciencia que estudia la detección (ataques pasivos) y/o anulación (ataques activos) de información oculta en distintas tapaderas, así como la posibilidad de localizar la información útil dentro de la misma (existencia y tamaño).

Teniendo en cuenta que pueden existir adversarios activos, una buena técnica esteganográfica debe ser robusta ante distorsiones, ya sean accidentales o fruto de la interacción de un adversario activo.

La robustez ante distorsiones también suele ser un objetivo de la criptografía, ahora bien, la esteganografía y la criptografía son campos distintos. En la criptografía, el objetivo es asegurar la confidencialidad de la información ante los ojos de un interceptor que es capaz de ver el criptograma, aun cuando éste conoce el algoritmo que lo genera. En cambio, la esteganografía busca ocultar la presencia del mensaje en sí; ya que si se llega a identificar la posición del mensaje se conoce directamente la comunicación (conocido el algoritmo de ocultación), lo que no ocurre en el caso del criptograma.

Por tanto, la esteganografía en solitario entra en profunda contradicción con uno de los principios básicos de la seguridad: la seguridad por oscuridad (desconocimiento) no funciona.

Para que la esteganografía sea de más utilidad se debe combinar con la criptografía. El mensaje a intercambiar se ha de cifrar (de forma robusta) y luego introducir en el objeto contenedor. De esta forma, aunque un interceptor descubra el patrón esteganográfico, jamás puede llegar a conocer el mensaje intercambiado.

La combinación de estas dos técnicas tiene otra ventaja adicional, cuando se emplea la criptografía en solitario se conoce que se están intercambiando mensajes, lo cual puede servir como punto de partida para un ataque con el fin de descubrir dicho mensaje. Al introducir la esteganografía, en una gran mayoría de casos ni siquiera se conoce que existe una comunicación cifrada.

Sustitución de bits del objeto contenedor

Esta técnica consiste en sustituir ciertos bits del fichero contenedor por los de la información a ocultar. La ventaja de este enfoque es que el tamaño del fichero contenedor no se ve alterado y, gracias a la redundancia y/o exceso de detalle en dichos ficheros, en muchas ocasiones tampoco su calidad.

Por ejemplo, en un fichero de sonido se pueden emplear los bits que no son audibles por el oído humano para ser reemplazados por los bits del mensaje.

Si se trabaja con imágenes, el método tradicional consiste en sustituir los bits menos significativos (LSB), en una escala de color de 24 bits (mas de 16 millones de colores). Esto se traduce tan sólo en que un píxel con un tono rojo se ve un 1% más oscuro. En muchos casos son cambios inapreciables a los sentidos humanos que tan sólo pueden ser detectados mediante análisis computacional de la estructura de los ficheros.

Los archivos BMP son un formato estándar de imagen de mapa de bits en sistemas operativos DOS, Windows y válido para MAC y PC. Soporta imágenes de 24 bits (millones de colores) y 8 bits (256 colores), y puede trabajar en escala de grises, RGB y CMYK.

Cada píxel de un archivo BMP de 24 bits está representado por tres bytes. Cada uno de estos bytes contiene la intensidad de color rojo, verde y azul (RGB: red, green, blue). Combinando los valores en esas posiciones podemos obtener los 2^{24}, más de 16 millones, de colores que puede mostrar un píxel. A su vez, cada byte contiene un valor entre 0 y 255, o lo que es lo mismo, entre 00000000 y 11111111 en binario, siendo el dígito de la izquierda el de mayor peso. Lo que demuestra que se pueden modificar los bits menos significativos de un píxel sin producir mayor alteración.

La implicación es que, utilizando cambios de un bit en cada componente de un píxel, se puede encajar tres bits de información oculta por píxel sin producir cambios notables en la imagen. Esto se puede hacer para cada píxel de una imagen. Se necesitan ocho píxeles para ocultar tres bytes de información, en codificación ASCII esto son 3 letras de información oculta. Así, en una imagen BMP de 502x126 píxeles se puede ocultar un mensaje de 23.719 caracteres ASCII.

Inserción de bits en el objeto contenedor

En este caso se añaden los bits de información a partir de una determinada marca estructural del fichero (fin de fichero o EOF, espacios de padding o alineamiento, etc.). Esta opción presenta el inconveniente de que sí se modifica el tamaño del objeto contenedor, con lo cual puede levantar sospechas.

Para extrapolar esta idea al ejemplo de las imágenes BMP hay que comprender primero como se estructura dicho formato. Los primeros 54 bytes contienen los metadatos de la imagen, que se dividen de la siguiente manera:

• 2 bytes - contienen siempre la cadena ‘BM’, que revela que se trata de un BMP.

• 4 bytes - tamaño del archivo en bytes.

• 4 bytes - reservados (para usos futuros), contienen ceros.

• 4 bytes - offset, distancia entre cabecera y primer píxel de la imagen.

• 4 bytes - tamaño de los metadatos (esta estructura en sí).

• 4 bytes - ancho (número de píxeles horizontales).

• 4 bytes - alto (número de píxeles verticales).

• 2 bytes - número de planos de color.

• 2 bytes - profundidad de color.

• 4 bytes - tipo de compresión (vale cero, ya que BMP es un formato no comprimido).

• 4 bytes - tamaño de la estructura imagen.

• 4 bytes - píxeles por metro horizontal.

• 4 bytes - píxeles por metro vertical.

• 4 bytes - cantidad de colores usados.

• 4 bytes - cantidad de colores importantes.

Dada esta estructura, la forma trivial de ocultar datos consiste en ocultarlos justo después de los metadatos (entre los metadatos y los datos de la imagen en sí) y modificar el campo offset (distancia entre los metadatos y los píxeles de la imagen). De esta forma se puede dejar espacio para todo el contenido adicional que se desee albergar.

Creación de un objeto contenedor ad-hoc partiendo de la información a ocultar

Esta alternativa consiste simplemente en generar un fichero contenedor con la propia información a ocultar, en lugar de obtener el fichero contenedor por separado y manipularlo para incluir dicha información.

Por ejemplo, dado un algoritmo específico de reordenamiento de los bytes de los datos a ocultar se puede generar una secuencia de píxeles de un archivo BMP que tengan cierto significado visual. Si el receptor conoce el algoritmo de reordenamiento, la transmisión de información es posible.

Estegoanálisis

Como ya se ha mencionado, el estegoanálisis es la técnica que se usa para recuperar mensajes ocultos o para impedir la comunicación por esteganografía. Existen dos tipos principales de estegoanálisis pasivo, que se explican brevemente a continuación.

- **Estegoanálisis manual:** Consiste en buscar de forma manual diferencias entre el objeto contenedor y el estego-objeto buscando cambios en la estructura para localizar datos ocultos. Los principales inconvenientes de esta técnica son que es necesario tener el objeto contenedor y que en muchas ocasiones se detecta que un objeto contiene información oculta pero es imposible recuperarla.

  No obstante, cuando no se dispone del fichero contenedor, se pueden buscar irregularidades en el fichero esteganografiado para tratar de encontrar signos de la existencia de datos ocultos.

  Los ataques visuales alertan al ojo humano de la presencia de información oculta gracias a la aplicación de filtros. Considérese el caso del BMP donde el bit menos significativo de las componentes de algunos de sus píxeles ha sido sustituido por información oculta. En tal escenario el estegoanálisis manual consiste en aplicar un filtro tal que sólo se considere el bit menos significativo de cada componente RGB de cada píxel.

- **Estegoanálisis estadístico:** Consiste en el cotejo de la frecuencia de distribución de colores del estego-objeto. Es una técnica lenta para la que se debe emplear software especializado. Estos programas suelen buscar pautas para ocultar los mensajes que utilizan los programas más habituales de esteganografía, este enfoque los hace muy eficaces cuando se trata de mensajes ocultos con estos programas típicos. Ahora bien, los mensajes ocultados manualmente son casi imposibles de encontrar para estos programas.

Esteganografía empleando el protocolo TCP/IP

El protocolo TCP/IP es apropiado para crear canales encubiertos de comunicación ya que a través de las cabeceras se pueden enviar datos relevantes para dos entes que acuerdan un protocolo encubierto. Usando este enfoque es posible empotrar datos en peticiones de conexión iniciales, conexiones establecidas u otros pasos intermedios.

Por ejemplo, considerando únicamente la cabecera TCP, se pueden ocultar datos en el número de secuencia inicial de una conexión. Esto ofrece 32 bits de datos ocultos por paquete de conexión inicial (SYN), es decir, 4 caracteres ASCII. Siguiendo esta filosofía se puede ocultar información en otros campos de las cabeceras de los distintos protocolos que componen TCP/IP, siempre y cuando los cambios no impliquen el rechazo de los paquetes intercambiados.

Control de malware

El malware de hoy día normalmente se comunica con un punto de control en posesión del atacante para recibir órdenes de descarga de módulos adicionales, para enviar datos robados, para indicar que una nueva víctima ha sido infectada, etc.

El protocolo más utilizado para este tipo de comunicación es HTTP ya que normalmente tiene lugar sobre un puerto que no está filtrado por los cortafuegos y porque puede pasar desapercibido en el resto de tráfico de red generado por la navegación legítima.

La facilidad de establecer un canal de control con peticiones HTTP GET/POST tradicionales también implica que la comunicación es fácilmente detectable (si no se emplean técnicas de cifrado) por las empresas que gestionan los servidores web/servidores de DNS asociados al enlace de control. Aun más fácil es la identificación e interpretación de dicha comunicación para un analista de malware. Esto significa que ante denuncia de actividad ilegal asociada a un determinado punto de control, las infraestructuras son cerradas más rápidamente por las empresas que las gestionan.

La consecuencia para el atacante es un tiempo de vida medio de su canal de control inferior, y por tanto un menor retorno de inversión. Para que la identificación y el cierre de las infraestructuras asociadas a un troyano no sea tan trivial, los atacantes han ideado diversas técnicas: desde el simple codificado de las instrucciones para generar cadenas sin significado aparente hasta el uso de P2P.

En este afán por encubrir y fortalecer los canales de comunicación maliciosa, la esteganografía se erige como una baza muy interesante. De hecho, los creadores del gusano Waledac ya han empleado esteganografía por inserción en la descarga e instalación de módulos adicionales que emplea el ejemplar malicioso.

Una de las funcionalidades de *Waledac* es la capacidad de descargar e interpretar un archivo de imagen JPEG especialmente manipulado. Dicho archivo es una imagen JPEG normal a la que se le ha añadido un ejecutable tras la imagen en sí, después de un determinado marcador JPEG para ser coherente con el estándar. El ejecutable se cifra con una operación XOR simple de un byte. El resultado es una imagen que se puede visualizar en la mayoría de navegadores y visores pero que transporta código malicioso adicional para ser instalado por un equipo ya infectado por Waledac.

Marcas de agua digitales

Una marca de agua digital es un código de identificación que se introduce directamente en el contenido de un archivo multimedia, normalmente para incluir información relativa a los derechos de autor o de propiedad del contenido digital en cuestión. La presencia de esta marca de agua debe ser inapreciable para el sistema de percepción humano a la vez que fácilmente extraíble por una aplicación telemática que conozca el algoritmo para recuperarla. Como consecuencia, en la actualidad se están empleando técnicas que en algunos casos pueden ser consideradas esteganografía para conseguir dicho propósito.

La **esteganografía** es una técnica en constante evolución, con una larga historia y con capacidad para adaptarse a nuevas tecnologías. A medida que las herramientas de esteganografía se hacen más avanzadas, las técnicas y las herramientas empleadas en el estegoanálisis también se hacen más complejas.

Los ficheros contenedores no tienen que ser forzosamente imágenes, cualquier medio es válido (audio, video, ejecutables, etc.). Lejos de ser un ingenio exclusivamente teórico, el malware ha demostrado hacer un uso activo de la esteganografía, y se espera que surjan nuevos enfoques de uso para dificultar la labor de los analistas.

Pero las aplicaciones de esta ciencia no sólo se restringen al ámbito de lo poco ético, pudiendo ayudar en campos como la medicina, protección de menores, etc.

En cualquier caso, la eficiencia de las nuevas técnicas de estegoanálisis hace necesario el uso de la esteganografía combinada con criptografía con el fin de alcanzar un nivel de seguridad razonable. La criptografía garantiza la confidencialidad de una conversación pero no esconde el hecho de que dicha conversación se está manteniendo. Por otra parte, la esteganografía en solitario puede ocultar el hecho de que una conversación se mantiene, pero una vez descubierta la interacción, es posible que un atacante conozca el contenido intercambiado. Aun cuando descubrir el contenido original fuera difícil, un atacante puede modificar el estego-objeto para impedir la comunicación (ataque activo). Conjugando ambas técnicas se alcanza una complementariedad que multiplica la seguridad de un intercambio de mensajes.

10.1.6 Seguridad por Oscuridad

La seguridad por oscuridad o por ocultación es un controvertido principio de ingeniería de la seguridad, que intenta utilizar el secreto (de diseño, de implementación, etc.) para garantizar la seguridad. Un sistema que se apoya en la seguridad por ocultación puede tener vulnerabilidades teóricas o prácticas, pero sus propietarios o diseñadores creen que esos puntos débiles no se conocen, y que es probable que los atacantes no los descubran.

Por ejemplo, podría pensarse que esconder una copia de la llave de la casa bajo el felpudo de la entrada sería una buena medida contra la posibilidad de quedar uno atrapado fuera de la casa, por culpa de un olvido o pérdida de la llave de uso habitual. Entonces estaríamos fiándonos de la seguridad por ocultación. La vulnerabilidad de seguridad teórica sería que alguien pudiera entrar en la casa abriendo la puerta con la copia de la llave. Sin embargo, los dueños de la casa creen que la localización de la llave no es conocida públicamente, y que es improbable que un ladrón la encontrara. En este ejemplo, dado que los ladrones suelen conocer los escondites frecuentes, habría que advertir al dueño de la casa contra esta medida.

En criptografía, lo contrario a la seguridad por ocultación es el principio de Kerckhoff de finales de 1880, que indica que los diseñadores del sistema deberían asumir que el diseño completo de un sistema de seguridad es conocido por todos los atacantes, con la excepción de la clave criptográfica: "la seguridad de un cifrado reside enteramente en la clave". Claude Shannon lo reformuló como "el enemigo conoce el sistema". Históricamente, la seguridad por ocultación ha sido un apoyo débil sobre

el que descansar en materia de criptografía. Código oscuro, cifrados y sistemas criptográficos han cedido repetidamente bajo los ataques sin importar el grado de ocultación de sus vulnerabilidades.

El movimiento de la divulgación total va más lejos, sugiriendo que los defectos de seguridad deberían ser divulgados lo antes posible, retrasando la información no más de lo necesario para lanzar una corrección o rodeo (workaround) de la amenaza inmediata.

Los operadores, desarrolladores y vendedores de sistemas que confían en la seguridad por oscuridad a menudo mantienen en secreto que sus sistemas tienen fallos, para evitar crear desconfianza en sus servicios o productos y por tanto, en su imagen de mercado. Es posible que esto pudiera conducir en algunos casos a una representación fraudulenta de la seguridad de sus productos, aunque la aplicación de la ley a este respecto ha sido poco contundente, en parte porque las condiciones de uso impuestas por los vendedores como parte del contrato de licencia redimen (con más o menos éxito) sus aparentes obligaciones bajo el estatuto legal de muchas jurisdicciones que requieren una adecuación para el uso o estándares de calidad similares.

A menudo esos diseñadores o vendedores, o incluso ejecutivos, realmente creen que han garantizado la seguridad al mantener el diseño del sistema en secreto. Para quienes abordan la seguridad de esta manera les resulta difícil tener la suficiente perspectiva para darse cuenta de que están dirigiéndose a un problema, y a veces un gran problema. El autoengaño o la ignorancia son generalmente problemas muy difíciles que tienen consecuencias (casi universalmente) desafortunadas.

10.1.7 Seguridad incondicional versus seguridad computacional

A los efectos de medir de algún modo, la efectividad de los diferentes tipos de criptosistemas existentes, se suele identificar teóricamente el grado de seguridad que estos proveen, haciendo uso de los términos “Seguridad Incondicional” y “Seguridad Computacional”.

Kerckhoffs, en su libro “La Criptografía Militar”, mencionaba en su regla número uno, que “No debe existir ninguna forma de recuperar mediante el criptograma, el texto inicial o la clave”. Este principio, se encuentra relacionado con el concepto teórico de Seguridad Incondicional y Seguridad Computacional, a los que a veces suele referirse como “Secreto Teórico o Incondicional” y “Secreto Práctico o Computacional” respectivamente

La Seguridad Incondicional se produce cuando se conoce un mensaje cifrado y no es posible por ningún medio conocer el mensaje original a partir de éste. Dicho de otra forma, la información disponible para el “enemigo” no es suficiente para quebrar el sistema.

Por su parte la Seguridad Computacional significa que, si bien es teóricamente posible deducir el mensaje a partir del código, la capacidad en tiempo, proceso y recursos económicos para obtener este resultado es, en la práctica, inalcanzable.

La seguridad incondicional es un concepto matemático y por lo tanto absoluto, la seguridad computacional es muy relativa ya que depende de la tecnología del momento, de los avances del criptoanálisis, etc. Un concepto importante en relación a esta última, radica en el sentido de oportunidad, esto es: Si bien es probable que un criptosistema sea quebrado en algún momento, si la ventana de tiempo necesaria para que esto suceda, es superior al tiempo por el cual esperamos que nuestros datos se encuentren a salvo, nos encontraremos, a los efectos prácticos, frente a un criptosistema efectivo.

En el sentido práctico, la **Criptografía** se manifiesta como nuestra principal herramienta, a la hora de asegurar datos, ya sea que éstos se encuentren en tránsito o almacenados de algún modo. La premisa básica detrás de esta utilidad, es la modificación de los datos a proteger, de tal manera que solamente las personas que tengan la llave adecuada puedan tener acceso a la versión original de los mismos.

La criptografía, tal como la conocemos hoy día, involucra varias formas de encriptación/

desencriptación, así como diferentes métodos de autenticación. Aunque sus métodos y aplicaciones siguen siendo cada vez más complejos, la criptografía como tal sigue girando fundamentalmente alrededor de problemas matemáticos difíciles de solucionar. Un problema puede ser difícil de resolver porque su solución requiere de cierto conocimiento secreto, como la llave para desencriptar un mensaje cifrado o para firmar un documento digital. También puede ser que sea intrínsecamente difícil de solucionar, en términos de los requerimientos matemáticos o de cómputo necesarios para solucionar o decodificar el mensaje encriptado.

10.1.8 Características

Como hemos mencionado en párrafos anteriores, en el caso de la criptografía, la protección de la información se basa principalmente en la transformación del texto original, también denominado Texto en Claro, en Texto Cifrado o Criptograma. Dicha transformación o Cifrado, se logra mediante la aplicación de distintos tipos de algoritmos, en combinación con un parámetro al que se denomina Clave. El conjunto de Algoritmos, Texto en Claro, Texto Cifrado y Clave, suele conocerse con el nombre de Criptosistema. Al respecto, resulta importante mencionar, que la fortaleza de un Criptosistema, suele estar dado por la fortaleza de su Clave, y no por el conocimiento de los métodos utilizados en la transformación del mensaje original.

10.1.9 Tipos de Algoritmos

Al momento de su catalogación, los diferentes tipos de algoritmos de cifrado, suelen dividirse en tres grandes grupos:

Según la naturaleza del algoritmo:

- Sustitución: Sustituye unos símbolos por otros (Ejemplo: Método César).
- Transposición: No sustituye los símbolos, sólo cambia el orden o ubicación de los mismos.
- Producto: Cifrado obtenido a partir de la aplicación de los métodos anteriores, dos o más veces. Cuantos más métodos se apliquen más seguridad se tiene. Este método en combinación con otros, se ha convertido en uno de los más aplicados en la actualidad.

Según la clave

- Simétricos (Clave Secreta): En este tipo de algoritmos, la clave utilizada para el cifrado de un mensaje es la misma que se emplea para descifrar éste. Puesto que si un atacante descubre la clave utilizada en la comunicación, se encontrará en posición de quebrar el criptosistema, estas claves suelen mantenerse como un secreto entre el emisor y el receptor.
- Asimétricos (Clave Pública): Para el caso de los algoritmos asimétricos, la clave de cifrado es de conocimiento general (Clave Pública). Sin embargo, no ocurre lo mismo con la clave de descifrado (Clave Privada), que se ha de mantener en secreto. Si bien es cierto que ambas claves no son independientes entre sí, del conocimiento de la Pública no es posible deducir la Privada sin ningún otro dato (Cosa que sí es factible en los sistemas de Clave Secreta).
- Irreversibles: Este tipo de algoritmos tienen la particularidad de poder cifrar un texto claro, no permitiendo su descifrado. Si bien a simple vista parecería ser un sistema sin utilidad, lo cierto es que existen cientos de aplicaciones que se aprovechan de esta facultad, como por ejemplo las Funciones de Hash.

Según el número de símbolos cifrados a la vez

- Bloque: Toman el texto en claro y lo dividen en bloques de igual longitud, para luego cifrar cada bloque en forma independiente. Generalmente, suelen emplearse bloques de 64 bits.

- Flujo: En este tipo de algoritmos, el Texto en Claro es cifrado símbolo tras símbolo (bit a bit), con la particularidad de que cada uno, se cifra con una clave diferente. Debido a esta característica, los algoritmos de flujo, suelen cumplir con algunas de las reglas necesarias para ser mencionados como de “Cifrado Invulnerable” o de “Secreto Perfecto”.

10.1.10 Tipos de Ataques Criptográficos

Si bien existe la posibilidad por parte de un atacante, de lanzar un ataque de denegación de servicio sobre un sistema criptográfico, lo cierto es que generalmente, el objetivo final de la mayoría de ellos, se encontrará relacionado con la posibilidad de obtener la información protegida por alguno de los métodos de cifrado conocidos.

Los ataques específicos a los distintos sistemas criptográficos, suelen ser divididos en los siguientes tres grupos:

Ataque a las Claves: También conocido como ataques por Fuerza Bruta. los ataques a las claves, suelen ser uno de los más populares. Básicamente consisten, en la realización de intentos de adivinación reiterados, ya sea mediante palabras comúnmente usadas o aleatorias. El objetivo de este tipo de ataques, suele estar conformado por passwords, mensajes encriptados o cualquier otro tipo de clave basada en encriptación.

Puesto que la cantidad de tiempo que toma el romper una password depende de la longitud de la misma y del tipo de caracteres seleccionados, claves más largas y complejas, tienden a hacer este tipo de ataques más complicados.

Birthday Attack o Ataque de Cumpleaños: Los ataques del cumpleaños se basan en una premisa simple. Si 25 personas se encuentran en un cuarto, el estudio de las probabilidades dicta que es probable que al menos dos de esas personas cumplan años el mismo día. Dicha probabilidad aumentará en caso de que más personas ingresen al cuarto. Si bien es cierto que esto no es una regla, sí, es una probabilidad. Un Ataque de Cumpleaños trabaja de la misma forma y suele ser aplicable, por ejemplo, a la evaluación de un hash. Si un proceso aleatorio pa, genera como salida un hash h de valor v, es probable que en un período de tiempo t, vuelva a repetirse la generación de un nuevo hash equivalente a v. Puesto que éste no es un ataque al algoritmo, sino a su resultado, suele ser referido como Ataque a la Clave.

- **Ataque al Algoritmo**

  Debido a su concepción, distintas implementaciones de un algoritmo de encriptación determinado, pueden ser susceptibles de contener vulnerabilidades o debilidades que habiendo pasado desapercibidas en su desarrollo, y hechas públicas a posterior, puedan servir de brecha utilizable por un atacante.

  Un caso común que suele aplicarse frecuentemente como ejemplo, es el del protocolo WEP (Wired Equivalent Privacy). Hace algún tiempo, se hizo público un documento, que discutía una debilidad teórica en el algoritmo que fue utilizado como base, para el sistema de seguridad de este protocolo. Unos días después, los desarrolladores de WEP expresaron a la comunidad, que la vulnerabilidad era teórica y no podría suceder en el mundo real. En el plazo de siete días a partir de estas declaraciones, se recibieron una docena de ejemplos prácticos de cómo romper las características de seguridad implementadas en WEP.

- **Intercepción**
  Los ataques de intercepción, generalmente suelen aprovecharse de la obtención de datos cifrados en un canal de comunicación, a fin de utilizar esta información como punto de partida para un “Ataque Matemático”. A mayor cantidad de datos obtenidos en el proceso de intercepción, mayor probabilidad de acierto será logrado por medio del análisis de los mismos.

Nota: Cuando hablamos de “Ataques Matemáticos”, nos referimos a aquellos que precisamente, usan modelos matemáticos en conjunto con análisis estadístico para determinar el funcionamiento de un sistema criptográfico en particular. Este tipo de ataques, dependen de interceptar grandes cantidades de datos, y metódicamente proceder a descifrar los mensajes utilizando un ataque al algoritmo o a la generación de la clave.

Meet-in-the-middle (Encuentro a medio camino): El ataque *por encuentro a medio camino* o *meet-in-the-middle* es un ataque similar al ataque de cumpleaños, que utiliza un compromiso entre tiempo y espacio.

Mientras que el ataque de cumpleaños trata de encontrar dos valores del dominio de una función que tienen como imagen el mismo resultado, este ataque trata de encontrar un valor en el rango del dominio de composición de dos funciones, de tal manera que la imagen de la primera función da lo mismo que la imagen inversa de la segunda función - de ahí el nombre del ataque-.

Fue desarrollado en 1977 por Whitfield Diffie y Martin Hellman, en un intento de expandir un bloque cifrado. En la búsqueda de una mejor seguridad del cifrado de un bloque, se podría intentar la idea de usar simplemente dos claves criptográficas para cifrar dos veces los datos. A priori, se podría pensar que esto debería elevar al cuadrado la seguridad del esquema de doble cifrado. Ciertamente, una búsqueda exhaustiva de todas las claves posibles requeriría 2^{2n} intentos, si cada clave fuera de n bits, comparado con los 2^n intentos requeridos para una clave única. Sin embargo, Diffie y Hellman encontraron un compromiso entre tiempo y memoria que podría quebrar el cifrado en solamente el doble de tiempo. El ataque se basa en el cifrado por un extremo y el descifrado por el otro, buscando un encuentro a medio

Deriva de reloj: Se refiere a varios fenómenos relacionados debido a los que un reloj no marcha exactamente a la misma velocidad que otro, lo que significa, que después de cierto tiempo la hora indicada por el reloj se ira separando (a esto se refiere la deriva) de la indicada por el otro. Este fenómeno es aprovechado por las computadoras para construir generadores de números aleatorios y también puede ser utilizado para ataques de tiempo en criptografía.

10.1.11 Claves

Como hemos podido observar hasta aquí, la gran mayoría de los sistemas criptográficos, se complementan o se basan en la generación y utilización de algún tipo de clave. De acuerdo a su uso, los diferentes tipos de clave, suelen pertenecer a alguno de los siguientes grandes grupos:

- **Clave privada:** Se denomina “Clave Privada”, a aquella que relacionada con un sistema criptográfico asimétrico, sólo es conocida por el propietario de la misma.
- **Clave pública:** También relacionado con un sistema criptográfico asimétrico, se llama “Clave Pública” a aquella clave que siendo propiedad de un sujeto, es dada a conocer públicamente.
- **Clave Compartida:** Si bien es cierto, que el desarrollo de los sistemas criptográficos entorno a los tipos de clave “Pública y Privada” ha significado un gran avance respecto de la criptografía práctica, el concepto de “Clave Secreta” o “Clave Compartida” ha permitido solucionar uno de los problemas comúnmente encontrados en los criptosistemas en la antigüedad: el intercambio seguro de claves. En rigor de verdad, una “Clave Compartida” es aquella que siendo secreta, se encuentra en poder y es conocida, tanto por el emisor como por el receptor.

Más allá del tipo de clave utilizado en cada caso, y a pesar de la existencia de algunos sistemas criptográficos cuya seguridad no se encuentre basada en ellas, el uso de claves largas y complejas, siempre será un factor que contribuya a la seguridad del sistema evaluado.

10.2 ALGORITMOS SIMÉTRICOS (Criptografía de clave simétrica)

Se denomina “Algoritmo Simétrico” a todo proceso criptográfico que utilice en su accionar una misma clave para encriptar y desencriptar. Para que este tipo de criptosistema funcione correctamente, tanto el emisor como el receptor del mensaje, deben encontrarse en conocimiento de la clave a utilizar , transformando ésta en su “Secreto Compartido”. Debido a ello, la existencia de un canal seguro a través del cual se pueda realizar el intercambio de claves, se convierte en un requisito indispensable. Puesto que este tipo de algoritmos, basa su seguridad en la privacidad de su clave, el espacio o longitud de las mismas, es de vital importancia a fin de lograr que éstas sean de difícil adivinación. Algunas de las características principales de este algoritmo, lo han vuelto muy popular, lo que ha llevado a que en la actualidad, varios de los más importantes sistemas criptográficos lo implementen con éxito.

Los sistemas criptográficos de **clave simétrica** se caracterizan porque la clave de descifrado x es idéntica a la clave de cifrado k, o bien se puede deducir directamente a partir de ésta.

Para simplificar, supondremos que en este tipo de criptosistemas la clave de descifrado es igual a la de cifrado: $x = k$ (si no, siempre podemos considerar que en el algoritmo de descifrado el primer paso es calcular la clave x a partir de k). Es por esto que estas técnicas criptográficas se denominan de clave simétrica, o a veces también de clave compartida.

La seguridad del sistema recae pues en mantener en secreto la clave k. Cuando los participantes en una comunicación quieren intercambiarse mensajes confidenciales, tienen que escoger un clave secreta y usarla para cifrar los mensajes. Entonces, pueden enviar estos mensajes por cualquier canal de comunicación, con la confianza que, aun que el canal sea inseguro y susceptible de ser inspeccionado por terceros, ningún espía Z será capaz de interpretarlos.

A continuación repasaremos las características básicas de los principales algoritmos criptográficos de clave simétrica, que agruparemos en dos categorías: algoritmos de cifrado en flujo y algoritmos de cifrado en bloque.

Algoritmos de cifrado en flujo: El funcionamiento de una cifrado en flujo consiste en la combinación de un texto en claro M con un texto de cifrado S que se obtiene a partir de la clave simétrica k. Para descifrar, sólo se requiere realizar la operación inversa con el texto cifrado y el mismo texto de cifrado S. La operación de combinación que se utiliza normalmente es la suma, y la operación inversa por tanto es la resta. Si el texto está formado por caracteres, este algoritmo sería como una **cifra de César** en que la clave va cambiando de un carácter a otro. La clave que corresponde cada vez viene dada por el texto de cifrado S (llamado keystream en inglés).

En los esquemas de cifrado en flujo, el texto en claro M puede ser de cualquier longitud, y el texto de cifrado S ha de ser como mínimo igual de largo. De hecho, no es necesario disponer del mensaje entero antes de empezar a cifrarlo o descifrarlo, ya que se puede implementar el algoritmo para que trabaje con un “flujo de datos” que se va generando a partir de la clave (el texto de cifrado). De ahí procede el nombre de este tipo de algoritmos.

Los algoritmos de cifrado en flujo actualmente en uso tienen la propiedad que son poco costosos de implementar. Las implementaciones en hardware son relativamente simples y, por lo tanto, eficientes en su rendimiento (en términos de bits cifrados por segundo). Pero también las implementaciones en software pueden ser muy eficientes.

Las características del cifrado en flujo lo hacen apropiado para entornos en los que se necesite un rendimiento alto y los recursos (capacidad de cálculo, consumo de energía) sean limitados. Para ello se suelen utilizar en comunicaciones móviles: redes locales sin hilos, telefonía móvil, etc. Un ejemplo de algoritmo de cifrado en flujo es el **RC4** (Ron’s Code 4). Fue diseñado por Ronald Rivest en 1987 y

publicado en Internet por un remitente anónimo en 1994. Es el algoritmo de cifrado en flujo mas utilizado en muchas aplicaciones gracias a su simplicidad y velocidad. Por ejemplo, el sistema de protección **WEP** (Wired Equivalent Privacy) que incorpora el estándar IEEE 802.11 para tecnología LAN inalámbrica utiliza este criptosistema de cifrado en flujo.

Algoritmos de cifrado en bloques: En una cifra de bloque, el algoritmo de cifrado o descifrado se aplica separadamente a bloques de entrada de longitud fija *b*, y para cada uno de ellos el resultado es un bloque de la misma longitud. Para cifrar un texto en claro de *L* bits debemos dividirlo en bloques de *b* bits cada uno y cifrar estos bloques uno a uno. Si *L* no es múltiple de *b*, se pueden agregar bits adicionales hasta llegar a un número lleno de bloques, pero luego puede ser necesario indicar de alguna forma cuántos bits había realmente en el mensaje original. El descifrado también se debe realizar bloque a bloque.

Muchos de los algoritmos del cifrado de bloque se basan en la combinación de dos operaciones básicas: **sustitución** y **transposición**.

- La **sustitución** consiste en traducir cada grupo de bits de la entrada a otro, de acuerdo con una permutación determinada.
- La **transposición** consiste en reordenar la información del texto en claro según un patrón determinado. Un ejemplo podría ser la formación grupos de cinco letras, incluidos los espacios en blanco, y rescribir cada grupo (1, 2, 3, 4, 5) en el orden (3, 1, 5, 4, 2)

Cuando se utiliza el cifrado simétrico para proteger las comunicaciones, se puede escoger el algoritmo que sea más apropiado a las necesidades de cada aplicación: normalmente, a más seguridad menos velocidad de cifrado, y viceversa.

Un aspecto que hay que tener en cuenta es que, aunque el cifrado puede conseguir que un atacante no descubra directamente los datos transmitidos, en ocasiones es posible que se pueda deducir información indirectamente. Por ejemplo, en un protocolo que utilice mensajes con una cabecera fija, la aparición de los mismos datos cifrados varias veces en una transmisión puede indicar dónde empiezan los mensajes.

Esto pasa con el cifrado en flujo si su periodo no es lo suficientemente largo, pero en un cifrado en bloque, si dos bloques de texto en claro son iguales y se utiliza la misma clave, los bloques cifrados también serán iguales. Para contrarrestar esta propiedad, se pueden aplicar distintos modos de operación al cifrado en bloque.

10.2.1 Modos de operar: ECB, CBC, CFB y OFB

Las técnicas utilizadas por los algoritmos simétricos, al momento de realizar su tarea, se basan en el cifrado de datos por bloques, los cuales pueden ser constantes o variables. Puesto que por lo general, la información de entrada, procesada por un algoritmo simétrico, comprende una cantidad arbitraria de información a cifrar, se requiere especificar la forma en la que estos datos serán procesados. Precisamente, a las diferentes formas en las que se procesan estos bloques de datos, se las conoce como “Modos de Operación”. A continuación se muestra una breve descripción de cada uno de ellos:

- ECB (Electronic Codebook o Libro de Códigos Electrónico): En este modo, se cifra cada bloque de 64 bits del mensaje en claro, uno tras otro con la misma clave. Un par de bloques idénticos de mensaje en claro producen bloques idénticos de mensaje cifrado; además si el mensaje presenta patrones repetitivos, el texto cifrado también los presentará, siendo esto peligroso especialmente cuando se codifica información muy redundante. A favor de este método podemos decir que es resistente a errores, pues si uno de los bloques sufriera una alteración, el resto quedaría intacto.

- CBC (Cipher Block Bhaining o Cifrado en Bloque Encadenado): Sobre cada bloque de 64 bits del mensaje en claro, se ejecuta un OR exclusivo (XOR) con el bloque previo del mensaje cifrado. De este modo, el cifrado de cada bloque depende del anterior y bloques idénticos de mensaje en claro producen diferentes mensajes cifrados. De todos modos, dos mensajes idénticos se codificarán de la misma forma usando el modo CBC. Más aún, dos mensajes que empiecen igual se codificarán igual hasta llegar a la primera diferencia entre ellos. Para evitar esto, se emplea un vector de inicialización, que puede ser un mensaje un bloque aleatorio como bloque inicial de la transmisión. Este vector será descartado en el destino, pero garantiza que siempre los mensajes se codifiquen de manera diferente, aunque tengan partes comunes.
- CFB (Cipher Feedback o Cifrado Realimentado): El cifrado de un bloque de mensaje en claro procede de ejecutar un OR exclusivo del bloque de mensaje en claro con el bloque previo cifrado. Una de las particularidades de CFB, es que puede modificarse para trabajar con bloques de longitud inferior a 64 bits.
- OFB (Output Feedback o Salida Realimentada): En este caso, se generan una serie de valores pseudo aleatorios de 64 bits (generalmente, tantos como bloques de datos existan). A cada uno de los bloques de mensaje en claro se les aplica un OR exclusivo junto con uno de los valores aleatorios, el resultado obtenido son los bloques de mensaje cifrado.

10.2.2 Ventajas y limitaciones

Gran parte de la popularidad alcanzada por los algoritmos simétricos, se basa esencialmente en su velocidad. Comparados con los algoritmos de Clave Pública o Asimétricos, suelen ser mucho más rápidos, motivo por el cual son la elección preferida en aquellos casos donde se requiere encriptar grandes cantidades de datos. Al mismo tiempo, suelen ser considerados fuertes y difíciles de romper. Por otra parte, una de las limitaciones más importantes de este tipo de algoritmos se encuentra relacionada con la distribución de la clave secreta. Puesto que es necesario, que ésta sea conocida de antemano, tanto por el emisor como por cada uno de los receptores, su distribución puede llegar a convertirse en algo realmente complicado, cuando la cantidad de participantes es elevada. Incluso si decidiéramos asumir la carga administrativa en torno a la distribución de la clave secreta por cada uno de los participantes del circuito de comunicación, aún deberíamos resolver cuál sería un buen canal seguro para intercambiar ésta.

Por último, puesto que los algoritmos simétricos, basan gran parte de su seguridad en el secreto mantenido respecto de su clave, el acceso a ésta por parte de un atacante, suele llevar al compromiso total del criptosistema.

10.2.3 DES

Este criptosistema, es probablemente uno de los más estudiados en la historia de la criptografía. Desarrollado originalmente por IBM como una variación de un criptosistema llamado Lucifer, revisado y comprobado por la NSA a mediados de los años setenta, y adoptado por gran cantidad de industrias y gobiernos, DES se ha convertido en un estándar de encriptación de clave simétrica. Desde el punto de vista de su funcionamiento , DES suele ser un algoritmo de cifrado por bloques en el cual, una entrada M (Mensaje) sufre en primer lugar, una transposición bajo una permutación denominada IP (Permutación Inicial) , originando To=IP(M). Después de pasar To dieciséis veces por una función f, se transpone bajo la permutación inversa IP', obteniéndose así el resultado final.

DES toma bloques de información de 64 bits y los cifra mediante el procedimiento descrito anteriormente con una clave de 56 bits, realmente la clave inicial es de 64 bits, pero debido a que los bits menos significativos de cada byte se utilizan como bits de paridad y no aportan ninguna información adicional, pueden ser eliminados, obteniéndose de esta forma una clave efectiva de 56 bits. Si bien es cierto que DES es considerado un algoritmo fuerte, el tamaño final de su clave (56 bits)

en conjunción con el poder de cómputo actual, lo vuelven computacionalmente vulnerable a un ataque de fuerza bruta.

10.2.4 3DES (triple DES)

Triple-DES (3DES) es considerado una mejora tecnología respecto del DES tradicional. Si bien su implementación no presupone ninguna característica demasiado innovadora, atenta a las críticas respecto del escaso tamaño de clave que representaban los 56 bits de DES, esta nueva versión utiliza un procedimiento por medio del cual el mensaje original es cifrado tres veces , consiguiendo de esta forma alcanzar claves de 128 bits (16 de paridad y 112 de clave efectiva) y 168 bits según el procedimiento utilizado. Existen tres implementaciones posibles de 3DES:

1. DES-EEE3 Se cifra tres veces con una clave diferente cada vez.
2. DES-EDE3 Primero se cifra, luego se descifra y por último se vuelve a cifrar, cada vez con una clave diferente.
3. DES-EEE2 / DES-EDE2 Similares a los anteriores, con la salvedad de que la clave usada en el primer y en el último paso coinciden.

3DES es considerablemente más duro de romper que muchos otros sistemas basados en algoritmos simétricos, quizás por ello, a pesar del surgimiento de nuevas opciones, continúa siendo uno de los más utilizados.

10.2.5 AES

En 2 de Enero de 1997, el NIST (National Institute of Standards and Technology) anunciaba formalmente el inicio de la búsqueda del algoritmo simétrico que reemplazaría a DES como estándar de encriptación. La gran particularidad de este programa, residía en que era abierto e instaba a participar a profesionales de todo el mundo. Unos años más tarde, los finalistas habían sido seleccionados. MARS, RC6, Rijndael, Serpent y Twofish, serían sometidos a algunas de las pruebas más exigentes, a fin de encontrar al que se convertiría en el nuevo estándar AES.

Finalmente el 2 de Octubre del 2000, el NIST anunciaba que Rijndael, un algoritmo de origen Belga, desarrollado por Joan Daemon y Vincent Rijmen, se convertiría en el sustituto de DES hasta entrado el siglo XXI. AES al igual que DES, es un sistema de cifrado por bloques, con la diferencia que éstos, en vez de ser de 64, son de 128 bits. Existen varias versiones de AES, utilizando claves de 128, 192 o 256 bits.

En la actualidad, AES es el estándar usado por las agencias gubernamentales de los Estados Unidos, y entre algunas de sus características principales, se encuentra su buena combinación de seguridad, velocidad, eficiencia, sencillez y flexibilidad.

10.2.6 Otros algoritmos

- **RC:** RC es una familia de cifrado producida inicialmente por los laboratorios RSA. Si bien los niveles RC2 y RC4 han sido y siguen siendo muy utilizados, suele considerarse seguros los actuales niveles RC5 y RC6. Estos últimos, tienen la particularidad de ser algoritmos parametrizables, donde tanto el bloque a cifrar, como el tamaño de la clave y el total de iteraciones son configurables. En su última versión, RC permite un tamaño de clave de hasta 2.048 bits.
- **IDEA:** IDEA fue creado en 1990 por Xuejia Lay y James Massey. Trabaja con bloques de 64 bits y opera siempre con números de 16 bits usando operaciones OR-Exclusiva, suma y multiplicación de enteros. Utiliza claves de 128 bits y ha probado ser muy resistente frente al

criptoanálisis. Este algoritmo es de libre difusión y no se encuentra sujeto a ningún tipo de restricciones, lo que ha contribuido a su amplia difusión.

- **CAST:** Este algoritmo, toma el nombre de las iniciales de sus desarrolladores: Carlisle Adams y Stafford Tavares. CAST es utilizado por algunos de los productos ofrecidos por Microsoft e IBM. Utiliza claves entre 40 y 128 bits y es conocido por ser muy rápido y eficiente. Si bien se encuentra patentado por Entrust Technologies, su uso libre ha sido permitido.
- **Blowfish:** Blowfish, es un sistema de cifrado producido por la firma Counterpane, de quien Bruce Schneier (autor del libro Applied Criptography)es su CEO. En este algoritmo, el cifrado se lleva a cabo mediante 16 vueltas en las que se opera con una función sencilla. Cada vuelta incluye una permutación y una sustitución en función de la clave y de los datos. El resto de operaciones elementales son XOR y la suma modular (módulo 2^32). Utiliza claves de hasta 448 bits, y hasta el momento ha resistido con éxito todos los ataques. Por ello y por su estructura suele ser considerado uno de los algoritmos más seguros, a pesar de lo cual no se utiliza masivamente.
- **Serpent:** Con 59 votos, Serpent ocupo el segundo lugar en el certamen en busca del estándar AES. Si bien su diseño es bastante conservador, logra gran velocidad al encriptar múltiples bloques en forma simultánea, utilizando para cada bloque solamente 1 bit del procesador. Dicho de otra forma, sobre un procesador de 32 bits es posible encriptar 32 bloques en paralelo. Esta técnica conocida como "bitslicing" es la misma que se utiliza en las implementaciones más veloces del DES. Muchos especialistas coinciden en que Serpent y Rijndael, son bastante similares, aunque suele decirse que Rijndael es más rápido mientras que Serpent es más seguro. Serpent es de dominio público y sus autores no han colocado restricciones a su uso.
- **MARS:** MARS, un nuevo desarrollo de IBM, posee un diseño innovador al incluir un núcleo criptográfico con una capa de difusión, lo que le permite utilizar varias funciones diferentes en sus iteraciones. En rigor de verdad, MARS combina en un algoritmo, cada una de las técnicas conocidas de criptografía. El largo de clave de MARS, puede ser variado entre 128 y 400 bits.
- **Twofish:** Twofisth, es originario de Estados Unidos. Su diseño se basó en "Blowfish" un algoritmo muy popular. Una de sus particularidades, es el uso de tablas internas de datos variables que dependen de la clave, respecto de las cuales, sus diseñadores han hecho un gran esfuerzo al comprobar que cada una de las variantes posibles, sea lo suficientemente fuerte. Utiliza bloques de 128 bits y claves de 256 bits.

10.3 ALGORITMOS ASIMÉTRICOS

La particularidad de los algoritmos asimétricos, o de clave pública radica en que, a diferencia de los algoritmos simétricos, utilizan dos claves y no una, en su proceso de cifrado y descifrado. Ambas claves suelen ser referidas como clave pública y clave privada.

En este tipo de esquema, el remitente utiliza la clave pública del destinatario para cifrar el mensaje, el cual una vez cifrado, sólo puede ser descifrado por la clave privada del mismo. Para que esto suceda, ambos extremos de la comunicación deben estar en conocimiento de la clave pública, lo cual no representa riesgo alguno puesto que es prácticamente imposible deducir una clave privada a partir de su contrapartida pública.

Esto último, se debe a que los sistemas de cifrado de clave pública suelen basarse en funciones-trampa de un solo sentido. Una función de un solo sentido es aquella cuya computación es fácil, mientras que invertir la función es extremadamente difícil. Puesto que la clave privada asociada a una clave pública, contiene la porción de información necesaria para resolver la función relativa a la encriptación, la pérdida de privacidad respecto de ésta, abriría una brecha de seguridad en el criptosistema.

10.3.1 Ventajas y limitaciones

Una de las ventajas más apreciables de los esquemas criptográficos basados en algoritmos asimétricos, radica en la posibilidad por parte de quien desea recibir información cifrada, de hacer llegar a sus potenciales emisores su clave pública, sin perjuicio de que ello signifique un riesgo, logrando de esta forma comenzar una conversación fiable sin necesidad de establecer previamente un canal seguro donde intercambiar claves privadas.

Esta característica de los sistemas basados en clave pública, hace que la limitación implícita en los algoritmos simétricos, respecto de la distribución de claves privadas, entre muchos participantes de una comunicación segura, encuentre en ella una aplicación fundamental al momento de resolver este dilema.

Como desventaja, los algoritmos asimétricos, deben utilizar claves de mayor tamaño para ofrecer una seguridad comparable a la de los algoritmos simétricos. A su vez, suelen resultar más lentos, mientras que producen mensajes cifrados de mayor tamaño. Cabe destacar que este tipo de algoritmos requieren una mayor utilización de recursos, por lo cual no suelen emplearse en mecanismos de encriptación de grandes volúmenes de datos.

10.3.2 Diffie Hellman

El algoritmo Diffie Hellman, fue concebido por Whitfield Diffie y Martin Hellman. Su publicación en 1976, supuso una verdadera revolución en el campo de la criptografía, debido al novedoso concepto relacionado con la utilización de dos claves diferentes, una pública y la otra privada. De hecho, su desarrollo es considerado el inicio de los sistemas asimétricos.

La utilización de este algoritmo, permite que dos entidades se pongan de acuerdo en un valor, a través de un canal público, sin que dicho valor pueda ser conocido por algún atacante que esté monitorizando la comunicación. De hecho, ambas entidades no necesitan compartir ningún secreto, por lo que puede utilizarse para comunicar de forma segura a dos entidades que nunca antes se hayan comunicado.

Matemáticamente se basa en las potencias de los números y en la función mod (módulo discreto). Uniendo estos dos conceptos se define la potencia discreta de un número como Y=Xa mod q. Si bien el cálculo de potencias discretas es fácil, la obtención de su función inversa, el logaritmo discreto, no tiene una solución analítica para números grandes.

En la práctica, este algoritmo solo es utilizado para el intercambio de claves simétricas, y debido a su potencialidad en este campo, suele implementarse exitosamente en diferentes tipos de sistemas seguros a través de Internet como por ejemplo: VPN (Virtual Private Network) y SSL (Secure Socket Layer).

Procedimiento

- Sea "p" un número entero grande y "a" un entero menor que "p"
- Los usuarios "A" y "B" eligen dos exponentes arbitrarios (x, y). los que se mantienen en secreto
- El usuario A calcula f(x)=(a)x mod p, enviándoselo a B
- El usuario B calcula f(y)=(a)y mod p, enviándoselo a A
- Ahora el usuario A calcula k=(f(y))x mod p, o lo que es lo mismo k=((a)y)x mod p
- Ahora el usuario B calcula k=(f(x))y mod p, o lo que es lo mismo k=((a)x)y mod p
- Por lo tanto k=k= (a)xy mod p

10.3.3 RSA

RSA desarrollado por Ron Rivest, Adi Shamir, y Leonard Adleman en 1978, es probablemente el sistema criptográfico asimétrico más conocido y utilizado, a la vez que es considerado un estándar de facto. Basado en las investigaciones de Diffie-Hellman, este equipo de trabajo creó su algoritmo y fundo la empresa RSA Security Inc. Puesto que su patente ha expirado hacia fines del 2000, en la actualidad es considerado de uso libre.

RSA ha sido implementado con éxito, tanto en la encriptación como en esquemas de firma digital. Su proceso involucra claves de 1024 bits y matemáticamente, se basa en la dificultad de factorizar números primos de gran tamaño. Si bien este último punto denota la complejidad que presupone la factorización de números primos en tiempo computacional, existe la posibilidad teórica de que algún desarrollo futuro, de nuevos métodos asociados a este problema, permitan realizar dicha operación matemática en tiempos que computacionalmente tornarían este sistema inseguro. A pesar de ello, de momento, este algoritmo continúa siendo considerado como uno de los más seguros.

Procedimiento

- Se toman dos números primos grandes, llamados "p" y "q"
- Se calcula "n" , llamado módulo, como el producto n=p.q
- Se elige un número "e", de tal modo que "e" es menor que "n" y primo relativo (no tiene factor común, excepto 1) de (p-1).(q-1)
- Se elige otro número "d" tal que (ed-1) es divisible por (p-1).(q-1), es decir que su resto es cero
- Los valores "e" y "d" son llamados exponentes público y privado respectivamente
- La Clave Pública es el par (n,e) mientras que la Clave Privada es el par (n,d)
- Los factores "p" y "q" pueden almacenarse con la clave privada o ser destruidos

10.3.4 Funciones de curva elíptica

Hacia 1985, la teoría de las curvas elípticas encontró de la mano de Neal Koblitz y Victor Miller, aplicación en la criptografía. Los sistemas basados en funciones de curva elíptica o ECC (Eliptic Curve Cryptosystem), representan un concepto bastante novedoso. Debido a que ECC proporciona una funcionalidad similar a RSA pero requiere menos potencia de cómputo y por ende menos energía para funcionar, han sido los elegidos en muchos casos para brindar soluciones criptográficas en pequeños dispositivos, como por ejemplo teléfonos celulares y dispositivos inalámbricos, PDA, etc. Los sistemas de ECC, se encuentran basados en el concepto de utilizar puntos sobre una curva a fin de definir un par de claves pública y privada. Si bien es cierto que la Criptografía de Curva Elíptica, suele ser considerado uno de los campos más prometedores dentro de las técnicas modernas de cifrado asimétrico, suele verse como un punto negativo la relativa falta de estudios teóricos sobre este formalismo matemático.

10.3.5 ¿Algoritmos simétricos o asimétricos?

Si intentáramos escoger un ganador entre los algoritmos simétricos y asimétricos, probablemente cometeríamos un gravísimo error. Precisamente la fortaleza de cada uno de éstos se percibe en su totalidad, cuando se los pone a trabajar en conjunto.

Como hemos visto a lo largo de estas secciones, las limitaciones respecto de la distribución de claves, relacionada con los algoritmos simétricos, se ve resuelta al emplear sistemas asimétricos o de clave pública. De esta forma, se logra la implementación de verdaderos “Sistemas Criptográficos” contando por un lado, con la velocidad y fortaleza provista por los algoritmos simétricos, mientras que por el otro, se aprovecha la fabulosa capacidad de distribución que nos brindan los algoritmos asimétricos o de clave pública.

Atributos	Criptografía simetrica	Criptografía asimetrica
Claves	Una cleve es compartida entre dos ó más entidades **64 bits** **112 bits**	Una cleve es compartida entre dos ó más entidades **312 bits** **1792 bits**
Intercambio de claves	Por un medio seguro	Por el mismo medio
Velocidad	Los algoritmos son menos complejos y más rápidos	Los algoritmos son más complejos y entre 1000 y 10000 veces más lentos
Uso	Encripción de archivos y enlaces de datos	Firma digital y distribución de claves
Servicio de seguridad positivo	Confidencialidad	autenticación y no repudio

10.4 CRIPTOGRAFÍA FÍSICA

Utilizamos el término de Criptografía Física, para referirnos a todo aquel método de cifrado que no altera los valores involucrados en dicha operación, por medio de un proceso matemático. La Criptografía Física, incluye varios métodos de cifrado. Alguno de los más comunes, implican la transposición o sustitución de caracteres o palabras, aunque otros como la esteganografía, poseen características más particulares. La gran mayoría de los métodos de cifrado, de los que se ocupa la criptografía física, suelen existir desde hace cientos de años, y si bien hoy día pueden no resultar muy efectivos utilizados individualmente, suelen constituir la base de sistemas más avanzados. Un buen ejemplo de esto, se encuentra en los algoritmos simétricos, quienes suelen utilizar como parte de su funcionamiento interno, el producto de operaciones de sustitución y transposición.

- **Sustitución:** El método de sustitución se basa, tal como su nombre lo indica, en sustituir un caracter o cadena de caracteres por otro caracter o cadena de caracteres. Dentro de este grupo, suelen identificarse dos categorías principales: “Sustituciones Monoalfabéticas” y “Sustituciones Polialfabéticas”. Los algoritmos de sustitución monoalfabética, son los más simples y su utilización se remonta a la edad media. Uno de los ejemplos más claros al respecto, lo representa el cifrado “César”. Por su parte, los algoritmos que utilizan sustituciones polialfabéticas, hacen uso de múltiples “alfabetos” previamente estipulados, sobre los que se basa la sustitución. Quizás, uno de los ejemplos más significativos de este tipo de sustitución, lo constituya el “Cifrado de Vigenére”. Una de las debilidades de los sistemas de sustitución, suele estar representada por la posibilidad por parte de un atacante, de analizar estadísticamente la ocurrencia de determinados valores conocidos que puedan servir de pista o patrón, al momento de resolver el criptosistema. Un ejemplo de esto, podría ser el de las vocales en el alfabeto español.
- **Transposición:** De la misma forma en la que los algoritmos de sustitución operan sobre los caracteres, los de transposición operan sobre las posiciones, sin alterar el carácter original. Esto suele representar en parte, una gran ventaja frente a los algoritmos de sustitución, puesto

que al estar operando sobre las posiciones, un análisis estadístico no sería suficiente para quebrar el criptosistema, debido a que cada carácter aparecerá en las proporciones en que deba aparecer. Por lo general, los algoritmos de transposición, suelen dividir el mensaje original en bloques de igual tamaño, sobre los que luego realizan las operaciones correspondientes.

10.5 FUNCIONES DE HASH

Podríamos definir una Función Hash, como aquella operación que se realiza sobre un conjunto de datos de cualquier tamaño, de tal forma que se obtiene como resultado, otro conjunto de datos en ocasiones denominado resumen o valor hash de los datos originales, de tamaño fijo e independiente del tamaño original, que además, tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es prácticamente imposible encontrar dos mensajes distintos que tengan un resumen hash idéntico.

Gracias a sus características, las aplicaciones principales de las Funciones de Hash, suelen ser fundamentalmente tres:

1. Contraseñas: Las funciones hash son una excelente opción al momento de almacenar contraseñas. Gracias a su característica de irreversibilidad, almacenar el valor hash de una contraseña es más seguro que almacenar la contraseña misma en forma criptográfica.
2. Firmas Digitales: Realizar operaciones de firma digital sobre mensajes grandes, puede ser computacionalmente muy costoso. En su lugar, suele aplicarse una Función Hash sobre el mensaje original, para finalmente firmar digitalmente el valor hash, de menor tamaño, obtenido como resultado de la primera operación.
3. Integridad y Autentificación: El valor obtenido al aplicar una Función de Hash, a un mensaje, suele ser utilizado para comprobar la integridad y autenticidad del mismo. Puesto que cualquier cambio sucedido sobre el mensaje original, alteraría el valor hash resultante, el eventual receptor podría ser capaz de utilizar la misma Función Hash, que el emisor para comparar que el resultado obtenido es coincidente con el calculado al inicio de la comunicación. La autentificación se da cuando la Función de Hash se calcula, no solamente tomando como argumento el mensaje a transmitir, sino también en base a un secreto compartido entre los corresponsales de la comunicación.

Nota: Es muy común referirse al valor hash obtenido a través de una función hash, como por los términos en inglés “message digest” o “fingerprint”.

Para que una Función de Hash pueda ser utilizada con fines criptográficos, debe poseer una serie de características básicas:

- La entrada debe poder ser de cualquier tamaño.
- El valor hash (salida) debe tener un tamaño fijo.
- Debe encontrarse libre de colisiones, esto es, que dadas dos cadenas como entrada “x'' e “y'', no se obtenga un mismo valor hash tal que H(x)=H(y).
- Debe ser Irreversible (one-way hash o hash de un solo sentido); es decir, dado un valor hash “h'', no sea posible encontrar una entrada “x'' tal que H(x)=h.
- Un valor hash debe ser computacionalmente fácil y rápido de calcular.

10.5.1 Ventajas y limitaciones

Las Funciones Hash, se han convertido en este último tiempo, en una poderosa herramienta en manos de profesionales de seguridad y usuarios en general. Sus características únicas, nos permiten obtener valores hash o resumen que pueden ser almacenados y luego comparados para verificar que los archivos o mensajes resumidos, no han sido modificados o, dicho de otra forma, conservan su integridad.

En ciertos ámbitos, como en la Informática Forense, los investigadores se ven obligados a someter la información recolectada en la escena del crimen, a operaciones de hash, a fin de que la evidencia pueda ser tomada como tal, en una posible instancia judicial.

Los administradores de sistemas, deben hacer uso de las bondades provistas por las funciones de hash, al instalar por ejemplo, un nuevo servidor web. El conservar en un lugar seguro, los valores hasheados, de cada uno de los archivos de sistema intervinientes en la instalación original, le permitirá corroborar el reemplazo no autorizado de alguno de estos archivos por parte de un atacante, ante un posible incidente de seguridad.

Nota: Herramientas como Tripwire, AIDE, md5sum y md5dep, suelen automatizar en parte la obtención y en algunos el almacenamiento seguro, de valores hash en una instalación de software. Por otro lado, sitios web como Know Goods o NIST, nos permiten consultar On-Line, bases de datos conteniendo las firmas MD5/SHA1 de prácticamente todos los archivos de los sistemas operativos conocidos

Pero la aplicación de Funciones de Hash, puede verse limitada en ciertas circunstancias. En aquellos casos en los que un atacante, consiga acceder tanto a la información original como a los valores resumidos, nada le impediría modificar la información y volver a generar un nuevo hash, que a los ojos del usuario final o remitente, pueda pasar por verdadero. Dicho de otro modo, si bien la utilización de funciones de hash, aporta su utilidad desde el punto de vista de la integridad, en muchos casos se requerirá de la combinación de otros métodos que acompañen su implementación.

	Algoritmo	Valor
1	**CRC-32**	ee44c1be6
3	**MD4**	8be578f00908e505f2497cfdad9a0f69
4	**MD5**	ca6cf096386381bd968554fab181abf7
5	**SHA1**	fc232dc1645592d6958cf4623a5dda9189a1402
6	**SHA2-256**	5e9205980bcb01815442beebc3d7c290008685a9ccb6e9844c27522669545856
7	**SHA2-384**	347cc8bbb9fea97905fa827a73d08807eaedad624f49a06 99cbf0d0d8f4190cd393799721f9596aec206505fe71234
8	**SHA2-512**	f6561739ccbe5b3c6fc889cc09ed9e748dcc41bfea2a687175a93e1381e6a1bac 5b5123aab727591230131ff49c4316df855ed2435b924679aa268e920489d15

10.5.2 MD5

MD5 (Message Digest), fue desarrollado por Ron Rivest (RSA Security, Inc.) y publicado por primera vez, en el RFC 1321 en Abril de 1992. Este algoritmo, es en verdad una versión ampliada de MD4, el cual si bien posee características similares, fue originalmente pensado, teniendo en mente la velocidad y no tanto la seguridad. MD5 incluye una serie de optimizaciones respecto de MD4, e incorpora algunos conceptos que lo hacen más seguro.

MD5 realiza una manipulación de bits para obtener, como resultante de cálculo, un valor hash de 128-bits, o lo que es lo mismo, una serie de 16 caracteres (32 dígitos hexadecimales), lo que da un conjunto de valores de 2 a la 128.

Una de los cuestionamientos que suelen hacerse a este algoritmo, es tal vez, su corta extensión. Puesto que gran cantidad de empresas como por ejemplo Microsoft, Sun, IBM y otras, han adoptado universalmente este algoritmo para controlar las versiones de algunas de sus aplicaciones (Objetos ActiveX, aplicaciones Java, etc.) resulta teóricamente posible, que en algún momento se encuentren dos valores hash MD5 iguales, para diferentes componentes.

Uno de los motivos principales que motivaron el desarrollo de MD5, fue la ruptura de MD4. A pesar de ello, dos investigadores, de nombre Boer y Bosselaers afirman haber encontrado pseudo-colisiones en la función de compresión de MD5, mientras que Dobbertin asegura haber hecho lo propio en la función de compresión del mismo algoritmo.

Hasta hace poco, el algoritmo de hash más usado era el MD5. Pero como el resumen que da es de sólo 128 bits, y aparte se han encontrado otras formas de generar colisiones parciales en el algoritmo, actualmente se recomienda utilizar algoritmos más seguros, como el SHA-1. El algoritmo SHA-1, publicado el 1995 en un estándar del NIST (como revisión de un algoritmo anterior llamado simplemente SHA), da resúmenes de 160 bits. El año 2002 el NIST publicó variantes de este algoritmo que generan resúmenes de 256, 384 y 512 bits.

10.5.3 SHA-1

SHA-1 (Secure Hash Algorithm), ha sido diseñado por el NIST (National Institute of Standards and Technology), a partir de MD4, motivo por el cual, su diseño guarda alguna relación con este algoritmo y con MD5. A pesar de ello, SHA-1 es considerado un algoritmo más fuerte, debido en parte a que la salida que produce es de 160-bits, lo que genera un conjunto de elementos resultantes de 2 a la 160. Si bien existieron algunos ataques exitosos a la primer versión denominada SHA, SHA-1, no ha sido roto de momento, motivo por el cual es considerado una excelente opción en relación al resto de las alternativas.

10.6 NECESIDAD DE AUTENTICAR

A partir del desarrollo de Internet, como medio de comunicación global, muchos han sido los comercios, empresas o entidades financieras, que atraídos por las virtudes de este nuevo medio, comenzaron a ofrecer servicios asociados a su rubro. Desde el principio, uno de los problemas fundamentales a resolver en este contexto, ha sido solventar la necesidad de corroborar en forma segura, que una persona es quien dice ser, al presentarse ante un servicio determinado.

Precisamente, se conoce con el término de autenticación, al proceso por el cual es posible confirmar la identidad, de cada una de las partes involucradas en el proceso de una comunicación o intercambio de mensajes. A continuación, presentaremos una serie de conceptos, tendientes a asegurar tres principios básicos referidos a la seguridad de la información:

- Integridad

- Autenticación
- No Repudio

Tal como mencionáramos en secciones anteriores, las funciones de hash nos proveían una herramienta fundamental a la hora de asegurar la integridad de un mensaje. Al mismo tiempo, presentábamos sus limitaciones, al mencionar algunos contextos en los cuales un valor hash, podía ser cambiado al mismo tiempo que su contenido original, provocando que el receptor del mensaje, termine por NO obtener la información tal como lo esperaba el emisor.

La respuesta a esta problemática, suele estar relacionada con la implementación de algún tipo de sistema que permita, no sólo asegurar la integridad, sino que también haga lo propio con la autenticidad. Es decir, siempre que un receptor B reciba un mensaje que parezca provenir del emisor A, el esquema implementado debería permitir averiguar, no sólo si el mensaje viene de A, si no también si fue modificado en su trayectoria.

Podemos distinguir dos tipos de autenticación:

- La autenticación de mensaje o autenticación de origen de datos permite confirmar que el originador A de un mensaje es auténtico, es decir, que el mensaje no ha sido generado por un tercero Z que quiere hacer creer que lo ha generado A.

  Como efecto adicional, la autenticación de mensaje proporciona implícitamente el servicio de integridad de datos, que permite confirmar que nadie ha modificado un mensaje enviado por A.
- La autenticación de entidad permite confirmar la identidad de un participante A en una comunicación, es decir, que no se trata de un tercero Z que dice ser A.

Existen dos grupos de técnicas para proporcionar autenticación de mensaje:

- Los códigos de autenticación de mensaje o MAC, basados en claves simétricas.
- Las firmas digitales, que se basan en la criptografía de clave pública.

10.6.1 MAC

Como una de las primeras alternativas surgidas a la hora de asegurar la integridad de la información transmitida o almacenada, surgió el concepto de MAC (Message Authentications Codes) o “Código de Autenticación de Mensajes”. En la práctica, el funcionamiento de MAC, radica en la inclusión de información adicional, como parte integral del mensaje a transmitir. Generalmente, esta información adicional suele estar formada por una clave compartida que es conocida por ambos extremos de la comunicación.

Si bien el concepto detrás de HMAC es el mismo, el uso de Funciones de Hash (he de aquí la “H” adicional) como parte integral del proceso de generación de este “Código de Autenticación”, lo transforma en una herramienta aún más efectiva. Cuando HMAC se pone en funcionamiento, el mensaje original es procesado junto a la clave de secreto compartido, por una función hash del estilo de MD5 o SHA-1. Esta operación produce como resultado, un valor de hash, el cual es transmitido junto al mensaje original al otro extremo de la comunicación. El receptor, recibe el mensaje y el valor de hash enviado por el emisor, y procede a recalcular un nuevo hash, ya que conoce la clave que se combinó con la información transmitida. Luego, el valor de hash enviado, es comparado con el valor de hash generado por el receptor. En caso de que ambos valores sean coincidentes, la integridad y autenticidad del mensaje estarán garantizadas. Si cualquier parte del mensaje original hubiera sido cambiada en tránsito o bien se hubiera falsificado el mensaje, los valores de hash serían diferentes, y la modificación o falsificación podrían ser detectadas.

Existen varias posibilidades a la hora de seleccionar el algoritmo de hash involucrado en una operación HMAC, aunque MD5 y SHA-1 suelen ser la elección más frecuente. Si bien es cierto que con ambos algoritmos se obtiene un resultado similar, el hecho de que SHA-1 produzca salidas de 160-bit, hace que esta combinación sea más fuerte que la de MD5 (128-bit).

10.6.2 Firma Digital

Desde el punto de vista conceptual, la Firma Digital, es básicamente una herramienta tecnológica, que permite garantizar la autoría e integridad de los documentos digitales, permitiendo que éstos gocen de una característica que únicamente era propia de los documentos en papel. Desde el punto de vista informático, una Firma Digital, puede ser vista como un grupo de datos asociados a un mensaje digital. Técnicamente hablando, el esquema de Firma Digital se basa en la utilización combinada de Criptografía Asimétrica o de Clave Pública y de Funciones de Hash o Resumen.

Veamos un ejemplo práctico de su funcionamiento:

El emisor genera, mediante una Función de Hash, una huella digital del mensaje. Esta huella digital se cifra con la clave privada del emisor. Como resultado de esta operación, se obtiene lo que se denomina Firma Digital, la cual será enviada adjunta al mensaje original. De esta forma, el emisor va a estar adjuntando al documento, una marca que es única para ese documento y que sólo él es capaz de producir. Al momento de realizar la verificación del mensaje, en primer lugar el receptor generará la huella digital del mensaje recibido, luego descifrará la Firma Digital del mensaje utilizando la Clave Pública del firmante y obtendrá de esa forma la huella digital del mensaje original; si ambas huellas digitales coinciden, significará que el mensaje no fue alterado y que el firmante es quien dijo ser.

Ahora bien, para que este circuito sea completado en forma eficiente, la Firma Digital, debe poseer las siguientes características:

- Debe ser única, pudiéndola generar solamente el usuario legítimo.
- No falsificable, el intento de falsificación debe llevar asociada la resolución de un problema numérico intratable.
- Debe ser fácil de autenticar, pudiendo cualquier receptor establecer su autenticidad aún después de mucho tiempo.
- Debe ser irrevocable, el autor de una firma no puede negar su autoría.
- Debe ser computacionalmente barata y fácil de generar.

Por otra parte, quizás una de las características principales que han de tener las Firmas Digitales, es que deben depender tanto del mensaje como del autor. De no cumplirse este principio básico, el receptor podría modificar el mensaje y mantener la firma, produciéndose de esta forma, un fraude. Es muy común oír hablar de Firma Electrónica, confundiendo a ésta con la Firma Digital. Se entiende por Firma Electrónica: "al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada Firma Digital".

La firma digital hace referencia, en la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, a un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje.

Los términos de firma digital y firma electrónica se utilizan con frecuencia como sinónimos, pero este uso en realidad es incorrecto. Mientras que firma digital hace referencia a una serie de métodos criptográficos, firma electrónica es un término de naturaleza fundamentalmente legal y más amplio

desde un punto de vista técnico, ya que puede contemplar métodos no criptográficos.

La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido y, seguidamente, aplicar el algoritmo de firma (en el que se emplea una clave privada) al resultado de la operación anterior, generando la firma electrónica o digital. El software de firma digital debe además efectuar varias validaciones, entre las cuales podemos mencionar:

- Vigencia del certificado digital del firmante,
- Revocación del certificado digital del firmante (puede ser por OCSP o CRL),
- Inclusión de sello de tiempo.

La función hash es un algoritmo matemático que permite calcular un valor resumen de los datos a ser firmados digitalmente. Funciona en una sola dirección, es decir, no es posible, a partir del valor resumen, calcular los datos originales. Cuando la entrada es un documento, el resultado de la función es un número que identifica inequívocamente al texto. Si se adjunta este número al texto, el destinatario puede aplicar de nuevo la función y comprobar su resultado con el que ha recibido. Ello no obstante, este tipo de operaciones no están pensadas para que las lleve a cabo el usuario, sino que se utiliza software que automatiza tanto la función de calcular el valor hash como su verificación posterior.

10.6.3 Infraestructura de clave Pública (PKI)

Como hemos visto hasta ahora, la criptografía de clave pública permite resolver el problema del intercambio de claves, utilizando las claves públicas de los participantes. Pero se platea otro problema: si alguien afirma ser *A* y su clave pública es *k*, ¿cómo podemos saber que realmente *k* es la clave pública de *A*? Porque es perfectamente posible que un atacante *Z* genere su par de claves y afirme "*yo soy A, y mi clave pública es k*".

Una posible solución a este problema es que exista una entidad de confianza que nos asegure que, efectivamente, las claves públicas pertenecen a sus supuestos propietarios. Esta entidad puede firmar un documento que afirme "*la clave pública de A es k*", y publicarlo para que todos los usuarios lo sepan. Este tipo de documento se llama certificado de clave pública o certificado digital, y es la base de lo que se conoce como infraestructura de clave pública.

Un certificado de clave pública o certificado digital consta de tres partes básicas:

- Una identificación de usuario como, por ejemplo, su nombre.
- El valor de la clave pública de este usuario.
- La firma de las dos partes anteriores.

Si el autor de la firma es alguien en quien confiamos, el certificado nos sirve como garantía de que la clave pública pertenece al usuario que figura identificado en el certificado. Quien firma el certificado puede ser una autoridad que se responsabilice de verificar fehacientemente la autenticidad de las claves públicas. En este caso, se dice que el certificado ha sido generado por una autoridad de **certificación** (***CA***).

Puede haber distintos formatos de certificados, pero el más usado es el de los certificados *X.509*, especificado en la definición del servicio de directorio *X.500*.

El directorio X.500 permite almacenar y recuperar información, expresada como atributos, de un conjunto de objetos. Los objetos X.500 pueden representar, por ejemplo, países, ciudades, o bien

empresas, universidades (en general, organizaciones), departamentos, facultades (en general, unidades organizativas), personas, etc. Todos estos objetos están organizados jerárquicamente en forma de árbol (en cada nodo del árbol existe un objeto) y, dentro de cada nivel, los objetos se identifican mediante un atributo distintivo. A nivel global, cada objeto se identifica con un nombre distintivo (DN), que no es más que la concatenación de los atributos distintivos que hay entre la raíz del árbol y el objeto en cuestión. El sistema de nombres es, pues, parecido al DNS de Internet, con la diferencia que los componentes de un nombre DNS son simples cadenas de caracteres, y los de un DN X.500 son atributos, cada uno con un tipo y un valor.

Un certificado nos soluciona el problema de la autenticidad de la clave pública si está firmado por una CA en la cual confiamos, Pero que pasa si nos comunicamos con un usuario que tiene un certificado emitido por una CA que no conocemos?

Existe la posibilidad que una CA tenga un certificado que garantice la autenticidad de su clave pública, firmado por otra CA. Esta otra CA puede que si que la conozcamos, o puede que a su vez tenga un certificado firmado por una tercera CA, y así sucesivamente. De esta forma, se puede establecer una jerarquía de autoridades de certificación, donde las CA de nivel más bajo emiten los certificados de usuario, y las CA de cada nivel son certificadas por una de nivel superior.

La Recomendación X.509, además de definir el formato de los certificados, también define otra estructura llamada lista de revocación de certificados o CRL. Una lista de este tipo sirve para publicar los certificados que han dejado de ser válidos antes de su fecha de caducidad. Los motivos pueden ser diversos: se ha emitido otro certificado que sustituye al revocado, ha cambiado el DN del titular (por ejemplo, ha dejado de trabajar en la empresa en la que estaba), le han robado su clave privada, etc.

De este modo, si queremos asegurarnos completamente de la validez de un certificado, no basta con verificar su firma, sino que debemos obtener la versión actual de la CRL (publicada por la CA que emitió el certificado) y comprobar que el certificado no aparece en esta lista. Una CA normalmente actualizará su CRL de forma periódica, añadiendo cada vez los certificados que hayan sido revocados. Cuando llegue la fecha de caducidad que constaba en el certificado, ya no será necesario volver a incluirlo en la CRL. Esto permite que las CRL no crezcan indefinidamente.

En este capítulo hemos visto que las técnicas criptográficas permiten cifrar un texto mediante una clave de cifrado, y solamente quien conozca la clave de descifrado correspondiente será capaz de obtener el texto original.

Según la relación que haya entre las dos claves, los algoritmos criptográficos se clasifican en algoritmos simétricos si la clave de cifrado y la de descifrado son la misma, o algoritmos de clave pública si las claves son distintas. Los algoritmos simétricos, a su vez, se pueden clasificar en algoritmos de cifrado en flujo, si el cifrado consiste en añadir al texto datos pseudoaleatórios calculados a partir de la clave, o algoritmos de cifrado en bloque, si el cifrado se realiza sobre bloques de medida fija del texto original.

La particularidad de la criptografía de clave pública es que a partir de la clave pública es prácticamente imposible deducir la clave privada. Esto permite que cualquiera que conozca la clave pública de un usuario pueda usarla para cifrar datos confidenciales, con la seguridad que solamente quien tenga la clave privada correspondiente podrá descifrarlos, y sin necesidad de acordar ninguna clave secreta a través de un canal seguro. El uso de las claves al revés (la privada para cifrar y la pública para descifrar) es la base de las firmas digitales.

Dado que la criptografía de clave pública es computacionalmente más costosa que la simétrica, no se utiliza nunca directamente para obtener confidencialidad, si no siempre a través de una clave de sesión simétrica. Del mismo modo, la firma de un texto no se calcula directamente a partir del texto, si no aplicándole una función hash segura. La propiedad de este tipo de función es que es muy difícil encontrar un mensaje que de el mismo hash que otro.

Para garantizar que las claves públicas son auténticas, y pertenecen a quien se supone que han de pertenecer, se pueden utilizar certificados digitales o de clave pública, como por ejemplo los certificados X.509. Cuando una autoridad de certificación (CA) firma un certificado, está dando fe de la

autenticidad entre el vínculo entre de la clave pública correspondiente y la identidad del usuario. Los certificados son un componente básico de la infraestructura de clave pública (PKI), como también lo son las listas de revocación de certificados (CRL). Las firmas digitales proporcionan el servicio de autenticación de mensaje. Los llamados códigos MAC también proporcionan este servicio, pero utilizando claves secretas compartidas en lugar de claves públicas.

Otro servicio de autenticación es el de autenticación de entidad. Este mecanismo permite comprobar que la otra parte de la comunicación es quien dice ser, y no un impostor. Esto se puede conseguir con técnicas de autenticación débil basadas en contraseñas o, si es necesario, con técnicas de autenticación fuerte basadas en protocolos de reto-respuesta, que a diferencia de las anteriores son resistentes a muchos más ataques que las primeras.

10.7 PREGUNTAS Y TIPS

- **¿Cuál es el estándar de certificados digitales que se utiliza en el marco PKI?** X.509 v3
- **¿Cuáles son características de una Función de Hash?** El valor de salida debe tener un tamaño fijo, Debe encontrarse libre de colisiones
- **¿A qué algoritmo de encriptación se lo considera una extensión directa de Diffie Hellman?** El Gamal
- **¿Cuál es la dificultad computacional de romper un cifrado RSA?** Factorizar números primos de gran tamaño
- **¿Cuál es el tipo de algoritmo de encriptación, donde la clave utilizada para el cifrado de un mensaje es la misma que se emplea para descifrar éste?** Simétricos
- **¿Cómo se conoce al conjunto de: Algoritmos, Texto Claro, Texto Cifrado y Clave?** Criptosistema
- **¿Cómo se denomina al chip cifrador que se utilizaba como parte del proyecto Key Escrow?** Clipper chip
- **¿Cuál es la utilización práctica del algoritmo Diffie Hellman?** Intercambio de claves simétricas
- **¿Cuáles son las técnicas que se combinan en un proceso de Firma Digital?** Criptografía asimétrica, Funciones de Hash
- **¿Cuáles son las longitudes efectivas de las claves AES?** 128, 192 y 256 bits
- **¿Qué tipo de seguridad se produce cuando se conoce un mensaje cifrado y no es posible por ningún medio conocer el mensaje original a partir de éste?** Seguridad Incondicional
- **¿Cuál es el tipo de algoritmo de encriptación en que el texto en claro es cifrado símbolo tras símbolo?** Flujo
- **¿Cuál es la longitud efectiva de una clave DES?** 56 bits
- **¿Cuál es el código de identificación de la sintaxis estándar de intercambio de información personal?** PKCS #12
- **¿Cuál es la principal limitación de los algoritmos de encriptación simétricos?** Distribución de la clave secreta
- En la firma electrónica, la identificación del firmante es posible gracias a el cifrado asimétrico
- Un certificado electrónico reconocido es un documento documento electrónico emitido por un prestador de servicios de certificación autorizado, acreditado y reconocido (que cumpla con los requisitos de la ley de firma electrónica)

CAPÍTULO 11

11.1 TÚNELES Y VPN

¿Qué es una VPN? Es una red privada implementada sobre una red pública o semipública, valiéndose de protocolos de encriptación y encapsulamiento que permiten interconectar los dos extremos de manera segura.

¿Por qué utilizar una VPN sobre una red pública? En general nos permiten un ahorro de costos de telecomunicaciones reemplazando las tecnologías tradicionales (Punto a Punto, Frame Relay, etc) que contratamos a los Carriers para unir dos puntos a larga distancia e incluso internacionales, garantizando confiabilidad e integridad a los datos transportados.

¿Cuáles son los protocolos más conocidos en las implementaciones de túneles?

- PPTP (Point to Point Tunneling Protocol)
- GRE (Generic Routing Encapsulation)
- L2TP (Layer 2 Tunneling Protocol)
- L2F (Layer 2 Fordwarding)
- IPSec (IP Security)

¿Qué protocolos agrupa IPSec? Este protocolo está integrado por un conjunto de estándares abiertos que garantizan la confidencialidad, integridad, autenticación del orígen, el intercambio de claves y anti-replay. Estos protocolos son:

- AH (Authentication Header)
- ESP (Encapsulating Security Payload)
- IKE (Internet Key Exchange)

¿Cuál es la diferencia de implementar IPSec en modo túnel o modo transporte? En el modo túnel se encapsula el datagrama original en un nuevo datagrama, el cual posee las direcciones IP de los gatways IPSec que mantienen el túnel, en cambio en el modo transporte, la seguridad es de extremo a extremo, donde solamente se asegura la carga útil del datagrama IP, puesto que se mantiene la cabecera IP original.

¿Qué es una Asociación de Seguridad (SA)? Representa un conjunto de políticas y claves utilizadas para proteger los datos involuncrados en una comunicación IPSec. Dentro de la SA se definen los algoritmos a emplear, las claves de autenticación, la definición del tráfico al que se debe aplicar y el protocolo y el modo a utilizar.

Muy atrás en el tiempo, han quedado aquellos primeros inicios en la historia de la informática, en donde el requerimiento fundamental por parte de un ambiente de cómputo, se encontraba relacionado con la posesión de un gran servidor o “computador principal” para satisfacer las necesidades de cálculo de una organización.

Este viejo modelo, fue reemplazado rápidamente, por otro que considera un número grande de

computadores separados pero interconectados, que efectúan el mismo trabajo, dando lugar al nacimiento de las redes informáticas. Pero el crecimiento que han sufrido las redes informáticas en los últimos años, ha superado cualquier expectativa al respecto. Un claro ejemplo, se encuentra dado por Internet, una red de redes de alcance mundial, que ha logrado convertirse en tan solo unos años, en uno de los instrumentos de comunicación más preciados de la edad moderna. Hoy en día, muchos de los servicios que utilizamos comúnmente, requieren de algún tipo de interconexión para poder funcionar eficientemente. Empleados que trabajan desde sus hogares, dispositivos móviles, teléfonos IP y una amplia gama de componentes de red, han pasado a convertirse en una realidad cotidiana. Pero el concepto de redes e interconexión, no necesariamente se encuentra relacionado con la seguridad o privacidad de los datos que sobre ellas se transfieren, de hecho puesto que las redes fueron pensadas originalmente, con el objeto de "compartir información", características tales como la seguridad, no han sido parte integral de su diseño. En las próximas secciones, veremos algunas de las tecnologías actuales, que permiten afrontar el desafío de interconectar redes, en forma segura y confiable.

Con el paso del tiempo, la complejidad en torno al diseño e implementación de redes, ha aumentado considerablemente. Empresas de todos los tamaños, han visto en Internet y las tecnologías que la soportan, una forma atractiva de solucionar sus problemas de comunicación, o transformar la manera en la que hacen negocios con sus clientes y proveedores. Debido en parte a estos hechos, y en función de otorgar diferentes esquemas de seguridad, al conjunto de redes interconectadas entre sí, ha surgido la necesidad de referirnos a ellas en función de la zona a la que pertenecen:

- **Internet:** Internet, es una red pública y global. Pública, porque puede ser utilizada por cualquier persona, a través del servicio provisto por alguno de los grandes proveedores de acceso a la misma y Global, debido a que conecta a miles de computadores alrededor del mundo. De acuerdo a sus características, Internet es un ambiente de trabajo sobre el cual debemos asumir, que no tenemos control alguno respecto de quiénes y cómo la utilizan. El usuario del otro lado, puede ser un potencial cliente, o un avezado atacante. En definitiva, no tendremos ninguna manera de conocer esta situación, al menos que estemos monitoreando sus acciones, en forma constante.
- **Intranet:** Se denomina Intranet a aquellas redes privadas, que siendo implementadas y mantenidas por una compañía u organización individual, utilizan como parte de su funcionamiento, las mismas tecnologías en las que se basa Internet. A diferencia de lo que sucede con esta última, el acceso a una Intranet, se limita a los sistemas incluidos dentro de la misma. Si bien es cierto, que frecuentemente, suele verse Intranets conectadas con Internet, los recursos situados dentro del ámbito de la Intranet, no se encuentran disponibles para el acceso a los usuarios, a los que no se autorice expresamente. Dicho de otra forma, el acceso a una Intranet, se concede a los usuarios confiados dentro de la red corporativa, o usuarios de la misma en posiciones remotas.
- **Extranet:** Una Extranet expande las posibilidades de conectividad de su Intranet, más allá de los límites de su propia organización, convirtiéndola en una red semi-privada. La implementación de una Extranet, brinda la posibilidad de conectar un socio de negocios u otra organización digna de confianza, por medio de una red privada, o de una conexión que utilice un canal de comunicaciones seguro, a través de Internet. Podría decirse que una Extranet es una WAN privada, pero que trabaja con protocolos abiertos no propietarios o, en otras palabras, sería como la interconexión de Intranets de diferentes empresas, que se encuentran bajo administraciones distintas.

11.1.1 Antecedentes de las VPN

En el transcurso de los últimos años, la implementación de VPNs, se ha vuelto un hecho sumamente popular. Alentadas en parte, por la potencialidad que brinda Internet, como red pública portadora, estas redes privadas virtuales, se han convertido en una herramienta fundamental, a la hora de servir de vínculo de comunicación seguro a empresas de todos los tamaños. Pero si bien es cierto, que

estas implementaciones incluyen nuevos protocolos y novedosas funcionalidades, el concepto detrás de VPN, lleva unos cuantos años junto a nosotros.

En un principio, aquellas empresas que requerían establecer algún tipo de comunicación de datos con sus socios de negocio, casa matriz o sucursales, recurrían a complejas y costosas soluciones que involucraban “Enlaces Dedicados” o redes del tipo “Frame Relay”, mediante los cuales conformaban generalmente, un esquema del tipo WAN (Redes de Área Amplia). De la misma forma, aquellos agentes o empleados que por sus tareas, debían realizar conexiones remotas a su sede central, veían en la implementación de sistemas del tipo Dial-Up o de acceso discado, la solución a su problema. En los últimos años, hemos sido testigos de algunos cambios que han permitido, que redes WAN evolucionen hacia soluciones VPN “Site to Site”, accesos discados se transformen en sistemas del tipo “Remote Access VPN” y comunicaciones de voz y video (V3PN) comiencen a reemplazar en algunos casos, parte del tráfico de la red telefónica tradicional.

Una Red Privada Virtual (VPN), no es más que una “red privada de comunicaciones, implementada sobre una infraestructura pública” . Valiéndose de diferentes tecnologías entre las que se cuentan protocolos de comunicación, servicios de encriptación y encapsulamiento, una VPN crea un pasillo privado a través de una red pública, con el objeto de interconectar dos extremos en forma segura. Probablemente el ejemplo más claro de su aplicación, se encuentre dado por implementaciones de este tipo a través de Internet, puesto que debido a su amplia extensión a nivel mundial, esta Red de Redes, permite extender el alcance de nuestra red local, de forma excepcional. Para llevar a cabo su función de manera segura, es necesario que una VPN provea los medios necesarios, a la hora de garantizar aspectos tales como la autenticación, integridad y confidencialidad de los datos que la atraviesan .

Funcionamiento Básico de una VPN:

- El usuario remoto llama a su ISP local y se conecta a la red del ISP de forma normal.
- Cuando requiere conectarse a la red corporativa, el usuario inicia el túnel enviando una petición a un servidor VPN de la red corporativa.
- El servidor VPN autentifica al usuario y crea el otro extremo del túnel.
- El usuario comienza a enviar datos a través del túnel, los cuales generalmente son cifrados por el software VPN (del cliente) antes de ser enviados sobre la conexión del ISP.
- En el destino, el servidor VPN recibe los datos y los descifra, re-enviando los datos hacia la red corporativa. Cualquier información enviada de vuelta al usuario remoto también es cifrada antes de enviarse por Internet, tarea que recae sobre el extremo contrario al cliente.

11.1.2 Ventajas y limitaciones de una VPN

Está claro que al momento de realizar cualquier tipo de implementación, un profesional deberá efectuar el análisis necesario respecto de la relación costo beneficio de su proyecto. A tal efecto es bueno conocer las ventajas y limitaciones respecto de la tecnología de VPN.

Ventajas

- Bajo Costo
- Baja Inversión Inicial
- Accesibilidad
- Escalabilidad
- Seguridad Integrada

Limitaciones

- Sobrecarga del Cliente
- Complejidad de Tráfico
- Dependencia de medios NO fiables

11.1.3 Configuraciones y Protocolos utilizados en las VPN

- En las VPN entre intranets, la situación más habitual es que en cada intranet hay una pasarela VPN, que conecte la red local con Internet. Esta pasarela se comunica con la de las otras intranets, aplicando el cifrado y las protecciones que sean necesarias a las comunicaciones de pasarela a pasarela a través de Internet. Cuando los paquetes llegan a la intranet de destino, la pasarela correspondiente los descifra y los reenvía por la red local hasta el ordenador que los tenga que recibir. De esta manera es utiliza la infraestructura pública de Internet, en lugar de establecer líneas privadas dedicadas, que supondrían un coste más elevado. También se aprovecha la fiabilidad y redundancia que proporciona Internet, ya que si una ruta no está disponible siempre se pueden encaminar los paquetes por otro camino, mientras que con una línea dedicada la redundancia supondría un coste aún más elevado.
- En las VPN de acceso remoto, a veces llamadas VPDN, un usuario se puede comunicar con una intranet a través de un proveedor de acceso a Internet, utilizando tecnología convencional como por ejemplo a través de un módem ADSL. El ordenador del usuario ha de disponer de software cliente. VPN para comunicarse con la pasarela VPN de la intranet y llevar a cabo la autenticación necesaria, el cifrado, etc. De este modo también se aprovecha la infraestructura de los proveedores de Internet para el acceso a la intranet, sin necesidad de llamadas a un módem de la empresa, que pueden llegar a tener un coste considerable.
- El caso de las VPN extranet puede ser como el de las VPN entre intranets, en que la comunicación segura se establece entre pasarelas VPN, o bien como el de las VPN de acceso remoto, en que un cliente VPN se comunica con la pasarela de la intranet. La diferencia, pero, es que en este caso normalmente el control de acceso es más restrictivo para permitir solamente el acceso a los recursos autorizados.

La definición de una red virtual lleva a cabo mediante el establecimiento de túneles, que permiten encapsular paquetes de la red virtual, con sus protocolos, dentro de paquetes de otra red, que normalmente es Internet, con su protocolo, es decir IP. Para la comunicación entre las distintas intranets, o entre el ordenador que accede remotamente y la intranet, se pueden utilizar los protocolos que sean más convenientes. Los paquetes de estos protocolos, para poderlos hacer llegar a su destino a través de Internet, se pueden encapsular en datagramas IP, que dentro suyo contendrán los paquetes originales. Cuando lleguen a su destino, se desencapsulan estos datagramas para recuperar los paquetes con el formato “nativo” del protocolo correspondiente.

Hay protocolos que pueden ser utilizados para establecer los túneles, dependiendo del nivel de la comunicación al cual se quiera realizar la protección.

Túneles a nivel de red. El protocolo utilizado en la gran mayoría de configuraciones VPN es IPsec en modo túnel, generalmente con ESP par cifrar los datos, y opcionalmente con AH para autenticar los paquetes encapsulados. Las pasarelas VPN son, en este caso, pasarelas seguras Ipsec.

Túneles a nivel de enlace. En el caso de las VPN de acceso remoto o VPDN, existe la posibilidad de encapsular tramas PPP, que son las que transmite normalmente un cliente VPN de este tipo, sobre datagramas IP. Hay diversas

11.1.4 VPN por Internet

Como mencionáramos en una sección anterior, probablemente haya sido Internet el disparador a partir del cual el concepto detrás de VPN se haya hecho tan popular. Y no es para menos, Internet se ha convertido en la red pública más importante de todos los tiempos. Hoy día, muy probablemente encuentre algún proveedor deseoso de brindarle acceso, en el lugar donde usted lo requiera. Hasta hace algunos años, cuando se requería comunicar oficinas distantes o sucursales, la única opción pasaba, dependiendo de la distancia que separara los puntos, por recurrir a la instalación de líneas dedicadas o enlaces por satélite. Con el advenimiento de Internet, sólo faltaba resolver los temas relacionados con la seguridad en la transmisión de datos, cuestiones que las VPN, han sabido resolver a la perfección. En la actualidad, el bajo costo de accesos de banda ancha a Internet, clientes VPN integrados en los sistemas operativos más utilizados, y equipos de networking con posibilidades de VPN "All in One", han transformado la implementación de este tipo de soluciones, en algo verdaderamente accesible desde el punto de vista económico y sencillo en relación a los requerimientos iniciales.

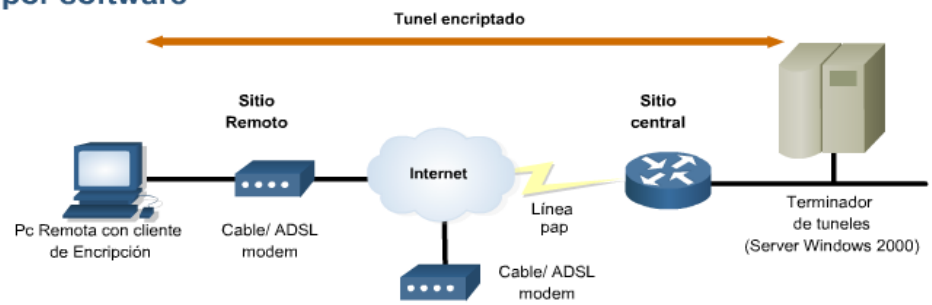
Pero no todo son buenas noticias cuando la idea es montar VPNs sobre Internet. A diferencia de lo que sucede en las redes privadas o los accesos dedicados, Internet, debe ser contemplada como una red "No Fiable". La volatilidad del ancho de banda efectivo, así como las interrupciones de servicio, o sencillamente la "libertad" subyacente a su concepción, sumado a que no se trata de "otra" red bajo nuestro control, hacen que debamos ser sumamente cuidadosos a la hora de decidir que "Nivel de Servicio" esperamos brindar con este tipo de soluciones.

11.1.5 Implementaciones y Outsourcing

Si bien en su generalidad, solemos referirnos a las VPN tal como una red privada de comunicaciones, implementada sobre una infraestructura pública, lo cierto es que desde el punto de vista de su implementación, podemos identificar al menos dos grandes categorías o modos, dependiendo de su propósito o aplicación.

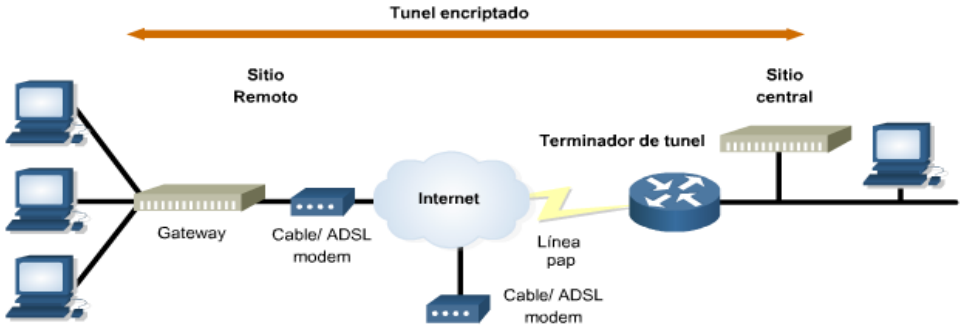
- **Remote Access VPN:** Las VPN de Acceso Remoto, suelen ser consideradas la evolución natural de aquel tipo de conexiones Dial-Up tan frecuentemente utilizadas. Suelen ser la solución acertada a la hora de asegurar las conexiones de usuarios móviles, tele-trabajadores o cualquier otro tipo de usuario tradicional, que desee aprovechar a la hora de establecer conexiones con sus redes corporativas, las ventajas brindadas por los clientes VPNs que acompañan la mayoría de los sistemas operativos tradicionales. En este tipo de VPN, generalmente un usuario establece un vínculo a través de Internet por intermedio de su ISP (Internet Service Provider), para luego poner en funcionamiento el cliente instalado en su estación de trabajo remota, el cual en conjunto con un dispositivo alojado en el mismo proveedor o en el extremo correspondiente a su compañía actuando como terminador, permite establecer la denominada "Red Privada Virtual".
- **LAN-to-LAN VPNs:** Las VPNs LAN-to-LAN, suelen ser implementadas, a fin de establecer un vínculo seguro y confiable entre redes de distintas organizaciones (extranet VPN, interconectando clientes, proveedores, socios de negocios, etc.), o bien entre redes distantes de una misma organización (Intranet VPN, interconectando oficinas centrales, oficinas remotas, etc.). En ambos casos, este tipo de conexión representa una evolución respecto de la utilización de "Líneas Punto a Punto" o del tipo "Frame Relay". De hecho, una VPN LAN-to-LAN o Site-to-Site, suele ser referida como una extensión de las clásicas redes WAN. Por lo general, una VPN de este tipo, requiere de Routers, Firewalls o Concentradores VPN, para ser construida.

VPN por software



En la actualidad, una VPN puede ser implementada mediante Software, Hardware o una combinación de ambos. Sistemas operativos como Windows 2000/2003, incorporan su propio servidor VPN, mientras que implementaciones como FreeSWAN, significan su contrapartida por parte del software libre. De la misma forma, cada vez son más los ISP que, con el objetivo de brindar un servicio diferencial a sus clientes, promocionan la tercerización de distintos tipos de implementaciones VPNs. De esta manera, es posible deslindar en ellos responsabilidades tales como el armado de túneles sobre sus propios backbone o nodos. En caso de estar pensando en esta posibilidad, debería tener en cuenta, cuál es el grado de privacidad que le ha llevado a pensar en una solución VPN, y en caso de que éste sea alto… por qué querría usted tercerizar este servicio.

VPN por hardware



11.1.6 Tunelización

Las redes privadas virtuales, habilitan como parte de su funcionamiento, la creación de túneles o conductos dedicados de un sitio a otro. La tecnología de túneles, comúnmente referida como “Tunneling”, representa un método válido al momento de transferir datos entre dos redes similares sobre una red intermedia diferente. Por medio de una técnica conocida como "encapsulación", estos túneles, suelen tener la capacidad de encerrar un tipo de paquete de datos, dentro del paquete de otro protocolo (Generalmente TCP/IP), y en el caso particular de los túneles VPN, proceder a la encriptación de los datos transmitidos a través del mismo, de forma tal que en caso de que se produzca algún tipo de intercepción sobre la red pública subyacente, estos resulten ilegibles a los ojos del atacante.

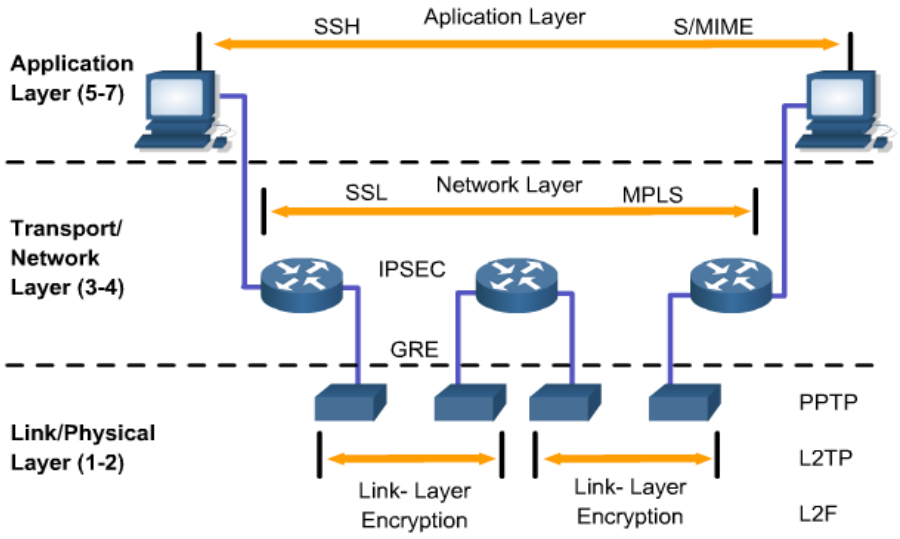
De acuerdo con este procedimiento, los paquetes encapsulados viajan a través de Internet o cualquier otro tipo de red pública, hasta que alcanzan su destino. Una vez allí, se separan y vuelven a su formato original. En resumen, un túnel podría ser definido como la senda o recorrido lógico, que siguen las PDUs de un protocolo (encapsulado en otro) atravesando una red pública.

Si bien es cierto que los túneles suelen ser parte fundamental de las tecnologías VPN, han existido desde hace mucho tiempo. Solo por citar un ejemplo, el tunelizado de protocolos tales como SNA e

IPX, se ha utilizado y se sigue utilizando con éxito en varias implementaciones. De igual forma, MBone hace uso de túneles multicast sobre una red unicast, así como 6Bone hace lo propio con túneles IPv6 sobre redes Ipv4. Respecto de su funcionamiento, con frecuencia, los túneles suelen ser establecidos en las capas 2 y 3 debido sobre todo a que ésto los hace independientes del medio, aunque SSH y S/MIME en capa 7 y SSL/TSL en capa 4, nos muestran la existencia de otras alternativas. Por su parte, aspectos tales como las fases (establecimiento / encapsulado) y los elementos que componen un túnel (Protocolo del carrier, Protocolo de encapsulamiento y Protocolo pasajero) , suelen ser características propias de esta tecnología.

En la actualidad, suele ser común referirse a las tecnologías de tunneling de acuerdo también, a su modo de generación. De esta forma, se distingue entre “Túneles Voluntarios” o “Túneles Obligatorios”.

- **Tuneles voluntarios**: Estos corredores se forman entre ordenadores de usuario o corredores de enrutamiento que utilizan software que actúa como agente cliente para establecer una conexión virtual contra un servidor virtual que tiene la función de ser el destino de la comunicación. En este caso, tanto los clientes como los servidores finales han de tener instalados y configurados los protocolos con los que entubat el camino, ya se en conexiones de tipo serie o por red. Una ventaja añadida a esta modalidad, es que las máquinas implicadas (finales e intermedias) pueden ser de propósito general y no estar espesíficamente diseñadas para operar con VPN
- **Tuneles obligatorios**: Cuando se utilizan dispositivos dedicados es cuando se habla de tunelización obligatoria o impuesta, donde los servidores de destino están diseñados con capacidad para generar el tunel al recibir la comunicación del cliente. Estos dispositivos reciben el nombre de Procesadores Front End (FEP) cuando emplean el protocolo PPTP; Concentrador de Acceso (LAC), cuando trabajan con L2TP; o pasarela de seguridad IP cuando emplean IPSec en su funcionamiento.



11.2 OpenVPN

OpenVPN es una solución de conectividad basada en software: SSL (Secure Sockets Layer) VPN Virtual Private Network (red virtual privada), OpenVPN ofrece conectividad punto-a-punto con validación jerárquica de usuarios y host conectados remotamente, resulta una muy buena opción en tecnologías Wi-Fi (redes inalámbricas EEI 802.11) y soporta una amplia configuración, entre ellas balanceo de cargas entre otras. Está publicado bajo la licencia GPL, de software libre. OpenVPN, es un excelente producto de software creado por James Yonan en el año 2001 y que ha estado siendo

mejorado desde entonces. Ninguna otra solución ofrece una mezcla semejante de seguridad a nivel empresarial, seguridad, facilidad de uso y riqueza de características. Es una solución multiplataforma que ha simplificado mucho la configuración de VPN's dejando atrás los tiempos de otras soluciones difíciles de configurar como IPsec y haciéndola más accesible para gente inexperta en este tipo de tecnología.

OpenVPN es una excelente nueva solución para VPN que implementa conexiones de capa 2 o 3, usa los estándares de la industria SSL/TLS para cifrar y combina todos las características mencionadas anteriormente en las otras soluciones VPN. Su principal desventaja por el momento es que hay muy pocos fabricantes de hardware que lo integren en sus soluciones. De todos modos no hay que preocuparse siempre que contemos con un Linux en el cual podremos implementarlo sin ningún problema mediante software. Para cifrar datos se usan Passwords o claves de cifrado.OpenVPN tiene dos modos considerados seguros, uno basado en claves estáticas pre-compartidas y otro en SSL/TLS usando certificados y claves RSA. Cuando ambos lados usan la misma clave para cifrar y descifrar los datos, estamos usando el mecanismo conocido como “clave simétrica” y dicha clave debe ser instalada en todas las máquinas que tomarán parte en la conexión VPN. Si bien SSL/TLS + claves RSA es por lejos la opción más segura, las claves estáticas cuentan con la ventaja de la simplicidad.

Ventajas: OpenVPN provee seguridad, estabilidad y comprobados mecanismos de cifrado sin sufrir la complejidad de otras soluciones VPN como las de Ipsec.

Además ofrece ventajas que van más allá que cualquier otra solución como ser:

- Posibilidad de implementar dos modos básicos, en capa 2 o capa 3, con lo que se logran túneles capaces de enviar información en otros protocolos no-IP como IPX o broadcast (NETBIOS).
- Protección de los usuarios remotos. Una vez que OpenVPN ha establecido un túnel el firewall de la organización protegerá el laptop remoto aun cuando no es un equipo de la red local. Por otra parte, solo un puerto de red podrá ser abierto hacia la red local por el remoto asegurando protección en ambos sentidos.
- Conexiones OpenVPN pueden ser realizadas a través de casi cualquier firewall. Si se posee acceso a Internet y se puede acceder a sitios HTTPS, entonces un túnel OpenVPN debería funcionar sin ningún problema.
- Soporte para proxy. Funciona a través de proxy y puede ser configurado para ejecutar como un servicio TCP o UDP y además como servidor (simplemente esperando conexiones entrantes) o como cliente (iniciando conexiones).
- Solo un puerto en el firewall debe ser abierto para permitir conexiones, dado que desde OpenVPN 2.0 se permiten múltiples conexiones en el mismo puerto TCP o UDP.
- Las interfaces virtuales (tun0, tun1, etc.) permiten la implementación de reglas de firewall muy específicas.
- Todos los conceptos de reglas, restricciones, reenvío y NAT10 pueden ser usados en túneles OpenVPN.
- Alta flexibilidad y posibilidades de extensión mediante scripting. OpenVPN ofrece numerosos puntos para ejecutar scripts individuales durante su arranque.
- Soporte transparente para IPs dinámicas. Se elimina la necesidad de usar direcciones IP estáticas en ambos lados del túnel.
- Ningún problema con NAT. Tanto los clientes como el servidor pueden estar en la red usando solamente IPs privadas.
- Instalación sencilla en cualquier plataforma. Tanto la instalación como su uso son increíblemente simples.

Diseño modular. Se basa en un excelente diseño modular con un alto grado de simplicidad tanto en seguridad como red.

Desventajas

- No tiene compatibilidad con IPsec que justamente es el estándar actual para soluciones VPN.
- Falta de masa crítica.
- Todavía existe poca gente que conoce como usar OpenVPN.
- Al día de hoy sólo se puede conectar a otras computadoras. Pero esto está cambiando, dado que ya existen compañías desarrollando dispositivos con clientes OpenVPN integrados.

Comparación entre OpenVPN e IPSec VPN

IPSec	OpenVPN
Estándar de la tecnología VPN	Aun desconocida y no compatible con IPsec
Plataformas de hardware (dispositivos, aparatos)	Solo en computadoras, pero en todos los sistemas operativos disponibles
Tecnología conocida y probada	Tecnología nueva y aun en crecimiento
Muchas interfaces gráficas disponibles	Sin interfaces gráficas profesionales, aunque ya existen algunos proyectos prometedores
Modificación compleja del stack IP	Tecnología sencilla
Necesidad de modificaciones críticas al kernel	Interfaces de red y paquetes estandarizados
Necesidad de permisos de administrador	Ejecuta en el espacio del usuario y puede ser chroot-ed
Diferentes implementaciones de distintos proveedores pueden ser incompatibles entre si	Tecnologías de cifrado estandarizadas
Configuración compleja y tecnología compleja	Facilidad, buena estructuración, tecnología modular y facilidad de configuración
Curva de aprendizaje muy pronunciada	Fácil de aprender y éxito rápido para principiantes
Necesidad de uso de muchos puertos y protocolos en el firewall	Utiliza solo un puerto del firewall
Problemas con direcciones dinámicas en ambas puntas	Trabaja con servidores de nombres dinámicos como DynDNS o No-IP con reconexiones rápidas y transparentes
Problemas de seguridad de las tecnologías IPsec	SSL/TLS como estándar de criptografía
	Control de tráfico (Traffic shaping)
	Velocidad (más de 20 Mbps en máquinas de 1Ghz)
	Compatibilidad con firewall y proxies
	Ningún problema con NAT (ambos lados puede ser redes NATeadas)
	Posibilidades para hackers y road warriors

11.3 PPTP

Sin lugar a dudas, en el ámbito de las redes de acceso remoto y VPNs, nada hubiera sido igual, sin el desarrollo de PPTP. Las siglas con las que se identifica este protocolo, se corresponden con su nombre en Inglés: "*Point-to-Point Tunneling Protocol"* y su concepción se atribuye a un consorcio de empresas, conformado por: Microsoft, P.Ascen Communications, 3Com, Primary Access, ECI Telematics y US.Robotics, entre otros.

Publicado en Julio de 1999 bajo el RFC 2637, PPTP se presenta como un protocolo que permite el intercambio seguro de datos, proveyendo soporte multi-protocolo, autenticación y cifrado, a la vez que extiende las posibilidades provistas hasta el momento por PPP (Point-to-Point Protocol. RFC 1171), al encapsular paquetes PPP en datagramas IP (utilizando una versión extendida de GRE) y posibilitar su transmisión en redes TCP/IP. El objetivo detrás del diseño de PPTP, fue el de obtener un protocolo simple, que brindara compatibilidad multiprotocolo y que tuviera la capacidad de cruzar una amplia gama de redes IP.

Uno de los aspectos que más han contribuido a la utilización de PPTP, es sin lugar a dudas la aceptación que el mismo ha tenido en la industria (de la cual forman parte alguna de las empresas que a su vez desarrollaron este protocolo). Sistemas operativos como Windows 98SE, Windows NT 4.0 y Windows 2000, tanto en sus versiones de escritorio como servidor, lo incluyen como parte de su instalación, provocando de esta forma, la disponibilidad casi inmediata de un cliente en cada uno de los equipos en los cuales se haya instalado alguno de estos sistemas operativos. De la misma forma, y a pesar de que muchas veces se lo ha considerado como un protocolo propiedad de Microsoft, existen varios clientes y servidores PPTP para gran parte del resto de los sistemas operativos (Linux, FreeBSD, NetBSD y OpenBSD).

Más allá de su disponibilidad en gran parte de los escritorios, puesto que PPTP es capaz de brindar comunicaciones encriptadas sobre las estructuras de comunicaciones existentes como PSTNs (Public Switched Telephone Networks) e Internet, su uso se ha extendido hasta convertirlo en algún momento, en uno de los protocolos preferidos a la hora de implementar las primeras VPNs. Si bien es cierto que una de las fortalezas de PPTP, es su utilización junto a PPP para establecer un primer vínculo a través de un módem y línea telefónica, sobre el cual finalmente montar PPTP, su uso podría ser requerido en redes internas o LANs, en cuyo caso no haría falta el establecimiento de conexión brindado por PPP, sino que la VPN podría ser establecida localmente vía PPTP contra un servidor en la misma red interna. Este tipo de implementación puede carecer de sentido en algunos casos, aunque la capacidad de soportar múltiples protocolos (IP, IPX y NetBEUI) puede ser un fin en sí mismo.

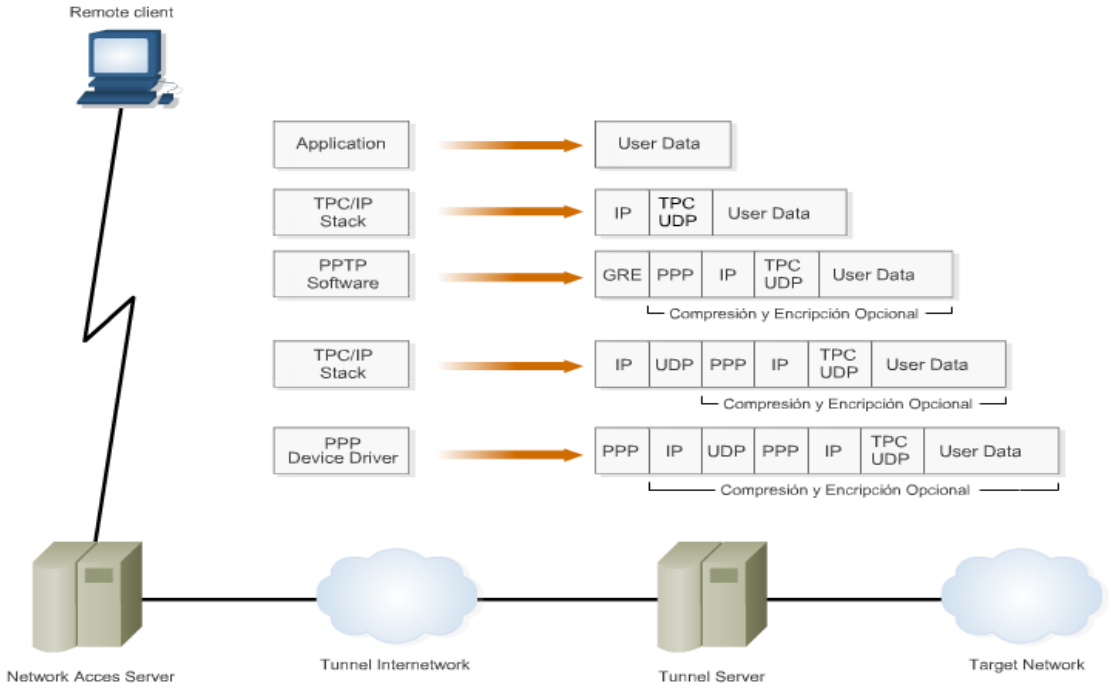
11.3.1 Proceso de conexión y funcionamiento

A pesar de sus amplias posibilidades, un escenario típico en el cual PPTP suele ser implementado, es aquel en donde un cliente establece una conexión dial-up con el servidor de acceso a la red (NAS) del proveedor del servicio, por medio de PPP. En este tipo de esquema, una vez conectado, el cliente establecerá una segunda conexión con el servidor PPTP el cual estará situado en la red privada. Dicho servidor será utilizado como intermediario de la conexión, recibiendo los datos del cliente externo y transmitiéndolos al correspondiente destino en la red privada. PPTP encapsula, como parte de su funcionamiento, paquetes PPP que contienen los datos en datagramas IP, para lo cual se vale del protocolo GRE, el cual se verá en detalle más adelante. Una vez que los datagramas llegan al servidor PPTP, son desensamblados con el fin de obtener el paquete PPP y desencriptados de acuerdo al protocolo de red transmitido (recordando la naturaleza multi protocolo de PPTP).

El protocolo PPTP especifica además una serie de mensajes de control con el fin de establecer, mantener y destruir el túnel PPTP previamente generado. Estos mensajes son transmitidos en paquetes de control en el interior de segmentos TCP. De este modo, los paquetes de control almacenan la cabecera IP, la cabecera TCP, el mensaje de control PPTP y los trailers apropiados.

La autenticación PPTP se basa en un sistema de acceso en el cual todos los clientes, deben

proporcionar un conjunto de usuario / contraseña. La autenticación remota de clientes PPTP es realizada empleando los mismos métodos de autenticación utilizados por cualquier otro tipo de servidor de acceso remoto (RAS). En el caso de Microsoft, la autenticación utilizada para el acceso a los RAS soporta los protocolos CHAP, MS-CHAP y PAP.



Referido a la encriptación de datos, PPTP utiliza el proceso de encriptación de “secreto compartido” en el cual sólo los extremos de la conexión comparten la clave. Dicha clave es generada empleando el estándar RC4 a partir de la contraseña del usuario. La longitud de dicha clave puede ser de hasta 128-bits.

11.3.2 Ventajas y limitaciones

Quizás una de las ventajas más apreciadas de PPTP, radica en el hecho de que reduce o elimina, casi por completo, la necesidad de uso de sofisticados y caros equipos de telecomunicaciones, a la vez que permite conexiones de equipos remotos haciendo uso de la red telefónica convencional de forma segura. Por otra parte, este protocolo es ampliamente soportado por la plataforma Windows de Microsoft, a la vez que existen clientes y servidores implementados en Linux, FreeBSD, etc. Esta característica, lo hace sumamente interesante al momento de implementar VPNs de bajo costo, utilizando a tal efecto, el software que se encuentra disponible en la mayoría de las empresas y clientes remotos. De la misma forma, su posibilidad multiprotocolo, hace de PPTP una opción sumamente atractiva en aquellos casos donde existe necesidad de conectar redes de protocolos disímiles. En contraposición a las ventajas observadas, sin dudas su limitación más importante, se encuentre relacionada con algunas falencias de seguridad tanto en su diseño, como en algunas de sus implementaciones, las cuales con el paso del tiempo, han vuelto a este protocolo menos seguro y algo obsoleto en relación a nuevas propuestas, como por ejemplo L2TP.

11.3.3 Consideraciones sobre seguridad

Puesto que el tráfico generado en una comunicación PPTP, utiliza por defecto el puerto destino TCP 1723, y puede ser identificado por el protocolo 47 (IP), se facilita su implementación al momento de

configurar routers y cortafuegos, al tener que habilitar únicamente este tipo de tráfico en dichos dispositivos.

PPTP ha sido largamente cuestionado desde su lanzamiento, por una serie de asuntos relativos a su seguridad. Desde el punto de vista de su diseño, antes de que el túnel GRE se establezca, una parte del inicio de la sesión, autenticación, y alguna información como las direcciones IPs del cliente y del servidor, se realizan vía TCP en texto claro. Esto permitiría a un eventual atacante a la escucha, utilizar parte de la información recolectada en algún tipo de ataque.

Por otra parte, el sistema de clave simétrico escogido por Microsoft para la autenticación en su implementación de PPTP, es RC4, significando por tanto, la utilización de claves de longitudes de 40 o 128-bits, las cuales no se consideran seguras en la actualidad. Adicionalmente a esta cuestión, la generación de la clave final a utilizar en un esquema de este tipo, se basa en la contraseña del usuario, lo que hace que en entornos donde las políticas de cambio de contraseñas no se encuentren bien implementadas, el riesgo de ataques a las mismas, y por ende, al compromiso del túnel, será aún mayor.

En resumen, el profesional de seguridad, deberá ser cuidadoso a la hora de decidir la implementación de VPNs basadas en PPTP, en aquellos entornos donde la seguridad juegue un rol preponderante. Si bien es cierto que en la mayoría de los casos, las prestaciones que nos brinda este protocolo, serán motivo suficiente para decidir su implementación, alternativas como L2TP e IPsec, deberían ser tenidas en cuenta en entornos que requieran mayor seguridad.

11.4 PROTOCOLO GRE

Hacia Octubre de 1994, se publicaba en el RFC 1701, el desarrollo de CISCO en torno a un nuevo protocolo de encapsulamiento de propósito general. Si bien por aquél entonces, existían varias propuestas previas, de características similares (RFC 1226, RFC 1234, RFC 1241, RFC 1479, etc.), el aspecto entorno a su concepción como protocolo de “propósito general”, lo llevó a convertirse rápidamente en un estándar de facto, a la hora de generar túneles de datos.

Sin lugar a dudas, la idea de un mecanismo sencillo a la hora de encapsular datos de un protocolo, de forma tal que éste pueda ser transportado por una red utilizando “otro” protocolo, no sólo ha resultado atractiva, sino también útil y eficiente.

GRE, son las siglas de “Generic Routing Encapsulation” y se consolidó como una respuesta acertada de CISCO y del grupo de personas que trabajaron en su desarrollo, en torno a resolver los inconvenientes relativos a la encapsulación de protocolos, manifestados hasta el momento.

Hasta la aparición de GRE, protocolos como “Internet Protocol Encapsulation of AX.25” (IPEAX, RFC 1226) que permitían la encapsulación de frames X.25 dentro de paquetes IP, o propuestas como la de Novell de Junio de 1991: “Tunneling IPX traffic through IP networks” (RFC 1234), que hacía lo propio con paquetes IPX a través de redes IP, cumplían con su cometido pero sólo lo hacían con tipo de protocolos para el cual habían sido desarrollados. En este punto es donde GRE ha conseguido diferenciarse del resto.

Debido a su concepción como protocolo de routing y encapsulamiento genérico, GRE ofrece a los profesionales de Networking la posibilidad de conocer y administrar un sólo protocolo de encapsulamiento con el que pueden trabajar en diferentes plataformas y entornos operativos.

11.4.1 Proceso de conexión y funcionamiento

En un escenario general, GRE entra en acción cuando se tiene un paquete de datos que necesita ser encapsulado y encaminado. A los efectos de su identificación, en la terminología GRE, este paquete suele ser denominado payload o carga útil. La carga útil primero se encapsula en un paquete de GRE, que también incluye posiblemente una ruta. El paquete de GRE resultante, puede entonces ser

encapsulado en otro “cierto” protocolo y después ser reenviado. Este otro protocolo, es mencionado entonces como delivery protocol o protocolo de entrega.

A fin de alcanzar su objetivo principal, un paquete GRE se compone básicamente, de tres secciones claramente definidas:

1. Delivery Header o Cabecera de entrega
2. GRE Header o Cabecera GRE
3. Payload Packet o Carga útil del paquete

De esta forma, se consigue obtener un paquete original (Payload Packet), con una cabecera GRE en donde se especifican valores tales como el tipo de protocolo contenido en la carga útil, y una cabecera de entrega dotada de la información de routing general, que posibilitará que este paquete cruce la red anfitrión, en busca del extremo que lo recibirá, lo desencapsulará y lo pondrá sobre la red destino.

11.4.2 Ventajas y limitaciones

Las ventajas de la utilización de GRE, son claras. Redes disímiles, funcionando en distinta forma (DECnet, Appletalk, IP, etc.), pueden ser interconectadas mediante la implementación de este protocolo. Debido a su utilidad, al efecto que ha causado en la industria y a su origen “abierto”, es hoy en día soportado por la mayoría de los dispositivos de Networking y sistemas operativos.

GRE es utilizado por protocolos como PPTP, quien se aprovecha de algunas de sus características elementales, sobre las cuales basa su potencial. Entre ellas, se encuentra el contenido de cierta información utilizada para verificar el estado de congestión del túnel y la detección de posibles errores en su creación y funcionamiento, lo cual le permite mantener un nivel de servicio aceptable.

11.4.3 Consideraciones sobre seguridad

Desde el punto de vista de su seguridad, los túneles GRE, no representan un problema en si mismo, aunque a lo largo del tiempo, se han detectado y solucionado, vulnerabilidades encontradas en diferentes tipos de implementaciones. Tal es el caso de Windows NT 4.0 y su implementación de PPTP/GRE, sistema operativo que hacia fines del año 2000 se confirmara vulnerable a distintos tipos de ataques de denegación de servicio, los cuales tenían como objetivo la malformación de paquetes GRE, que una vez recibidos por las plataformas afectadas, provocaban una parada inesperada en el sistema.

11.5 PROTOCOLO L2TP

Algún tiempo después de que CISCO y Microsoft, hicieran sus intentos con L2F (Cisco Layer 2 Forwarding) y PPTP (Point-to-Point Tunneling Protocol) respectivamente, ambos decidieron que era tiempo de consolidar esfuerzos y trabajar sobre un protocolo de tunneling que, implementando características de sus desarrollos anteriores, lograse convertirse en un verdadero estándar. Fruto de esta unión, surgiría en Agosto de 1999 bajo el RFC 2661, un protocolo denominado L2TP (Layer 2 Tunneling Protocol), el cual poco tiempo después, se convertiría en uno de los más utilizados al momento de establecer túneles de datos. A lo largo de la próxima sección, recorreremos algunos de los aspectos más destacados de esta tecnología, así como también la forma en la que la misma es implementada en el ámbito de las Redes Privadas Virtuales (VPNs).

Tal como se menciona en el correspondiente RFC, PPP define un mecanismo de encapsulación tendiente a transportar, paquetes multi-protocolo a través de la capa 2 (L2) en una comunicación de

extremo a extremo. En este escenario, típicamente un usuario obtiene una conexión del tipo L2, contra un Servidor de Acceso a la Red (NAS por “Network Access Server”) a través de cualquiera de los métodos tradicionales como ser: Dial-Up, ADSL, ISDN, etc.; para luego levantar o ejecutar, un enlace PPP sobre la mencionada conexión. En tal configuración, el punto de terminación L2 y el punto final de la sesión PPP residen en el mismo dispositivo físico (es decir, el NAS).

L2TP extiende el modelo típico utilizado por PPP, permitiendo que los puntos finales de L2 y de PPP residan en distintos dispositivos interconectados. Con L2TP, un usuario tiene una conexión L2 a un concentrador de acceso, como por ejemplo un banco de módems, y el concentrador genera entonces un túnel de frames individuales de PPP al NAS. Esto permite que el proceso real de los paquetes PPP, pueda ser separado de la terminación del circuito de capa 2.

Si bien este nuevo esquema no representa diferencias desde el punto de vista funcional para el usuario, tecnológicamente, permite a los proveedores de acceso, separar funciones en cuanto a la conexión de estos servicios, al permitir que una comunicación no necesariamente deba terminar en un NAS (Network Access Server) y sí pueda terminar en un nodo local.

Al margen de esta particularidad, L2TP es un protocolo de tunneling y como tal brinda la capacidad de transportar múltiples protocolos. De esta forma IP, IPX y SNA se encuentran soportados.

Características:

- Publicado en agosto de 1999 bajo el RFC 2661
- Desarrollado por un consorcio conformado primeramente por Microsoft y Cisco
- Debido a su concepción, L2TP es considerado el sucesor de L2F y PPTP
- Define un mecanismo de encapsulación de capa 2
- Se plantea como el complemento ideal de IPSec
- Utiliza Network Control Protocol (NCP) para negociar la asignación de una dirección IP
- Provee los mismos métodos de autenticación que PPP, PAP (Password Authentication Protocol) y CHAP (Challenge Handshake Authentication Protocol)

11.5.1 Antecedentes: PPTP y L2F

Tal como mencionáramos brevemente en un indicador anterior, L2TP tiene su origen en un emprendimiento conjunto de las compañías CISCO y Microsoft, tendiente a diseñar un protocolo que, basado en los desarrollos individuales de cada uno de ellos, tuviera las características necesarias como para convertirse en un nuevo estándar, a la hora de implementar tecnología de tunneling avanzada.

Cuando hablamos de los desarrollos individuales de Microsoft y de CISCO, nos referimos a PPTP (Point-to-Point Tunneling Protocol) y L2F (Layer 2 Forwarding) respectivamente, los cuales si bien fueron concebidos como competidores, se consideran el antecedente de L2TP (Layer 2 Tunneling Protocol).

Puesto que PPTP, ha sido presentado en secciones anteriores, tan solo recordaremos que, debido principalmente a su facilidad de uso y a que se encuentra incluido en un gran porcentaje de los sistemas operativos más utilizados, ha sido considerado desde su concepción, una alternativa sencilla y económica a la hora de implementar tecnología de tunelización y VPN.

L2F por su parte, presentado por CISCO en sociedad en Mayo de 1998, a través del RFC 2341, propone el establecimiento de un túnel en capa 2 que posibilita el encapsulamiento de paquetes PPP y SLIP, a fin de que los mismos puedan ser transmitidos a través de Internet. Claramente orientado a la creación de túneles en conexiones del tipo Dial-Up, L2F posee características similares a PPP,

aunque no comprende encriptación. L2F utiliza el port TCP 1701 para sus conexiones.

El proceso de tunneling en L2F, involucra tres protocolos diferentes: Protocolo pasajero, Protocolo encapsulador, y Protocolo portador. El protocolo pasajero representa el protocolo de nivel superior que debe encapsularse (IPX, DECNET, etc.). El protocolo encapsulador indica el protocolo que será empleado para la creación, mantenimiento y terminación del túnel de comunicación (L2F). Por último, el protocolo portador es el encargado de realizar el transporte de todo el conjunto. Por lo general, este protocolo suele ser IP, dadas sus capacidades de enrutamiento, su acople a los diferentes medios y su carácter de estándar en el ámbito de Internet.

Entre las principales ventajas que ofrece L2F es posible mencionar su soporte multiprotocolo, la existencia de un menor overhead en comparación con PPTP, la multiplexación de numerosas sesiones remotas (minimizando el número de túneles abiertos en un momento dado), y la gestión dinámica de los túneles, en la cual los recursos de los servidores de acceso a la red se minimizan al iniciar los túneles únicamente cuando existe tráfico de usuario. Además, por cada túnel L2F establecido, el proceso de seguridad genera una clave aleatoria como medida de prevención ante posibles ataques basados en spoofing. A su vez, en el interior de los túneles, cada una de las sesiones multiplexadas mantendrá un número de secuencia para evitar problemas debidos a la duplicidad de paquetes.

11.5.2 Proceso de conexión y funcionamiento

Cuando se utiliza entre redes IP, L2TP es bastante similar a PPTP. En su esquema más básico, se crea un túnel L2TP entre un cliente L2TP y un servidor L2TP. El cliente puede incluirse a una red IP (tal como una LAN) que puede alcanzar el servidor del túnel, o un cliente puede llamar a un servidor de acceso a la red (NAS) para establecer la conectividad IP (por ejemplo, para usuarios de Internet con conexiones Dial-Up).

L2TP utiliza en su funcionamiento, dos tipos de mensajes: mensajes del control y mensajes de datos. Los mensajes de control se utilizan en el establecimiento, el mantenimiento y la terminación de túneles y llamadas, a la vez que se valen de un canal confiable dentro de L2TP, para garantizar la entrega. Los mensajes de datos en cambio, son utilizados para encapsular los marcos PPP que son transportados sobre el túnel y no se retransmiten cuando ocurre la pérdida de un paquete. En definitiva, el tráfico de datos es encapsulado en un link virtual PPP y tunelizado por medio de un túnel L2TP. La negociación y asignación de direcciones IP, recaen de esta forma, sobre NCP (Network Control Protocol), el mecanismo propio de PPP. Dentro de un esquema típico L2TP, se reconocen una serie de componentes cuyas funciones permiten, actuando en conjunto, el correcto funcionamiento de esta arquitectura.

- **LAC (L2TP Access Concentrator):** Se añade un dispositivo LAC a los componentes físicos de la red conmutada, como la red telefónica convencional o ISDN, o se coloca con un sistema de terminación PPP capaz de gestionar el protocolo L2TP. Un LAC sólo necesita implementar el medio sobre el cual opera el L2TP para admitir el tráfico de una o más LNS. Puede "tunelizar" cualquier protocolo que incluya PPP. LAC es el iniciador de las llamadas entrantes y el receptor de las llamadas salientes. Se encuentra implementado generalmente en un ISP, aunque también puede existir en un cliente remoto.
- **LNS (L2TP Network Server):** Un LNS opera sobre cualquier plataforma con capacidad de terminación PPP. LNS gestiona el lado del servidor del protocolo L2TP. Ya que L2TP se apoya sobre el medio al que llegan los túneles L2TP, LNS sólo puede tener una única interfaz LAN o WAN, aunque es capaz de terminar las llamadas entrantes en cualquiera de la amplia gama de las interfaces PPP LAC (asíncronos, ISDN, PPP sobre ATM, PPP sobre Frame Relay). Se localiza del lado de la red corporativa.
- **NAS (Network Access Server):** Este dispositivo proporciona a los usuarios acceso temporal a la red bajo demanda. Este acceso es punto a punto, de uso típico en líneas de la red telefónica

convencional o ISDN. En la implementación Cisco, un NAS sirve como LAC. Mediante los mencionados componentes, el protocolo L2TP, posibilita el encapsulamiento de diferentes protocolos, haciendo uso de las capacidades de PPP a la vez que incorpora, facilidades mejoradas y una integración estupenda con IPSec (Protocolo que estudiaremos en detalle, en nuestra próxima sección).

11.5.3 Ventajas y limitaciones

De acuerdo a su estructura y funcionamiento, L2TP, es sumamente flexible al momento de su implementación, al permitir el manejo de varios túneles entre dos puntos o multiplexando varias conexiones sobre el mismo túnel. Puede correr sobre una variedad de redes de transporte además de IP, X.25 o ATM. Debido al manejo que realiza con mensajes de control y de datos, suele ser considerado “confiable” desde el punto de vista de la entrega.

Al ser Impulsado inicialmente por dos grandes compañías (Microsoft y CISCO), L2TP dispone hoy en día, de un amplio soporte por parte de la mayoría de los proveedores de equipos de acceso a redes, así como una probada interoperabilidad. A pesar de sus potentes características, los desarrolladores y proveedores de equipamiento con implementaciones L2TP, han hecho un esfuerzo por hacer que éstos sean de fácil configuración, aunque al requerir en algunos escenarios, alguna de las ventajas adicionales de IPSec, esta facilidad deja de ser tal.

11.5.4 Consideraciones sobre seguridad

Uno de los aspectos claves de L2TP, en relación a su seguridad, radica en que éste no provee encriptación de datos (aunque existen implementaciones propietarias que utilizan algoritmos de encriptación simétricos, particularmente RC5 de 128 bits), motivo por el cual, suele deslindarse esta responsabilidad a protocolos como IPSec, el cual se integra fácilmente con L2TP al momento de brindar soluciones de calidad reconocida en entornos VPNs.

Desde el punto de vista de la autenticación, a pesar de que L2TP incluye su propio mecanismo, generalmente se vale de los existentes en PPP: PAP, CHAP y MSCHAP (implementación de Microsoft del protocolo CHAP), al momento de validar usuarios, cuestión que en determinadas circunstancias, puede significar una estructura NO muy sólida de autenticación. De todas formas, tal como mencionáramos en el párrafo anterior, puesto que en la práctica, la mayoría de las implementaciones serias de VPNs, se realizan combinando L2TP con IPSec, y gracias a que IPSec prevé mecanismos de autenticación y cifrado basado en estándares, no debería verse la autenticación básica de L2TP como un problema sin solución.

Puesto que las implementaciones L2TP, suelen utilizarse sobre redes públicas, tanto los paquetes de control como los paquetes de datos pueden ser vulnerables frente a posibles ataques de snooping, que tengan como objetivo la interceptación de los procesos de negociación de la encriptación (ECP) y de la compresión (CCP) con el fin de provocar la supresión de los mecanismos de confidencialidad o llegado el caso, obtener acceso a los passwords de los usuarios, cuestiones todas, que encuentran solución en la aplicación de protección adicional de paquetes mediante IPSec.

11.5.5 PPTP versus L2TP

Si bien es cierto que muchas veces suelen ser vistos como competidores, y que existen coincidencias importantes entre ellos, PPTP y L2TP poseen ciertas características que los diferencian, contribuyendo a que cada uno sea más propicio que el otro, en función del escenario en el cual deban implementarse. Comenzaremos por decir que tanto PPTP como L2TP utilizan PPP al momento de encapsular los datos en frames, antes de que estos sean enviados a través de la red. Por su parte, algunas de las diferencias existentes entre ambos protocolos, pueden resumirse de la siguiente forma:

- PPTP requiere que la red sea IP, mientras que L2TP requiere que sólo el túnel provea conectividad punto a punto orientada a paquetes. L2TP puede ser utilizado sobre IP (utilizando UDP), Circuitos virtuales permanentes (PVC's) en Frame Relay, Circuitos virtuales en X.25 o ATM.
- PPTP solamente soporta un túnel simple entre dos puntos, mientras que L2TP permite la utilización de múltiples túneles entre dos puntos. Además se pueden crear diferentes túneles para diferentes calidades de servicio (QoS).
- L2TP permite compresión de cabeceras. Cuando esta compresión está habilitada, éste opera con 4 bytes de overhead en comparación con los 6 bytes de PPTP.
- L2TP permite autenticación de túnel, mientras que PPTP no lo permite. Sin embargo cuando cualquiera de estos protocolos es utilizado sobre IPSec, la autentificación de túnel es realizada por IPSec de manera que la autentificación en la capa 2 no es necesaria.

11.6 PROTOCOLO IPSEC

Es un hecho que Internet está cambiando rápidamente la forma de hacer negocios, pero al mismo tiempo que esta Red de Redes se hace cada vez más grande en su extensión, mayores son las amenazas que se ciernen a su alrededor.

El desarrollo de la pila de protocolos TCP/IP, tuvo lugar en una época en la cual la seguridad no representaba un desafío, de hecho, el desafío concreto se encontraba mas bien relacionado con la posibilidad de interconexión y la expansión resultante de su aplicación en el campo real. Años más tarde, y especialmente con el advenimiento de Internet, las falencias de este protocolo respecto de su seguridad entre otras, se hicieron notar con fuerza. En respuesta a estos inconvenientes, en Noviembre de 1998, se publicaba bajo el RFC 2401, el que sería el primero de una serie de memos, mediante los cuales se presentaría en sociedad un nuevo protocolo denominado IPSec (IP Security).

Según lo definido oportunamente por el IETF (Internet Engineering Task Force), “IPSec es un conjunto de estándares abiertos, tendientes a asegurar la privacidad y seguridad de las comunicaciones sobre redes IP, por medio del uso de servicios criptográficos”. Esta definición, nos permite entrever algunos de los aspectos más importantes detrás de IPSec, comenzando con el término “estándares abiertos”, lo cual representa sin lugar a dudas un buen comienzo.

Cuando IETF hace mención a “estándares abiertos”, se refiere a que, a diferencia de otros métodos de comunicación segura, IPSec no se encuentra limitado a algún sistema o algoritmo de autentificación o encriptación en particular, permitiendo a quien decida implementarlo, escoger entre distintos métodos o conjuntos de métodos estándares que se utilizarán como parte de dicha implementación.

En concordancia con lo enunciado en el RFC 2401, IPSec se ha diseñado con el objeto de proporcionar interoperabilidad, alta calidad y seguridad basada en criptografía no sólo para IPv6 donde es mandatario, sino también en IPv4.

El conjunto de servicios de seguridad ofrecidos por IPSec, incluye control de acceso, confidencialidad, integridad, autentificación del origen de datos, antireplay y no repudio (cuando se utiliza Firma Digital como medio de autenticación).

Una de las particularidades de IPSec, es que a diferencia de alguno de los viejos conjuntos de estándares, en los cuales la seguridad se aplicaba sobre la capa de aplicación del modelo OSI, IPSec hace lo propio en la capa de red. Al funcionar de esta forma, la protección se hace efectiva para la capa IP y/o los protocolos de capa superior, transformándose en la mayoría de las oportunidades, en una solución sumamente transparente en relación a las aplicaciones.

De acuerdo a sus características, IPSec se ha transformado en la actualidad, en el método obligado, a la hora de implementar sistemas del tipo VPNs que requieran atravesar con seguridad un medio público, como por ejemplo Internet.

En las próximas secciones, recorreremos cada uno de los componentes de esta tecnología, a la vez que intentaremos describir el funcionamiento de cada uno de ellos.

11.6.1 Componentes

IPSec es considerado un grupo de extensiones de la familia del protocolo IP. Como tal, su funcionalidad se encuentra basada en un conjunto de componentes, cada uno con funciones específicas claramente definidas.

Recordemos, por cierto, que las tres principales condiciones de una mensajería segura son:

- Privacidad o Confidencialidad: que el mensaje sea leído sólo por el destinatario previsto.
- Autenticación: que el mensaje venga de quién dice que viene.
- Integridad: que el mensaje no haya sido modificado en su camino entre los extremos.

A modo de introducción, mencionaremos brevemente en la presente sección, algunos de estos componentes principales que garantizan estas condiciones y algunas otras complementarias como son el antireplay y la administración de claves. Posteriormente serán desarrollados en indicadores posteriores con mayor detalle.

AH (Authentication Header): Este componente es utilizado al momento de proveer autenticación del origen de datos, integridad y protección a la réplica en los datagramas IP. Si bien es cierto que AH hará su mejor intento a la hora de proteger cabeceras IP, debido al propio funcionamiento de IP, siempre existirán determinados campos, que siendo susceptibles a ser cambiados en tránsito, no se encuentren dentro del ámbito de protección provisto por AH. De todas formas, a diferencia de ESP, AH permite asegurar partes de la cabecera IP como ser las direcciones de origen y destino.

ESP (Encapsulating Security Payload): ESP, es otro de los protocolos provistos por IPSec. Como parte de su funcionamiento, ESP provee autenticación, integridad y protección a la réplica al igual que AH, aunque a diferencia de este último, ESP se ocupa también de asegurar la confidencialidad de los datos. Al implementar ESP, el analista de seguridad, tiene la posibilidad de decidir, en algunos casos por medio de las asociaciones de seguridad, cual de los servicios provistos por este protocolo, requieren ser utilizados (protección a la réplica e integridad, confidencialidad con o sin autenticación, etc.). De acuerdo a sus características particulares, AH y ESP pueden ser utilizados en conjunto, aunque en la mayoría de los casos la utilización de uno de ellos será suficiente.

IKE (Internet Key Exchange): Una de las características más interesantes del conjunto de componentes relacionados con IPSec, es sin lugar a dudas el servicio de intercambio de claves provisto por IKE. Puesto que gran parte del funcionamiento de IPSec, se basa en principios criptográficos, claves y algoritmos, éstos se encuentran presentes en la mayoría de los procesos involucrados. Como en cualquier esquema de este tipo, el conjunto de claves utilizadas, debe ser conocido de antemano por los extremos de una comunicación, este servicio es precisamente brindado por IKE. Si bien es cierto que IKE no es un requerimiento de IPSec, puesto que la labor de administrar claves de sesión en forma manual puede ser un gran inconveniente, la mayoría de las implementaciones actuales, hacen uso de esta tecnología.

11.6.2 Modo Túnel o modo Transporte

Tanto AH (Authentication Header) como ESP (IP Encapsulating Security Payload), permiten diferentes modos de operación a la hora de realizar su labor. Dependiendo de los servicios de IPSec a

implementar y del propósito de dicha implementación, el modo indicado en cada caso, podría variar. A continuación describiremos los dos modos probables, así como las situaciones en las que uno u otro deberían ser implementados.

Modo Tunel: Cuando el modo túnel se pone en funcionamiento, entran en juego los denominados gateways IPSec (Básicamente Routers o Firewalls con facilidades IPSec), los cuales implementan protección completa al paquete IP, encapsulando el datagrama original en otro datagrama que posee las direcciones IP de los gateways IPSec que mantienen el túnel, a la vez que se responsabilizan por la generación de túneles sobre los host ubicados generalmente del lado de la red interna. Esta operatoria, permite que cada uno de estos host se comunique en forma segura con el gateway implementado a tal fin, sin la necesidad de que IPSec esté presente en cada uno de ellos. Debido a esta operatoria, solemos referirnos al modo túnel, como modo transparente, puesto que su funcionamiento, hace que los clientes finales en cada uno de los extremos, por lo general no se enteren de que IPSec está protegiendo el tráfico de sus comunicaciones.

El modo túnel, suele ser utilizado entre dispositivos de frontera, en aquellos casos donde se requiere protección transparente sobre redes no confiables. Como característica particular, en este tipo de implementaciones, la cabecera exterior puede poseer direcciones origen y destino diferentes a la cabecera interna (encapsulada), puesto que se crea un nuevo encabezado IP con las direcciones IP de los gateways de origen y destino. Respecto de los protocolos IPSec en este modo, ESP cifra y opcionalmente autentica el paquete IP interno, mientras que AH autentica el paquete IP interno y parte de la cabecera IP externa.

En resumen, el modo túnel provee seguridad para el paquete IP completo, puesto que el paquete IP original es encriptado, encapsulado en un nuevo paquete IP y la dirección IP externa, es la utilizada para rutear el paquete a través de Internet, pudiendo corresponder a las IP internas un esquema de direccionamiento privado.

En el modo túnel, el datagrama original se encapsula entero, con su cabecera y sus datos, dentro de otro datagrama. Este otro datagrama tendrá una cabecera IP en la cual las direcciones de origen y de destino serán las de los nodos inicio y final de la SA. Por tanto, se dice que entre estos dos nodos hay un “túnel” dentro del cual viajan intactos los datagramas originales. A continuación de la cabecera IP del datagrama “externo” hay la cabecera AH o ESP.

Modo Transporte: Este modo suele ser el indicado en aquellas circunstancias donde la seguridad se establece de extremo a extremo, aplicándose solamente a las comunicaciones de Host a Host. En este tipo de escenarios, cada host realiza la encapsulación de sus propios datos, requiriéndose la ejecución de IPSec, en ambos puntos de la conexión, determinando de esta forma, que cada extremo de una comunicación IPSec, signifique a su vez, el final mismo de la aplicación. Cuando el modo transporte es implementado se asegura la protección de la carga útil IP. En este esquema, ESP cifra y opcionalmente autentica el campo de datos de IP, mientras que AH autentica campo de datos de IP y parte de la cabecera. En modo transporte, el encabezado IPSec se inserta entre el encabezado IP y el encabezado siguiente, generalmente de Capa 4 (TCP o UDP). El modo transporte, protege la carga útil de los paquetes pero mantiene la información referente a direcciones IP en texto claro, puesto que ésta es utilizada para rutear los paquetes a través de Internet. Es importante tener en cuenta, que en esta modalidad, los datos de los paquetes bajo IPSec viajan encriptados tanto en la red pública (Internet) como en la propia LAN de los extremos. En el modo transporte, la cabecera AH o ESP se incluye después de la cabecera IP convencional, como si fuera una cabecera de un protocolo de nivel superior, y a continuación van los datos del datagrama (por ejemplo, un segmento TCP con su cabecera correspondiente, etc.).

El protocolo IP prevé que un datagrama se pueda fragmentar, y se puede dar el caso que los fragmentos de un mismo datagrama vayan por caminos diferentes hasta llegar a su destino final. Esto representaría un problema en una SA entre pasarelas seguras (o entre un nodo extremo y una

pasarela segura) si se utilizara el modo transporte: por ejemplo, algunos fragmentos podrían quedar sin proteger, otros podrían resultar indescifrables porque no han pasado por la pasarela que los había de descifrar, etc. Para evitar estas situaciones, en IPsec sólo se permite el modo transporte en las SA extremo a extremo.

El modo túnel no tiene este problema porque, aunque la SA sea entre pasarelas, cada datagrama tiene como dirección de destino la del nodo que hay al final del túnel, y todos los fragmentos finalmente tienen que llegar a este nodo. Por tanto, el modo túnel se puede utilizar en cualquier SA, tanto si es extremo a extremo como si interviene una pasarela segura.

11.6.3 Protocolo AH

AH (IP Autentication Header o Cabecera de Autenticación IP) definido en el RFC 2406 es utilizado en IPSec, a fin de proveer integridad y autenticación del origen de datos para los datagramas IP, pudiendo opcionalmente, proporcionar protección a la réplica por parte del receptor, cuando se establece una asociación de seguridad (puesto que esto se logra incrementando un número de secuencia, este último servicio sólo será eficaz en aquellos casos donde el receptor, controla este número de secuencia.). Como mencionáramos en su descripción general, AH realiza su mejor intento a la hora de proteger cabeceras IP y datos de los protocolos superiores. Sin embargo, puesto que el valor de algunos campos de la cabecera IP puede cambiar en tránsito, el paquete finalmente en poder del receptor, puede no ser fiable. Los valores de tales campos no se pueden proteger por AH, lo que provoca en definitiva, que la protección proporcionada por AH a la cabecera IP sea un tanto fragmentaria.

AH, puede ser aplicado sólo, en combinación con ESP o lo que es aún más común, como parte del modo túnel. Como el resto de los servicios de seguridad incluidos en IPSec, AH puede ser utilizado en comunicaciones host a host, entre gateways, o en una combinación de gateways y host. A diferencia de ESP (IP Encapsulating Security Payload), AH no provee encriptación y por ende confidencialidad, como parte de su funcionamiento.

AH, se identifica en IPv4, con el valor 51 en el campo “protocolo”. Su formato, contiene fundamentalmente, un valor de 32-bit en el sector indicado como SPI (índice de parámetro de seguridad), que en combinación con la IP destino y el protocolo de seguridad (AH) identifica unívocamente la asociación de seguridad (SA) para este datagrama. Un número de secuencia de 32-bit, utilizado al momento de actuar como prevención a la réplica y un campo de longitud variable, conteniendo el valor HMAC del paquete.

Por último, si bien es cierto que AH y ESP, ofrecen servicios similares, algunas de las razones del uso de AH, se encuentran relacionadas con su bajo overhead respecto de ESP, su utilización mandataria en IPv6 y el hecho de que por su concepción, no existan restricciones en cuanto a su exportación.

11.6.4 Protocolo ESP

ESP, se encuentra definido en el RFC 2406 y es utilizado para proveer privacidad o confidencialidad a datagramas IP por medio de la encriptación, y adicionalmente, puede brindar autenticación del origen de datos, integridad y protección a la réplica.

Se encuentra definido con el identificador 50 en relación al protocolo IP y al igual que el resto de los servicios provistos por el marco IPSec, los brindados por ESP, dependen de la selección de opciones y de la configuración de la asociación de seguridad (SA).

Respecto a esto último, si bien es cierto que “protección a la réplica e integridad” y “confidencialidad con o sin autenticación”, son algunas de las variantes válidas al momento de configurar este servicio, decisiones incorrectas respecto de estas combinaciones, pueden generar que finalmente, la propuesta montada sea susceptible a algún tipo de ataque. Al mismo tiempo, corresponde aclarar, que servicios tales como la autenticación del origen de datos y la integridad, son ofrecidos como una opción

indivisible, a la que puede o no, por ejemplo, agregarse el servicio de confidencialidad. Por su parte, el servicio de protección a la réplica, sólo puede ser seleccionado, si la autenticación del origen de datos es también de la partida.

11.6.5 ¿AH y/o ESP?

Dependiendo de los aspectos que se busquen garantizar sobre la seguridad de los datos, podremos implementar AH o ESP o bien combinar ambos. Si sólo buscamos garantizar la integridad de un datagrama incluyendo la dirección de IP origen, podemos implementar simplemente AH. Ahora bien, si buscamos confidencialidad o privacidad en cuanto a la recepción por parte del host determinado, deberemos encriptar con ESP.

Ninguno de los dos mecanismos, en principio, ofrece una solución total, dado que no es conveniente el encriptado sin autenticación. Si necesitamos garantizar ambos aspectos, se presentan dos alternativas: ESP con autenticación o bien combinar ESP y AH.

ESP con autenticación propia ofrece mejor rendimiento que la combinación entre ESP y AH, debido a que emplea una única operación HMAC. Sin embargo, el nivel de autenticación es inferior puesto que ESP no autentica el primer encabezado IP, ya sea el original en modo transporte o el agregado por el modo túnel.

ESP puede utilizarse sólo para encriptado o para encriptado y autenticado. También, puede ser empleado en modo encriptado Nulo, es decir sin encriptado pero con autenticación para hacer las veces de una especie de AH sin autenticar el encabezado IP, permitiendo la operación sobre entornos con traducción de direcciones.

11.6.6 Compresión IP

En aquellos entornos donde la decisión de proveer servicios de encriptación a un conjunto de datos en tránsito se lleva a la práctica, es inevitable el impacto negativo obtenido. Esto se debe básicamente a dos aspectos claves, el tiempo de procesamiento en los extremos a la hora de encriptar y des-encriptar la información y, el tamaño efectivo de los paquetes a ser transmitidos.

A fin de solucionar el segundo de estos inconvenientes, varias alternativas de compresión de datos han sido discutidas a lo largo de los últimos años. Algunos RFCs se han encargado incluso de echar luz sobre alguno de los aspectos relacionados con este asunto, tal es el caso del RFC 2393. Uno de los principales problemas a los que se enfrenta la compresión IP, en particular al momento de ser aplicada en conjunto con IPSec, se encuentra relacionado con la pérdida de datos innata en todo proceso de compresión.

Como hemos mencionado, la compresión IP es especialmente útil cuando un proceso de encriptación es aplicado a un datagrama IP. La propia encriptación de un datagrama IP hace que los datos obtenidos como producto sean en esencia aleatorios, transformando la compresión en las capas más bajas del protocolo ineficaz. Por tal motivo, en aquellos casos donde encriptación y compresión sean requeridos, la compresión debe ser aplicada, antes de la encriptación.

11.6.7 IPSec versus NAT

Uno de los inconvenientes principales al que todo profesional de seguridad informática deberá enfrentarse en algún momento al implementar VPNs basadas en IPSec, es aquel relacionado con el despliegue de IPSec en combinación con NAT (Network Address Transalation). Responder a la pregunta de si es posible implementar IPSec en conjunto con NAT, no es cosa sencilla, puesto que ambos pueden ser utilizados perfectamente en algunas configuraciones mientras que no podrán hacer lo propio en otras.

Por ejemplo, cuando AH (Authentication Header), se pone en funcionamiento en una configuración IPSec, este toma un paquete IP entero, incluyendo partes del encabezado que no cambian (Direcciones IP de origen y destino) y calcula un valor hash con esta información.

Por el puesto que tiene este hash, es el utilizado a posteriori para que la autenticidad del paquete en cuestión, pueda ser comprobada por el receptor. Si cualquier campo del paquete IP original es modificado, la autenticación fallará. En definitiva, debido a su propio funcionamiento, debido a que NAT modifica en su accionar parte del paquete IP tratado, AH y NAT simplemente, no son compatibles.

Con ESP sucede algo similar, aunque en este caso la compatibilidad con NAT se encontrará relacionada con algunos de los seteos de seguridad propios de ESP. Por ejemplo, debido a su funcionamiento NAT seguirá funcionando cuando el modo implementado sea el de “túnel”, mientras que para que lo propio suceda en modo transporte, usted deberá estar en condición de deshabilitar la verificación o checksum implementada en los terminadores. De todas formas, habiendo sorteado en este caso el primero de los inconvenientes, aún se debería revisar las incompatibilidades entre NAT y la utilización de IKE (Internet Key Exchange)

Una variante que ha tomado fuerza últimamente, y se encuentra soportada por la mayoría del nuevo equipamiento relacionado con VPN y algunos sistemas operativos (ejemplo: Windows 2003), es el método denominado ”NAT Traversal (NAT-T)”. Cuando dos dispositivos entienden NAT-T (cuestión que se resuelve en la primera fase de la negociación IKE), lo que sucede es que se encapsulan los paquetes generados por ambos extremos en UDP, decidiéndose la implementación de dos nuevos modos: “UDP-Encapsulated-Tunnel” y “UDP-Encapsulated-Transport” (más información en referencias 3 y 4).

Al día de hoy, la solución respecto de este dilema, se encuentra dada por la aplicación de alguna de las siguientes implementaciones:

- Realizar NAT sobre un dispositivo situado detrás de un dispositivo IPSec.
- Utilizar un dispositivo IPSec híbrido, que también realice NAT.
- Implementar NAT-T (NAT Traversal)

11.6.8 Manejo de claves

Sin lugar a dudas, como todo sistema basado en servicios criptográficos, IPSec requiere de diferentes tipos de claves a la hora de proporcionar los distintos servicios de seguridad para los que fue creado. De esta forma, tanto las asociaciones de seguridad, como la negociación de los diferentes aspectos requeridos para llevar a cabo una comunicación segura, al igual que la generación de los valores de hash participantes de un esquema de autenticación, requieren en algún punto de servicios de generación y administración eficiente de claves.

Si bien es cierto que existen mecanismos manuales de administración de claves utilizados generalmente en ambientes pequeños y estáticos (para cumplir las normas, una implementación IPSec debe soportar tanto manejo de claves manual y automático), en entornos grandes o distribuidos, esta acción estaría repleta de aspectos negativos.

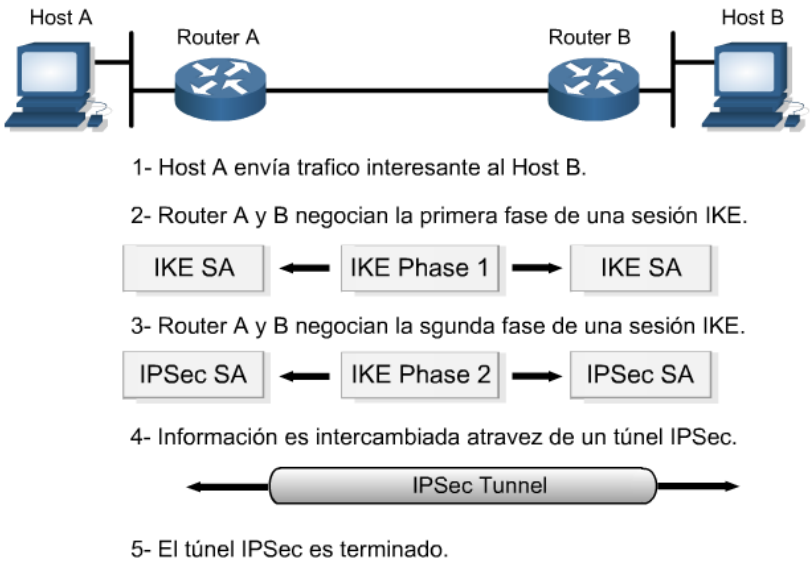
Por su parte, como el resto de las posibilidades provistas por IPSec, una mala elección del método escogido a la hora de administrar claves es capaz de afectar la seguridad ofrecida por el conjunto. IPSec, provee como parte de su set de servicios asociados, la posibilidad de utilizar un estándar denominado IKE (Internet Key Exchange) para resolver los temas relacionados con el manejo de claves y potenciar en gran medida el uso de IPSec a gran escala. Las secciones dispuestas a continuación intentarán discutir su funcionalidad e implementación.

11.6.9 IKE

En Noviembre de 1998, se presentaba el RFC 2409, mediante el cual se definía un protocolo conocido como IKE (Internet Key Exchange), el cual valiéndose del agrupamiento de implementaciones previas en relación a algunas de las particularidades del manejo de claves, se convertiría rápidamente en el protocolo utilizado en las implementaciones IPSec. IKE negocia en forma automática las Asociaciones de Seguridad (SA) de IPSec, permitiendo su utilización sin preconfiguración manual. Este esquema de manejo automático de claves es necesario para el servicio antireplay, ya que en el mismo se debe cerrar la SA actual y abrir una nueva en determinada situación para evitar el ciclado del contador de secuencia, dado que estos números de secuencia son los que permiten la implementación del mencionado servicio de seguridad.

Tal como se encuentra referido en su RFC, IKE se encuentra basado en ISAKMP (Internet Security Association and Key Management Protocol), el cual provee un marco de trabajo (más concretamente "pasos") para la autenticación y el intercambio de claves, pero no define éste. OAKLEY, el cual describe una serie de intercambios de claves llamados "modos" y detalla el tipo de servicio provisto por cada uno (por ejemplo: Re-envío del Secreto Perfecto, Protección de Identidad y Autenticación). Por último SKEME, donde se describe una técnica sumamente versátil de intercambio de claves, la cual provee anonimato, repudiabilidad y un rápido refresco de claves.

En resumen, IKE es un protocolo que utiliza parte de OAKLEY y parte de SKEME, en conjunto con ISAKMP, a fin de obtener un protocolo capaz de trabajar en forma segura con asociaciones de seguridad en protocolos como AH y ESP.



Esquema de funcionamiento

IKE provee como parte de su funcionamiento, los siguientes beneficios:

- Elimina la necesidad de especificar manualmente los parámetros de seguridad de IPSec en ambos extremos.
- Permite a los administradores especificar el tiempo de vida de una asociación de seguridad (SA) en IPSec.
- Permite que las claves de encriptación cambien durante una sesión IPSec.
- Le permite a IPSec proveer servicio contra la réplica.

- Permite soportar Autoridades de Certificación (CA), logrando una implementación IPSec escalable.
- Permite la autenticación dinámica entre pares.

11.6.10 Autenticación IKE

Los mecanismos de seguridad de IPSec, se basan en que las entidades deben establecer una negociación inicial, mediante la cual ambas partes se ponen de acuerdo en cuanto a los algoritmos criptográficos, claves y otros parámetros a utilizar en una comunicación segura. Puesto que esta negociación no puede ser llevada a cabo a nivel de la capa de red, se debe recurrir a protocolos de nivel superior, y allí es donde entra en juego IKE (Internet Key Exchange).

El proceso de autenticación provisto por IKE, algunas veces referenciado como two-way o de “ida y vuelta”, permite establecer si cada uno de los extremos es quien dice ser y si lo sigue siendo en el transcurso de una sesión.

IKE define básicamente tres mecanismos de autenticación:

- Autenticación con Clave Pre-compartida (Authentication with a Pre-Shared Key)
  En este tipo de esquema, ambos extremos comparten una clave secreta o password, la cual es utilizada durante la autenticación IKE al intercambiar, al igual que CHAP lo hiciera en PPP, una serie de valores aleatorios hasheados con la inclusión de la clave secreta pre-compartida. Debido a que en parte, este sistema de autenticación se basa en hashing, suele resultar muy rápido.
- Autenticación con Encriptación de Clave Pública (Authentication with Public Key Encryption)
  La autenticación con Encriptación de Clave Pública, utiliza como parte de su funcionamiento, el criptosistema RSA, del cual se vale al momento de concretar la autentificación entre las partes. Del mismo modo, que en toda infraestructura de clave pública, ambos extremos se encuentran en posesión de un par de claves, siendo necesario el intercambio de la pública, protegiendo la privada. En este esquema, un extremo encripta un string aleatorio, utilizando la clave pública del receptor, para luego demandar que el valor previamente encriptado, sea desencriptado por el otro extremo. Si este último logra desencriptar correctamente el valor aleatorio previamente encriptado, significará que cuenta con la clave privada correcta y por tanto, merece ser autenticado.
- Autenticación con Firma Digital (Authentication with Digital Signatures)
  En aquellos esquemas donde este tipo de autenticación es establecida, ambos extremos envían una serie de datos al otro, esperando que los mismos sean firmados digitalmente con sus respectivas claves privadas. Al regreso, se confirma dicha firma en comparación con el contenido de cada una de las claves públicas. Si el proceso es correcto, los extremos se llaman autenticados. Este método, es probablemente más lento que el anterior, puesto que en principio requiere algunas operaciones de clave pública adicionales, pero por otro lado habilita la posibilidad de no-repudio de la sesión IKE. Generalmente, la autenticación con firma digital, suele ser utilizada con certificados (X.509) y PKI.

Una vez que un dispositivo reconoce la identidad del otro y viceversa, el intercambio de información vía IKE se realiza por medio de mensajes UDP al port 500.

11.6.11 Fases de negociación

Como parte del funcionamiento principal de IKE como protocolo de intercambio de claves, es posible identificar dos fases a través de las cuales se completa el mecanismo que permite establecer un canal

de comunicación entre dos extremos, que pretende ser seguro.

- **Fase I:** Esta fase, se utiliza para establecer una asociación de seguridad (SA) ISAKMP (Internet Security Association and Key Management Protocol), mediante la cual, las entidades realizan la negociación y autenticación inicial, a fin de asegurar el canal de datos. Dicha negociación, puede ser llevada a la práctica en varios modos de establecimiento, cada uno con características particulares (ver sección 3.6.13). La denominada Fase I, hace uso de los métodos de autenticación mencionados en la sección anterior (Autenticación con Clave Pre-compartida, Autenticación con Encriptación de Clave Pública y Autenticación con Firma Digital), y así como los modos de establecimiento, dependerá de la elección de los parámetros configurados en el circuito IPSec y del escenario de implementación.
- **Fase II:** Una vez concluida la Fase I, se pone en funcionamiento la Fase II, la cual tiene como objetivo primordial establecer la asociación de seguridad (SA) que será utilizada para comunicar ambos extremos. Por medio de este diálogo, se acuerda entre las partes el tipo de protocolo a utilizar (AH, ESP), el modo (túnel, transporte) y algunos de los algoritmos involucrados (3DES, MD5, SHA-1, etc.)

11.6.12 Asociación de Seguridad (SA)

La Asociación de Seguridad (SA), es sin lugar a dudas, uno de los conceptos básicos dentro del mundo IPSec. Una Asociación de Seguridad (SA) representa un conjunto de políticas y claves utilizadas para proteger los datos involucrados en una comunicación IPSec. Puede ser definida como una conexión lógica unidireccional entre dos puntos extremos, estableciendo el contexto de seguridad en el que la comunicación se desarrollará. Todo el tráfico asociado a una SA recibe el mismo procedimiento de seguridad. Debido a su funcionamiento, IPSec brinda la posibilidad de que cada una de las conexiones realizadas, pueda proveer diferentes características como ser: encriptación, integridad y autenticación, o ambas. Cuando los servicios a ser brindados en una comunicación IPSec son determinados, los dos extremos deben especificar en forma exacta, los algoritmos a utilizar. Una vez tomada esta decisión, nuevamente los dos extremos deben acordar una clave de sesión. La Asociación de Seguridad, es precisamente el método que IPSec utiliza al momento de “recordar” este conjunto de datos, o dicho de otra forma, de realizar el seguimiento de todos aquellos parámetros involucrados en una comunicación IPSec.

Muchas veces el término SA, obtiene diferentes sentidos respecto del ámbito de aplicación. Por ejemplo al hablar de IKE, una SA es una Asociación de Seguridad, pero entre dos dispositivos IKE.

Una Asociación de Seguridad (SA), contiene en concreto, los siguientes parámetros:

- La definición de los algoritmos de encriptación y autenticación, el largo de las claves y otros parámetros a utilizar tal como el tiempo de vida de las claves.
- Claves de sesión para la autenticación, o HMACs y encriptación (las cuales como hemos visto, pueden ser entradas manualmente o automáticamente negociadas con la ayuda de IKE).
- Una especificación del tráfico de red al cual la SA debería ser aplicada (ejemplo: todo el tráfico IP o sólo las sesiones de TELNET).
- El tipo de protocolo (AH, ESP) y modo (Túnel, Transporte) a utilizar.

Por último, es importante mencionar que cada Asociación de Seguridad (SA), es identificada por medio de un SPI (Security Parameters Index) el cual se representa con un número de 32-bit. Un SPI, es un identificador unívoco que se encuentra localizado en la cabecera IPSec del paquete.

11.6.13 Modos de establecimiento

En secciones anteriores, mencionábamos la forma en que se lograba la autenticación inicial de una sesión IPSec, por intermedio del protocolo IKE, y hacíamos referencia a los denominados “Modos de Establecimiento”. A lo largo de las dos fases IKE de autenticación, es posible identificar al menos tres modos de establecimiento diferentes , de los cuales dos son exclusivos de la Fase I mientras que el tercero, lo es de la Fase II.

- **Modo Principal o Main mode:** De acuerdo a lo dispuesto en el RFC 2409, este modo sólo debe ser utilizado en la Fase I del intercambio IKE. El modo principal, posee tres etapas en donde se intercambian, en primer lugar, los algoritmos de autenticación y hashing a utilizar; en segundo lugar las claves públicas; y por último, se comprueba mediante el secreto compartido la autenticidad del otro extremo. El proceso completo, utiliza 6 mensajes divididos en 3 pares.
- **Modo Agresivo o Aggressive Mode:** El modo agresivo, debe ser utilizado, al igual que el modo principal, tan solo en la Fase I del intercambio IKE. Cuando el modo seleccionado es el agresivo, el intercambio de parámetros de IKE SA se realiza sin encriptación de por medio. De esta forma, se consigue que dicho intercambio, se realice en forma mucho más rápida, aunque los riesgos son mayores (no provee protección de identidad), puesto que en rigor de verdad, también se minimiza el número de mensajes transmitidos (3 contra los 6 del Modo Principal).
- **Modo Rápido o Quick Mode:** De la misma forma en la que los modos “agresivo” y “principal”, deben ser utilizados únicamente en la Fase I del intercambio IKE, el modo rápido debe ser utilizado tan solo como parte de la Fase II, una vez establecido un canal seguro (Fase I). El modo rápido, no funciona como un intercambio completo en sí mismo, aunque es el utilizado a la hora de intercambiar parámetros en torno a una Asociación de Seguridad (SA) como son el tipo de protocolo a emplear (AH, ESP o ambos) junto con el SPI, así como los algoritmos correspondientes.

En resumen, en su nivel más básico, el proceso general de una conexión IPSec podría verse como un circuito de tres pasos:

1. Se arranca una conexión ISAKMP SA utilizando el Modo Principal o el Modo Agresivo.
2. Se utiliza el Modo Rápido para negociar una SA, utilizando el IKE SA establecido.
3. Se utilizan los métodos, algoritmos y claves establecidos en el SA para la comunicación de datos entre los puntos hasta la expiración del SA gobernante.

En los apartados anteriores hemos visto los mecanismos básicos de protección, que proporcionan servicios como la confidencialidad o la autenticación.

En el momento de aplicar estos mecanismos a las redes de computadores, existen diversas opciones en cuanto al nivel de las comunicaciones donde se introduzcan les funciones de seguridad.

- La protección a nivel de red garantiza que los datos que se envíen a los protocolos de nivel superior, como TCP o UDP, se transmitirán protegidos. El inconveniente es que puede ser necesario adaptar la infraestructura de la red y, en particular los encaminadores (routers), para que entiendan las extensiones que es preciso añadir al protocolo de red (IP) para proporcionar esta seguridad.
- La protección a nivel de transporte, por su lado, tiene la ventaja de que sólo se precisa adaptar las implementaciones de los protocolos (TCP, UDP, etc.) que haya en los nodos extremos de la comunicación, que normalmente están incorporadas al sistema operativo o en librerías especializadas. En este caso, pues, sólo sería necesario un cambio en el software.
- La protección a nivel de aplicación puede responder mejor a las necesidades de ciertos

protocolos. Un ejemplo concreto es el del correo electrónico, en el que interesa proteger los datos de aplicación, es decir, los mensajes de correo, más que los paquetes a nivel de transporte o de red. Esto es así porque un mensaje es vulnerable a ataques de acceso ilegítimo o de falsificación no sólo cuando se está transmitiendo por la red sino también cuando está almacenado en el buzón del destinatario.

11.6.14 Protección a nivel de transporte: SSL/TLS/WTLS

Tal y como hemos visto en el apartado anterior, el uso de un protocolo seguro a nivel de red puede requerir la adaptación de la infraestructura de comunicaciones, por ejemplo cambiar los encaminadores IP por otros que entiendan Ipsec.

Un método alternativo que no necesita modificaciones en los equipos de interconexión es introducir la seguridad en los protocolos de transporte. La solución más usada actualmente es el uso del protocolo SSL o de otros basados en SSL.

Este grupo de protocolos comprende:

- El protocolo de transporte **Secure Sockets Layer** (SSL), desarrollado por Netscape Communications a principios de los años 90. La primera versión de este protocolo ampliamente difundida y implementada fue la 2.0. Poco después Netscape publicó la versión 3.0, con muchos cambios respecto a la anterior, que hoy ya casi no e utiliza.
- La especificación **Transport Layer Security** (TLS), elaborada por la IETF (Internet Engineering Task Force). La versión 1.0 del protocolo TLS está publicada en el documento RFC 2246. Es prácticamente equivalente a SSL 3.0 con algunas pequeñas diferencias, por lo que en ciertos contextos se considera el TLS 1.0 como si fuera el protocolo “SSL 3.1”.
- El protocolo **Wireless Transport Layer Security** (WTLS), perteneciente a la familia de protocolos WAP (Wireless Application Protocol) para el acceso a la red des de dispositivos móviles. La mayoría de los protocolos WAP son adaptaciones de los ya existentes a las características de las comunicaciones inalámbricas, y en particular el WTLS está basado en el TLS 1.0. Las diferencias se centran principalmente en aspectos relativos a el uso eficiente del ancho de banda y de la capacidad de cálculo de los dispositivos, que puede ser limitada.

El objetivo inicial del diseño del protocolo SSL fue proteger las conexiones entre clientes y servidores web con el protocolo HTTP. Esta protección debía permitir al cliente asegurarse que se había conectado al servidor auténtico, y enviarle datos confidenciales, como por ejemplo un número de tarjeta de crédito, con la confianza que nadie más que el servidor sería capaz de ver estos datos. Las funciones de seguridad, pero, no se implementaron directamente en el protocolo de aplicación HTTP, si no que se optó por introducirlas a nivel de transporte. De este modo podría haber muchas más aplicaciones que hicieran uso de esta funcionalidad.

Una característica distintiva del WTLS es que no solamente permite proteger conexiones TCP, como hacen SSL y TLS, si no que también define un mecanismo de protección para las comunicaciones en modo datagrama, usadas en diversas aplicaciones móviles.

Los servicios de seguridad que proporcionan los protocolos SSL/TLS son:

- **Confidencialidad**. El flujo normal de información en una conexión SSL/TLS consiste en intercambiar paquetes con datos cifrados mediante claves simétricas (por motivos de eficiencia y rapidez). Al inicio de cada sesión, cliente y servidor se ponen de acuerdo en que claves utilizarán para cifrar los datos. Siempre se utilizan dos claves distintas: una para los paquetes enviados del cliente al servidor, y la otra para los paquetes enviados en sentido contrario.

  Para evitar que un intruso que esté escuchando el diálogo inicial pueda saber cuales son las

claves acordadas, se sigue un mecanismo seguro de intercambio de claves, basado en criptografía de clave pública. El algoritmo concreto para este intercambio también se negocia durante el establecimiento de la conexión.

- **Autenticación de entidad**. Con un protocolo de reto-respuesta basado en firmas digitales el cliente pude confirmar la identidad del servidor al cual se ha conectado. Para validar las firmas el cliente necesita conocer la clave pública del servidor, y esto normalmente se realiza a través de certificados digitales.

  SSL/TLS también prevé la autenticación del cliente frente al servidor. Esta posibilidad, pero, no se usa tan a menudo porque muchas veces, en lugar de autenticar automáticamente el cliente a nivel de transporte, las mismas aplicaciones utilizan su propio método de autenticación.

- **Autenticación de mensaje.** Cada paquete enviado en una conexión SSL/TLS, a más de ir cifrado, puede incorporar un código MAC para que el destinatario compruebe que nadie ha modificado el paquete. Las claves secretas par el cálculo de los códigos MAC (una para cada sentido) también se acuerdan de forma segura en el diálogo inicial.

Un ejemplo de autenticación de cliente a nivel de aplicación son las contraseñas que pueden introducir los usuarios en formularios HTML. Si la aplicación utiliza este método, al servidor ya no le hace falta autenticar al cliente a nivel de transporte.

Una situación típica en que se utiliza SSL/TLS es la de un navegador web que accede a una página HTML que contiene imágenes: con HTTP “no persistente” (el único modo definido en HTTP 1.0), esto requiere una primera conexión para la página y a continuación tantas conexiones como imágenes haya. Si las conexiones pertenecen a la misma sesión SSL/TLS, sólo hace falta realizar la negociación una vez.

A más, los protocolos SSL/TLS están diseñados con estos criterios adicionales:

Eficiencia. Dos de las características de SSL/TLS, la definición de sesiones y la compresión de los datos, permiten mejorar la eficiencia de la comunicación.

- Si el cliente pide dos o más conexiones simultáneas o muy seguidas, en lu gar de repetir la autenticación y el intercambio de claves (operaciones computacionalmente costosas porque intervienen algoritmos de clave pública), hay la opción de reutilizar los parámetros previamente acordados. Si se hace uso de esta opción, se considera que la nueva conexión pertenece a la misma sesión que la anterior. En el establecimiento de cada conexión se especifica un identificador de sesión, que permite saber si la conexión empieza una sesión nueva o es continuación de otra.
- SSL/TLS prevé la negociación de algoritmos de compresión para los datos intercambiados, para compensar el tráfico adicional que introduce la seguridad. Pero ni SSL 3.0 ni TLS 1.0 especifican ningún algoritmo concreto de compresión.

Extensibilidad. Al inicio de cada sesión, cliente y servidor negocian los algoritmos que utilizarán para el intercambio de claves, la autenticación y el cifrado (a más del algoritmo de compresión). Las especificaciones de los protocolos incluyen unas combinaciones predefinidas de algoritmos criptográficos, pero dejan abierta la posibilidad de añadir nuevos algoritmos si se descubren otros que sean más eficientes o más seguros.

La capa de transporte seguro que proporciona SSL/TLS se puede considerar dividida en dos subcapas.

- La subcapa superior se encarga básicamente de negociar los parámetros de seguridad y de transferir los datos de la aplicación. Tanto los datos de negociación como los de aplicación se intercambian en mensajes.
- En la subcapa inferior, estos mensajes son estructurados en registros a los cuales se les aplica, según corresponda, la compresión, la autenticación y el cifrado.

El protocolo de registros SSL/TLS es el que permite que los datos protegidos sean convenientemente codificados por el emisor y interpretados por el receptor. Los parámetros necesarios para la protección, como pueden ser los algoritmos y las claves, se establecen de forma segura al inicio de la conexión mediante el protocolo de negociación SSL/TLS.

El protocolo de registros SSL/TLS se encarga de formar cada registro con sus campos correspondientes, calcular el MAC, y cifrar los datos, el MAC y el padding con los algoritmos y las claves que pertocan. En la fase de negociación, mientras no se hayan acordado los algoritmos, los registros no se cifran ni se autentican, es decir, se aplican algoritmos nulos.

El protocolo de negociación SSL/TLS, también llamado protocolo de encajada de manos (“Handshake Protocol”), tiene por finalidad autenticar el cliente y/o el servidor, y acordar los algoritmos y claves que se utilizaran de forma segura, es decir, garantizando la confidencialidad y la integridad de la negociación. Como todos los mensajes SSL/TLS, los mensajes del protocolo de negociación se incluyen dentro del campo de datos de los registros SSL/TLS para ser transmitidos al destinatario.

11.6.15 Ataques contra el protocolo SSL/TLS

Los protocolos SSL/TLS están diseñados para resistir los siguientes ataques:

Lectura de los paquetes enviados por el cliente y servidor. Cuando los datos se envían cifrados, un atacante que pueda leer los paquetes, por ejemplo utilizando técnicas de sniffing, se enfrenta al problema de romper el cifrado si quiere interpretar su contenido. Las claves que se utilizan para el cifrado se intercambian con métodos de clave pública, que el atacante tendría que romper si quiere saber cuales son los valores acordados.

Es preciso advertir, pero, que dependiendo de la aplicación que lo utilice, el protocolo SSL/TLS puede ser objeto de ataques con texto en claro conocido. Por ejemplo, cuando se utiliza juntamente con HTTP para acceder a servidores web con contenidos conocidos.

Si la comunicación es totalmente anónima, es decir sin autenticación de servidor ni cliente, sí que existe la posibilidad de capturar las claves secretas con un ataque conocido como “hombre a medio camino” (en inglés, “man-in-themiddle attack”). En este ataque el espía genera sus propias claves públicas y privadas, y cuando una parte envía a la otra información sobre su clave pública, tanto en un sentido como en el otro, el atacante la intercepta y la sustituye por la equivalente con la clave pública fraudulenta. Dado que el intercambio es anónimo, el receptor no tiene manera de saber si la clave pública que recibe es la del emisor auténtico o no.

En cambio, si se realiza la autenticación de servidor y/o cliente, es necesario enviar un certificado donde tiene que haber la clave pública del emisor firmada por una autoridad de certificación que el receptor reconozca, y por tanto no puede ser sustituida por otra.

Suplantación de servidor o cliente. Cuando se realiza la autenticación de servidor o cliente, el certificado digital debidamente firmado por la CA sirve para verificar la identidad de su propietario. Un atacante que quiera hacerse pasar por el servidor (o cliente) auténtico debería obtener su clave privada, o bien la de la autoridad de certificación que ha emitido el certificado para poder generar otro con una clave pública diferente y que parezca auténtico.

Alteración de los paquetes. Un atacante puede modificar los paquetes para que lleguen al destinatario con un contenido distinto del original (si están cifrados no podrá controlar cual será el contenido final descifrado, solamente sabrá que será distinto al original). Si pasa esto, el receptor detectará que el paquete ha sido alterado porque el código de autenticación (MAC) casi con total seguridad será incorrecto.

Si la alteración se realiza en los mensajes de negociación cuando aun no se aplica ningún código MAC, con la finalidad por ejemplo de forzar la adopción de algoritmos criptográficos más débiles y vulnerables, esta manipulación será detectada en la verificación de los mensajes Finished.

Repetición, eliminación o reordenación de paquetes. Si el atacante vuelve a enviar un paquete correcto que ya había sido enviado antes, o suprime algún paquete haciendo que no llegue a su destino, o los cambia de orden, el receptor lo detectará porque los códigos MAC no coincidirán con el valor esperado. Esto es así porque en el cálculo del MAC se utiliza un número de secuencia que se va incrementando en cada paquete.

Tampoco se pueden copiar los mensajes enviados en un sentido (de cliente a servidor o de servidor a cliente) al sentido contrario, porque en los dos flujos de la comunicación se utilizan claves de cifrado y de MAC diferentes.

Como consideración final, cabe destacar que la fortaleza de los protocolos seguros recae no solamente en su diseño si no en el de las implementaciones. Si una implementación solamente soporta algoritmos criptográficos débiles (con pocos bits de clave), o genera números pseudoaleatórios fácilmente predecibles, o guarda los valores secretos en almacenamiento (memoria o disco) accesible por atacantes, etc., no estará garantizando la seguridad del protocolo.

11.7 PREGUNTAS Y TIPS

- **¿Cuál es el modo más seguro para la implementación de la Fase I de IPSec?** Modo agresivo
- **¿Cuál de los protocolos componentes de SSL, se encarga de la autenticación entre los extremos?** Handshake Protocol
- **¿Cuál es el protocolo utilizado por IPSec para proporcionar confidencialidad?** ESP
- **¿Qué necesita IPSec para proporcionar servicio contra la réplica?** ESP
- **¿Qué utiliza IPSec para negociar en forma automática las Asociaciones de Seguridad?** IKE
- **¿Cuáles son redes de transporte válidas para la implementación de L2TP?** ATM, IP, X.25
- **¿Cuáles de las siguientes son ventajas de una implementación VPN?** Bajo costo, Accesibilidad
- **¿Con qué valor se identifica al protocolo AH en IP v4?** 51
- **¿Cuál es el modo de operación IPSec indicado, cuando se requiere seguridad extremo a extremo en las comunicaciones de host a host?** Modo Transporte
- **¿Es posible utilizar PPTP en un ambiente de red interna o LAN?** Si
- **¿Qué utiliza PPTP para encapsular PPP en datagramas IP?** GRE
- **¿Cuáles son los protocolos de los cuales deriva L2TP?** L2F, PPTP

CAPÍTULO 12

12.1 SEGURIDAD EN E-COMMERCE

Seguramente han sido muchas, las veces que hemos escuchado en boca de empresarios, responsables de áreas de tecnología y público en general, la frase “Internet ha cambiado la forma de hacer negocios”.

A tan solo algunos años del surgimiento de Internet como plataforma global de comunicaciones, ya eran varios los emprendedores que, con visión de futuro y un porcentaje de riesgo importante, apostaban al desarrollo de un mercado, que poco tiempo después, se convertiría quizás, en uno de los ámbitos más prominentes para el desarrollo comercial.

A lo largo de esta unidad, estudiaremos los principales conceptos detrás de las transacciones comerciales en general y del comercio electrónico en particular. Revisaremos algunas de las tecnologías claves que asisten a los profesionales de seguridad informática a la hora de diseñar una plataforma de cómputo segura orientada específicamente a brindar servicios de E-Commerce, y nos detendremos a evaluar aquellos aspectos que no siendo técnicos, influyen en su ámbito de aplicación.

¿Cuál es la diferencia entre HTTP y HTML? El protocolo de transferencia de hipertexto (HTTP) es un protocolo de nivel de aplicación del stack TCP/IP que define una serie de métodos e instrucciones simples, basadas en ASCII, para comunicar al servidor Web con el cliente (Browser) mientras que HTML (Lenguaje de marcas de hipertexto) es el lenguaje definido por medio de una serie de “etiquetas” que establecen las características y el formato de los elementos dispuestos en un documento Web.

¿Qué ventajas y desventajas poseen las aplicaciones CGI? Las aplicaciones CGI (Interfaz Común de Gateway) son una forma flexible y potente al momento de generar contenidos Web dinámicos, permitiendo nutrir al sitio Web a partir de información ingresada por los clientes y así personalizar la información. Por otro lado, muchas veces, las malas prácticas de programación en estos componentes generan un grave riesgo desde el punto de vista de la seguridad.

¿Cuál es la ventaja de un escáner de vulnerabilidades? Es una herramienta de evaluación de vulnerabilidades que buscará determinar, en los dispositivos de la red, los puertos abiertos y las vulnerabilidades o exploits conocidos, entorno a las aplicaciones o servicios que se encuentren activos en éstos.

¿Qué características debe cumplir una comunicación segura? Debe satisfacer 4 requisitos a saber: privacidad o confidencialidad del mensaje, garantizando su interpretación por parte del destinatario previsto, identificación del remitente, integridad del contenido del mensaje y conocimiento de la recepción.

12.2 SERVICIOS WEB

A pesar de que los servicios WEB tal como hoy los conocemos, suele ser mencionado como una tecnología sumamente novedosa, lo cierto es que conceptualmente, ya en 1945, el director de la Oficina de Desarrollo e Investigación Científica de los EE.UU. (Dr. Vannevar Bush), dejaba entrever su preocupación en un artículo aparecido en “The Athlantic Online”, en el cual mencionaba que la cantidad de información que estaba siendo generada por aquella época, se transformaba en contenido inútil al no existir ningún sistema que permitiera encontrar y relacionar una búsqueda puntual. En el

mismo artículo, Vannevar, proponía el desarrollo de un dispositivo personal, llamado “memex”, un aparato que según su creador, permitiría a cada individuo almacenar su información en microfilmes, consultarlos rápidamente, y lo que es más importante, crear vínculos entre un documento y otro.

Algunos años más tarde, a fines de los 60, Douglas Engelbart, presentaba un método denominado NLS (oNLine System), el cual requería de un entorno de trabajo por computadora, el cual permitía almacenar publicaciones con catálogos, índices y reglas específicas para citar documentos en forma rápida y sencilla por parte del lector. En este sistema, los archivos de documentos se almacenaban en forma jerárquica para facilitar su acceso.

Pero fue en 1965, cuando el término “hipertexto”, acuñado por Ted Nelson en un artículo publicado bajo el nombre “A File Structure for the Complex, the Changing, and the Indeterminate", pasaría a formar parte de la historia. En su trabajo, Nelson presentaba un modelo para la interconexión de documentos electrónicos, que serviría de base para lo que en 1989, se daría a conocer como “World Wide Web”, un desarrollo conceptual de Tim Berners-Lee, un investigador del CERN (Organización Europea de Investigación Nuclear), el cual comprendía un sistema de Hipertexto, para compartir información basado en Internet, concebido originalmente para servir como herramienta de comunicación entre los científicos nucleares del CERN. Finalmente en 1990, Tim Berners-Lee escribiría junto a Robert Cailliau, el primer browser de la historia: “WorldWide Web”.

Mucho tiempo ha pasado ya, desde aquellos primeros momentos en donde Internet, mostraba su cara a través de una Word Wide Web estática, en donde podía encontrarse sólo información respecto de investigaciones universitarias o de organizaciones gubernamentales. Hoy en día, una gran cantidad de propuestas, se ciernen sobre la web, creando de ésta un espacio de alcance mundial, con información de todo tipo y color.

Nuevas tecnologías, han hecho que los servicios web se vuelvan atractivos, interactivos y en muchos casos necesarios para el normal funcionamiento de los negocios. Aplicaciones WEBs, en torno a esta tecnología, se han transformado en el nuevo estándar de facto al momento de ser distribuidas a través de Intranet, transformando la forma en la que los nuevos desarrolladores, diseñan y distribuyen sus aplicaciones.

En líneas generales, un servicio web, es referido como la acción de publicar información en un servidor conectado a una red (Internet, Intranet, etc.), por medio de un conjunto de métodos y tecnologías estándares (TCP/IP, HTTP, HTML, etc.).

Un esquema típico, suele encontrarse conformado, por un servidor conectado a Internet, en el cual se ha configurado la posibilidad de “servir” páginas web, generalmente a través de un puerto específicamente designado a tal efecto (80, 443). De esta forma, valiéndose de la estructura de nombres provista por DNS (Domain Name Service), usuarios conectados a la RED, pueden acceder un servicio web, haciendo referencia a lo que se conoce como URL (Uniform Resource Locator). Dicha conexión, suele realizarse en la mayoría de los casos, por medio de un tipo de software cliente denominado “browser”, el cual interpreta de una determinada forma, la información contenida en el servidor que se encuentra publicando el servicio a acceder, y la presenta al cliente que realizará el requerimiento.

Pero la tecnología no se detiene y es importante mencionar que en este último tiempo, el término de Servicio WEB, ha comenzado a ser utilizado para hacer referencia a un pequeño grupo de componentes, desarrollados sobre tecnologías web, que a través de una interfaz claramente definida y conocida, puede ser accedidos a través de Internet de la misma forma que una página web, pero que apuntan a cambiar una Internet centrada en las personas, y basada en los contenidos, a aquella que se piensa, estará centrada en aplicaciones y basada en servicios.

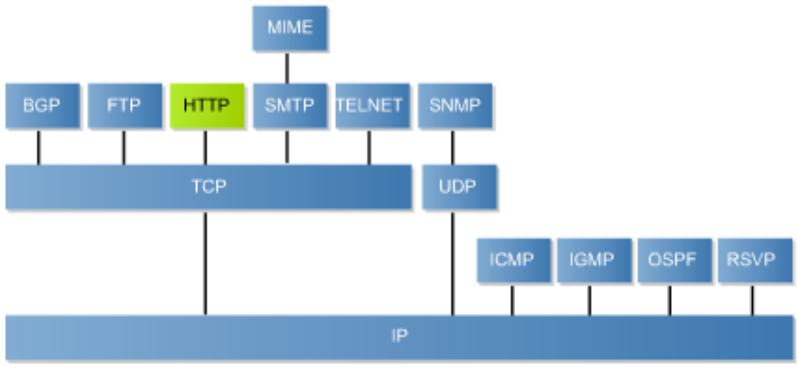
12.2.1 HTTP y HTTP/S

Como mencionáramos en indicadores anteriores, una arquitectura típica basada en World Wide Web,

tiene como participantes principales, un servidor sirviendo una página web en un formato determinado y un cliente que entiende e interpreta la información provista por dicha página web.

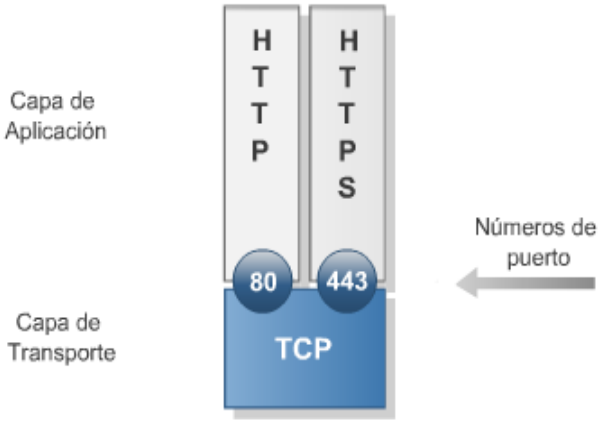
¿Pero cuál es el método utilizado por un cliente al momento de requerir información a un web server?

De acuerdo como se encuentra definido en el RFC 1945, HTTP (Hypertext Transfer Protocol) es un protocolo de nivel de aplicación, con la liviandad y velocidad necesaria al momento de entrelazar sistemas de información de hypermedia, como por ejemplo la World Wide Web.



Sin dudas una de los aspectos que más a contribuido al éxito de HTTP, como medio de comunicación entre cliente y servidor, se encuentra relacionado con la simplicidad de su definición como protocolo ASCII, sin estado, y basado en un pequeño set de posibilidades, solicitudes y respuestas.

HTTP, define un mecanismo tendiente a solicitar un recurso determinado a un servidor web, al cual suele denominarse URI (Uniform Resource Identifiers) o Identificador Uniforme de Recurso. Un URI puede resultar ser, desde una página de texto estática, hasta una que contenga videos o cualquier otro tipo de información que se encuentre dentro de los formatos soportados por su especificación.



Como parte de su definición, HTTP propone una serie de métodos o instrucciones tendientes a administrar un conjunto de respuestas y solicitudes, entre las que se encuentran: GET, PUT, HEAD, etc.

Un aspecto sumamente importante respecto de HTTP, desde el punto de vista de su seguridad, radica en su condición de protocolo ASCII, y la posibilidad de que pueda ser interpretado por cualquier persona con la capacidad de interceptar una solicitud enviada a un servidor remoto, sin necesidad de recurrir a complicadas técnicas de traductores, decompiladores o demás herramientas.

A fin de resolver esta última cuestión, surgieron diferentes propuestas de la industria, aunque una de las más aceptadas ha sido sin lugar a dudas, la denominada HTTPS, la cual en su nivel más básico, no es más que la implementación de HTTP, sobre SSL/TLS (Secure Socket Layer/Transport Layer Security). Puesto que tanto SSL como TLS pueden proporcionar cifrado en la capa de transporte, un posible intermediario encontraría alguna dificultad adicional, a la hora de interpretar, el tráfico HTTP interceptado.

Métodos HTTP	
OPTIONS	Este método representa un petición de información sobre las opciones de comunicación disponibles en la cadena petición-respuesta identificada por la URI de la petición. Esto permite al cliente conocer las opciones y requisitos asociados con un recurso o las capacidades del servidor.
GET	El método GET requiere la devolución de información al cliente identificada por la URI. Si la URI se refiere a un proceso que produce información, se devuelve la información y no la fuente del proceso.
HEAD	El método HEAD es igual que el método GET, salvo que el servidor no tiene que devolver el contenido, sólo las cabeceras. Estas cabeceras que se devuelven en el método HEAD deberían ser las mismas que las que se devolverían si fuese una petición GET.
POST	El método POST se usa para hacer peticiones en las que el servidor destino acepta el contenido de la petición como un nuevo subordinado del recurso pedido. El método POST se creó para cubrir funciones como la de enviar un mensaje a grupos de usuarios, dar un bloque de datos como resultado de un formulario a un proceso de datos, añadir nuevos datos a una base de datos, etc.
PUT	El método PUT permite guardar el contenido de la petición en el servidor bajo la URI de la petición. Si esta URI ya existe, entonces el servidor considera que esta petición proporciona una versión actualizada del recurso. Si la URI indicada no existe y es válida para definir un nuevo recurso, el servidor puede crear el recurso con esa URI. Si se crea un nuevo recurso, debe responder con un código 201 (creado), si se modifica se contesta con un código 200 (OK) o 204 (sin contenido). En caso de que no se pueda crear el recurso se devuelve un mensaje con el código de error apropiado.
DELETE	Este método se usa para que el servidor borre el recurso indicado por la URI de la petición. No se garantiza al cliente que la operación se lleve a cabo aunque la respuesta sea satisfactoria.
TRACE	Este método se usa para saber si existe el receptor del mensaje y usar la información para hacer un diagnóstico. En las cabeceras el campo Via sirve para obtener la ruta que sigue el mensaje. Mediante el campo Max-Forwards se limita el número de pasos intermedios que puede tomar. Esto es útil para evitar bucles entre los proxy.

Algunas de las Respuestas HTTP más comúnes:	
100, continuar. 101, cambio de protocolo. 200, éxito. 201, creado. 202, aceptado. 203, información no autoritativa. 204, sin contenido. 205, contenido reestablecido. 206, contenido parcial. 300, múltiples elecciones. 301, movido permanentemente. 302, movido temporalmente. 303, ver otros. 304, no modificado. 305, usar proxy. 400, petición errónea. 401, no autorizado. 402, pago requerido. 403, prohibido.	404, no encontrado. 405, método no permitido. 406, no se puede aceptar. 407, se requiere autentificación proxy. 408, límite de tiempo de la petición. 409, conflicto. 410, gone. 411, tamaño requerido. 412, falla una precondición. 413, contenido de la petición muy largo. 414, URI de la petición muy largo. 415, campo media type requerido. 500, error interno del servidor. 501, no implementado. 502, puerta de enlace errónea. 503, servicio no disponible. 504, tiempo límite de la puerta de enlace. 505, versión de protocolo HTTP no soportada.

12.2.2 Formatos: HTML, ASP, PHP, JSP y XML

Desde un primer momento, el concepto de Hipertexto aplicado a la World Wide Web, se encontraba basado en la necesidad de vincular diferentes tipos de información, de acuerdo a características en

común. La forma práctica de realizar esta tarea en una arquitectura Web, depende en gran parte de las características propias de los lenguajes o recursos técnicos desarrollados a tal efecto. Si bien en un principio, el requerimiento fue tan solo presentar texto enlazado, hoy en día, suele requerirse interactividad y diseños atractivos, motivo por el cual, nuevas herramientas se suman a aquellas que han hecho historia.

A continuación, repasaremos brevemente alguno de los recursos más ampliamente utilizados por los desarrolladores, a la hora de diseñar, desde sencillas páginas estáticas, hasta grandes aplicaciones basadas en web.

HTML son las siglas de “Lenguaje de Marcado de Hipertexto” y como su nombre lo indica, se define como una serie de “etiquetas” que serán las responsables de establecer el formato o las características de los elementos dispuestos en un documento. En HTML, las etiquetas se encuentran delimitadas por caracteres del tipo “<” y “>”, y su función es la de delimitar un conjunto de formatos y funcionalidades definidas en la especificación HTML.

El funcionamiento de HTML, es sumamente sencillo. Cuando se visualiza un documento escrito en HTML, en un explorador Web, este interpreta las etiquetas y su función específica, y muestra el resultado de la misma. A pesar de ser el primer lenguaje utilizado al momento de presentar páginas Web, HTML sigue siendo una tecnología ampliamente utilizada en la actualidad.

ASP, son las siglas de “Activate Server Pages”, designadas para definir una tecnología introducida por Microsoft en 1996. Es parte del Internet Information Server (IIS) desde la versión 3.0 y es una tecnología de páginas activas que permite el uso de diferentes scripts y componentes en conjunto con el tradicional HTML para mostrar páginas generadas dinámicamente.

ASP es una tecnología dinámica funcionando del lado del servidor, por lo tanto, cuando un usuario solicita un documento ASP a un servidor web, las instrucciones de programación dentro del script (Documento ASP) son ejecutadas para enviar al navegador únicamente el código HTML resultante. Una de las principales ventajas detrás de ASP, radica en la seguridad que tiene el programador sobre su código, ya que éste se encuentra únicamente en los archivos del servidor que al ser solicitado a través del web, es ejecutado, por lo que los usuario no tienen acceso más que a la página resultante en su navegador.

XML (eXtensible Markup Language, Lenguaje de Marcación Extensible), es una especificación de la W3C (World Wide Web Consortium) tendiente principalmente (no únicamente) a especificar un nuevo método para almacenar y estructurar datos, de forma tal que los mismos puedan ser transmitidos a través de la Web. XML se muestra en realidad, como un conjunto de tecnologías asociadas, capaces de colaborar en la resolución de muchos de los problemas a los que suele enfrentarse un desarrollador al momento de presentar servicios y documentos en la Web. En pocas palabras, XML es un metalenguaje, un lenguaje a partir del cual es factible definir otro tipo de lenguajes. Asi mismo, a pesar de partir de la idea propuesta por SGML (Standard Generalized Markup Language,ISO 8879), XML no es ningún tipo de documento SGML sino que es una versión abreviada de SGML optimizada para su utilización en Internet. Esto significa que a través de él, es factible definir nuestros propios tipos de documentos (Lo cual incluye por ejemplo etiquetas propias) y por lo tanto, ya no dependeremos de un único e inflexible tipo de documento HTML.

PHP es un lenguaje de programación interpretado, diseñado originalmente para la creación de páginas web dinámicas. Es usado principalmente en interpretación del lado del servidor (server-side scripting) pero actualmente puede ser utilizado desde una interfaz de línea de comandos o en la creación de otros tipos de programas incluyendo aplicaciones con interfaz gráfica usando las bibliotecas Qt o GTK+. PHP es un acrónimo recursivo que significa PHP Hypertext Pre-processor (inicialmente PHP Tools, o, Personal Home Page Tools). Fue creado originalmente por Rasmus Lerdorf en 1994; sin embargo la implementación principal de PHP es producida ahora por The PHP Group y sirve como el estándar de facto para PHP al no haber una especificación formal. Publicado

bajo la PHP License, la Free Software.

El gran parecido que posee PHP con los lenguajes más comunes de programación estructurada, como C y Perl, permiten a la mayoría de los programadores crear aplicaciones complejas con una curva de aprendizaje muy corta. También les permite involucrarse con aplicaciones de contenido dinámico sin tener que aprender todo un nuevo grupo de funciones.

Cuando el cliente hace una petición al servidor para que le envíe una página web, el servidor ejecuta el intérprete de PHP. Éste procesa el script solicitado que generará el contenido de manera dinámica (por ejemplo obteniendo información de una base de datos). El resultado es enviado por el intérprete al servidor, quien a su vez se lo envía al cliente. Mediante extensiones es también posible la generación de archivos PDF, Flash, así como imágenes en diferentes formatos. Permite la conexión a diferentes tipos de servidores de bases de datos tales como MySQL, Postgres, Oracle, ODBC, DB2, Microsoft SQL Server, Firebird y SQLite.

PHP también tiene la capacidad de ser ejecutado en la mayoría de los sistemas operativos, tales como UNIX (y de ese tipo, como Linux o Mac OS X) y Windows, y puede interactuar con los servidores de web más populares ya que existe en versión CGI, módulo para Apache, e ISAPI.

PHP es una alternativa a las tecnologías de Microsoft ASP y ASP.NET (que utiliza C# VB.NET como lenguajes), a ColdFusion de la compañía Adobe (antes Macromedia), a JSP/Java de Sun Microsystems, y a CGI/Perl.

Ventajas:

- Es un lenguaje multiplataforma.
- Capacidad de conexión con la mayoría de los manejadores de base de datos que se utilizan en la actualidad, destaca su conectividad con MySQL.
- Capacidad de expandir su potencial utilizando la enorme cantidad de módulos (llamados ext's o extensiones).
- Posee una amplia documentación en su página oficial ([2]), entre la cual se destaca que todas las funciones del sistema están explicadas y ejemplificadas en un único archivo de ayuda.
- Es libre, por lo que se presenta como una alternativa de fácil acceso para todos.
- Permite las técnicas de Programación Orientada a Objetos.
- Biblioteca nativa de funciones sumamente amplia e incluida.
- No requiere definición de tipos de variables.
- Tiene manejo de excepciones (desde PHP5).

JavaServer Pages (**JSP**) es una tecnología Java que permite generar contenido dinámico para web, en forma de documentos HTML, XML o de otro tipo.

Esta tecnología es un desarrollo de la compañía Sun Microsystems. La Especificación JSP 1.2 fue la primera que se liberó y en la actualidad está disponible la Especificación JSP 2.1.

Las JSP's permiten la utilización de código Java mediante scripts. Además, es posible utilizar algunas acciones JSP predefinidas mediante etiquetas. Estas etiquetas pueden ser enriquecidas mediante la utilización de Librerías de Etiquetas (TagLibs o Tag Libraries) externas e incluso personalizadas. JSP puede considerarse como una manera alternativa, y simplificada, de construir servlets. Es por ello que una página JSP puede hacer todo lo que un servlet puede hacer, y viceversa. Cada versión de la especificación de JSP está fuertemente vinculada a una versión en particular de la especificación de servlets.

El funcionamiento general de la tecnología JSP es que el Servidor de Aplicaciones interpreta el código

contenido en la página JSP para construir el código Java del servlet a generar. Este servlet será el que genere el documento (típica mente HTML) que se presentará en la pantalla del Navegador del usuario.

En JSP se crean páginas de manera parecida a como se crean en ASP o PHP. Generamos archivos con extensión .jsp que incluyen, dentro de la estructura de etiquetas HTML, las sentencias Java a ejecutar en el servidor. Antes de que sean funcionales los archivos, el motor JSP lleva a cabo una fase de traducción de esa página en un servlet, implementado en un archivo class (Byte codes de Java). Esta fase de traducción se lleva a cabo habitualmente cuando se recibe la primera solicitud de la página .jsp, aunque existe la opción de pre compilar en código para evitar ese tiempo de espera la primera vez que un cliente solicita la página.

12.2.3 Arquitectura

Como todo proyecto, el desarrollo y puesta en marcha de un sitio web, comienza con la definición de su arquitectura. Siguiendo con el patrón lógico a la hora de velar por la seguridad de la información, es de suma importancia, que el profesional de seguridad informática, se encuentre involucrado en la implementación de un proyecto WEB, desde el momento mismo en el cual se define su arquitectura. Todo punto de control mencionado en esta etapa, hará la diferencia entre un sitio web seguro y uno con claras deficiencias de diseño, fácilmente aprovechables por un atacante. Cuando hablamos de Arquitectura, en relación a un sitio web, nos estamos refiriendo específicamente, a los distintos componentes que forman parte de la misma, y el modo en el que interactúan entre sí. En su nivel más básico, una arquitectura WEB típica, se encuentra conformada por los siguientes cuatro elementos:

1. Un servidor central conectado a Internet, configurado con los servicios necesarios a la hora de servir páginas web (Básicamente un demonio o servicio HTTP)
2. Protocolos en común (TCP/IP, HTTP, HTTPS, S-HTTP, etc.)
3. Formato de documentos estandarizados (HTML, ASP, PHP, JSP, etc.)
4. Clientes estándares capaces de interpretar la información publicada.

Al margen de los mencionados componentes, existen quienes suscriben como parte fundamental de una arquitectura Web, a aquellos aspectos que siendo propios de la etapa de diseño (Usabilidad, estructura de documentación jerárquica en cuanto a su publicación, nivel de interactividad, etc.) repercuten fuertemente en el resultado final de cara al usuario.

Por otra parte, debemos ser conscientes que este modelo básico, poco a poco ha ido cambiando hasta transformar un sitio web, en algo verdaderamente complejo. Este nuevo escenario, se encuentra conformado por aplicaciones, en donde diseño gráfico, programación avanzada, esquemas de redundancia, técnicas de clustering y utilización de bases de datos, se dan cita para conformar arquitecturas específicas en torno a cada uno de estos nuevos componentes, haciendo de ella, un verdadero desafío para todo profesional relacionado con la tecnología de la información en general y la seguridad informática en particular.

12.2.4 Control de acceso

Probablemente, uno de los principales inconvenientes a los que se enfrenta todo aquel individuo o empresa, a la hora de montar sus servicios web en Internet, es el de controlar quienes deben tener acceso a la información allí publicada y bajo que condiciones. La exposición a nivel mundial, que otorga una red pública como Internet, en conjunto con los mínimos requerimientos necesarios por parte de un usuario (browser y cuenta con un ISP), al momento de acceder alguno de estos recursos desde la comodidad de su hogar, hacen del control de acceso a sitios y aplicaciones web, un tema que merece ser tratado con el mayor de los cuidados.

Con frecuencia, suele suceder que información pública (de libre acceso) y privada (con acceso discrecional) compartan un mismo Website. Si bien es cierto que como punto de partida, nunca debería publicarse información confidencial en un sitio web dispuesto en Internet, en rigor de verdad la dinámica de los negocios ha hecho que hoy en día, estrictas políticas al respecto, no siempre sean factibles de ser llevadas a la práctica.

A fin de resolver en parte, el inconveniente planteado en los párrafos anteriores, diversos métodos de autenticación, han venido siendo implementados con mayor o menor grado de éxito, por desarrolladores web y oficiales de seguridad. Entre los más frecuentes se encuentran:

- Autenticación basada en formularios Suele ser uno de los métodos más utilizados a la hora de solicitar identificación On-Line. En este escenario, se solicita por medio de un formulario diseñado a tal efecto, nombre de usuario y contraseña, tras lo cual se intenta validar el usuario ya sea contra un archivo plano almacenado localmente en el webserver, una base de datos en backend o algún otro tipo de soporte de datos.
- Autenticación Básica Este método, fue uno de los primeros implementados y se basa en la codificación en base64, de la información de usuario y contraseña proporcionada por el usuario que solicita el acceso.
- Autenticación Digest (Resumen) Cuando el método de autenticación seleccionado es aquel basado en Digest, el funcionamiento del proceso relacionado, es idéntico al utilizado en un esquema de autenticación básica, con la única diferencia que en este caso la información de usuario y contraseña en tránsito, se resumen utilizando un algoritmo criptográfico como MD5.
- NTLM Se trata de un método de autenticación propiedad de Microsoft, por medio del cual se implementa el esquema LM (Lan Manager) en las cabeceras de solicitud y respuesta HTTP.
- Microsoft Passport Es uno de los métodos más novedosos. Utiliza claves compartidas entre Microsoft y sitios asociados, así como también información dispuesta en cookies. Cuando es implementado, permite a los sitios web asociados a este servicio, autenticar usuarios basándose en su afiliación al servicio “Microsoft Passport Single Sing-In”

12.2.5 Estructura de directorio

Cualquiera que sea la plataforma o el software de servidor Http, que se haya decidido implementar a la hora de servir páginas Web, la definición de una adecuada estructura de directorios, debe ser uno de los principales puntos a tener en cuenta a la hora de pensar la seguridad de un sitio desde el momento mismo de su diseño. La forma en la que se proceda en este paso, incidirá directamente en las posibilidades de segurización con las que podrá contar al momento de administrar cuestiones tales como: listas de control de acceso, generación de logs detallados, etc.

Por definición, todo software de servidor web que instale, generalmente creará como parte del proceso estándar de instalación, un directorio de inicio por cada sitio web que se requiera administrar, al cual comúnmente solemos referirnos como “root” o “raíz”. También conocido como “webroot”, esta será la carpeta donde se encontrara la página de inicio (La cual tendrá un nombre del tipo: index.htm, index.html, default.htm, default.html, etc.) además de convertirse en el nivel más alto de la jerarquía, desde donde se desprenderá la estructura de directorios tendiente a contener la información a publicar. A continuación mencionaremos brevemente, algunos de los puntos más importantes a tener en cuenta, precisamente a la hora de definir la estructura de directorio más adecuada para un webserver:

- La estructura de directorio en general, deberá ser pensada en torno al tipo de ACL o DACL que se requerirá implementar, en función del tipo de contenido dispuesto en cada directorio (Scripts, Contenido Estático, Contenido Dinámico, etc.)
- Deberán proveerse directorios específicos para albergar todo contenido dinámico o Scripts, que requieran de permisos de escritura o modificación por parte del usuario. Estos a su vez

deberán contar con el seguimiento de auditoria necesario a fin de detectar actividad sospechosa. En caso de que sea posible, deberá tratar de evitarse la escritura en CUALQUIER directorio del webserver por parte de los usuarios y Scripts ejecutados.

- Si el servicio a implementar es IIS, deberá cambiarse el webroot por defecto, a una partición distinta a la que contiene el sistema operativo. Al mismo tiempo, se deberá mover, renombrar o restringir el acceso a cualquier utilidad potencialmente dañina (Ejemplo: CMD.EXE).
- En caso de que el webserver a implementar sea Apache, se recomienda prestar atención a la forma en la que se configurarán los enlaces simbólicos. Si bien es cierto que en algunos casos, su implementación puede tener alguna ventaja desde el punto de vista de la seguridad, mal implementado podría permitir a un atacante, escapar del webroot.
- La utilización de dispositivos externos como ser CD Roms, para el almacenamiento de información estática contenida en el webserver, suele resultar una buena opción bajo ciertas circunstancias.
- En lo posible, se deberá tratar de almacenar los directorios correspondientes a información de logueo y archivo temporales, en particiones o equipos diferentes a aquel donde se publica el Website a asegurar.

12.2.6 Control de archivos y logs

Uno de los principios fundamentales, a la hora de administrar un sitio web, es el de conocer con exactitud, todo aquello que sucede respecto del funcionamiento del mismo. A partir del conocimiento detallado de esta información, el administrador podrá entre otras cuestiones:

- Evaluar aspectos relacionados con la performance del equipo o servicio.
- Detectar algún tipo de utilización fraudulenta respecto del servicio prestado.
- Identificar el origen de un ataque.
- Obtener las pruebas necesarias a la hora de iniciar algún tipo de acción judicial.
- Detectar la modificación de archivos fundamentales para el sistema.

La mayoría de las plataformas utilizadas en la actualidad, poseen su propio esquema de auditoria y generación/administración de logs. A pesar de ello, con frecuencia el profesional de seguridad informática, requerirá prestaciones dispuestas en herramientas de terceros o Scripts específicamente diseñados, a la hora de visualizar en forma ágil, rápida y ordenada, aquella información que contenida en el syslog/eventlog, en relación a los distintos eventos de sistema previamente configurados, pueda servir de utilidad ante un incidente o cualquier acción administrativa que dependa de dicha información.

Como hemos visto en indicadores anteriores, gran parte de la funcionalidad de un webserver, se encuentra relacionada con información contenida en archivos o carpetas. Puesto que generalmente, el destino de estos servidores, se encuentra relacionado con su exposición a Internet, el control de los mismos es imprescindible a la hora de asegurar el correcto funcionamiento del site administrado.

Por otro lado, probablemente, una de las prácticas de seguridad más importantes en relación a un webserver, se encuentra relacionada con el control de cambios en los archivos que lo componen. Bien sean estos, archivos de configuración del sistema o el propio contenido del webserver, se deberá contemplar la utilización de herramientas de integridad de archivos del estilo de Tripwire o AIDE. A pesar de las diferencias entre si, este tipo de herramientas permiten básicamente, obtener una instantánea al momento de instalar un webserver, para lo cual generan un valor de resumen o digest, por cada uno de los archivos presentes en la instalación. Esta información debería luego ser almacenada en algún tipo de medio no re-gravable, sobre el cual planificar comparaciones con la

periodicidad que se considere necesaria en cada caso.

AIDE (Advanced Intrusion Detection Environment, Entorno Avanzado de Detección de Intrusos): AIDE es un sistema de detección de intrusos basado en host (HIDS, Host-Based Intrusion Detection System), una alternativa libre a Tripwire (si usted ya conoce Tripwire no debería tener dificultades para aprender a configurar AIDE). Los HIDS se usan para detectar cambios en los ficheros de configuración y binarios importantes, generalmente generando un resumen cifrado ("hash") único de los ficheros a ser verificados, y almacenándolos en un lugar seguro. Con un procedimiento regular (tal que una vez al día), los resúmenes "buenos" se comparan con los generados a partir de la copia actual de cada fichero, para determinar si el fichero ha cambiado. Los HIDS son una gran herramienta para detectar cambios no permitidos en un sistema, pero necesitan un poco de trabajo para implementarlos adecuadamente y hacer un buen uso de ellos.

Tripwire una herramienta de seguridad e integridad de datos. Tripwire compara los archivos y directorios con una base de datos de la ubicación de archivos, las fechas en que han sido modificados y otros datos. Tripwire genera la base tomando una instantánea. Esta base de datos contiene fundamentos — los cuales son instantáneas de archivos y directorios específicos en momentos particulares. Los contenidos de la base de datos de fundamentos deberían ser generados antes de que el sistema esté en riesgo, esto es antes de que se conecte a la red. Después de crear la base de datos de fundamentos, Tripwire compara la base de datos actual con la base de datos de fundamentos e informa de cualquier modificación, adición o eliminación. El software de aseguramiento de integridad de los datos Tripwire, monitorea la consistencia de archivos y directorios de sistema críticos identificando todos los cambios hechos a ellos. Esto lo hace mediante un método automatizado de verificación que se ejecuta a intervalos regulares. Si Tripwire detecta que uno de los archivos monitoreados ha sido cambiado, lo notifica al administrador del sistema vía email. Debido a que Tripwire puede fácilmente identificar los archivos que son modificados, agregados o eliminados, se agiliza el proceso de recuperación luego de una entrada forzada pues mantiene el número de archivos que deben ser restaurados a un mínimo. Estas habilidades hacen de Tripwire una herramienta excelente para los administradores de sistemas que requieren tanto de facilidades para detección de intrusos como de control de daños para sus servidores.

12.2.7 Desbordamiento de Bufer

A fin de comprender el significado del término “Desbordamiento de Buffer” o “Buffer Overflows”, deberemos conocer la forma en la que comúnmente funciona un programa en tiempo de ejecución. En líneas generales y explicado breve mente, un programa o código ejecutable típico, utiliza un espacio de memoria determinado, para el almacenamiento del propio código y de los datos que vaya a utilizar en su corrida. De igual forma, cualquier tipo de dato o parámetro adicional que requiera ser recibido por el código ejecutable, a partir de una input externo al procedimiento en ejecución, requerirá ser almacenado también en un espacio de memoria temporal. Dicho esto, podremos establecer en su definición más amplia, que un desbordamiento de buffer es una vulnerabilidad que se produce cuando un programa, es poco estricto en la gestión de su espacio de memoria o no comprueba adecuadamente la longitud correcta de las entradas. Malas prácticas de programación, en conjunto con el descuido y la falta de control en las etapas de desarrollo y testing de aplicaciones, suelen ser frecuentemente la causa principal de este tipo de vulnerabilidades. A fin de aprovecharse de éstas, muchas veces es posible programar exploits, que actúen engañando a un programa vulnerable, para que introduzca código máquina en su espacio de memoria y modifique el puntero de retorno de una función, a fin de que pueda conseguirse la ejecución de código arbitrario a elección del atacante, dotado de los privilegios correspondientes al usuario utilizado en la corrida del proceso original o bien con derechos de sistema.

Contramedidas generales:

- En plataformas Unix/Linux desactivar todos aquellos programas que hagan uso del bit setuserid o setgroupid
- instalar parches de Kernel que hagan que el espacio de la pila no sea ejecutable (ejemplo Grsecurity)
- Compilar programas utilizando software de control como StackGuard
- Instalar todos los parches del proveedor
- Eliminar DLLs relacionadas con funcionalidades IIS que no se encuentren en uso
- Eliminar los servicios innecesarios
- Realizar auditorias de código
- Establecer políticas de desarrollo que incluyan que funciones se encuentran permitidas y de que forma deben ser empleadas, a la hora de realizar la codificación de software, prestando especial atención a las funciones estándar de tratamiento de cadenas en C: strcat(), strcpy(), sprintf(), vsprintf(), scanf() y ges()
- Testear cada ingreso de parámetros y la forma en la que el software reacciona frente a ellos.

12.2.8 Desbordamiento de Pila

Un desbordamiento de pila (stack overflow/overrun) es un problema aritmético que hace referencia al exceso de flujo de datos almacenados en la pila de una función, esto permite que la dirección de retorno de la pila pueda ser modificada por otra por parte de un atacante para obtener un beneficio propio, que generalmente es malicioso.

12.2.9 Desbordamiento de montículo

Un desbordamiento de montículo (heap overflow/overrun) es un problema aritmético que hace referencia al exceso de flujo de datos sobre un montículo, esto permite un acceso no autorizado a la memoria por parte de un comando o de un programa o script denominado shellcode. Un montículo (heap en inglés) es una estructura de Árbol con información perteneciente a un conjunto ordenado. Los montículos tienen la característica de que cada nodo padre tiene un valor mayor que el de todos sus nodos hijos. Un árbol cumple la condición de montículo si satisface dicha condición y además es un árbol binario completo.Un árbol binario es completo cuando todos los niveles están llenos, con la excepción del último que puede quedar exento de dicho cumplimiento.

12.2.10 Programación Segura

La programación segura es una rama de la programación que estudia la seguridad del código fuente de un software cuyo objetivo es encontrar y solucionar los errores de software, esto incluye: Utilización de funciones seguras para proteger de desbordamientos de pila, declaración segura de estructuras de datos, control del trabajo con el flujo de datos, análisis profundo de otros errores de software mediante testeos del software en ejecución y creación de parches para los mismos, diseño de parches heurísticos y metaheurísticos para proveer un cierto grado de seguridad proactiva, utilización de criptografía y otros métodos para evitar que el software sea crackeado.

12.2.11 Scripts

Los Scripts son una poderosa herramienta, a la hora de automatizar tareas repetitivas, que realizadas de otra forma, llevarían mucho más tiempo o serían susceptibles a algunos de los típicos errores humanos por repetición. Los administradores no son la excepción y puesto que, un Script representa una forma ordenada de ejecutar instrucciones tendientes a realizar algún tipo de acción, suelen codificar sus propios Scripts en lenguajes como Sh (Bourne Shell), TCL, WScript, JScript, VBScript, ADSI e inclusive Perl, a fin de aliviar su tarea diaria. Como toda secuencia de comandos o código de programación, un Script administrativo, mal programado, u olvidado en un servidor web, puede representar un riesgo potencial. Puesto que con el transcurso de los años, la tecnología de Scripting ha avanzado hasta constituirse en muchos casos, en poderosos lenguajes capaces de interactuar con algunas de las características más importantes del sistema operativo en el que corren, el daño que son capaces de causar bajo el control de un atacante, es inversamente proporcional a las ventajas que significan para un buen administrador.

En otro orden, suelen identificarse aquellos Scripts que dispuestos en un sitio web, apuntan a dotar al mismo de algún tipo de interactividad. En estos casos, una vez más, defectos en su programación, o fallas en su implementación, podrían permitir una gran diversidad de ataques, que van desde la utilización de su funcionalidad en provecho del atacante, hasta la acción de saltearse aquellas restricciones, que el desarrollador web inexperto, intento implementar en su Website como parte de su seguridad.

12.2.12 CGI

Como hemos visto en indicadores anteriores, un sitio web se encuentra conformado entre otros componentes, por contenido estático, el cual generalmente suele ser actualizado por el administrador o webmaster y contenido dinámico, el cual es generado on-the-fly o en vuelo por programas a tal efecto, dispuestos del lado de servidor.

CGI, son las siglas de Common Gateway Interface o Interfaz de Pasarela Común, y precisamente su función es la de especificar la forma en la que cliente y servidor, deben “interactuar” en un esquema web. A pesar de ello, comúnmente solemos utilizar el término CGI, para referirnos a aquellos programas que permiten desarrollar poderosos guiones a la hora de mostrar contenido Web en forma dinámica. Desde su concepción, los programas CGI se han establecido como una de las formas más potentes y flexibles a la hora de generar contenidos dinámicos. Sin embargo, podemos establecer sin temor a equivocarnos, que debido esencialmente, a malas prácticas de programación, suele ser muy frecuente toparse con programas CGIs mal escritos, lo cual significa un grave riesgo desde el punto de vista de la seguridad (No olvidemos que un programa CGI, no es ni más ni menos que “código ejecutable” en un servidor web!!, el cual la mayoría de las veces se encuentra escrito en lenguajes tales como: C/C++ , Fortran , PERL , TCL , Shell de Unix , Visual Basic , AppleScript, etc.)

A lo largo de los años muchos han sido los programas CGIs que se han hecho famosos al ser descubiertos en ellos, vulnerabilidades que permitían su explotación. Distribuciones de Linux, y software de Microsoft, han incorporado inclusive, códigos de ejemplos o programas CGIs con graves deficiencias en su codificación. Muchas herramientas han sido desarrolladas a la hora de detectar CGIs problemáticos, pero sin lugar a dudas, ninguna de ellas merece más formar parte del kit de herramientas del profesional de seguridad informática que Nikto. Nikto es una herramienta basada el Lib Whisker, que incluye una gran base de datos con CGIs vulnerables, la cual utiliza al momento de chequear un webserver, a fin de informar de coincidencias encontradas.

Contra medidas generales:

- Ejecutar periódicamente herramientas de verificación de CGIs vulnerables

- Limitar la ejecución de CGIs a un directorio en particular.
- Eliminar la mayor cantidad de CGIs que sean incluidos como parte de la instalación estándar de un Web Server
- No ejecutar bajo ningún punto de vista CGIs que no hayan sido programados concienzudamente y auditados por personal calificado
- Al programar CGIs, evitar dar por contado que solo se recibirán los datos esperados. Siempre deberán ser verificados los datos recibidos.
- Realizar validaciones adecuadas en los campos de ingreso de datos.

12.2.13 Java Scripts, Applets y ActiveX

En la actualidad, ya no es suficiente la codificación de HTML estático o programas CGIs que generen contenido dinámico, a la hora de satisfacer la demanda de diseñadores y usuarios, respecto de nuevas funcionalidades a través de la web. Quizás en parte debido a ello, han surgido en los últimos años una serie de tecnologías, que si bien han sido pensadas como herramientas válidas a la hora de mejorar la experiencia del usuario en la web, también pueden significar nuevos riesgos de seguridad.

Java Script, es un lenguaje de Script, con una sintaxis idéntica a Java. A diferencia de lo que ocurre con Java, no es posible escribir aplicaciones Java Script del tipo standalone. El código Java Script brinda la posibilidad de ser embebido en etiquetas HTML, y es ejecutado, al ser interpretado por el browser del cliente. Esta característica, hace del código Java Script, una potente herramienta puesto que entre otras cosas, permite acceder a los recursos del sistema, del equipo donde se esta ejecutando. Java Script puede ser utilizado tanto del lado del cliente como del servidor. Desde el punto de vista de la seguridad, un atacante puede llegar a utilizar componentes Java Script a su favor en varias formas diferentes, ya sea aprovechándose de su funcionalidad (Ejemplo: rutinas de escritura y lectura de archivos, envío de mails, etc.) o salteando validaciones de preproceso de formularios, tan solo enviando peticiones HTTP directas que no utilicen el browser (La herramienta denominada Netcat, puede resultar una magnífica herramienta al momento de testear esta tipo de circunstancias).

Applets: Se denomina Applets Java, a pequeños programas escritos en Java que al ser descargados, son ejecutados del lado del cliente, haciendo uso para ello de plugins denominados Virtual Machine. La idea inicial detrás de este tipo de componentes, es aislar su ejecución en un área restringida de memoria o sandbox, de forma tal, que él mismo no tenga la posibilidad de ganar acceso a cualquier otro sector. A lo largo del tiempo, se han detectado varios defectos en diferentes tipos de implementaciones respecto de sandbox´s, o VMachine´s que permitían al código contenido en un applet Java, escapar a las limitaciones impuestas e interactuar con componentes de sistema a los cuales no deberían tener acceso bajo ninguna circunstancia.

ActiveX: Se denomina ActiveX, a la implementación de Microsoft del Modelo de Componentes de Objetos (COM, Component Object Model). Los controles ActiveX, son pequeños componentes de software escritos en Visual Basic o C++, con la capacidad de ser descargados como un pequeño programa, o ser utilizados por otra aplicación. La tecnología ActiveX, incluye una serie de características importantes respecto de su seguridad, una de ellas, denominada Authenticode, se refiere a la posibilidad de que un componente ActiveX sea validado por un server. De la misma forma, firmas incluidas en los componentes, podrían ser verificadas por la parte cliente. En cuanto al riesgo inherente a los controles ActiveX, el mismo se encuentra relacionado con la potencial descarga y ejecución de código ejecutable al equipo víctima.

Contra medidas generales:

- Utilizar las opciones de verificación de firmas en aquellos componentes que lo admitan
- Establecer políticas de software corporativo, tendiente a configurar las opciones de seguridad necesarias en los Browser instalados en las máquinas clientes, a fin de prevenir la utilización de contenido activo en caso de que este no sea necesario
- No utilizar servidores o equipos críticos para navegar en Internet. Nuevas técnicas de explotación de vulnerabilidades del lado del cliente, pueden provocar la ejecución desatendida de código activo a través de la Web
- Mantener actualizados lo sistemas protegidos, respecto de los parches del fabricante
- Mantener actualizado el software antivirus instalado.
- Desde el punto de vista del Webmaster o administrador del Webserver, no se debería permitir la utilización de componentes de software que hayan sido testeados y posteriormente auditados
- Utilizar usuarios sin privilegios al navegar por Internet, en combinación con ACLs fuertes y bien pensadas en los sistemas clientes

12.2.14 Políticas de implementación

Al momento de desplegar servicios web, se deberán tener en cuenta una serie de aspectos fundamentales, el conjunto de los cuales impactará en forma directa, en el nivel de seguridad alcanzado. A continuación, haremos mención a algunas de las Políticas de Implementación que suelen ser consideradas imprescindibles, a la hora de impartir seguridad en cualquier tipo de implementación relacionada con Webservers y tecnologías web en general:

Elección del Software a Instalar: Deberá evaluar cuidadosamente la plataforma y el software de servidor a implementar. El despliegue, puesta a punto y mantenimiento de un site, muchas veces requiere de personal especializado, y un grupo interdisciplinario (Desarrolladores, Base de Datos, Plataforma, etc.). En caso de que su elección pase por plataformas Windows, deberá asegurarse que cuenta con las copias originales necesarias, a fin de evitar inconvenientes con software en mal estado. Si su decisión pasa por plataformas Open Source o de Software Libre, probablemente quiera asegurarse de que elige la distribución correcta. Debian y Slackware suelen ser la mayoría de las veces, la mejor elección desde el punto de vista de su funcionalidad y seguridad, mientras que comercialmente, SuSe y RedHat suelen ser las alternativas más atractivas para el ambiente corporativo, debido principalmente a su alineamiento con empresas como Oracle, SAP e IBM, quienes ofrecen productos y servicios certificados en dichos sistemas.

Diseño e Implementación de Seguridad física: En caso de que el hosting o housing no sea de su elección, deberá prever el diseño e implementación de los esquemas de seguridad física en su centro de cómputos, especialmente, si planea desplegar servicios de E-Commerce o correo corporativo vía webmail, con cobertura 7x24x365. Si por el contrario, se decidiera tercerizar el servicio, deberá requerir al prestatario, copias de los contratos de servicio, LSA (Level Service Agreement) y la documentación correspondiente a las políticas de seguridad que este se compromete ha implementar en su emplazamiento.

Hardening del Sistema Operativo y Aplicaciones: Eliminación de servicios innecesarios, implementación de las features de seguridad avanzadas dispuestas por la plataforma u aplicación instalada en sus servidores, auditoria de código sobre las aplicaciones, configuración de las

características avanzadas de login y auditoria, definición de ACLs en la estructura de directorios, y otros cientos de tips deberán formar parte de su lista de verificación a la hora de realizar el Hardening o segurización de su instalación. En lo posible, deberá pensar en su servidor Web, como un bastión host, administrando en el, diversas características de seguridad en profundidad.

Ubicación del servidor desde el punto de vista de la RED: Partiendo de la base, de que la mayoría de los servidores web son utilizados en la publicación de contenido, que de una u otra forma se encuentra expuesto al público en general, suele ser recomendable la instalación del mismo en una subred separada a la de la LAN corporativa, a efectos de que el tráfico proveniente de Internet, no atraviese la misma. De esta forma, se evita a su vez, que la red Interna sea visible desde el exterior. El armado de una DMZ fuerte, suele ser la mayoría de las veces, una buena opción.

Consideraciones de Networking y Seguridad en el Perímetro: Ya sea en la definición especifica del armado de la DMZ a utilizar, como en el filtrado provisto por los dispositivos de border routing, la implementación de estrictas políticas de filtrado, representará gran parte del porcentaje de éxito de su estrategia de seguridad, al momento de implementar servidores web seguros. No solo deberán estar previstas las ACLs de INPUT, sino que deberá prestarse absoluta atención, a las reglas de OUTPUT. En caso de que el webserver requiera comunicarse con otros servers en el segmento, las reglas establecidas en los dispositivos de filtrado, deberán ser estrictos en cuanto al típico de tráfico habilitado en dichas conexiones, así como los tipos de puertos desde los que se deberán permitir.

Diseño e Implementación de Soluciones de Disponibilidad: Deberá ser cuidadoso a la hora de definir procedimientos de contingencia. Políticas de backup, sitios alternativos, sistemas de protección eléctrica, armado de clusters y balanceo de carga, son sólo algunos de los asuntos que deberán ser tenidos en cuenta a la hora de montar una solución, con una tasa de disponibilidad aceptable.

Evaluación periódica de la seguridad: De acuerdo con el principio que dicta, que la seguridad es un proceso continuo, deberá planificar y ejecutar, evaluaciones periódicas de seguridad sobre los sitios que administra. Por su parte, la implementación de nuevas funcionalidades, siempre implicará nuevos seteos o ajustes al esquema previamente planteado.

Política de Actualización de Software y de Seguridad en General: Un webserver seguro, relacionado con una red insegura, probablemente no pueda ser considerado una buena elección. Confirme que la política de seguridad general a nivel compañía, está siendo aplicada correctamente y que los procedimientos de actualización de software, cumplen sus necesidades de testing y despliegue.

Muchos profesionales de seguridad informática, coincidimos en que las probabilidades de que un site sea víctima de un ataque, son de un ciento por ciento. La experiencia dicta que tarde o temprano, un atacante con el skill adecuado y con el tiempo de su lado, logrará impartir algún tipo de daño. Con esta idea en mente, la planificación de adecuadas técnicas de resguardo y recuperación ante incidentes, deben encontrarse entre los lineamientos básicos de toda implementación que involucre servidores web.

A pesar de que la mayoría de las técnicas tradicionales, de almacenamiento en cinta o dispositivos del tipo NAS (Network Attach Storage), continúan siendo efectivas, cada vez son más las compañías que hacen uso de soluciones de clustering y balanceo de carga.

Otra alternativa, suele pasar por mantener dos servers separados, siendo uno de acceso público y el otro copia del original, dispuesto en una zona privada accesible sólo para el administrador del Website, en el cual se alberga una copia actualizada del sitio publicado. En caso de que la integridad

en el servidor primario, sea vulnerada, se estará en condiciones de realizar una rápida publicación del contenido de resguardo, simplificando en gran medida las tareas administrativas entorno al armado de un nuevo server.

Nota: Si bien es cierto que esta última alternativa, apunta a restaurar rápidamente un Website, deberá contar con los procedimientos de respuesta a incidentes, necesarios, a la hora de identificar cuales han sido los puntos que permitieron a un atacante, vulnerar la seguridad del site atacado.

12.2.15 Aplicaciones: generalidades

Sin lugar a dudas, una de las decisiones más importantes a la hora de montar un servidor web, es aquella que se encuentra relacionada con la propia aplicación, responsable de brindar dicho servicio. A continuación, mencionaremos algunas de las principales características, provistas por dos de las implementaciones de software más populares en la actualidad.

Apache Web Server: Apache, es considerado hoy día, como el servidor web más utilizado en Internet. Un rápido vistazo a la información provista por Netcraft, basta para ilustrar de que forma se encuentra posicionado con cerca del 70% del Market Share, respecto del resto de las alternativas. Apache es software libre, bajo licencia GNU y como tal su código fuente se encuentra disponible. A su vez, se encuentra incluido en la mayoría de las distribuciones Linux, motivo que ha contribuido en gran parte a su amplia distribución.

Algunas de las características principales de Apache, se encuentran relacionadas con que: es altamente configurable, extensible (gracias a su esquema de módulos asociado), gratuito, su código fuente es libre y a pesar de su largo historial de vulnerabilidades, la respuesta por parte de la comunidad, respecto de la liberación de parches, es excepcional.

Precisamente desde el punto de vista de su seguridad, muchas vulnerabilidades se han encontrado y corregido en el software, pero por lo general, las mismas se encuentran relacionadas con los módulos de extensión y no con el núcleo mismo de Apache. Pero… ¿a qué nos referimos con módulos? La estructura de Apache se compone de un módulo principal o kernel de producto, y una serie de módulos adicionales que se incorporan al mismo a fin de brindar alguna funcionalidad en particular. Por ejemplo, requerirá “mod_perl” para habilitar la posibilidad de corrida de Scripts escritos en Perl, tanto como el módulo “mod_php4” para utilizar la funcionalidad PHP4 al momento de servir este tipo de contenido.

Apache provee una serie de características avanzadas en cuanto al seteo de su seguridad, y la totalidad de las mismas, pueden ser fácilmente configuradas por medio de los correspondientes archivos de configuración. Uno de los puntos más significativos de este producto, es que al poseer el código fuente, una auditoría completa es posible, al igual que el desarrollo de nuevas funcionalidades.

Internet Information Server: Internet Information Server o IIS, constituye la solución propuesta por Microsoft a la hora de servir aplicaciones web en la plataforma Windows. De hecho, a partir de Windows 2000 Internet Information Server es parte integral del sistema operativo, y no un componente del famoso “Option Pack” entregado junto a Windows NT 4.0.

Una de las particularidades respecto de IIS, se encuentra relacionada con la implementación de sus módulos de extensión en la figura de filtros ISAPI (Internet Server Application Programming Interface), por medio del cual se puede precisamente extender la funcionalidad del servidor web, desarrollando nuevas DLLs con un fin determinado. Desde un punto de vista de diseño, los filtros ISAPI en conjunto con la utilización de secuencias ASP (Active Server Pages) brindan gran poder a la hora de resolver situaciones complejas, que antes requerían la codificación de lentos programas CGIs. Desde el punto de vista de su seguridad, IIS, ha constituido un objetivo constante en la mira de atacantes quienes vieron con asombro la frecuencia con la que a lo largo del tiempo, se descubrían vulnerabilidades tales como: los ataques de revelación de código fuente (:::$DATA), el revelado de información

mediante errores en la codificación de guiones del estilo de “showcode.asp”, el soporte para la ejecución de comandos privilegiados en las consultas de bases de datos de backend (MDAC/RDS) y ataques por desbordamiento de buffers como los mencionados en el indicador 5.2.8. Al mismo tiempo, es justo decir que IIS, en sus versiones 5.0 y 6.0, ha mostrado ser una solución madura capaz de soportar eficientemente el tunning necesario a fin de proveer una plataforma web sumamente segura.

12.2.16 Consideraciones sobre seguridad

A nivel general, los aplicativos utilizados a la hora de servir páginas web, al igual que los sistemas operativos y aplicaciones que dan soporte a los mismos, pueden ser tan seguros como queramos que lo sean. Gran parte de ello depende de la forma en la que son implementados, administrados, auditados y mantenidos en el tiempo. Si bien es cierto que el código fuente de Apache se encuentra disponible, de nada servirá esta ventaja si no es bien aprovechada. De la misma forma, muy poco útil serán las cerradas configuraciones por defecto de IIS 6.0, si lo primero que realiza un administrador desprevenido, es habilitar todas sus características, cuando en realidad sólo requeriría servir páginas estáticas.

Respecto de las consideraciones de seguridad, relativas a servidores web en general y a IIS/Apache en particular, probablemente una de las más importantes sea aquella que dicta, la obligatoriedad de mantenerse actualizado en cuanto al nivel de parches aparecidos para la plataforma administrada. Esto disminuirá notablemente el riesgo de ser atacados por un atacante por medio de alguna herramienta automática que haga uso del último Exploit.

De la misma forma, nada será más valioso para el profesional de seguridad informática, que el estar actualizado respecto de todos aquellos descubrimientos que se realizan a diario en torno a los sistemas operativos y aplicativos con los que trabajamos frecuentemente. En el área multimedia, encontrará algunas de las listas de correo o fuentes de información recomendables, a la hora de realizar esta tarea. Por último, herramientas como las presentadas en el área multimedia, en conjunto con dispositivos IDS (como Snort), Firewalls, honeypots, políticas, procedimientos, hardening de sistema operativo, etc. suelen ser necesarios, a la hora de diseñar un ambiente de cómputo seguro, en torno a brindar servicios web.

12.2.17 Penetrando sitios Web

Tal como hemos mencionado en los puntos anteriores, no existe Firewall que proteja “los puertos 80 o 443”, es decir, no existe Firewall que proteja aquellos servicios (puertos) que se encuentran abiertos para brindar servicios hacia una red pública. Muchas veces, los analistas de seguridad, enfocan toda su dedicación en seleccionar e implementar el mejor sistema de borde por medio de los Firewalls más reconocidos, olvidando que simplemente están solucionando el 1% del problema de seguridad, tratando de evitar todos los accesos indebidos. Cualquier individuo que inicie un ataque y detecte un Firewall, simplemente va a cambiar la visión de sus objetivos, desplazando su accionar a atacar aquellos servicios que se encuentran publicados a través de dicho dispositivo, sería demasiado costoso en tiempo tratar de vulnerar un dispositivo de borde, si bien, también pueden presentar vulnerabilidades propias y de configuración.

Está claro que debemos implementar un dispositivo de borde que limite los accesos sólo a los servicios permitidos, pero también debemos tener presente que ésto solo no alcanza. En ese sentido, debemos tener en cuenta que además de emplear dispositivos IDS (Intrusión Detection System) e IPS (Intrusión Prevention System)que analicen cualquier tipo de tráfico malicioso que busque explotar alguna vulnerabilidad en nuestros servidores Web, debemos considerar realizar periódicamente, escaneos con herramientas específicas que identifiquen vulnerabilidades sobre nuestros servicios ya sean, propiamente de configuración o bien de los productos en sí.

No debemos confundir un escáner con un IDS, podemos decir que generalmente las herramientas IDS detectan intrusiones, mientras que las herramientas de evaluación de vulnerabilidades las previenen.

Un escáner de vulnerabilidades debería realizar en otras muchas, las siguientes evaluaciones:

- Construir un esquema de la red
- Identificar los puertos o servicios disponibles
- Identificar versiones de productos y service packs de esos servicios
- Descubrir recursos y dispositivos conectados a la red
- Analizar información SNMP
- Descubrir información de direccionamiento y enrutamiento
- Intentar acceso a nivel usuario
- Atacar contraseñas por fuerza bruta y diccionario
- Obtención de accesos con sesiones nulas
- Identificar vulnerabilidades conocidas sobre los servicios disponibles

Existen dos tipos de escaneos: pasivo o activo. El escaneo pasivo inspecciona y recolecta información pero no busca vulnerar directamente las instalaciones, en cambio, el escaneo activo realiza exprofeso una serie de ataques conocidos y registra los resultados de los mismos. Muchas veces los directivos de sistemas e incluso los oficiales de seguridad, son reacios a implementar los escaneos de red o test de penetración, por desconocer los resultados negativos que podrían provocar. Si recordamos capítulos anteriores, donde estudiamos la " Rueda de la Seguridad" y la importancia de probar continuamente la efectividad de nuestras defensas para generar mejoras contínuas. Por ultimo, es importante tener en cuenta la evaluación de seguridad de las aplicaciones web implementadas, puesto que las mismas suelen ser un objetivo concreto de gran parte de los atacantes. Numerosas vulnerabilidades suelen explotarse a diario en tal sentido, algunas de las mas importantes se encuentran relacionadas con: SQL Injection, Cross-Site-Scripting, etc. Auditoría de código, testing específico sobre su comportamiento, y conceptos de programación segura, suelen formar parte de las "mejores prácticas" entorno a su seguridad.

12.3 SERVICIOS DE CORREO ELECTRÓNICO

Hacia finales de 1971, Ray Tomlinson, se encontraba trabajando en un proyecto de mensajería electrónica denominado SNDMSG, el cual debía poseer la habilidad de intercambiar mensajes electrónicos entre investigadores que utilizaban una máquina PDP-10 para sus labores diarias. Pero el concepto hasta allí, no resultaba novedoso. De hecho, desde mediados de 1960 ya existían una serie de programas que dejaban mensajes locales en un receptorio central, que eran accedidos por diversas personas en un mismo equipo, cada una de las cuales tenía derecho de acceso sobre su propio buzón, de forma que cada cual podía ver los mensajes que recibía.

Algunos meses más tarde, Tomlinson aplicó los conocimientos que había adquirido durante el desarrollo de un protocolo experimental de transferencia de archivos, al producto SNDMSG en el que había estado trabajando tiempo atrás. Un dato histórico importante, radica en el hecho de que Ray, decidió en dicha oportunidad, utilizar el símbolo @ (arroba) para de esta forma distinguir entre direcciones de buzones en la propia máquina y aquellas que se referían a máquinas remotas en la Red.

El éxito de SNDMSG fue instantáneo, una vez que la gente dispuso de la nueva versión de SNDMSG, y pudo aplicarlo en lo que en aquel momento se denominaba ARPANET (antecedente de Internet) todas las comunicaciones comenzaron a ser vía e-mail. Dos años más tarde se descubriría que el 75 % del tráfico de ARPANET consistía en lo que se había dado en llamar "correo electrónico".

Unos de los motivos principales que han hecho del correo electrónico, el servicio de Internet más utilizado a través del tiempo, radica en las posibilidades que se desprenden de su utilización. Al igual que otro tipo de tecnologías, el e-mail ha transformado la vida de gran parte de la población mundial, a la vez que ha contribuido en gran medida al desarrollo de los negocios y a la baja de costos en comunicaciones, que de otra forma, requerirían de medios más onerosos.

En la actualidad, muchas organizaciones “dependen” de una u otra forma de los servicios de correo en ellas implementado. Esta dependencia, ha impactado directamente en los niveles de disponibilidad, fiabilidad y seguridad que son requeridos a la hora de mantener este servicio 7x24x365 funcionando. Al mismo tiempo, el correo electrónico tal como fue inicialmente concebido, ha evolucionado. Hoy día, algunos productos brindan funcionalidades adicionales, generalmente relacionadas con soluciones de workflow, colaboración, seguimiento de reuniones y agendas compartidas. Estos servicios adicionales junto al servicio básico de mensajería, hacen de este tipo de herramientas, un potente instrumento a la hora de establecer un vínculo de comunicación efectivo.

Pero no todo es tan sencillo a la hora de mantener un sitio de correo electrónico funcionando. Problemas en las diferentes implementaciones, protocolos poco seguros, riesgos y amenazas propios del medio público de transmisión de datos, y nuevos requerimientos a la hora de incluir dispositivos móviles como clientes válidos de nuestra solución, hacen que se requiera un cuidadoso diseño respecto de la seguridad necesaria, a la hora de cumplir con los objetivos de negocio detrás de toda implementación de un servidor de correo electrónico corporativo.

12.3.1 Arquitectura

La arquitectura básica detrás de una solución de correo electrónico, se encuentra conformada por una serie de componentes principales, cada uno de ellos con funciones claramente definidas, entre las que se encuentran los procesos de trasmitir y administrar mensajes de correo electrónico. Su funcionamiento en conjunto, es lo que permite aprovechar, este magnifico medio de comunicación. A continuación, mencionaremos brevemente, cada uno de estos componentes principales:

MUA (Mail User Agent, Agente de Usuario de Correo): El MUA (Mail User Agent, Agente de Usuario de Correo), probablemente sea el componente con el que los usuarios suelen estar más familiarizados, puesto que precisamente, su función específica es la de actuar como interfaz entre el usuario final y el MTA (Mail Transfer Agent, Agente de transferencia de correo). Respecto de su implementación, el MUA no es ni más ni menos que el software que conocemos como “Cliente de Correo Electrónico”. Mediante su uso, es posible como mínimo, leer y escribir mensajes. Ejemplos de este tipo de software, son: Microsoft Outlook, Outlook Express, Mutt, Pine, Eudora, Pegasus, etc.

MTA (Mail Transfer Agent, Agente de Trasnferencia de Correo): Un programa MTA (Mail Transfer Agent, Agente de Transferencia de Correo) transfiere los mensajes de correo electrónico entre máquinas que usan el protocolo SMTP. Un mensaje puede pasar por varios MTA hasta llegar a su destino final. Algunos de los MTA más populares son: Sendmail, Qmail, Postfix, Exchange, GroupWise y Lotus Notes.

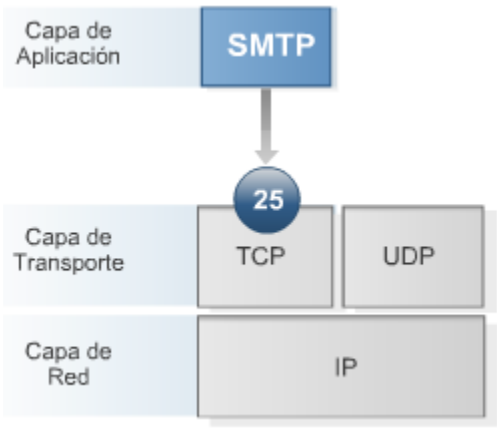
Nota: Muchos de los agentes MUA actuales, sirven también para enviar correo. Sin embargo, no se debe confundir esta acción con las funciones propias y verdaderas de un MTA. Un agente MUA no entrega directamente el mensaje al servidor de correo del destinatario final; esta función está reservada al agente MTA.

MDA (Mail Delivery Agent, Agente de Entrega de Correo): Los agentes MTA utilizan programas MDA (Mail Delivery Agent, Agente de entrega de correo) para entregar el correo electrónico al buzón de un usuario concreto. En muchos casos, el agente MDA es realmente un LDA (Local Delivery Agent, Agente de entrega local), como bin/mail o Procmail en el mundo Unix o Local Delivery en productos

como Exchange Server. Cualquier programa que gestione realmente un mensaje para entregarlo al punto donde lo leerá un agente MUA se puede considerar un agente MDA.

12.3.2 SMTP

SMTP, son las siglas de "Simple Mail Transfer Protocol" o “Protocolo Simple de Transmisión de Correo”. Este protocolo fue publicado en Agosto de 1982 en el RFC 821, y su función principal, es la de transmitir correo electrónico de manera confiable y eficiente, bien sea de cliente a servidor, o entre servidores. En la pila de protocolos TCP/IP, SMTP se ubica en la capa de aplicación y utiliza como parte de su funcionamiento, el puerto 25 TCP.



El protocolo SMTP, define una serie de comandos y mensajes, los cuales son utilizados al momento de establecer y mantener una comunicación o conversación entre las partes.

Desde el punto de vista de su funcionamiento, un intercambio SMTP básico, comienza con la emisión del comando MAIL From: <Dirección de Correo Electrónico> para iniciar el intercambio. El sistema que recibe este comando, responde con un mensaje 250 para informar de que se ha recibido el primer comando. A continuación, el sistema conectado comunica las direcciones de correo electrónico para recibir el mensaje del sistema receptor, seguido de un mensaje con el comando DATA. Este mensaje notifica al sistema receptor que la siguiente parte de la comunicación será el cuerpo real del mensaje de correo electrónico. Cuando el sistema conectado finaliza de enviar el mensaje de correo electrónico, coloca un punto sencillo (.) en una línea. A partir de ese momento, se considera que el mensaje se ha enviado.

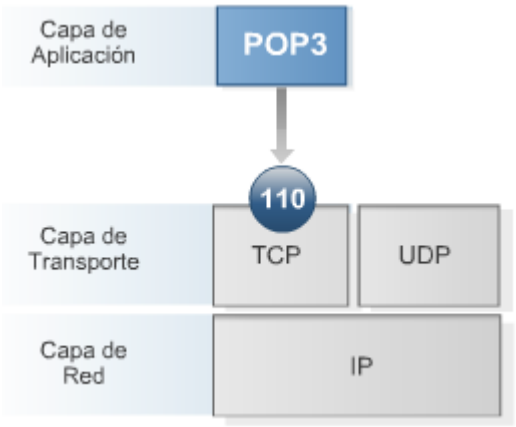
Un aspecto importante respecto de SMTP, es que a diferencia de protocolos tales como IMAP4 o POP3, este no requiere autenticación en su forma más básica. Desde el punto de vista de su seguridad, esto ha provocado la proliferación de correo basura o spam, puesto que un usuario remoto, puede en determinadas circunstancias, utilizar el sistema de otro para enviar correo a listas completas de destinatarios, haciendo uso de los recursos y ancho de banda de dicho sistema. Si bien es cierto que las aplicaciones SMTP actuales, han progresado en tal sentido al minimizar este comportamiento y restringir las transmisiones de modo que sólo los hosts conocidos envíen correo electrónico; este aspecto sumado a la característica de “protocolo en texto plano” propia de SMTP, deben ser puntos a considerar, a la hora de administrar seguridad.

Ejemplos de respuestas SMTP:

- 220 Servicio listo
- 250 Solicitud aceptada
- 450 buzón no hallado (transitoria)
- 452 Insuficiente espacio
- 502 Comando no existe
- 550 Buzón no hallado (permanente)
- 552 Capacidad de almacenamiento excedida

12.3.3 POP3

POP3, son las siglas de "Post Office Protocol " o “Protocolo de Oficina de Correo”. POP3, fue hecho público en Mayo de 1991 mediante la publicación del RFC 1225, el cual a su vez, se encuentra basado en el RFC 918, publicado en Octubre de 1984. La idea principal detrás de POP en general y POP3 en particular, se encuentra relacionada con la necesidad de contar con un protocolo que permita a los clientes de correo electrónico, recuperar mensajes de servidores remotos y almacenarlos en forma local. En la pila de protocolos TCP/IP, POP3 se ubica en la capa de aplicación y utiliza como parte de su funcionamiento, el puerto 110 TCP.



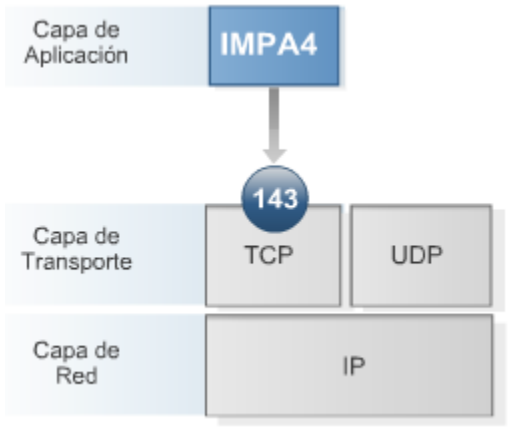
Debido a sus características de recuperación, almacenamiento local y eliminación de correos en el servidor central, POP3 suele ser uno de los protocolos más utilizados por usuarios finales.

Al mismo tiempo, POP3 funciona adecuadamente sin necesidad de utilizar una conexión permanente a Internet o a cualquiera que sea la red que contenga el servidor de correo accedido.

A la hora de establecer una conexión a un servidor POP, el cliente de correo abre una conexión TCP en el puerto 110 del servidor. Cuando la conexión se ha establecido, el servidor POP envía al cliente POP una invitación, tras lo cual las dos máquinas se envían entre sí otros comandos y respuestas especificadas en el protocolo. Como parte de esta comunicación, al cliente POP se le pide que se autentifique en lo que se denomina Estado de autenticación, donde el nombre de usuario y la contraseña del usuario se envían al servidor POP. Si la autenticación es correcta, el cliente POP pasa al Estado de transacción, fase en la que se pueden utilizar comandos del tipo LIST, RETR y DELE para mostrar, descargar y eliminar mensajes del servidor, respectivamente. Los mensajes definidos para su eliminación no se quitan realmente del servidor hasta que el cliente POP envía el comando QUIT para terminar la sesión. En ese momento, el servidor POP pasa al Estado de actualización, fase en la que se eliminan los mensajes marcados y se limpian todos los recursos restantes de la sesión.

12.3.4 IMAP4

IMAP, son las siglas de “Internet Message Access Protocol“ o “Protocolo de Acceso a Mensajes de Internet“, el cual en su versión 4, se encuentra definido en el RFC 1730 desde Diciembre de 1994. En el nivel más básico, IMAP4 consiste en un método de acceso a mensajes almacenados remotamente. Una de sus características principales, radica en que los mensajes de correo electrónico administrados por este protocolo, se conservan en el servidor de correo remoto, donde el usuario puede leerlos o eliminarlos, además de cambiar el nombre o eliminar los buzones de correo utilizados para su almacenamiento.



Al igual que el resto de los protocolos revisados en los últimos indicadores, el protocolo IMAP4, se ubica en la capa de aplicación del modelo TCP/IP y hace uso del puerto TCP 143 Debido a su funcionamiento, IMAP4 suele permitir al usuario, una serie de posibilidades añadidas, que no se encuentran en otros protocolos. Usuarios que se conectan a Internet o a una red privada a través de una conexión Dial-Up, suelen verse beneficiados por su uso, debido a que, sólo la información de cabecera del correo se obtiene inicialmente, existe la posibilidad de visualizar éstas, para luego decidir posponer la

descarga de aquellos mensajes que por ejemplo, contengan archivos adjuntos de gran tamaño. De la misma manera, el usuario puede eliminar el correo electrónico que no le interesa sin tener que ver antes el cuerpo del mensaje, lo cual evita tener que descargar un mensaje mediante la conexión de red que utilicen.

12.3.5 Servicio de Relay

La mayoría de los servidores de correo, poseen entre sus características, la posibilidad de realizar lo que se conoce como “Relay”. Esta funcionalidad, consiste en que un servidor de correo procese un mensaje de correo en el que ni el remitente ni el destinatario son usuarios locales. Cuando esta posibilidad, se encuentra habilitada, solemos referirnos a ella como “Open Relay” o “Relay Abierto”.

Pero ¿por qué quisiera usted dejar abierto un Relay de Correo? La verdad es que en la actualidad, no suele ser necesario en la mayoría de los casos, aunque aún así, existen algunas situaciones puntuales, en las que múltiples servidores de correo de su propia organización, podrían por ejemplo, verse favorecidos con este tipo de configuración.

Desafortunadamente, Internet ya no es lo que solía ser en sus inicios y abusos reiterados a servidores conteniendo Relay’s Abiertos, suelen ser a menudo responsables de gran parte del volumen de SPAM o correo basura que recibimos a diario. Software específicamente escrito para aprovecharse de esta condición, suele ser utilizado por individuos sin escrúpulos, que hacen uso del tiempo de proceso y ancho de banda de terceros si autorización.

Como profesionales en seguridad, deberemos incluir como parte de nuestra rutina de control, el testing de esta funcionalidad en los servidores de correo de nuestro cliente u organización, a fin de detectar sistemas con servicio de Relay Abierto. Si bien es cierto que existe la posibilidad de realizar dicha tarea ingresando comandos vía Telnet al puerto 25, la mayoría de las veces, resultará más práctico utilizar guiones automáticos o herramientas específicamente pensadas para dicha tarea. Relay Check , es un pequeño programa escrito en Perl, con la capacidad necesaria para escanear la red en busca de host SMTP que permitan “relaying”. Otra posibilidad, es la de utilizar alguno de los servicios On-Line. Un buen ejemplo de estos últimos, es www.ordb.org (Open Relay Database).

El proceso de configuración de Relay, difiere de un software de servidor a otro. Las versiones 8.9 y posteriores de Sendmail por ejemplo, rechazan de forma predeterminada el reenvio de correo. Lo mismo ocurre con las versiones posteriores a la 0.91 de Qmail. A diferencia de estos últimos, Postfix ha rechazado siempre el reenvío de forma predeterminada. En el caso de los productos Exchange de Microsoft, deberá seguir las instrucciones descriptas en la siguiente URL: http://www.ordb.org

12.3.6 Backup de mailbox

Como toda aplicación empresarial, la disponibilidad de los servidores de correo corporativo, es uno de los aspectos más importantes a tener en cuenta a la hora de organizar los procedimientos de resguardo de datos en nuestro cliente o compañía. Ante un incidente de seguridad, gran parte del éxito en nuestra tarea, probablemente se encuentre relacionado con la posibilidad de devolver al usuario final, el acceso a la información almacenada en su mailbox.

A fin de poder actuar rápidamente, resultará imprescindible contar con una política clara de resguardo y restauración de datos, así como procedimientos detallados en cada caso.

Gran parte de los nuevos productos de servidor para correo electrónico (Por ejemplo Exchange Server), se comportan en muchos aspectos, en forma similar a verdaderas bases de datos transaccionales a la hora de albergar y acceder información de mensajería, por tal motivo, siempre que sea necesario establecer procedimientos de resguardo, deberán ser tenidas en cuenta, las posibilidades y limitaciones particulares brindadas por cada uno de los productos seleccionados.

En la mayoría de los productos del mundo Unix/Linux, las operaciones de resguardo suelen llevarse a

cabo de la misma forma que con cualquier archivo o directorio de File System. Generalmente utilizando alguna utilidad del tipo rsync. Microsoft por su parte, prevé procedimientos específicos de resguardo y recuperación, que han ido mejorado con el tiempo y varían de acuerdo a la versión de servidor (Exchange 5.5/2000/2003). Otros productos de terceros, específicos de backup, permiten hacer un resguardo a nivel de una mailbox específica (ArcServe, Veritas).

Por ultimo, en aquellos sitios donde los clientes sean pocos, existe la posibilidad de gestionar copias de resguardo automatizadas, por medio del propio cliente de correo. Outlook por ejemplo, permite ejecutar tareas periódicas de resguardo, con tan solo configurar una serie de opciones.

12.3.7 SPAM

Se utiliza el término Spam, para referirse a la práctica de enviar indiscriminadamente mensajes de correo electrónico no solicitados. El Spam, suele ser también conocido como UCE (Unsolicited Commercial Email) o UBE (Unsolicited Bulk Mail). Desde el punto de vista técnico, generalmente suele catalogarse un correo como Spam, cuando este es no solicitado y masivo a la vez.

- No solicitado Porque el receptor no dio un permiso verificable al remitente para que este le envíe el mensaje.
- Masivo Porque el mensaje es enviado como parte de una colección mayor de mensajes, donde todos tienen idéntico contenido.

En los últimos años, el Spam ha crecido a pasos agigantados. Se estima que aproximadamente el 70% del tráfico internacional de correo electrónico es Spam. Estos valores, han hecho que un manto de preocupación generalizada, se cierna sobre la comunidad informática en general.

Aquellos que realizan la acción de enviar correo masivo y no solicitado, se los conoce con el término de Spammers. Muchas veces, sus servicios suelen ser contratados por empresas o individuos, que pagan a estos por cantidad de correos enviados, otras, las propias compañías se encargan de repartir cientos, miles o millones de correos al mes, intentando comunicar sus productos. Muchas son las técnicas utilizadas por los spammers a la hora de realizar su tarea, y éstas suelen ser cada vez más avanzadas.

Como profesionales de seguridad informática, existen una serie de tareas que podemos emprender a efectos de reducir el potencial impacto del Spam en nuestras compañías o clientes:

1. Configurar en forma correcta nuestros servidores de correo, a fin de que los mismos no posean, por ejemplo, un Servicio de Relay Abierto.
2. Implementar filtros (Bayesianos, De firma digital, Heurísticos, etc.)
3. Configurar la utilización de listas negras del tipo RBL (Realtime Blackhole Lists), SBL de Spamhouse, etc en nuestro servidor de correo electrónico.
4. Denunciar al Spammer frente al ISP (Internet Service Provider)

Desde el punto de vista legal, existen algunos lineamientos y recomendaciones prácticas, como las presentadas en el área multimedia, aunque ninguna ley específica.

12.3.8 HOAX

Por lo general, suele utilizarse el término de Hoax (Broma o Engaño), para referirse a un falso virus, el cual no realiza por si mismo ninguna acción. Generalmente consiste en un mensaje de correo electrónico en el que se alerta sobre la supuesta existencia de un nuevo virus que ningún antivirus detecta. Este tipo de mensaje generalmente apela a técnicas de ingeniería social, mediante las que se insta a los usuarios a eliminar en forma manual, los supuestos archivos infectados por este virus inexistente, generando de esta forma que el propietario del sistema sea quien se auto-inflija el

daño.Los Hoax más efectivos, son aquellos que suelen distribuirse en cadena. Algunos tienen textos alarmantes sobre catástrofes (virus informáticos, perder el trabajo o incluso la muerte) que pueden sucederle al usuario receptor del correo, si este no reenvía el mensaje a todos y cada uno de los contactos de su libreta de direcciones. Si bien es cierto que muchos de estos mensajes o cadenas, pueden ser detenidos configurando determinado tipos de reglas en nuestro software de administración de contenidos, lo cierto es que el profesional en seguridad informática, deberá implementar, planes de capacitación específicos, dirigidos a los usuarios del sitio que administra, a fin de explicar las consecuencias negativas (utilización de ancho de banda, perdida de productividad, etc.) de este tipo de prácticas.

12.3.9 Open Relay

El ataque de Open Relay consta en usar el MTA (Mail Transport Agent, Agente de Transporte de Correo) como puente para correos (usualmente spam, aunque pueden ser muchas otras cosas, como los Hoax) que de otra manera no podrían llegar a destino, gracias a que los servidores bloquearon la dirección IP de origen. De esta manera, la gente que manda spam de forma indiscriminada se ve obligada a usar otros servidores para esta tarea. Estos servidores que permiten que se envíe correos a través de ellos, se los denomina Open Relay. Para solucionar esto (o castigar a la gente que tiene el MTA aceptando este "puenteo de correos" para cualquier lugar) se crearon listas negras en tiempo real que bloquean dichos hosts en los cuales se detectó un MTA que hacía Open Relay. Y para que se saque una IP de estas listas negras, se deben pasar ciertas pruebas y esperar cierto tiempo.

Hay muchos tipos de servicios que bloquean estas direcciones. Pero los más importantes realizan el bloqueo por IP y algunos otros bloquean por rangos de IP. Los que bloquean por rangos de IP investigan primero cual es el rango de IP que tiene la compañía (basándose en la IP que encontraron haciendo Open Relay), y bloquean dicho rango. Cabe destacar también, que no se considera que está en falta a quien realiza estos ataques, sino a quien tiene un servidor que los permite (por acción u omisión). Existe cierta divergencia en la definición del acrónimo RBL. Una sería Relay Black List (Lista Negra de Relays), y la otra sería Realtime Black List (Lista Negra en Tiempo Real).

12.3.10 Políticas de implementación

Por su naturaleza, los puntos mencionados anteriormente, aplican perfectamente a las políticas de implementación necesarias, a la hora de implementar un sitio de correo electrónico. Por tal motivo, deberán ser tenidas en cuenta específicamente. Al margen de ello, existe una consideración especial que suele ser implementada con éxito en la mayoría de los sitios de correo corporativo, comúnmente denominada Gateway de Correo Electrónico. El término *Gateway de Correo Electrónico*, se utiliza para definir un sistema por el cual se implementa un servidor de correo electrónico “dentro” del perímetro interno (Privado) a nivel de red, y un segundo equipo corriendo tan solo un servicio de “Gateway de Correo Electrónico” (Generalmente un Relay SMTP convenientemente configurado), dispuesto en el perímetro externo (público).

En su configuración típica, un esquema de este tipo funciona de la siguiente forma:

1. Un Gateway de Correo Electrónico (También llamado Gateway SMTP) dispuesto sobre el lado público de su esquema de filtrado (Por ejemplo dentro de su primer zona DMZ), se configura para aceptar mails entrantes, provenientes de Internet, mediante un servicio SMTP.
2. Este procesa el mail recibido, realiza los chequeos que fueran necesarios (Anti Spam, Antivirus, Filtro de Contenidos, etc.) y reenvía el correo al servidor de la zona segura, en nuestra LAN interna.

De la misma forma, el Gateway de Correo Electrónico, recibe el correo saliente, proveniente del servidor interno, ejecuta los chequeos que hayan sido planificados y finalmente envía el mismo a

través de Internet. De esta manera, se logra fundamentalmente, no exponer el Servidor de Correo en el cual se albergan los mailboxes, a una zona poco segura de nuestra DMZ. Independientemente del control de virus, spam y contenido que se realiza en el equipo de Relay que se encuentra en la red de perímetro, también es altamente recomendable colocar un sistema antivirus sobre el sistema de correo corporativo para evitar, que en caso de ingresar un virus a la empresa por otra vía, éste se propague a todos los dispositivos utilizando el correo interno. Como recomendáramos en unidades anteriores, en caso de atender esta ultima alternativa, lo recomendable sería instalar dos productos antivirus de diferentes fabricantes, en cada uno de los puntos mencionados (Relay / Mailserver).

12.3.11 Aplicaciones: generalidades

Muchas son las alternativas posibles, a la hora de seleccionar un software servidor de correo electrónico. A continuación, mencionaremos algunas de las más populares:

Microsoft Exchange: Exchange Server, es la plataforma Mensajería Electrónica y Colaboración, propuesta por Microsoft. A lo largo del tiempo distintas versiones de este producto, han sido implementadas con éxito. De esta forma Exchange Server 5.5 significó el principio de una trilogía que se completaría años más tarde con la aparición de Exchange Server 2000 y Exchange Server 2003, estos últimos, considerados sendos paquetes de software tendientes a resolver problemas no sólo de mensajería, sino también de workflow, mensajería instantánea y colaboración. Entre las características diferenciales de Exchange Server 2003, se encuentra su fantástica integración con el resto de productos de la plataforma Microsoft así como su servicio de webmail denominado OWA (Outlook Web Access), el cual en su versión 2003 posee características de gran valor agregado.

Sendmail, Qmail, Postfix y Exim: En el mundo Unix y Linux, varios son los productos Open Source que se han implementado con éxito a lo largo de los años. Sin lugar a dudas, **Sendmail** ha sido la plataforma con el mayor market share respecto de un servidor de correo electrónico. A pesar de ello, **Sendmail** ha pasado por momentos en donde se encontraban y parcheaban, vulnerabilidades frecuentemente. Desde el punto de vista de su configuración, suele ser considerado uno de los más difíciles, en parte, debido a su críptico sistema de Scripts. Al contrario, **Postfix** ha resultado un buen reemplazo para Sendmail, debido en parte a que es muy fácil de configurar. **Exim**, es considerado una opción sumamente poderosa, escalable y se encuentra muy bien documentado, motivo por el cual son muchas ya, las grandes compañías que lo han adoptado a la hora de manejar sus comunicaciones de correo electrónico. Por último, **Qmai** tiene la fama de ser una de las opciones más seguras, al punto de que existe una recompensa de u$s 10000 para cualquiera que pueda realizar un Exploit que le afecte. Al día de hoy, dicha recompensa no ha sido reclamada.

Lotus Notes: Lotus Notes, ha sido por años el servidor de correo corporativo utilizado por grandes corporaciones. Pionero respecto de todas aquellas cuestiones relacionadas con soluciones del tipo workflow y colaboración en línea, Lotus Notes, mantiene un concepto levemente diferente respecto del resto de los servidores populares, en cuanto a aspectos tales como por ejemplo los métodos de almacenamiento de mensajes. En cuanto a su funcionalidad, Lotus Notes posee todas aquellas características avanzadas en cuanto al manejo de correo, agenda, trabajo cooperativo en línea, mensajería instantánea, administración de documentos y contactos.

12.3.12 Consideraciones sobre seguridad

Como hemos mencionado en alguna oportunidad, la seguridad respecto del software de correo electrónico en general, se encuentra sujeta a la forma en la que el mismo es implementado, administrado, auditado y mantenido en el tiempo. Si bien es cierto que con el transcurso de los años

algunos paquetes de software en particular, han mostrado ser menos vulnerables que otros, existen una serie de lineamientos principales, que deberán ser tenidos en cuenta, a la hora de administrar seguridad en un servidor de correo electrónico:

- Mantenerse al día, con los parches indicados por el proveedor del software.
- Configurar correctamente, las funciones de seguridad propias del aplicativo implementado.
- Realizar el Hardening correspondiente, tanto sobre el sistema operativo como sobre los dispositivos de red y el propio software de correo electrónico.
- Implementar Gateways SMTP en el perímetro externo y servidores de correo en el perímetro interno siempre que sea posible.
- Realizar auditorias periódicas sobre su instalación.
- Implementar software Antivirus, Bloqueos AntiSpam y Filtros de Contenido.
- Implementar sistemas de cifrado como por ejemplo PGP o GnuPG, a la hora de asegurar privacidad en el envío y recepción de mensajes.
- Restringir el ingreso de archivos adjuntos con extensiones que puedan contener código malicioso (EXE, BAT, PIF, WS, VBE, SCR, JS, etc.) utilizando filtros de contenido.
- Configurar los servicios de autenticación segura, en aquellos clientes POP que cuenten con dicha capacidad.
- Desactivar aquellos comandos extendidos como EXPN y VRFY siempre que no sean necesarios.
- Editar los banners o fingerprints de aquellos servicios que se estén ofreciendo.
- Escribir políticas y procedimientos efectivos, respecto del resguardo y recuperación de la información contenida en los maiboxes.

12.3.13 Mensajería Segura

Hasta el momento, durante el transcurso de las unidades, hemos dejado claro que un e-mail seguro debe satisfacer cuatro aspectos:

- Privacidad o confidencialidad
- Identificación del remitente
- Integridad del contenido del mensaje
- Conocimiento de la recepción (acuse de recibo)

Si bien solamente el protocolo MSP (Protocolo de Seguridad de Mensajes) satisface la totalidad de estos requisitos, está acotado a un entorno militar del DoD (Departamento de Defensa Americano) implementado sobre la norma X.400.

Dentro del ámbito de Internet, contamos con dos protocolos que cumplen los tres primeros requisitos pero no implementan un mecanismo de reconocimiento de recepción. Estos protocolos son:

- S/MIME (Extensiones Multipropósito de Correo de Internet Seguro)
- PGP/MIME (Privacidad Muy Buena/MIME)

MIME Seguro: Dado que S/MIME se encuentra más normalizado y es más extensible a grandes

sistemas, es el más difundido de los tres. S/MIME es un proyecto de RSA Data Security basado en formato de datos para mensajes PKCS # 7 v 1.5 y el formato X.509 v3 de certificados digitales.

S/MIME trabaja conforme a PKI, con un formato de mensajes binario y compatible con CMS (Sintaxis de Mensajes Encriptados) pues permite una amplia variedad de opciones en el soporte de contenido y algoritmo.

- Otros componentes a emplear por S/MIME son:
- Diffie-Hellman (X9.42) con DSS (Norma de Firma Digital) como algoritmo de firma
- SHA-1 (Algoritmo de Hash Seguro) como algoritmo de Hash
- DES, 3DES y RC2 como algoritmos de encriptación simétricos

PGP / OpenPGP: Pretty Good Privacy (PGP) es un paquete de software, creado por Philip Zimmermann en 1991, que prevee rutinas criptográficas para E-mail y almacenamiento de archivos. Básicamente, implementa criptosistemas y protocolos criptográficos existentes en un programa multiplataforma. Dentro de sus funcionalidades podemos contar: encriptación de mensajes, firma digital, compresión de datos y compatibilidad con E-mail por medio de la conversión Radix-64 (PGP/MIME).

A partir del PGP de Zimmermann, el OpenPGP Working Group del IETF (Internet Engineering Task Force propuso el OpenPGP como un estándar más utilizado de encriptación de e-mail en el mundo (RFC 2440). Los algoritmos empleados por defecto que se definen son:

- El Gamal y RSA para transporte de claves
- DES, IDEA y CAST5 para encriptación
- DSA para firmar
- SHA-1 y MD5 para el cálculo de los hashes

12.3.14 Las 10 vulnerabilidades de seguridad más críticas en aplicaciones Web

Con vulnerabilidades anunciadas casi semanalmente, muchos negocios pueden sentirse agobiados tratando de mantenerse actualizados. Sin embargo, existe ayuda en la forma de listas concienzudas de vulnerabilidades y defensas. "El Proyecto Abierto de Seguridad de Aplicación Web (OWASP por sus siglas en inglés) ha producido una lista similar de las 10 principales vulnerabilidades de aplicaciones Web y bases de datos más criticas, así como la forma más efectiva de resolverlas. Las vulnerabilidades de aplicación son a veces desatendidas, pero son tan importantes de resolver como los problemas de redes. Si cada compañía eliminara estas vulnerabilidades comunes, su trabajo no estaría del todo hecho, pero ellos y la Internet, serian significativamente más seguros."

El desafió de identificar las “principales” vulnerabilidades de aplicaciones Web es una tarea virtualmente imposible. No hay ni siquiera un acuerdo generalizado de qué exactamente está incluido dentro del término “seguridad de aplicaciones Web.” Algunos han argumentado que sólo deberíamos enfocarnos en los puntos de seguridad que afectan a los desarrolladores que escriben código de aplicaciones Web a la medida. Otros abogan por una definición más amplia que abarque la capa de aplicación entera, incluyendo bibliotecas, configuración de servidores y protocolos de la capa de aplicación. Con la esperanza de crear conciencia sobre los riesgos más serios que enfrentan las organizaciones, hemos decido dar una interpretación relativamente amplia al concepto de seguridad de aplicaciones Web, mientras seguimos manteniendo claros los puntos de seguridad de red e infraestructura.

El siguiente es un breve sumario de las vulnerabilidades más significantes de la seguridad de aplicaciones Web:

1. **Entrada no validada:** La información de llamadas Web no es validada antes de ser usadas por la aplicación Web. Los agresores pueden usar estas fallas para atacar los componentes internos a través de la aplicación Web.
2. **Control de acceso interrumpido:** Las restricciones de aquello que tienen permitido hacer los usuarios autentificados no se cumplen correctamente. Los agresores pueden explotar estas fallas para acceder a otras cuentas de usuarios, ver archivos sensitivos o usar funciones no autorizadas.
3. **Administración de autenticación y Sesión interrumpida:** Las credenciales de la cuenta y los tokens de sesiones no están propiamente protegidos. Los agresores que pueden comprometer las contraseñas, claves, cookies de sesiones u otro token, pueden vencer las restricciones de autenticación y asumir la identidad de otros usuarios.
4. **Fallas de Cross Site Scripting (XSS):** La aplicación Web puede ser usada como un mecanismo para transportar un ataque al navegador del usuario final. Un ataque exitoso puede comprometer el token de sesión del usuario final, atacar la maquina local o enmascarar contenido para engañar al usuario.
5. **Desbordamiento del búfer:** Los componentes de aplicaciones Web en ciertos lenguajes que no validan adecuadamente las entradas de datos pueden ser derribados y, en algunos casos, usados para tomar control de un proceso. Estos componentes pueden incluir CGI, bibliotecas, rutinas y componentes del servidor de aplicación Web.
6. **Fallas de inyección:** La aplicación Web puede pasar parámetros cuando accede a sistemas externos o al sistema operativo local. Si un agresor puede incrustar comandos maliciosos en estos parámetros, el sistema externo puede ejecutar estos comandos por parte de la aplicación Web.
7. **Manejo inadecuado de errores:** Condiciones de error que ocurren durante la operación normal que no son manejadas adecuadamente. Si un agresor puede causar que ocurran errores que la aplicación Web no maneja, éste puede obtener información detallada del sistema, denegar servicios, causar que mecanismos de seguridad fallen o tumbar el servidor.
8. **Almacenamiento inseguro:** Las aplicaciones Web frecuentemente utilizan funciones de criptografía para proteger información y credenciales. Estas funciones y el código que integran a ellas han sido difíciles de codificar adecuadamente, lo cual frecuentemente redunda en una protección débil.
9. **Negación de servicio:** Los agresores pueden consumir los recursos de la aplicación Web al punto de que otros usuarios legítimos no puedan ya acceder o usar la aplicación. Los agresores también pueden dejar a los usuarios fuera de sus cuentas y hasta causar que falle una aplicación entera.
10. **Administración de configuración insegura:** Tener una configuración de servidor estándar es crítico para asegurar una aplicación Web. Estos servidores tienen muchas opciones de configuración que afectan la seguridad y no son seguro desde la instalación original del software.

CAPÍTULO 13

13.1 SEGURIDAD EN DATACENTERS

¿Qué se conoce bajo el término de Seguridad física? Se trata del conjunto de mecanismos de prevención y detección, destinados a evitar que la información confidencial, los recursos informáticos o su entorno, sean accedidos de forma no autorizada.

¿Cuál es la definición de un ataque de Ingeniería Social? Suele definirse como el proceso por el cual un atacante intenta adquirir información acerca de su red y sistemas de información, conversando con personas relacionada con la organización. Puede ser realizado vía telefónica, por correo electrónico o personalmente.

¿Qué significa el concepto de Clustering? Se trata de un grupo de computadoras independientes trabajando juntas, como un recurso unificado, brindando de cara a las aplicaciones la visión de estar siendo ejecutadas en una única computadora. Es una solución a los problemas de disponibilidad ya que cualquiera de los nodos puede mantener el servicio en caso que otro falle.

¿Qué propósito tiene la implementación de un mecanismo Single Sign-On? Dada la complejidad de administrar usuarios y contraseñas en entornos de cómputo con múltiples plataformas que requieren ser accedidas por un mismo usuario, los sistemas Single Sign-On implementan mecanismos para integrar el control de acceso con un solo usuario y contraseña.

¿Cuál es la finalidad de un plan de contingencia? Tiene como fin enumerar procedimientos completos a la hora de actuar frente a un incidente puntual que comprometa la continuidad del negocio, con el perjuicio económico que ésto significaría

Sin lugar a dudas, la seguridad física es uno de los aspectos menos tenido en cuenta a la hora de diseñar sistemas informáticos. A pesar de ello, algunos de los incidentes de seguridad más terribles, suelen estar relacionados frecuentemente, con deficiencias en el esquema de seguridad física, planteado para una instalación de cómputo pobremente diseñada.

Lamentablemente, el profesional en seguridad informática, suele ser contactado frecuentemente por clientes que solicitan la implementación de distintos tipos de “productos” o dispositivos de seguridad tales como Firewalls y Detectores de Intrusos, con la intención de proteger su red, a pesar de no poseer, por ejemplo, sistemas de resguardo eficientes.

Como profesional en seguridad informática, parte de su trabajo se encontrará relacionado con la evaluación de riesgos y la utilización de métricas efectivas, a la hora de determinar el factor de ocurrencia de un incidente y la contramedida que, en su relación costo beneficio, sea considerada la adecuada a la hora de minimizar el riesgo informático inherente a toda implementación tecnológica. Los indicadores dispuestos a lo largo de la presente unidad, pondrán a su disposición, toda aquella información que le será de utilidad, a la hora de recomendar a su empresa o cliente, las políticas, procedimientos y tecnologías necesarias, al momento de planear y diseñar una estrategia eficiente, respecto de la seguridad física y sus aspectos relacionados.

Para comenzar, definiremos bajo el término de Seguridad Física, al conjunto de mecanismos de prevención y detección, destinados a evitar que la información confidencial, los recursos de los sistemas protegidos o su entorno, sean accedidos de forma no autorizada. Cuando hablamos de recursos del sistema, nos referimos a componentes, que van desde un simple teclado, pasando por una cinta de resguardo conteniendo toda la información de una organización o la propia CPU y discos

de los equipos servidores, hasta la integridad del propio centro de cómputos o emplazamiento físico.

Si bien es cierto, que dependiendo del entorno y los activos a proteger, esta seguridad será más o menos importante y restrictiva, aunque siempre deberá ser un punto central a la hora de establecer una estrategia de seguridad efectiva.

Uno de los aspectos generales, que nunca debe ser pasado por alto, es aquel que se encuentra relacionado con el daño potencial, que un incidente relacionado con la seguridad física puede provocar. De nada servirá tomar medidas para prevenir o detectar accesos no autorizados a nuestra red en forma lógica, de aquellos que requieren la explotación de fallos en el software, si un atacante puede acceder físicamente a nuestro Datacenter y robar una cinta conteniendo una imagen completa del sistema en cuestión, o un disco removible con información confidencial. Sin ir tan lejos, un empleado de maestranza sin malicia, por simple desconocimiento, por ejemplo podría conectar una aspiradora a una línea de UPS de nuestro Centro de Cómputos y provocar un apagón eléctrico en el corazón de nuestra red con el perjuicio que ésto implicaría.

Se denomina centro de procesamiento de datos o CPD a aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización. También se conoce como centro de cómputo (Iberoamérica) o centro de cálculo (España) o centro de datos por su equivalente en inglés data center. Dichos recursos consisten esencialmente en unas dependencias debidamente acondicionadas, computadoras y redes de comunicaciones.

Entre los factores más importantes que motivan la creación de un CPD se puede destacar el garantizar la continuidad del servicio a clientes, empleados, ciudadanos, proveedores y empresas colaboradoras, pues en estos ámbitos es muy importante la protección física de los equipos informáticos o de comunicaciones implicados, así como servidores de bases de datos que puedan contener información crítica.

El ***diseño de un centro de procesamiento de datos*** comienza por la elección de su ubicación geográfica, y requiere un balance entre diversos factores:

- Coste económico: coste del terreno, impuestos municipales, seguros, etc.
- Infraestructuras disponibles en las cercanías: energía eléctrica, carreteras, acometidas de electricidad, centralitas de telecomunicaciones, bomberos, etc.
- Riesgo: posibilidad de inundaciones, incendios, robos, terremotos, etc.

Una vez seleccionada la ubicación geográfica es necesario encontrar unas dependencias adecuadas para su finalidad, ya se trate de un local de nueva construcción u otro ya existente a comprar o alquilar. Algunos requisitos de las dependencias son:

- Doble acometida eléctrica.
- Muelle de carga y descarga.
- Montacargas y puertas anchas.
- Altura suficiente de las plantas.
- Medidas de seguridad en caso de incendio o inundación: drenajes, extintores, vías de evacuación, puertas ignífugas, etc.
- Aire acondicionado, teniendo en cuenta que se usará para la refrigeración de equipamiento informático.
- Almacenes.
- Etc.

Aún cuando se disponga del local adecuado, siempre es necesario algún despliegue de infraestructuras en su interior:

- Falsos suelos y falsos techos.
- Cableado de red y teléfono.
- Doble cableado eléctrico.
- Generadores y cuadros de distribución eléctrica.
- Acondicionamiento de salas.
- Instalación de alarmas, control de temperatura y humedad con avisos SNMP o SMTP.
- Etc.

Una parte especialmente importante de estas infraestructuras son aquellas destinadas a la seguridad física de la instalación, lo que incluye:

- Cerraduras electromagnéticas.
- Torniquetes.
- Cámaras de seguridad.
- Detectores de movimiento.
- Tarjetas de identificación.
- Etc.

Una vez acondicionado el habitáculo se procede a la instalación de las computadoras, las redes de área local, etc. Esta tarea requiere un diseño lógico de redes y entornos, sobre todo en aras a la seguridad. Algunas actuaciones son:

- Creación de zonas desmilitarizadas (DMZ).
- Segmentación de redes locales y creación de redes virtuales (VLAN).
- Despliegue y configuración de la electrónica de red: pasarelas, routers, conmutadores, etc.
- Creación de los entornos de explotación, pre-explotación, desarrollo de aplicaciones y gestión en red.
- Creación de la red de almacenamiento.
- Instalación y configuración de los servidores y periféricos.
- Etc.

13.1.1 Riesgos

Como mencionáramos con anterioridad, gran parte del éxito en las tareas emprendidas por el analista de seguridad, se basan en la acertada administración del riesgo, por tal motivo, la identificación del mismo suele ser un factor clave en toda estrategia de seguridad. Si bien es cierto que pueden existir diferentes visiones al respecto, la mayoría de los especialistas suelen coincidir en que, el acceso físico no autorizado, los desastres naturales (Inundaciones, Tormentas Eléctricas, Terremotos, etc.) y las alteraciones del entorno (Electricidad, Ruido Eléctrico, Humo, Incendios, Temperaturas Extremas, etc.) suelen ser algunos de los grupos de riesgo más importantes. Debido a que gran parte de estas amenazas han sido comentadas en la primera unidad de ESR 1 “Seguridad de la Información”, no nos

detendremos a enumerarlas en detalle.

Desde el punto de vista “físico”, los riesgos suelen encontrarse por lo general, relacionados con alguna de las siguientes categorías:

Robo y Hurto: Para comenzar, diremos que pese a que en definitiva el resultado final de un Robo o Hurto, traerá aparejada por lo general, la pérdida de un bien, es preciso establecer la diferencia entre ambos conceptos a los efectos de una eventual denuncia policial y posterior causa judicial. Por definición, suele hablarse de robo, cuando la sustracción del bien se lleva a cabo mediante intimidación o fuerza, mientras que deberíamos referirnos a hurto, cuando dicha sustracción se realiza sin la presencia del propietario. De cualquier forma, pocas amenazas suelen causar tanto daño económico como el robo o hurto perpetrado en un centro de cómputos, pues éste va más allá del costo de recuperación de lo robado. Paradas de servicio provocadas por el tiempo de espera en los reemplazos de los componentes robados, puede significar por ejemplo, pérdidas económicas varias veces superiores al costo mismo del componente a reponer.

Destrucción: A diferencia de otro tipo de riesgos, la “Destrucción” cuenta con la característica adicional, de que el daño puede ser inflingido de forma “Accidental” o de forma “Intencional”. El tropiezo con uno de los cables principales relacionados con el tendido eléctrico, podría ocasionar la caída física de un server mal ubicado, provocando su rotura y por ende un corte abrupto en los servicios ofrecidos por el sistema afectado. De la misma forma, el derramamiento de café o bebidas gaseosas sobre un componente electrónico, podría volver inutilizable una placa principal. Por otra parte, un empleado descontento, podría dañar intencionalmente las cintas de backup almacenadas, volviéndolas inservibles, provocando un enorme perjuicio al momento de que las mismas sean requeridas.

13.1.2 Necesidad de protección

Claro está, que las amenazas existen y que los riesgos asociados, pueden la mayoría de las veces ser elevados. Frente a este escenario, la alternativa por parte del profesional de seguridad, pasa por establecer todas aquellas medidas de detección y prevención estudiadas hasta el momento, a fin de limitar la superficie de exposición y minimizar el riesgo producido por amenazas conocidas. Ahora bien, ¿qué hay de aquellos incidentes del tipo accidental o bien los relacionados con causas naturales? En general, cuando un incidente de seguridad de cualquier tipo es "Intencional", el mismo probablemente pueda ser prevenido, pero cuando es "Accidental" no podremos en la mayoría de los casos anticiparnos al hecho. A fin de estar preparado para este tipo de circunstancias, será de vital importancia, el diseño e implementación de planes de contingencia, de continuidad de negocios y de recuperación de desastres, los cuales en conjunto con las diferentes tecnologías a disposición del profesional de seguridad informática, serán de gran utilidad, en el momento oportuno. Cuando hablamos de protección o prevención, muchas veces debemos hacer referencia al costo de adquisición, implementación o mantenimiento, implícito en los mismos. Por este motivo, es importante recalcar que la inversión realizada a fin de proteger un bien, debe guardar relación con el valor del mismo.

13.1.3 Responsabilidades

Muchas veces, luego de ocurrido un incidente, suele existir una etapa en la cual se requiere asignar responsabilidades respecto de lo ocurrido. En algunos casos, la misma podrá recaer en una persona, o quizás en un grupo de ellas. Frecuentemente, el siguiente paso después de la asignación de responsabilidades, suele estar signado por consecuencias económicas, laborales o incluso penales para los involucrados. Generalmente, éstas suelen ser establecidas en forma proporcional al daño o

perjuicio sufrido como parte del incidente, aunque todo dependerá en gran parte de la organización o empresa involucrada.

En este sentido, es sumamente importante tener claro que uno de los requisitos fundamentales en toda organización, es precisamente, la de contar con políticas y procedimientos claros a la hora de pre-establecer, aquellos puntos que deberán ser considerados clave, a la hora de asignar responsabilidades. Entre los más importantes se encuentran:

- ¿Quiénes serán los responsables?
- ¿Cuál es el alcance de la responsabilidad y en qué circunstancias?
- ¿Cuáles son las consecuencias de no cumplir con una responsabilidad implícita?
- ¿Existe una cadena de responsabilidad? En caso de que la respuesta sea afirmativa ¿Quién es responsable de qué?
- Las responsabilidades, ¿han sido informadas en forma correcta?

Ahora bien, a pesar de ser necesaria, la definición y formalización de estos puntos como parte de una política de seguridad, es imprescindible referirnos una vez más, a la importancia que tiene para el éxito de la estrategia de seguridad, que Ejecutivos y Directores empresariales, se encuentren involucrados al nivel correspondiente. Sólo de esta forma, se podrá conseguir implantar las políticas necesarias, a la hora de determinar responsabilidades y asignar sus consecuencias.

13.1.4 Panorama actual

Día a día, crece el número de empresas que comprenden la necesidad de identificar sus activos de información, de asignarles un valor y de protegerlos en consecuencia. A pesar de ello, el analista de seguridad o el administrador de sistemas, muchas veces se encontrará con situaciones en las que la falta de presupuesto asignado al área de seguridad informática, afectará en forma directa la continuidad del negocio en caso de que la compañía en cuestión, sea víctima de un incidente de seguridad. Este hecho, no debería ser motivo para dejar de relevar y documentar formalmente, las recomendaciones realizadas oportunamente en ocasión de una auditoria. Dicho ejercicio, podrá ser de utilidad, desde el punto de vista de la posición del analista o administrador en cuanto a su “responsabilidad” una vez producido un incidente, así como ante la eventual asignación de una cuota adicional de presupuesto que permita implementar el proyecto en carpeta.

Por último, debemos volver a mencionar, que parte del trabajo de un analista de seguridad, se encuentra relacionado, no sólo con la evaluación del riesgo, sino también con la realización de informes precisos, a la hora de presentar opciones a la gerencia o dirección de la empresa, en donde se muestre claramente el valor de la información a proteger y la inversión relacionada.

13.2 SEGURIDAD DEL PERSONAL

Suele decirse que el éxito o fracaso en la implementación de una estrategia de seguridad, se encuentra de una u otra forma relacionado con los recursos humanos en ella involucrados. Esto es especialmente cierto, en varios aspectos. En primer lugar, la selección de las personas correctas redundará en beneficios, no sólo al colaborar con los objetivos específicos propuestos al momento de su incorporación sino también con la receptibilidad que los mismos tendrán respecto de los asuntos relacionados con la seguridad informática. En segundo lugar, sabemos que una estrategia de seguridad, es tan efectiva como su eslabón más débil, y muchas veces éste suele encontrarse representado, por el personal involucrado.

Teniendo en cuenta lo mencionado en el párrafo anterior, deberemos ser concientes de que el

conjunto de Políticas y Procedimientos utilizados en una organización tendrán un gran impacto a la hora de administrar un entorno seguro, por tanto deberán ser considerados un aspecto fundamental de toda estrategia de seguridad. De la misma forma, la adecuación por parte de las empresas a normas internacionales tales como la ISO 17799, suelen colaborar de forma acertada, con el logro de los objetivos planteados. A través de los siguientes indicadores, presentaremos precisamente, algunas de las tareas que, relacionadas con la selección, capacitación y demás aspectos involucrados principalmente con el factor humano de una organización, suelen ser desarrolladas con el fin de establecer un marco acorde a la implementación de una estrategia de seguridad efectiva.

13.2.1 Selección y política de personal

Cuando una organización, se encuentra involucrada por completo con la estrategia de seguridad en ella implementada, la tarea misma de selección de personal, al momento de cubrir cualquier tipo de puesto, involucra determinados aspectos que de no ser tenidos en cuenta, podrían devenir en circunstancias no deseadas. Siempre que sea posible, el departamento de seguridad informática, debería participar del desarrollo de la "Política de Contratación" o "Hiring Policies" establecida por el departamento de recursos humanos. Por ejemplo, probablemente usted querría asegurarse que uno de los requisitos al momento de incorporar un nuevo empleado (o un nuevo usuario, visto desde la perspectiva del administrador de red) sea verificar que el postulante no sea un adicto a las drogas o que posea antecedentes policiales. Éste y otros aspectos pueden ser cubiertos al momento de establecer precisamente la "Política de Contratación" en su compañía.

Por su parte, la definición de una "Política de Uso Aceptable" o "Aceptable Use Policy", suele ser un gran aliado del oficial de seguridad informática, a la hora de establecer con claridad, un marco en la empresa, respecto de lo que se puede y no se puede hacer, bien sea con la información por ella provista así como respecto a la utilización del equipamiento suministrado. La "Política de Uso Aceptable", puede ser tan general o específica como se requiera. Mientras que muchas veces, el desarrollo de la misma implica la creación de secciones específicas orientadas a normar el uso aceptable de recursos tales como Internet o el Sistema Telefónico, tan solo por dar un ejemplo; al mismo tiempo, varias son las compañías que resumen su "Política de Uso Aceptable", en una única frase del tipo "Los equipos de cómputo y sistemas informáticos provistos por la compañía, sólo deberán ser utilizados con fines laborales". Por último, la elaboración de una cuidada "Política de Ética" o "Ethics Policies", tenderá un manto sobre aquellos aspectos de comportamiento general, que deben ser adoptados por cada uno de los empleados de la compañía.

Un aspecto sumamente importante a la hora de establecer políticas en una corporación, pasa por la necesidad de definir a la vez, un método efectivo de comunicación y aceptación por parte de los empleados. Sin éste, la aplicación de sanciones por incumplimiento de las mismas, probablemente sea una causa perdida.

13.2.2 Acuerdos de confidencialidad

Al momento de establecer una relación laboral, empleado y empleador, aceptan en forma implícita el grado de confianza que será necesario a la hora de realizar las tareas encomendadas. No obstante, un "Acuerdo de Confidencialidad", suele ser visto como la confirmación explícita de la confianza pre-establecida al momento de iniciar una relación laboral.

Si bien el detalle contenido en un acuerdo de confidencialidad, puede variar de organización en organización, normas tales como la ISO 17799 (Inciso 6.1.3), establecen en forma clara y sintética algunos lineamientos generales, entre los que se encuentran:

- Un "Acuerdo de Confidencialidad" o "No Divulgación", debe ser utilizado para reseñar que la información es confidencial o secreta.
- Debe ser firmado por los empleados, como parte de sus términos y condiciones iniciales de

empleo, al momento de su contratación.

- El personal ocasional y los usuarios externos aún no contemplados en un contrato formalizado (que contenga el acuerdo de confidencialidad) deberán firmar el acuerdo mencionado antes de que se les otorgue acceso alguno a las instalaciones de procesamiento de información.
- Los acuerdos de confidencialidad deben ser revisados cuando se producen cambios en los términos y condiciones de empleo o del contrato, en particular cuando el empleado está próximo a desvincularse de la organización o el plazo del contrato está por finalizar.

13.2.3 Finalización de empleo

Por diversos motivos, la terminación de un contrato laboral, muchas veces puede estar signado por aspectos emocionales que en determinadas circunstancias, pueden desembocar en un incidente de seguridad. Por este motivo, el mismo cuidado puesto en la incorporación del nuevo personal, deberá existir a la hora de terminar la relación laboral establecida entre empleado y empleador. A tal efecto, la definición de una “Política de Finalización” o “Termination Policies” deberá ser considerada.

Ya sea que la desafectación de un empleado respecto de la compañía para la cual presta servicios, sea voluntaria o involuntaria, aspectos tales como la inmediata cancelación del acceso a la red por medio de prácticas tales como la desactivación de cuentas de sistema, deberán ser considerados. Un aspecto fundamental en tal sentido, pasa por la correcta comunicación de la ocurrencia de desvinculaciones, por parte del departamento de recursos humanos o del sector que corresponda. En tal sentido, una “Política de Finalización”, debería incluir en forma clara y concisa, el procedimiento a seguir desde el punto de vista de la organización, al momento de producida la baja. Muchas empresas, deciden agregar a su “Política de Finalización” procedimientos por los cuales se establece que el empleado despedido, deberá ser escoltado/acompañado desde el momento mismo de comunicado el despido, hasta su salida del predio ocupado por la organización.

En caso de que la finalización de un contrato laboral, sea involuntario, el profesional de seguridad, podría sugerir acciones tales como la separación inmediata de todo sistema de cómputo por parte de la persona despedida, y el resguardo de aquellos sistemas o archivos de datos que sean considerados de importancia para la organización. Si bien es cierto que la mayoría de las personas no suelen comportarse de manera inusual, el oficial de seguridad podría de esta forma asegurar los activos en caso de que algo no salga bien.

13.2.4 Capacitación en materia de seguridad de la información

Como mencionáramos al inicio de este capítulo, gran parte del éxito en la implantación de una estrategia de seguridad en la compañía, se encontrará íntimamente relacionada con cuan involucrado se encuentre el personal en general con la misma. A fin de lograr este objetivo, todo departamento de seguridad informática, debe tener como tarea, el diseño e implementación, de un plan de capacitación a usuarios, el cual deberá cubrir al menos, los siguientes puntos principales:

- Importancia de la Seguridad de la Información.
- Responsabilidad de las personas que conforman la organización, respecto de la Seguridad de la Información.
- Políticas y Procedimientos relacionados.
- Políticas de Uso.
- Criterio y aspectos a tener en cuenta, a la hora de seleccionar claves de acceso.
- Generación de una “Conciencia de Seguridad”.

- Prevención contra la Ingeniería Social.

Respecto de este último punto, vale la pena detenernos a fin de establecer algunos de los aspectos principales, relacionados con la amenaza dispensada por ataques de Ingeniería Social. Generalmente, suele definirse como Ingeniería Social, al proceso por el cual, un atacante intenta adquirir información acerca de su red y sistemas de información, conversando con personas relacionadas con su organización. Un ataque de Ingeniería Social, puede ser realizado ya sea vía telefónica, por correo electrónico o personalmente y generalmente se basa en todo tipo de técnicas, engaños y cualquier otro tipo de artilugio válido, a la hora de convencer a un usuario a que ejecute código conteniendo un troyano, obtener contraseñas, o cualquier otra información que pueda ser de utilidad a un atacante al momento de planear un ataque más elaborado

A diferencia de lo que ocurre con la mayoría de los ataques vistos hasta el momento, en donde diversos aspectos técnicos pueden ser aplicados a la hora de prevenirlos, la Ingeniería Social brinda un desafío adicional al oficial de seguridad, puesto que su mejor defensa frente a este tipo de ataques, se encuentra directamente relacionada con la capacitación brindada a los usuarios, staff técnico y dirección de la empresa, como parte de su tarea de "Educación y Prevención".

13.2.5 Comunicación de incidentes

Como hemos mencionado en más de una oportunidad, ninguna empresa u organización, se encuentra exenta de ser víctima de un incidente de seguridad. Cuando este momento llegue, probablemente usted querrá contar antes que nada, con los mecanismos necesarios para estar al tanto de que un incidente ha ocurrido o está ocurriendo en ese mismo momento. De no existir este hito, no se podrá actuar en consecuencia.

De acuerdo a lo que dicta el punto 6.3 de la ISO 17799 ("Respuesta a Incidentes y Anomalías en Materia de Seguridad"), "Los incidentes relativos a la seguridad deben comunicarse a través de canales gerenciales apropiados tan pronto como sea posible"

A tal efecto, parte de la responsabilidad de un oficial de seguridad, radica en establecer un procedimiento formal de comunicación, junto con un procedimiento de respuesta a incidentes, que establezca en forma clara, aquellas acciones que deberán emprenderse al recibir un informe relacionado con algún tipo de incidente.

De la misma forma en que se asegura la correcta comunicación del resto de las políticas relativas a la seguridad de la información en la organización, deberá comunicarse el "Procedimiento de Comunicación de Incidentes". Un buen momento para presentar el tema a los empleados de la organización, se encuentra dado por ejemplo, por la inclusión de este tema, como parte del contenido de la capacitación en seguridad informática mencionada en indicadores anteriores.

Beneficios de IKE:

- Elimina la necesidad de especificar manualmente los parámetros de seguridad de IPSec en ambos extremos
- Permite a los administrador especificar el tiempo de vida de una asociación de seguridad (SA) en IPSec
- Permite que las claves de encriptación cambien durante una sesión IPSec
- Le permite a IPSec proveer servicio contra la réplica
- Permite soportar autoridades de certificación (CA), logrando una implementación IPSec escalable
- Permite la autenticación dinámica entre pares

13.3 SEGURIDAD FÍSICA Y AMBIENTAL

Tal como lo definiéramos al inicio de esta unidad, el término de Seguridad Física, suele ser utilizado para referirnos al conjunto de mecanismos de prevención y detección, destinados a evitar que la información confidencial, los recursos de los sistemas protegidos o su entorno, sean accedidos de forma no autorizada. Suele decirse que la seguridad física, es algo más sencilla de lograr que la seguridad lógica. Parte de esta afirmación, se encuentra relacionada, con que habitualmente, las amenazas capaces de producir un daño físico a las instalaciones de nuestro cliente o compañía, suelen ser más fáciles de identificar que amenazas de tipo lógicas.

La Seguridad Física y Ambiental, es una rama en si misma de la Seguridad Informática en general. Sus procedimientos asociados, involucran el conocimiento y entendimiento de cada una de las posibles amenazas, así como también los métodos, procedimientos y tecnologías con las que cuenta un profesional al momento de minimizar el riesgo.

13.3.1 Selección de la ubicación

Pocas medidas producen un impacto tan grande respecto del nivel final de seguridad a obtener, como la selección de la ubicación al montar un centro de cómputo. El analista de seguridad, debe saber que el accionar a conciencia al realizar esta tarea, redundará en beneficios a la hora de diseñar un sitio seguro, a partir de esta primera elección.

Conciente de que el grado de dependencia que tenga una organización respecto de sus sistemas de información, es proporcional al grado de trastorno que la eventual avería o destrucción de parte de los componentes dispuestos en un datacenter puede ocasionar a la gestión de la misma, diferentes serán los grados de detalle, con el que usted debería plantear un estudio respecto de las características físicas del sitio donde planea instalar su centro de cómputos.

La evaluación de la ocurrencia respecto de catástrofes meteorológicas en la zona es un buen ejemplo de dichos estudios. El promedio de lluvia caído en los últimos años, en conjunto con la selección de una ubicación elevada y alejada de grandes caudales de agua brindará la posibilidad de estar a salvo de los perjuicios ocasionados por inundaciones o maremotos.

El relevamiento previo, acerca de la existencia de señales o rayos de radar que puedan incidir en el correcto funcionamiento de los servicios dispensados desde el centro de cómputos, suele ser a menudo un aspecto no tenido en cuenta. Procure mantener su sitio alejado de estas fuentes de emisión o en su defecto, correctamente protegido.

La acción del fuego puede ser impredecible, y el daño producido por las llamas y el humo, a un datacenter, puede ocasionar serios inconvenientes. Al seleccionar la ubicación de un centro de cómputos, deberá tener en cuenta que el lugar elegido, se encuentre alejado de depósitos con contenido inflamable, o zonas de riesgo

Por último, suele ser recomendable que la instalación de su datacenter, se haga efectiva en zonas tranquilas de bajo tránsito, evitando la exposición a riesgos de alto grado, a su vez debería evitar seleccionar lugares desolados o desprotegidos.

13.3.2 Perímetro de seguridad física

Varias son las formas de proteger físicamente un emplazamiento. Generalmente, la disposición de barreras físicas alrededor de las locaciones utilizadas por una organización, suele ser una decisión acertada, aunque desde el punto de vista práctico, la mayoría de las veces, más de una barrera física deberá ser implementada, marcando de esta forma, diferentes “Perímetros de Seguridad” cada uno de los cuales incrementa la protección total provista por el esquema diseñado. Tal como se encuentra definido en el punto 7.1.1 de las normas ISO 17799 “*Un perímetro de seguridad es algo delimitado por*

una barrera, por ejemplo: una pared, una puerta de acceso controlada por tarjeta o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada barrera dependerán de los resultados de una evaluación de riesgos".

A continuación, citaremos algunos de los controles y lineamientos principales, que forman parte de la norma anteriormente mencionada:

- El perímetro de seguridad debe estar claramente definido.
- El perímetro de un edificio o área que contenga instalaciones de procesamiento de información debe ser físicamente sólido (por ej. no deben existir claros [o aberturas] en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser de construcción sólida y todas las puertas que comunican con el exterior deben ser adecuadamente protegidas contra accesos no autorizados, por ej., mediante mecanismos de control, vallas, alarmas, cerraduras, etc.
- Debe existir un área de recepción atendida por personal u otros medios de control de acceso físico al área o edificio. El acceso a las distintas áreas y edificios debe estar restringido exclusivamente al personal autorizado.
- Las barreras físicas deben, si es necesario, extenderse desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo, la ocasionada por incendio e inundación.
- Todas las puertas de incendio de un perímetro de seguridad deben tener alarma y cerrarse automáticamente, con apertura desde el interior solamente.

13.3.3 Control de acceso físico

Parte de la estrategia de seguridad en torno a la protección física de los activos de la empresa, se encuentra relacionada con el correcto diseño e implementación de sistemas de control de acceso adecuados. Hay quienes afirman que un esquema mínimo en torno al control de acceso y las barreras físicas dispensadas a fin de proteger un centro de cómputo, debe estar conformado por al menos tres barreras físicas: Una primera que delimite la entrada al edificio, separando el interior del exterior (generalmente protegida por algún tipo de sistema de alarma), la segunda bloqueando el acceso al recinto donde se encuentra físicamente el centro de cómputo y por último, una tercer barrera consistente en la puerta que finalmente brinda acceso al mismo

Claro está que muchas veces el requerimiento de seguridad de una organización, puede llegar a sugerir la incorporación de otro tipo de dispositivos. Una alternativa utilizada en entornos de alta seguridad, se encuentra dada por un pequeño espacio intermedio entre dos barreras. La implementación de este tipo de medidas, permite una identificación visual y la posterior facultad de permitir o denegar el acceso de acuerdo al resultado de la misma

Pero las barreras, muchas veces requieren de diversos mecanismos de control de acceso, que amparen su operación. Lectores de tarjetas por proximidad, molinetes de acceso que responden a la inserción de tarjetas magnéticas, suelen encontrarse entre los más utilizados, aunque en los últimos años, los sistemas biométricos han ganado terreno

Un sistema biométrico, utiliza alguno de los aspectos biológicos propios de la persona, que permiten su identificación. Algunos de los métodos utilizados son: lectura de huellas digitales, reconocimiento de retina, escaneo de iris, reconocimiento facial, análisis de la voz, y lectura de la geometría de las palmas de las manos. Muchas veces este tipo de sistemas, se utilizan en combinación con códigos de acceso, conformando una solución bastante más efectiva. Es de esperar que en el transcurso de los próximos años, mejoras respecto de este tipo de tecnologías, logren volver este tipo de soluciones, más comunes.

13.3.4 Protección de locales

Muchas organizaciones poseen dentro de su ubicación, distintas oficinas, recintos o instalaciones dispuestas con un fin en particular. Desde el punto de vista de su seguridad, frecuentemente solemos referirnos a dichas locaciones, como “áreas seguras”. Un área segura, puede ser una oficina cerrada con llave o tal como mencionáramos algunas líneas más arriba, diversos recintos dentro de un mismo perímetro de seguridad física, los cuales pueden estar bloqueados y contener cajas fuertes o gabinetes con cerraduras. Varios son los aspectos a tener en cuenta al seleccionar estas áreas seguras, y su protección ante las posibles amenazas. El punto 7.1.3 de las normas ISO 17799, provee de una lista de verificación, respecto de aquellos lineamientos generales a tener en cuenta a la hora de velar por su seguridad

13.3.5 Normas ambientales

Todo centro de cómputo, debe cumplir con una serie de normas ambientales a fin de mantener el grado de seguridad necesario para que el equipamiento instalado, trabaje en forma eficiente y se conserve en buen estado. Dichas prácticas, no sólo suelen redundar en beneficios a la hora de proteger la conservación del equipamiento, sino que por el contrario, reducirá el riesgo inherente a incidentes producidos por su mal funcionamiento.

Por lo general, la aplicación del conjunto de normas ambientales a disposición del profesional en seguridad informática, suele estar relacionado con el control de factores tales como:

- La emanación de gases corrosivos.
- La degradación de componentes por la acción del polvo.
- La humedad del ambiente.
- La temperatura adecuada, en relación al equipamiento instalado.
- Los campos magnéticos actuantes.
- La condensación y el vapor.
- La tensión eléctrica.

Por otra parte, la calidad y potencia lumínica dispuesta en instalaciones de trabajo, el nivel de ruido, así como diferentes normas ergonométricas, suelen con frecuencia ser contempladas en determinados entornos de trabajo, debido a que pueden incidir sobre los recursos humanos que se encuentran trabajando en una locación específica.

13.3.6 Sistemas contra incendios

Los sistemas contra incendios, suelen ser un aspecto clave al momento de diseñar un centro de cómputos seguro. En la actualidad, es posible encontrar al menos dos tipos principales de sistemas contra incendios. A continuación, mencionaremos algunas de las características principales de cada uno de ellos:

- **Extinguidores de Fuego:** La selección y uso de extinguidores, debe ser considerada una tarea crítica. Una mala elección en tal sentido, puede ser contraproducente, a la hora de enfrentar un siniestro. Los extinguidores, se clasifican en “clases” de acuerdo al tipo de fuego a combatir. Por su parte los fuegos a combatir, han sido clasificados en cuatro tipos, de acuerdo con los materiales combustibles que los alimentan. Estas clases de fuegos se denominan con

las letras "a", "b", "c" y "d". Más allá de lo comentado, existen en el mercado, los denominados “Extinguidores Multipropósito”, los cuales combinan capacidades propias de distintas clases, en un solo tubo. Los extinguidores multipropósito más comúnmente utilizados son A-B, B-C, y A-B-C.

Una adecuada política respecto de los extinguidores de incendio, deberá estar compuesta básicamente por el procedimiento al momento de su utilización, y por el control y mantenimiento periódico de su carga útil

- **Sistemas Fijos:** Los sistemas fijos más comunes, son aquellos que combinan detectores de fuego con sistemas de extinción. Por lo general, los detectores de incendios dispuestos en lugares estratégicos de la locación a proteger, detectarán cambios bruscos de temperatura o humo excesivo, actuando consecuentemente disparando diversos mecanismos de supresión de fuego. Entre los más utilizados, se encuentran la distribución de agua como elemento de extinción, o el suministro de algún tipo de gas a fin de desplazar el oxígeno del ambiente, eliminando de esta forma uno de los componentes necesarios al momento de generar fuego.

13.3.7 Suministro de energía

La energía, es un factor fundamental en todo centro de cómputos, y como tal debe ser administrado cuidadosamente, a fin de evitar cualquier tipo de incidente producido en torno a ella. Por lo general, el centro de cómputos es el sitio donde se aloja el equipamiento más crítico y costoso, motivo por el cual debe estar protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas.

A la hora de diseñar un centro de cómputo, se deberán realizar los estudios necesarios respecto de los requisitos del equipamiento a instalar en dicha locación, a fin de proveer a los mismos de un adecuado suministro de energía, el cual se encuentre en sintonía con las especificaciones propiciadas por fabricante o proveedor de los equipos a utilizar. Tal como se menciona en las normas ISO 17799 en su punto 7.2.2, entre las alternativas para asegurar la continuidad del suministro de energía podemos enumerar las siguientes:

- Múltiples bocas de suministro para evitar un único punto de falla en el suministro de energía.
- Suministro de energía ininterrumpible (UPS)
- Generador de respaldo.

Todo equipamiento relacionado con los procesos críticos de la compañía, deberá encontrarse conectado a un equipo de energía ininterrumpible (UPS), a fin de asegurar el correcto apagado en caso de un corte repentino en el suministro. Como todo componente involucrado en la seguridad de un centro de cómputos, deberán existir normas y procedimientos que exijan que los UPS sean probados en forma regular. Por otra parte, en aquellos casos donde la operación informática no pueda ser interrumpida, deberá considerarse la implementación de sistemas generadores de electricidad, sobre los cuales necesariamente deberán recaer controles periódicos y evaluaciones de operación y desempeño.

13.3.8 Protección del cableado

El cableado en todo Datacenter, debe ser tenido en cuenta al momento de realizar el diseño e implementación del esquema de seguridad. Cualquier descuido en dicho procedimiento, podría significar serios problemas en el correcto funcionamiento de los dispositivos que de él dependen, de la misma forma que en algunos casos, podrían llegar a comprometer la integridad y privacidad cuando de cableados de red se trata.

Cortes accidentales o intencionales, producidos por los propios empleados o por un tercero, suelen significar a menudo un incidente de seguridad que debe ser considerado como un riesgo más. En relación a los tendidos eléctricos y el cableado de datos o telefonía, los daños podrían llegar a ser fruto de un cuidadoso ataque de denegación de servicio, mientras que puntualmente hablando del cableado de red, tanto el desvío como la escucha pasiva de los datos por él transmitidos, deben ser considerados un riesgo probable.

Cableados de alto nivel de seguridad, deberán ser implementados en aquellos puntos donde deba asegurarse la integridad y confidencialidad de los datos.

En relación a estos puntos, la norma ISO 17799 plantea los siguientes puntos de control:

- Las líneas de energía eléctrica y telecomunicaciones que se conectan con las instalaciones de procesamiento de información deben ser subterráneas, siempre que sea posible, o sujetas a una adecuada protección alternativa.
- El cableado de red debe estar protegido contra interceptación no autorizada o daño, por ejemplo mediante el uso de conductos o evitando trayectos que atraviesen áreas públicas.
- Los cables de energía deben estar separados de los cables de comunicaciones para evitar interferencias.
- Entre los controles adicionales a considerar para los sistemas sensibles o críticos se encuentran los siguientes:
    - Instalación de conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección.
    - Uso de rutas o medios de transmisión alternativos
    - Uso de cableado de fibra óptica
    - Iniciar barridos para eliminar dispositivos no autorizados conectados a los cables.

13.4 EQUIPAMIENTO

Pocas cosas son tan importantes en un centro de cómputos o datacenter, como el propio equipamiento en él instalado. A diferencia de lo que ocurre con el resto del parque de la empresa, probablemente los equipos utilizados en el centro de datos, requieran una serie de cuidados especiales. De la misma forma, la elección de dicho equipamiento, podrá significar gran parte del éxito respecto de los servicios informáticos que planea brindar a su corporación. Por este motivo, deberá ser extremadamente cuidadoso al momento de realizar dicha selección.

Por otra parte, del mismo modo en que los conceptos de “Defensa en Profundidad”, son aplicados a la seguridad lógica, físicamente, los servidores dispuestos en un datacenter, deberán poseer una serie de características básicas de seguridad, que sirvan como la última barrera a vencer por un atacante, que haya logrado acceder al perímetro controlado. Cerraduras bloqueando la extracción de discos hotswap, alarmas dispuestas en el chasis del equipamiento crítico, discos con controladoras especiales que impiden su utilización en otro que no sea el equipo original, lockers de teclados, racks con cerraduras y claves en el setup, son sólo algunas de las tecnologías a implementar, al momento de velar por la seguridad física del equipamiento instalado.

13.4.1 Selección

Como mencionáramos en párrafos anteriores, la selección del equipamiento a utilizar en un centro de cómputos, tendrá gran incidencia en el resultado final del esquema de seguridad planteado. Como es de esperar, las características de seguridad inherentes al equipamiento a adquirir, por lo general se encontrarán relacionadas con el costo del mismo. Por este motivo, como analista de seguridad,

deberá realizar un estudio previo, que avale su selección, teniendo en cuenta los riesgos que presupondrá, no contar con las prestaciones recomendadas.

Para empezar, usted deberá realizar el correcto dimensionamiento, en cuanto a capacidad de proceso y almacenamiento. Puesto que este es un factor fundamental, deberá realizarse teniendo en cuenta el software a correr, la cantidad de usuarios a soportar, las recomendaciones del proveedor y la infraestructura general de la empresa. La mayoría del los paquetes de software implementados en el sector corporativo, poseen sus propios métodos a la hora de realizar un dimensionamiento efectivo, téngalos en cuenta a la hora de realizar sus previsiones.

Por otra parte, se deberá prestar especial atención a todo aquel equipamiento, que haya sido identificado como crítico en su etapa de relevamiento, respecto de los sistemas que soporta y la calidad de servicio a brindar (Dada por ejemplo, por el tiempo máximo de downtime permitido en su negocio). Estos, deberán poseer la mayor cantidad de componentes redundantes que sea posible, teniendo en cuenta el presupuesto asignado, la tecnología a implementar y el tipo de componente.

Por último, un aspecto sumamente importante a la hora de seleccionar el equipamiento a utilizar en su implementación de un centro de cómputos, radica en el soporte brindado por el proveedor del mismo. De nada servirá un servidor de gran potencia, si al momento de requerir el reemplazo de un componente, el mismo no es provisto a tiempo o directamente no se consigue en el mercado. Del mismo modo, una adecuada política de update del firmware necesario para el correcto funcionamiento de los componentes, deberá ser contemplada.

13.4.2 Clustering

Con el correr del tiempo, muchas fueron las empresas que establecieron el crecimiento de su negocio, en torno a soluciones informáticas. Grandes sistemas de e-commerce, completas soluciones ERP (Enterprise Resource Planning) y centros de atención a usuarios on-line, son tan solo algunos de los negocios que requieren velar por uno de los factores críticos en toda implementación: Disponibilidad. Como una de las principales herramientas, a la hora de garantizar precisamente, la disponibilidad en los diferentes servicios prestados por el equipamiento instalado en nuestro datacenter, ha surgido el concepto de Clustering y su tecnología relacionada.

En su definición más elemental, un Cluster, no es más que un grupo de computadoras independientes trabajando juntas, como un recurso unificado, brindando de cara a las aplicaciones que en él se ejecutan, la visión de estar siendo ejecutadas en una única imagen. De acuerdo a su funcionamiento, un cluster provee entre otras facilidades, una solución excelente a los problemas de disponibilidad, debido a que en la mayoría de las configuraciones probables (Activo-Activo, Activo-Standby, Tolerante a Fallos), cualquiera de los “nodos” participantes del cluster, se encuentra en posición de atender requerimientos de la aplicación, en caso de que el nodo principal sufra un desperfecto

Para que un cluster sea implementado, no sólo deberá poseerse el equipamiento necesario, sino también sistemas operativos y en algunos casos software complementario que posibilite su funcionamiento o monitoreo. Windows 2000 en sus versiones Advanced Server and Datacenter Server, Windows 2003, Unix y Linux suelen ser algunas de las alternativas de sistemas operativos con estas posibilidades.

Muchas veces, puede suceder que el motivo principal para la implementación de un cluster, no sea el aseguramiento de la disponibilidad, pero sí, la potencia de cómputo a obtener. Soluciones Open Source del tipo OpenMosix, en conjunto con software del tipo Linux y equipos de bajo costo, han logrado llevar el poder de supercomputadores, que hasta hace algunos años se encontraba subscripto a grandes empresas o gobiernos, a un público más amplio

13.4.3 Redundancia

Otra de las tecnologías al alcance del profesional de seguridad informática, al momento de asegurar

aspectos tales como la disponibilidad, es aquella que se encuentra relacionada con los dispositivos redundantes. Si bien es cierto, que comúnmente esta tecnología es implementada en sistemas de discos, lo cierto es que las capacidades de redundancia, no se restringen únicamente a este tipo de dispositivos. Fuentes, placas de red y memoria, son tan solo algunos de los componentes a tener en cuenta, al momento de solicitar esta característica al equipamiento seleccionado.

RAID (Redundant Arrays of Independent Disks o Arreglo Redundante de Discos Independientes) Se denomina RAID, a la tecnología que utiliza múltiples discos, a la hora de proveer tolerancia a fallos y mejoras en la performance de operaciones de lectura y escritura (Esta última característica, en alguna de sus configuraciones). Dicho de otra forma, un RAID es una colección de discos que integran uno o más subsistemas, combinados con un software de control el cual se encarga de controlar la operación del mismo y de presentarlo al Sistema Operativo como un sólo gran dispositivo de almacenamiento.

A nivel general, existen dos posibilidades al implementar un sistema basado en RAID: que el mismo se realice por software, o por medio de hardware especialmente diseñado a tal efecto. Las soluciones por hardware funcionan gestionando el subsistema RAID, en forma totalmente independientemente del host, presentándole a este un solo disco. Generalmente se trata de placas especiales en donde se encuentra implementada esta funcionalidad. En las soluciones por software por el contrario, este dispositivo es emulado. Esta última opción puede ser lenta, pero no requiere de la compra de hardware adicional.

De acuerdo a sus características, varias son las designaciones de sistemas RAID. Algunas de las implementaciones más comúnmente utilizadas se encuentran dadas por los niveles RAID 0, 1 y 5. Hoy en día, algunos de los sistemas operativos más populares como por ejemplo Windows 2000/2003 Server y Linux, soportan este tipo de configuración por software.

RAID 0 (Arreglo de discos divididos sin tolerancia a fallas - No Redundante)

El RAID de nivel 0 requiere al menos 2 discos para ser implementado. En esta modalidad, se implementa un arreglo de discos divididos, la información es separada en bloques y cada bloque es grabado en una unidad de disco diferente. El desempeño de Entrada/Salida se ve muy beneficiado por la dispersación de la carga a través de muchos canales y discos.

El mejor desempeño se alcanza cuando los datos son divididos a través de múltiples controladoras con tan solo un disco por controladora. No existe sobrecarga por el cálculo de paridad. Suele referirse como un diseño muy simple de implementar. Al mismo tiempo, generalmente no suele ser realmente considerado como un RAID, ya que no es tolerante a fallas. La falla de una sola unidad resultaría en una pérdida de información en el arreglo

RAID 1 (Espejeado y Duplexing – Espejeo): El nivel de RAID 1 requiere al menos dos unidades de disco para ser implementado. Una unidad de datos y una unidad de réplica. Cuando se describen datos en una unidad, también se escriben en la otra. El disco redundante es una réplica exacta del disco de datos, por lo que se conoce también como disco espejo. Los datos pueden leerse de cualquiera de las dos unidades de forma que si se dañara la unidad de datos, es posible acceder a la unidad de réplica, permitiendo que el sistema pueda seguir funcionando. Con este nivel de RAID se obtiene la misma velocidad de lectura/ escritura que una configuración normalizada de disco, por lo que constituye la mejor opción para aplicaciones que conllevan un gran número de operaciones de escritura.

RAID 3: Conocido también como Striping con paridad dedicada. Utiliza también un disco de protección de información separado para almacenar información de control codificada con lo que se logra una forma más eficaz de proporcionar redundancia de datos. Este control de información codificada o paridad proviene de los datos almacenados en los discos y permite la reconstrucción de información

en caso de fallas. Se requieren como mínimo 3 discos y se utiliza la capacidad de un disco para la información de control. Los datos se dividen en fragmentos que se transfieren a los discos que funcionan en paralelo, lo que permite enviar más datos de una sola vez, y aumentar en forma sustancial la velocidad general de transferencia de datos. Esta última característica convierte a este nivel en idóneo para que estas aplicaciones que requieran la transferencia de grandes ficheros contiguos hacia y desde el ordenador central.

RAID 5: Se necesita un mínimo de tres unidades para implementar una solución RAID 5. Este array ofrece tolerancia al fallo, pero además, optimiza la capacidad del sistema permitiendo una utilización de hasta el 80% de la capacidad del conjunto de discos. Esto lo consigue mediante el cálculo de información de paridad y su almacenamiento alternativo por bloques en todos los discos del conjunto. La información del usuario se graba por bloques y de forma alternativa en todos ellos. De esta manera, si cualquiera de las unidades de disco falla, se puede recuperar la información en tiempo real, sobre la marcha, mediante una simple operación lógica de OR exclusivo, sin que el servidor deje de funcionar. RAID 5 es la solución más económica por megabyte, que ofrece la mejor relación de precio, rendimiento y disponibilidad para la mayoría de los servidores.

13.4.4 Políticas de backup y restore

Sin lugar a dudas, la definición de políticas y procedimientos relacionados con las operaciones de Backup y Restore de información, es el punto más importante en toda estrategia de seguridad. Cuando todo lo demás falle, el profesional en seguridad informática, deberá ser capaz de recuperar su sistema acudiendo a las copias de resguardo. Para que ésto sea posible, deberá contarse con normas claras que regulen: qué información resguardar, la frecuencia con que esta operación deberá ser llevada a cabo, las personas que serán responsables de las mismas, la periodicidad con la que se comprobará la efectividad del sistema implementado y el lugar físico donde descansarán las copias generadas.

Otra de las cuestiones que deberá definir a la hora de resguardar información, se encuentra relacionada con el software a utilizar y con la modalidad en la que la operación será llevada a cabo.

Tipos de copia de seguridad:

- **Normal o Full**: Copia todos los archivos seleccionados, restableciendo el atributo de archivo modificado a cero.
- **Intermedia o Copia**: Copia todos los archivos seleccionados, no marca los archivos como copiados, es decir, no restablece a cero el atributo de archivo modificado. Este método se utiliza cuando se quieren hacer copias de archivos entre procesos normales e incrementales sin que se invaliden los mismos (cintas de resguardo adicionales o espontáneas).
- **Diferencial**: Copia los archivos creados o modificados desde la última copia de seguridad full o **incremental**. No marca el atributo del archivo como copiado, es decir, no se restablece su valor a cero, el mismo sigue siendo uno.
- **Incremental o Progresiva**: Copia los archivos creados o modificados desde la última copia de seguridad full o incremental. Marca los archivos como copiados, es decir, cambia el atributo de archivo modificado a cero.
- **Diaria**: Copia los archivos seleccionados modificados durante el día en el que se realiza la copia de seguridad diaria. No marca al archivo como copiado.

Nota: La marca de copiado (archive) es un atributo o indicador propio de cada archivo, es un bit que los programas de backup ponen en cero cuando realizan una copia del archivo. Cuando los archivos

sufren modificaciones el sistema operativo, cambia el valor de este atributo, indicando al programa de copia de seguridad, que ha sido modificado.

Un esquema de resguardo semanal del tipo diferencial hace una copia de todos los archivos creados o modificados desde la copia full anterior, aumentando el tamaño y el tiempo necesario para realizar el resguardo a medida que pasan los días, en cambio, un esquema incremental, realiza un salvado de los archivos modificados o creados desde el día anterior, requiriendo menos tiempo y espacio en cinta. La desventaja de éste método, radica en el momento de realizar la recuperación ya que requiere la copia full y las sucesivas copias incrementales hasta el día solicitado.

13.4.5 Housing y Hosting

Tanto el Hosting como el Housing, son en principio diferentes esquemas de servicios, generalmente provistos por compañías especializadas, tendientes a brindar a terceros la posibilidad de albergar el desarrollo de sus sitios web, en instalaciones especialmente dispuestas a tal fin. Si bien el objetivo final de ambos esquemas, radica en brindarle a usted la posibilidad de desligarse en cierto modo, del mantenimiento de la infraestructura necesaria, al momento de brindar servicios web de cara a Internet, lo cierto es que las consideraciones de seguridad relacionadas deben ser evaluadas cuidadosamente.

Estas últimas, frecuentemente se encuentran relacionadas con el hecho de que toda la responsabilidad respecto de los componentes de Networking (Firewalls, IDS, Routers, etc.) utilizados al momento de brindarle el servicio, recae en el proveedor. Esto hace que de cierta forma, usted no tenga incidencia respecto de la manera en la que este tipo de componentes son configurados y administrados por el personal contratado por el proveedor de servicio, lo cual en algunas circunstancias, puede no ser recomendable.

Al margen de ello, la principal diferencia entre Housing y Hosting, radica que en el primero, el destino final de nuestro sitio, aplicación o servicio web, será un servidor independiente, mientras que en el segundo, un mismo equipo y recursos de hardware, serán utilizados para albergar diferentes sitios, correspondientes a diferentes empresas.

Esto último, hace mucho menos recomendable el esquema de Hosting respecto del Housing, especialmente en aquellos casos donde el servicio web a prestar, requiera por ejemplo, la utilización de prestaciones dependientes de bases de datos.

Debemos ser conciente, que si bien es cierto que ambos esquemas, presentan la desventaja de utilizar una infraestructura en común, aspecto que podría llegar a ser provechoso para un eventual atacante, el hecho de que varios sitios sean administrados en el mismo servidor físico, con las mismas configuraciones a nivel de hardening del sistema operativo y servicios, permitiría a un atacante, aprovecharse de algún defecto de programación encontrado en un sitio que no siendo el nuestro, se encuentra alojado en el mismo server, el cual le permitiría eventualmente comprometer el sistema operativo local y a través de él, el resto de los sitios gestionados, entre ellos el nuestro.

Alguna de las opciones al momento de contratar este tipo de servicios, pasa por: solicitar las políticas de seguridad utilizadas por el proveedor, consultar acerca del procedimiento utilizado a la hora de llevar a cabo la actualización de parches del sistema operativo y solicitar el permiso necesario a la hora de auditar en forma periódica, el sitio en forma remota.

13.5 CONTROL DE ACCESO LÓGICO

Uno de los principios básicos de la seguridad, es aquel que involucra algún tipo de método de control de acceso. Estos, definen cómo se comunicarán usuarios y sistemas y en qué forma lo harán. El principal objetivo detrás de todo control de acceso lógico, es el de proteger la información almacenada a través de operaciones informáticas. En tal sentido y en su nivel más general, tres son los modelos básicos utilizados para explicar el control de acceso como tal. A continuación mencionaremos brevemente cada uno de ellos

Uno de los principios básicos de la seguridad, es aquel que involucra algún tipo de método de control de acceso. Estos, definen cómo se comunicarán usuarios y sistemas y en qué forma lo harán. El principal objetivo detrás de todo control de acceso lógico, es el de proteger la información almacenada a través de operaciones informáticas. En tal sentido y en su nivel más general, tres son los modelos básicos utilizados para explicar el control de acceso como tal. A continuación mencionaremos brevemente cada uno de ellos:

- **DAC (Discretionary Access Control o Control de Acceso Discrecional):** En el modelo de Control de Acceso Discrecional (DAC), un usuario bien identificado (típicamente, el creador o propietario del recurso) decide cómo protegerlo estableciendo cómo compartirlo, mediante controles de acceso impuestos por el sistema. Una de las características principales en este esquema, radica en que el propietario del recurso puede cederlo a un tercero. En este modelo, se establecen ACLs (Access Control List o Listas de Control de Acceso) mediante las cuales es posible para el propietario del recurso, otorgar o revocar acceso a individuos o grupos. DAC, permite que la información sea compartida fácilmente entre los usuarios, puesto que se presenta como un modelo dinámico y natural.
- **MAC (Mandatory Access Control o Control de Acceso Mandatorio):** En el modelo de Control de Acceso Mandatorio (MAC), es el sistema quien protege los recursos. Todo recurso del sistema, y todo principal (usuario o entidad del sistema que represente a un usuario) debe poseer una etiqueta de seguridad. Esta etiqueta de seguridad sigue el modelo de clasificación de la información militar, en donde la confidencialidad de la información es lo más relevante, formando lo que se conoce como política de seguridad multinivel. Una etiqueta de seguridad se compone de una clasificación o nivel de seguridad (número en un rango, o un conjunto de clasificaciones discretas, desde DESCLASIFICADO hasta ALTO SECRETO) y una o más categorías o compartimentos de seguridad. El modelo MAC, se denomina estático, debido principalmente a que utiliza un conjunto predefinido de privilegios de acceso para los archivos del sistema. En la práctica, los administradores del sistema establecen estos parámetros y los asocian con una cuenta, archivo o recurso. En este esquema, los administradores son las únicas personas autorizadas a realizar cambios en los niveles de acceso.
- **RBAC (Role-Based Access Control o Control de Acceso Basado en Roles):** El modelo de Control de Acceso Basado en Roles (RBAC), es considerado como un intento de unificar los modelos DAC y MAC consiguiendo una arquitectura donde el sistema impone el control de acceso, pero sin las rígidas restricciones impuestas por las etiquetas de seguridad existentes en el modelo MAC. Las políticas de control de accesos, basado en roles, regulan el acceso de los usuarios a la información en términos de sus actividades y funciones de trabajo, representándose así de forma natural la estructura de las organizaciones. Debido a sus características, el modelo RBAC suele ser uno de los más implementados en algunos de los sistemas operativos más conocidos.

13.5.1 Administración de acceso de usuarios

Varias son las tareas que deben ser tenidas en cuenta a la hora de administrar el acceso de usuarios a los sistemas informáticos. Identificación de las necesidades de acceso, diseño de las normas y procedimientos a la hora de solicitar la apertura de cuentas o de realizar algún tipo de cambio en las claves otorgadas, métodos tendientes a administrar privilegios, derechos y contraseñas, y tecnologías aplicadas al control de acceso.

Respecto de este último punto, mencionaremos a continuación alguno de los métodos o tecnologías aplicadas a la identificación y el control de acceso de usuarios.

Passwords: La solicitud de un password o clave de acceso, en conjunto con el nombre de cuenta de un usuario, es el método comúnmente implementado en la mayoría de los sistemas informáticos, a fin de identificar por medio de un proceso de logon que usted es quien dice ser . Para que este

procedimiento funcione, la información ingresada por el usuario, deberá ser comparada con los datos previamente almacenados, mediante algún proceso seguro.

Sistemas OTP (One Time Passwords o Passwords de un Sólo Uso): Una de las características clave, detrás del concepto utilizado por OPT, radica en que el password del usuario, nunca se trasmite por la red, en su defecto lo que sí se trasmite es una clave de sesión previamente negociada, que es utilizada por única vez para luego ser descartada. Como parte del funcionamiento de OTP:

1. El usuario se conecta al servidor (la máquina en la que quiere abrir una sesión).
2. El servidor envía al usuario un reto ("challenge").
3. El usuario calcula la respuesta al reto (el one-time password), utilizando para ello una clave privada, y la envía de vuelta al servidor.
4. El servidor por su parte calcula también la respuesta, y la compara con la que ha recibido. Si ambas coinciden, se permite la entrada al servidor y el OTP queda invalidado para futuras entradas

Puesto que la función que se utiliza para calcular la respuesta a un desafío, es tal que resulta imposible calcular un OTP a partir de los anteriores, aunque se intercepte alguno de los OTP, éste no se podrá utilizar para entrar en la cuenta del usuario, ni tampoco para averiguar los OTPs que se utilizarán a continuación. Otro tipo de implementación de OTP, consiste en calcular previamente un número fijo de OTP. De esta forma, en lugar de calcular la respuesta al desafío, el usuario tendrá que consultar en su lista de valores conocidos y teclear el password adecuado.

SmartCards: Una SmartCard, es una tarjeta, mediante la cual es posible acceder a múltiples recursos, entre los cuales se incluyen: edificios, estacionamientos y computadoras. En este tipo de esquema, cada computadora a la que se requiera el acceso, deberá contar con un lector capaz de leer la información (Básicamente la identidad de quien la posee y los privilegios concedidos) contenida en dicha tarjeta.

Single Sign-On (SSO): Sin lugar a dudas, uno de los mayores problemas a resolver en grandes entornos de cómputo con múltiples sistemas y aplicaciones que requieren ser accedidas por un mismo usuario, es aquel que requiere memorizar y administrar diferentes combinaciones de usuario y contraseña. El propósito de la soluciones de Single Sign-On, es precisamente el de lograr que el usuario obtenga acceso a los sistemas y aplicaciones que requiera, utilizando para ello, un solo par de usuario/contraseña. Esta funcionalidad, se ha convertido en una realidad en muchos entornos operativos. Kerberos, Microsoft Active Directory y Novell eDirectory son tan solo algunos ejemplos de este tipo de implementaciones.

13.5.2 Control de acceso a la red

ISO 17799: Control de Acceso a la red. Objetivo: La protección de los servicios de red

Se debe controlar el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a los servicios de red no comprometan la seguridad de estos servicios, garantizando:

- interfaces inadecuadas entre la red de la organización y las redes de otras organizaciones, o redes públicas
- mecanismos de autenticación apropiados para usuarios y equipamiento

- control de acceso de usuarios a los servicios de información

13.5.3 Control de acceso al sistema operativo

Uno de los principales objetivos, detrás del control de acceso al sistema operativo, es el de impedir el acceso no autorizado al computador. A fin de cumplir con este objetivo, será de vital importancia conocer e implementar las facilidades propias de la plataforma administrada.

A continuación enumeraremos algunos de los puntos principales a tener en cuenta, al momento de asegurar el control de acceso al sistema operativo:

- La identificación de identidad por medio de la utilización de alguno de los métodos comentados en indicadores anteriores, debe ser requisito indispensable.
- En lo posible, se deberá restringir el acceso a usuarios, teniendo en cuenta la terminal desde la cual se conectan
- Se deberán registrar tanto los accesos exitosos como los fallidos.
- Las horas de logon, deberán ser restringidas únicamente al horario laboral
- Los tiempos de conexión deberán ser administrados.
- Deberán activarse las facilidades de auditoria necesaria, a fin de adquirir la información que fuera requerida ante un incidente de seguridad.
- Políticas claras respecto del bloqueo de terminales cada vez que un usuario deje su puesto de trabajo, deberán ser implementadas y auditadas.
- Siempre que sea posible, se deberá implementar la visualización de mensajes al ingreso del sistema, mediante los cuales se deberá advertir que sólo los usuarios autorizados pueden acceder a la computadora en cuestión.
- Las políticas de cuentas implementadas, deberán restringir los intentos de conexión a no más de 3 intentos siempre que sea posible

13.5.4 Control de acceso a las aplicaciones

Si bien es cierto que los controles sobre el acceso al sistema operativo limitarán en gran medida, la posibilidad de que usuarios ilícitos accedan a un sistema de cómputo correctamente asegurado, las diferentes aplicaciones empresariales, utilizadas a fin de acceder la información dispensada en los sistemas de información corporativos, la mayoría de las veces poseerán su propio esquema de autorización y control, posibilitando no sólo validar el acceso a la misma, sino también los privilegios que corresponden a cada uno de los perfiles en ellas configurados.

Ejemplos claros al respecto, se encuentran dados por aplicaciones de bases de datos. Muchas veces, desarrolladores implementan como parte de la distribución del software desarrollado, clientes de bases de datos como Oracle o SQL Server necesarios al momento de que las aplicaciones instaladas accedan a los datos albergados en este tipo de repositorios. En algunas circunstancias, errores en la selección de componentes a instalar, podrían provocar que el usuario designado para utilizar la aplicación desarrollada, encuentre en su menú de programas, opciones que le permitan acceder los datos en forma directa y no mediante la utilización de la aplicación desarrollada, salteando de esta forma muchos de los controles que el desarrollador se habrá esmerado en codificar

Por último, aplicaciones del tipo ERP (Enterprise Resource Planning) como por ejemplo J.D.Edwards, SAP o People Soft, suelen poseer un complejo mecanismo de administración de usuarios, grupos, permisos y derechos, el cual suele ser de suma utilidad a la hora de dispensar seguridad, en parte debido a la granularidad con la que es posible asignar dichos privilegios. Si su empresa o cliente,

posee implementaciones de este tipo, será sumamente recomendable encarar un proyecto tendiente a aprovechar las características de seguridad en ellos incorporadas.

13.5.5 Supervisión y/o control

Las tareas de supervisión, son parte fundamental de todo proceso de seguridad. Cada departamento de IT debería establecer normas claras al respecto, al igual que procedimientos tendientes a evaluar la necesidad de identificar qué supervisar y cómo hacerlo.

Como lineamiento general, la revisión periódica de logs dará al administrador de sistemas o al analista de seguridad, una visión bastante detallada de lo que ha estado sucediendo en su red, y en las aplicaciones sobre ella montadas. Tal como se menciona en el punto 9.7 de las normas ISO 17799, respecto de los objetivos del "Monitoreo del Acceso y Uso de los Sistemas":

"Los sistemas deben ser monitoreados para detectar desviaciones respecto de la política de control de accesos y registrar eventos para suministrar evidencia en caso de producirse incidentes relativos a la seguridad. El monitoreo de los sistemas permite comprobar la eficacia de los controles adoptados y verificar la conformidad con el modelo de política de acceso"

Claro está que muchas veces, la propia lectura de los eventos registrados en el conjunto de aplicaciones y sistemas administrados, conlleva tiempo y requiere en algunos casos de perfiles correctamente entrenados, a la hora de detectar posibles anomalías. Un método efectivo a fin de aliviar esta tarea, se encuentra relacionado con la implementación de sistemas de syslog centralizados y una correcta definición inicial de que eventos serán registrados. El paso posterior consistirá en configurar distinto tipos de alertas, que prevengan al oficial de seguridad responsable de la tarea, con diferentes niveles de criticidad. La implementación de este tipo de sistemas, permitirá administrar efectivamente los diversos registros existentes en un departamento de tecnología típico, informando sólo de aquellos eventos que de acuerdo a una configuración inicial, se hayan marcado como críticos.

Por último, un aspecto pocas veces tenido en cuenta y de suma utilidad al momento de realizar tareas como las mencionadas, radica en la imperiosa necesidad de mantener sincronizado los relojes de todo el equipamiento implementado en la red. Esta característica, posibilitará realizar una correlación de eventos efectiva, a la hora de seguir los pasos de un incidente detectado.

ISO 17799 Registro de eventos:

Deben generarse registros de auditoria que contengan excepciones y otros eventos relativos a seguridad, y deben mantenerse durante un período definido para acceder en futuras investigaciones y en el monitoreo de control de acceso. Los registros de auditoria también deben incluir:

- ID de usuario
- Fecha y hora de inicio y terminación
- Identidad o ubicación de la terminal
- Registros de intentos exitosos y fallidos de acceso al sistema
- Registros de intentos exitosos y fallidos de acceso a datos y otros recursos

Podría requerirse que ciertos registros de auditoria sean archivados como parte de la política de retención de registros o debido a los requerimientos de recolección de evidencia

13.6 CONTINUIDAD DEL NEGOCIO

En un momento en el que las amenazas a los sistemas informáticos de empresas e instituciones, se

suceden con mayor frecuencia de lo deseado, la continuidad del negocio se ha convertido en una de las prioridades fundamentales para empresarios y responsables de las áreas de tecnología de la información. De hecho, a pesar de las consecuencias derivadas de la contención del gasto en TI (Tecnología de la Información) por parte de las mayoría de las empresas en nuestro país, muchos son los analistas, que aseguran que el área de la seguridad informática a nivel mundial, es una de las pocas en las que se ha invertido y se seguirá invirtiendo de cara al futuro, mientras que otros segmentos como el del hardware, el cual ha sufrido fuertes caídas en el transcurso de los últimos años y el software, se mantendrán en los niveles de evolución observados en los últimos años.

A lo largo de esta sección, intentaremos revisar algunos de los motivos por el cual un plan de continuidad de negocios, es un asunto que debe ser tenido en cuenta, por cualquier organización a fin de que su negocio, pueda ser puesto en marcha en el menor lapso de tiempo posible, luego de producido un incidente de seguridad grave.

Probablemente, una de las definiciones más claras respecto de la finalidad detrás de toda implementación de un Plan de Continuidad del Negocio, se encuentre descripta en el punto 11.1 de las normas ISO 17799. Allí se define como objetivo básico de todo Plan de Continuidad del Negocio, el "Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos críticos de los negocios de los efectos de fallas significativas o desastres".

En la misma sección, se describe la necesidad de implementar un proceso de administración de la continuidad de los negocios, a fin de reducir la discontinuidad ocasionada por desastres y fallas de seguridad (que pueden ser el resultado de, por ejemplo, desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas, etc.) a niveles aceptables, a través de la combinación de una serie de controles preventivos y de recuperación previamente estipulados. Por tal motivo, planes de contingencia, deben ser desarrollados e implementados, para garantizar que los procesos de negocios puedan restablecerse dentro de los plazos por éste requeridos.

Varias acciones son necesarias al momento de llevar a la práctica, un plan de este tipo, en tal sentido, el análisis previo respecto de las consecuencias de desastres, fallas de seguridad e interrupciones del servicio probables en el entorno estudiado, es un punto fundamental.

Según un informe publicado por "PC Week", las estadísticas muestran que "el 50% de las empresas que pierden sus sistemas críticos durante más de 10 días (tras un desastre) nunca llegan a recuperarse... Es más, el 93% de las empresas que no tienen un plan de recuperación desaparecen en 5 años". Por otra parte, se calcula que, hasta el 2005, un 20 por ciento de las empresas en funcionamiento alrededor del mundo, sufrirán un incidente serio en sus sistemas de información y/o comunicaciones. Esto último, debido en parte a que con más de 600 millones de usuarios de Internet, se ha multiplicado peligrosamente la cantidad de incidentes.

Si bien es cierto que gran cantidad de empresas, ya han comenzado a trabajar proactivamente en la implementación de planes que aseguren la continuidad del negocio, aún siguen siendo pocas en porcentaje global. Según una dato de Gartner Dataquest, "*Habrá que esperar hasta el ejercicio 2007 para que al menos el 35 por ciento de las grandes empresas dispongan de una infraestructura de continuidad de negocio. Así, ajenas a las amenazas (terrorismo, virus, gusanos, Hackers, crackers...) viven la mayor parte de las empresas del mundo. Tanto es así que, en el 2002, sólo el 25 por ciento de las 2.000 firmas más importantes del mundo habían diseñado un plan de continuidad de negocio, que les salvara del desastre en caso de incidencia*"

Pero, muchas veces, la implementación de planes tendientes a asegurar la continuidad del negocio, suele iniciarse luego de que un incidente, haya demostrado ser lo suficientemente importante. Y no hay que remontarse mucho en el tiempo para observar las lamentables repercusiones de un desastre a gran escala. Además de las vidas perdidas como consecuencia de los atentados del 11 de septiembre en Nueva York, varias fueron las empresas que desaparecieron debido a la falta de backups, almacenados fuera de las Torres Gemelas y la imposibilidad de retomar sus operaciones comerciales, luego de producido el atentado.

Poco a poco, las empresas en general van tomando conciencia de la necesidad de diseñar e implementar un Plan de Continuidad del Negocio, efectivo. Nuestra tarea como analistas de seguridad, deberá ser entonces, recomendar esta práctica y lograr una implementación efectiva.

13.6.1 Proceso de administración

La realización de un Plan de Continuidad del Negocio, no es tarea sencilla. A menudo, el analista de seguridad, se encontrará con escenarios complicados en donde la realidad económica, muchas veces imperará a la hora de establecer medidas con costo asociado. Por tal motivo, a fin de promover un proyecto exitoso, los procesos involucrados, deberán formalizarse adecuadamente, a la vez que la participación activa por parte de los actores principales de la organización, deberá ser juzgado como un aspecto fundamental a la hora de organizar las tareas.

La primera parte del proceso de administración de un proyecto de Continuidad del Negocio, deberá apuntar a concienciar a la organización, respecto de los riesgos que enfrenta en su operatoria diaria. Ningún riesgo podrá ser prevenido o administrado, si se desconoce el perjuicio al que se encuentra relacionado. A tal efecto, el profesional deberá proveerse de la información necesaria, relevando no sólo los factores externos, sino también los internos, de forma tal de comunicar éstos en forma efectiva. El procedimiento habitual, suele conformarse de una presentación oral y un documento que avale el estudio realizado. Esta primer etapa, también deberá contar sin excepción, con el compromiso total por parte de la dirección de la compañía, dejando claro que no se trata de un asunto "a resolver por el departamento de Sistemas y Tecnología", sino de un proceso que eventualmente, servirá para devolver el "negocio", a los carriles normales, motivo por el cual deberá ser considerado "un proceso crítico". En síntesis, "*La administración de la continuidad de los negocios debe incluir controles destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables.*"

13.6.2 Análisis de impacto

Una vez identificado los riesgos a los que una organización se encuentra expuesta, el analista de seguridad deberá trabajar en conjunto con los diferentes sectores de la compañía, a los efectos de evaluar, definir y formalizar, el impacto económico y operativo, que cada uno de los riesgos o amenazas previamente relevadas, tendría en caso de que fuera concretada. Gran parte del éxito en la definición de un plan de Continuidad del Negocio efectivo, se encuentra relacionado con esta tarea, y muchas veces puede ser una de las más críticas, dependiendo del tamaño de la organización y de la complejidad de los procesos de negocio involucrados. Como resultado del trabajo de Análisis de Impacto, realizado en el transcurso de esta etapa, el analista de seguridad, deberá ser capaz de formalizar, los siguientes dos aspectos principales, en forma detallada:

1. Impacto de las posibles interrupciones al negocio en términos de magnitud del daño.
2. Impacto de las posibles interrupciones al negocio en términos del período de recuperación.

13.6.3 Elaboración e implementación de planes

La correcta documentación del plan de Continuidad del Negocio desarrollado, deberá ser parte integral de los objetivos del proyecto. Dicha documentación, debería referirse a todos y cada uno de los procesos necesarios, a la hora de realizar las tareas previstas al momento de responder a un desastre, el tiempo asignado a cada una de ellas y las responsabilidades de cada sector, entre otros. De acuerdo a lo mencionado en el punto 11.1.3 de las normas ISO 17799, el proceso de planificación de la continuidad de los negocios, debería considerar los siguientes puntos:

1. Identificación y acuerdo con respecto a todas las responsabilidades y procedimientos de emergencia.
2. Implementación de procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos. Se debe dedicar especial atención a la evaluación de la dependencia de negocios externos y a los contratos vigentes.

3. Documentación de los procedimientos y procesos acordados.
4. Instrucción adecuada del personal en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis.
5. Prueba y actualización de los planes.

A fin de resultar exitoso, el proceso de planificación, deberá estar centrado en aquellos objetivos de negocios, que en etapas anteriores, hubieren sido identificados como claves a los efectos de preservar la continuidad del negocio, en los plazos estipulados. A su vez, aspectos tales como: dotación de personal, recursos que no procesan información y acuerdos por reanudación de emergencia en sitios alternativos deberán formar parte integral del plan a implementar.

13.6.4 Plan de contingencia

Gran parte de las tareas previstas en un Plan de Continuidad del Negocio, se encuentran relacionadas con la correcta definición de un Plan de Contingencia. El objetivo principal del desarrollo de un plan de contingencia, es el de enumerar procedimientos concretos, a la hora de actuar frente a un incidente puntual. Como parte del desarrollo del proceso de formulación del un plan de contingencia, lo principal es cumplir todas las tareas necesarias de la fase proactiva, que es la fase anterior a la contingencia. Una vez que se produce la eventualidad, se inicia la fase reactiva y se debe ejecutar el plan correspondiente.

En términos generales, un plan de contingencia tipo, debería contener:

1. Objetivo del plan Se deben indicar aquellos componentes de la función crítica que se pretenden cubrir frente a la contingencia puntualmente considerada. Estos componentes pueden variar, así como su grado de cobertura para las distintas contingencias analizadas.
2. Criterio para la ejecución del plan Este debe indicar con el mayor grado de certeza, las condiciones bajo las cuales se considerará, que un plan de contingencia previamente definido, debe comenzar a aplicarse.
3. Tiempo esperado máximo de duración del plan Entendiendo como tal, el tiempo máximo en que se podrá continuar operando bajo condiciones de contingencia.
4. Roles, Responsabilidad y Autoridad Este punto, debe ser considerado de suma importancia a fin de asegurar la correcta puesta en marcha del plan de contingencia. Se debe determinar en forma clara, cuál es el papel de cada uno de los sectores de la organización ante la contingencia y cómo se alteran los procedimientos habituales para dar lugar a los procedimientos de contingencia. Así mismo, coordinadores en la contingencia, deberán ser designados y entrenados a tal efecto.
5. Requerimiento de recursos Qué recursos serán requeridos a la hora de operar en el modo contingencia y cuáles de los recursos habitualmente utilizados no se deberán utilizar, son aspectos que deben encontrarse debidamente documentados y verificados lo más exhaustivamente posible.

Por último, un plan de contingencia, podría ser tan sencillo como evaluar la necesidad de proveer un listado de artículos con sus precios asociados, a los vendedores de una sucursal, para que sean utilizados en caso de que el sistema central no está disponible, o tan complejo como la implementación de un centro de procesamiento alternativo, que contando con réplicas exactas del equipamiento y los datos contenidos en el sitio primario, brinde la posibilidad de continuar con las tareas de un gran centro de cómputos

13.6.5 Prueba, mantenimiento y re-evaluación

Para que un Plan de Continuidad del Negocio, sea efectivo el mismo deberá mantener su vigencia y transformarse en parte integral del resto de los procesos de administración y gestión relacionados con la organización. Un plan bien desarrollado pero desactualizado, podría causar costos innecesarios y comprometer seriamente la situación de una organización frente a un incidente. Suposiciones incorrectas, negligencias o los propios cambios en el equipamiento o el personal involucrado, podría ser motivo de fallas en un proceso previamente estipulado, por tal motivo, la evaluación continua y la definición de procesos de pruebas efectivas, en relación de los procedimientos descritos en el plan, deben ser considerados prácticas esenciales. Un cronograma de pruebas para los planes de continuidad del negocio deberá ser parte integral del proceso. El mismo deberá indicar claramente, cómo y cuándo debe probarse cada elemento dispuesto en el plan. En el punto 11.1.5 de las normas ISO 17799, se recomienda en forma explícita, probar con frecuencia cada uno de los componentes del plan y utilizar diversas técnicas para garantizar que los planes funcionarán en la vida real, en el momento que sea necesario. Entre los tipos contemplados por dicha norma se encuentran:

1. Pruebas de discusión de diversos escenarios (discutiendo medidas para la recuperación del negocio utilizando ejemplo de interrupciones).
2. Simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis).
3. Pruebas de recuperación técnica (garantizando que los sistemas de información puedan ser restablecidos con eficacia).
4. Pruebas de recuperación en un sitio alternativo (ejecutando procesos de negocio en paralelo, con operaciones de recuperación fuera del sitio principal).
5. Pruebas de instalaciones y servicios de proveedores (garantizando que los productos y servicios de proveedores externos cumplan con el compromiso contraído).
6. Ensayos completos (probando que la organización, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones).

13.7 EL ESTÁNDAR TIA-942

En temas anteriores mencionamos estos dos aspectos y analizamos al fuego como un factor de riesgo crítico porque conspira contra la disponibilidad al atacar la infraestructura soporte, pero a su vez la propia infraestructura debe funcionar 7x24. Trasladada esta propiedad al campo de acción del datacenter, se debe considerar a este como la interrelación de una serie de subsistemas de infraestructura que dan respaldo al equipamiento crítico (hardware), para mantener una disponibilidad de sistemas adecuada para las características propias del negocio en que nos encontremos. Hay que tener en cuenta que no todas las actividades requieren el mismo nivel de disponibilidad y esto surgirá de un análisis previo llamado BIA (Business Impact Análisis) que cuantifica económicamente el impacto que produce una parada del datacenter en el negocio de la organización. En líneas generales podemos establecer a priori una clasificación aproximada de la criticidad de los sistemas para distintas áreas de actividad.

13.7.1 La infraestructura y el estándar TIA-942

En abril de 2005, la *Telecomunication Industry Association* publica su estándar TIA-942 con la intención de unificar criterios en el diseño de áreas de tecnología y comunicaciones. Este estándar que en sus orígenes se basa en una serie de especificaciones para comunicaciones y cableado estructurado, avanza sobre los subsistemas de infraestructura generando los lineamientos que se deben seguir para clasificar estos subsistemas en función de los distintos grados de disponibilidad que

se pretende alcanzar. En su anexo G (informativo) y basado en recomendaciones del Uptime Institute, establece cuatro niveles (tiers) en función de la redundancia necesaria para alcanzar niveles de disponibilidad de hasta el 99.995%.

A su vez divide la infraestructura soporte de un datacenter en cuatro subsistemas a saber:

- Telecomunicaciones
- Arquitectura
- Sistema eléctrico
- Sistema Mecánico

Dentro de cada subsistema el estándar desarrolla una serie de ítem como los de la tabla:

Telecomunicaciones	Arquitectura	Eléctrica	Mecánica
Cableado de racks	Cableado de racks	Cantidad de accesos	Sistemas de climatización
Accesos redundantes	Accesos redundantes	Puntos únicos de falla	Presión positiva
Presión positiva	Presión positiva	Cargas críticas	Cañerías y drenajes
Área de distribución	Requerimientos NFPA 75	Redundancia de UPS	Chillers
Backbone	Barrera de vapor	Topología de UPS	CRAC´s y condensadores
Cableado horizontal	Techos y pisos	PDU's	Control de HVAC
Elementos activos redundantes	Área de oficinas	Puesta a tierra	Detección de incendio
Alimentación redundante	NOC	EPO (Emergency Power Off)	Sprinklers
Patch panels	Sala de UPS y baterías	Baterías	Extinción por agente limpio (NFPA 2001)

Telecomunicaciones	Arquitectura	Eléctrica	Mecánica
Patch cords	Sala de generador	Monitoreo	Detección por aspiración (ASD)
Documentación	Control de acceso	Generadores	Detección de líquidos
	CCTV	Transfer switch	

Uno de los mayores puntos de confusión en el campo del uptime (tiempo disponible de los sistemas) es la definición de datacenter confiable; ya que lo que es aceptable para una persona o compañía no lo es para otra. Empresas competitivas con infraestructuras de datacenter completamente diferentes proclaman poseer alta disponibilidad; esto puede ser cierto y dependerá de la interpretación subjetiva de disponibilidad que se realice para el tipo de negocio en que se encuentre una compañía. Lo cierto es que para aumentar la redundancia y los niveles de confiabilidad, los puntos únicos de falla deben ser eliminados tanto en el datacenter como en la infraestructura que le da soporte. Los cuatro niveles de tiers que plantea el estándar se corresponden con cuatro niveles de disponibilidad, teniendo que a mayor número de tier mayor disponibilidad, lo que implica también mayores costos constructivos. Esta clasificación es aplicable en forma independiente a cada subsistema de la infraestructura (telecomunicaciones, arquitectura, eléctrica y mecánica). Hay que tener en cuenta que la clasificación global del datacenter será igual a la de aquel subsistema que tenga el menor número de tier. Esto significa que si un datacenter tiene todos los subsistemas tier IV excepto el eléctrico que es tier III, la clasificación global será tier III.

Es importante tener en cuenta esto porque cuando se pretende la adecuación de datacenters actuales a tier IV, en lugares como América Latina, hay limitaciones físicas difíciles de salvar en los emplazamientos edilicios actuales. Prácticamente para lograr un datacenter tier IV hay que diseñarlos de cero con el estándar en mente como guía. Un ejemplo claro de esto es que es muy difícil lograr la provisión de energía de dos subestaciones independientes o poder lograr las alturas que requiere el estándar en los edificios existentes (3 m mínimo sobre piso elevado y no menor de 60 cm entre el techo y el equipo más alto).

La norma describe, resumidamente, los distintos tiers de la manera que sigue:

- ***Tier I:*** datacenter básico Un datacenter tier I puede se susceptible a interrupciones tanto planeadas como no planeadas. Cuenta con sistemas de aire acondicionado y distribución de energía; pero puede o no tener piso técnico, UPS o generador eléctrico; si los posee pueden no tener redundancia y existir varios puntos únicos de falla. La carga máxima de los sistemas en situaciones críticas es del 100%. La infraestructura del datacenter deberá estar fuera de servicio al menos una vez al año por razones de mantenimiento y/o reparaciones. Situaciones de urgencia pueden motivar paradas más frecuentes y errores de operación o fallas en los componentes de su infraestructura causarán la detención del datacenter. La tasa de disponibilidad máxima del datacenter es 99.671% del tiempo.
- ***Tier II:*** componentes redundantes Los datacenters con componentes redundantes son ligeramente menos susceptibles a interrupciones, tanto planeadas como las no planeadas. Estos datacenters cuentan con piso falso, UPS y generadores eléctricos, pero están conectados a una sola línea de distribución eléctrica. Su diseño es “lo necesario mas uno” (N+1), lo que significa que existe al menos un duplicado de cada componente de la infraestructura. La carga máxima de los sistemas en situaciones críticas es del 100%. El mantenimiento en la línea de distribución eléctrica o en otros componentes de la infraestructura pueden causar una interrupción del procesamiento. La tasa de disponibilidad máxima del datacenter es 99.749% del tiempo.
- ***Tier III:*** mantenimiento concurrente Las capacidades de un datacenter de este tipo le permiten realizar cualquier actividad planeada sobre cualquier componente de la infraestructura sin interrupciones en la operación. Actividades planeadas incluyen mantenimiento preventivo y programado, reparaciones o reemplazo de componentes, agregar o eliminar elementos y

realizar pruebas de componentes o sistemas, entre otros. Para infraestructuras que utilizan sistemas de enfriamiento por agua significa doble conjunto de tuberías. Debe existir suficiente capacidad y doble línea de distribución de los componentes, de forma tal que sea posible realizar mantenimiento o pruebas en una línea, mientras que la otra atiende la totalidad de la carga. En este tier, actividades no planeadas como errores de operación o fallas espontáneas en la infraestructura pueden todavía causar una interrupción del datacenter. La carga máxima en los sistemas en situaciones críticas es de 90%. Muchos datacenters tier III son diseñados para poder actualizarse a tier IV, cuando los requerimientos del negocio justifiquen el costo. La tasa de disponibilidad máxima del datacenter es 99.982% del tiempo.

- ***Tier IV:*** tolerante a fallas Este datacenter provee capacidad para realizar cualquier actividad planeada sin interrupciones en las cargas críticas, pero además la funcionalidad tolerante a fallas le permite a la infraestructura continuar operando aun ante un evento crítico no planeado. Esto requiere dos líneas de distribución simultáneamente activas, típicamente en una configuración system + system; eléctricamente esto significa dos sistemas de UPS independientes, cada sistema con un nivel de redundancia N+1. La carga máxima de los sistemas en situaciones críticas es de 90% y persiste un nivel de exposición a fallas, por el inicio una alarma de incendio o porque una persona inicie un procedimiento de apagado de emergencia o Emergency Power Off (EPO), los cuales deben existir para cumplir con los códigos de seguridad contra incendios o eléctricos. La tasa de disponibilidad máxima del datacenter es 99.995% del tiempo.

Para poner en perspectiva la tasa de disponibilidad que se pretende para los distintos tiers, el cuadro 2 expresa su significado expresado en el tiempo de parada anual del datacenter. Estos porcentajes deben considerarse como el promedio de cinco años. Hay que tener en cuenta que para un tier IV se contempla que la única parada que se produce es por la activación de un EPO y esto sólo sucede una vez cada cinco años. No obstante para la exigencia que demanda un tier IV algunas empresas u organizaciones manifiestan necesitar una disponibilidad de “cinco nueves”, esto significa un 99,999% de disponibilidad. Esto es poco más de cinco minutos anuales sin sistemas. El propósito del estándar TIA 942 es proveer una serie de recomendaciones y guidelines para el diseño e instalación de un datacenter. La intención es que sea utilizado por los diseñadores que necesitan un conocimiento acabado del facility planning, el sistema de cableado y el diseño de redes. El estándar TIA 942 y la categorización de tiers se encuentran en pleno auge en América Latina. Esto es bueno porque lleva al replanteo de las necesidades de infraestructura de una manera racional y alineada con las necesidades propias de disponibilidad del negocio en que se encuentran las organizaciones.

13.8 ESTÁNDAR NFPA 75

Debido a que la protección contra incendios es una parte integral de la continuidad del negocio, la NFPA desarrolló la NFPA 75, Protección de equipos electrónicos procesadores de datos por computadora , que presenta un enfoque lógico de la protección contra incendios y la continuidad del negocio basado en el riesgo. Desde el punto de vista del negocio, el factor de riesgo más importante usualmente es el perjuicio económico ocasionado por la pérdida de equipos o registros. Aquí es donde muchos gerentes de negocios centran su atención. En lugar de comenzar por el devastador punto final de la interrupción del negocio, mitigación, control de daños, recuperación del desastre, y reanudación del negocio; comencemos por el principio. Asumamos que existen factores de riesgo que lo han llevado a utilizar la NFPA 75 y veamos qué tiene esta norma para usted.

El enfoque lógico es en primer lugar prevenir incendios, lo que simplemente implica eliminar todas las fuentes de ignición y reducir la cantidad de materiales combustibles en la sala. En el improbable caso de que un incendio se propague desde otra área a una sala de TI, minimizar los combustibles tanto de papel como electrónicos, le dará al incendio menos materiales de los cuales alimentarse. El área por debajo de pisos elevados puede ser la pesadilla de las tareas domésticas. No sólo se acumula la basura y otros combustibles debajo de él, sino que también a veces allí se almacenan cosas. Una

inspección periódica del área, conducida por alguien cuya prioridad sea la protección contra incendios, puede eliminar muchos innecesarios combustibles potenciales. Las áreas de subsuelo también suelen contener cables. Los que no estén actualmente en uso pero que serán utilizados en el futuro deben ser etiquetados e identificados como tales. Todos los otros cables abandonados deberían ser removidos siempre que fuera posible. Esto es necesario por varias razones. Una gran cantidad de cables no utilizados puede interferir con el flujo de aire destinado a mantener la temperatura de la computadora dentro del margen de funcionamiento. En el caso de un incendio, el aislamiento del cable puede generar humo corrosivo. Y si existe una gran cantidad de cables enmarañados, el incendio podría llegar a estar arraigado en lo profundo, haciéndolo más desafiante para combatir que un incendio de superficie. Los cables excedentes pueden también obstruir los patrones de descarga de los sistemas de extinción de incendios. Cuando se remueven los cables, cualquier infiltración debe ser prevenida con un 'cortafuegos' a través de construcciones de clasificación ignífuga. Dado que remover cables abandonados puede dañar otros cables, su remoción debe ser planeada cuidadosamente.

Dado que la historia nos dice que la mayoría de los incendios comienzan fuera del área de la TI, se colocan barreras en forma de construcción con clasificación ignífuga de una hora de resistencia para impedir que las llamas se propaguen a tales áreas.

Básicamente, la sala del equipo de TI está rodeada por una construcción de clasificación ignífuga de una hora de resistencia, y cualquier filtración a través de estas paredes de clasificación ignífuga debe ser rellenada con materiales cortafuegos. Las salas que rodean la sala del equipo de TI, que contienen equipos de ventilación, almacenamiento de medios de cinta, y oficinas de soporte, con frecuencia son importantes para la actividad de TI, entonces ellos, también, deberían tener una mínima construcción de clasificación ignífuga de una hora de resistencia todo alrededor. Se recomienda la construcción con clasificación de dos horas.

Las salas mecánicas y eléctricas, que con frecuencia son extremadamente importantes para la operación continuada de las sala de informática, también deberían tener una construcción de clasificación ignífuga de una hora de resistencia. Además, los conductos de ventilación deben estar equipados con reguladores de tiro activados mediante detectores de humo. Cualquier conducto que preste servicio a otras partes del edificio o que pase a través del área de TI debe tener reguladores de tiro de humo e incendio automáticos.

Es interesante observar la lógica de los sistemas de protección contra incendios para los espacios de TI. Regla número uno: si el edificio esta completamente protegido por rociadores, el área de TI también debe tener un sistema de rociadores automáticos. ¿Por qué? Si el área instalada sin rociadores resultara ser el punto del origen del incendio, el mismo podría terminar devastando el sistema de rociadores del edificio. Con frecuencia, se le teme al agua en los espacios de TI. Sin embargo, este temor usualmente es infundado. Otro temor es que la tubería del rociador pueda gotear. Normalmente, las tuberías de los rociadores no comienzan de repente a gotear a menos que estén físicamente dañadas, como podría ser en un depósito. La posibilidad de daño de impacto a la tubería de los rociadores en una sala de informática es remota.

Los registros siempre son un punto de discusión cuando se refiere a las áreas de TI. Aquí hay unas pocas reglas básicas. Los registros en la sala de TI se deben mantener en el mínimo absoluto y deberían ser sólo aquellos necesarios para la operación esencial. Todos los registros importantes se deben duplicar y almacenar en una ubicación remota de modo de no estar expuestos al mismo incendio que los originales. Los registros se deben almacenar en gabinetes metálicos cerrados. Los sistemas automatizados de almacenamiento de información (AISS por sus siglas en inglés) son permitidos en las salas de TI sólo si un sistema dedicado de rociadores o sistema de agente gaseoso está instalado en cada unidad. Las salas de bibliotecas de cintas y de almacenamiento de medios deben estar fuera de la sala de TI, estar protegidas con un sistema de extinción de incendios, y tener al menos una construcción de clasificación ignífuga de una hora de resistencia. No debería haber nada más en estas salas, y no se deberían permitir actividades sino aquellas relacionadas al almacenamiento.

La construcción de clasificación ignífuga alrededor de la sala de TI y de toda el área de TI debería extenderse desde el piso estructural hasta el piso/cielorraso estructural de arriba. Esto con frecuencia

se lo conoce como construcción “losa a losa”. Esto sirve a dos propósitos. El primero debería ser obvio: usted no quiere que el humo o las llamas fuera del área se traslade dentro del área de TI. El segundo entra en juego cuando se emplea un sistema de agente gaseoso. Uno de los componentes más críticos del sistema de inundación total de agente limpio es “el gabinete” que contiene la concentración del agente extintor suficiente tiempo para extinguir el incendio y prevenir la re-ignición. Las paredes de la sala de TI deben ser lo bastante herméticas como para contener la concentración del agente extintor por este período de tiempo. Los instaladores de sistemas extintores de incendios saben bien esto, pero tienen poco o ningún control sobre la construcción de la sala, y el problema de “filtración” no se descubre hasta que la prueba de presurización de la sala es efectuada durante la puesta en servicio del sistema extintor de incendios. Prestar atención a este detalle durante la construcción ayuda a evitar dolores de cabeza y demoras de ocupación más tarde.

Cada operación de TI debe contar con tres planes: plan de emergencia de incendios, plan de control de daños, y plan de procedimientos de recuperación. El más ignorado de estos planes es, con frecuencia, el plan de procedimientos de recuperación, el cual delinea las tareas que el personal debe emprender, incluyendo transporte y comunicación críticos para la continuidad de las operaciones del negocio. Al desarrollar un plan de recuperación, el objetivo es regresar la operación del negocio al nivel en que estaba el día antes de la catástrofe. Si su negocio es tomar pedidos por medio de una línea telefónica gratuita y continúa con la entrega de productos, el esfuerzo de recuperación debería estar dirigido hacia el restablecimiento de la operación telefónica y la conexión del personal a los sistemas de procesamiento informático y telefónico, lo cual permitirá que continúen los envíos. El plan final incluiría una instalación redundante en un sitio remoto que tenga acceso a los datos de las copias de seguridad. Si la operación no es tan crítica o la instalación redundante ha sido considerada poco realista por razones económicas, es imprescindible un buen plan de recuperación en sitio. Una vez que ha ocurrido un incendio o algún evento catastrófico, el lugar no necesita ser desalojado. Si la instalación incorpora las características de diseño delineadas en la NFPA 75 y tiene planes efectivos de control de daños e incendio, el plan de recuperación es el que hay que implementar.

Al desarrollar un plan de recuperación, deben producirse discusiones sobre los daños ocasionados por el agua, humo y calor. El daño por el calor es con frecuencia la razón por la que los artículos expuestos son irrecuperables. Los daños por agua y humo usualmente son menos severos, pero con frecuencia son los que más se malinterpretan. El humo de una sala de informática usualmente contiene cloruro y azufre que corroe el delicado equipo electrónico. Siempre es necesario remover cualquier remanente de estos contaminantes. El humo puede ocasionar pequeños daños inmediatos, pero cuando se los deja desatendidos por un período prolongado, los derivados corrosivos de la combustión actúan con la humedad en el aire para comenzar el proceso de corrosión.

Toda compañía que tenga una instalación TI deberá desarrollar un plan o enfrentar las consecuencias el día del desastre. No hacer nada podría ser la peor alternativa.

CAPÍTULO 14

14.1 AUDITORIA DE SISTEMAS DE INFORMACIÓN

Enuncie, en términos generales, la misión de auditoria. Consiste en las actividades de relevar e informar a la Dirección de la organización, sobre el diseño y funcionamiento de los controles implementados y sobre la fiabilidad de la información suministrada, a fin de que por medio de cursos de acción alternativos, sea factible lograr una utilización más eficiente y segura de esta información, la que servirá como base para una adecuada toma de decisiones.

¿Qué se entiende por auditoria interna? Es aquella que se realiza con recursos materiales y humanos pertenecientes a la organización auditada. Ésta es creada por expresa por expresa decisión de la empresa, con sus recursos internos, pudiendo eventualmente ser disuelta en cualquier momento.

¿Qué comprende el control preventivo? Dentro de esta categoría, se encuentran todos aquellos controles que apuntan a evitar un evento o incidente, descartando problemas antes que los mismo aparezcan.

¿Qué significa la característica de "independencia" del auditor? Consiste en la libertad profesional que caracteriza al auditor, para que éste pueda expresar su opinión libre de todo tipo de presiones, como ser: políticas, religiosas, familiares, intereses de grupo, etc.

¿En qué consiste la técnica de muestreo? El muestreo, cualquiera que sea su forma, consiste en la aplicación de una serie de pruebas a una muestra suficientemente representativa de la población total.

En su nivel más general, solemos referirnos a la Auditoria de los Sistemas de Información, como el proceso por el cual, se recolecta y evalúan evidencias, a fin de establecer si los activos relacionados con la información, se encuentran protegidos y sus controles funcionando. Así mismo, generalmente el auditor es responsable no sólo de revisar, sino también de informar a la Dirección de la Organización, sobre el diseño y funcionamiento de los controles implantados y sobre la fiabilidad de la información suministrada. Los procesos evaluados por medio de la práctica de la "Auditoria", involucran no sólo procedimientos automáticos o de procesamiento electrónico, sino también los procedimientos no-automáticos relacionados con ellos y las interfaces intervinientes, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones. Debido a las características propias de esta actividad, la Auditoria de Sistemas de Información, engloba aspectos técnicos, legales, normativos y por sobre todo un fuerte componente de ética personal y profesional, sin la cual ninguno de los componentes anteriormente citados tendría sentido.

Proceso de auditoria:

- Recolectar evidencia
- Evaluar evidencia
- Verificar controles
- Informar a la Dirección

Aspectos relacionados con la auditoria de sistemas de información:

- Aspectos técnicos
- Aspectos normativos
- Ética profesional
- Aspectos legales
- Ética personal

14.1.1 Misión de auditoria

Resumiendo en un sólo concepto, lo comentado en el indicador anterior, la misión de auditoria, suele encontrarse relacionada principalmente, con la tarea de relevar e informar a la Dirección de la Organización, sobre el diseño y funcionamiento de los controles implantados y sobre la fiabilidad de la información suministrada, a fin de que por medio del señalamiento de cursos alternativos sea factible lograr una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones. Desde otro punto de vista, la Auditoria Informática, analiza la función informática que engloba, el análisis de la organización, seguridad, segregación de funciones y gestión de las actividades de proceso de datos. En el plano práctico, es posible identificar al menos tres grupos de funciones principales a realizar por un auditor informático:

- Participar en las revisiones antes, durante y después del diseño, realización, implantación y explotación de aplicaciones informáticas, así como en las fases análogas de realización de cambios importantes en circuitos y sistemas.
- Revisar y juzgar los controles implantados en los circuitos y sistemas informáticos para verificar su adecuación a las órdenes e instrucciones de la Dirección, requisitos legales, protección de confidencialidad y cobertura ante errores y fraudes.
- Revisar y juzgar el nivel de eficacia, utilidad, fiabilidad y seguridad de los equipos, sistemas, e información utilizada en la organización.

La auditoria se caracteriza por:

- Ser independiente
- No tener carácter ejecutivo, es decir, no genera acciones inmediatas
- No son vinculantes sus conclusiones
- Decidida por la Dirección
- Ser un elemento consultivo
- Análisis, verificación, exposición de debilidades y disfunciones

14.1.2 Necesidad de auditar

Desde hace ya algunos años, gran parte de las organizaciones han comprendido, lo crítico que resulta la administración efectiva de la información y su tecnología asociada, a la hora de llevar adelante un negocio exitoso, capaz de sobrevivir a los embates de la economía global. Este hecho, ha motivado que hoy en día la dependencia de las tecnologías de la información, por parte de las empresas, haya crecido en forma exponencial.Los Sistemas de Información actuales, suelen estar orientados a la reducción de los costos asociados a los procesos y a la generación de nuevas oportunidades de negocio. La necesidad de que los mismos, brinden información fidedigna, creíble y oportuna es un requisito fundamental, a fin de que los ejecutivos puedan tomar decisiones acertadas acerca de las condiciones de negocio Por otra parte, tal como se menciona en el CobiT (Objetivos de Control para la Información y Tecnologías afines), “Muchas organizaciones reconocen los beneficios potenciales que

la tecnología puede proporcionar. Las organizaciones exitosas, sin embargo, también comprenden y administran los riesgos asociados con la implementación de nueva tecnología". Con este concepto en mente, es fundamental para toda organización interesada en proteger uno de sus activos más importantes: La Información, reconocer los riesgos y limitantes de las tecnologías afines, de forma tal que pueda proporcionarse una dirección efectiva y controles adecuados, a la hora de velar por su seguridad.

Puesto que la Auditoria de los Sistemas de Información, propone normas, métodos y procedimientos de relevamiento y control, tendientes a asegurar el correcto funcionamiento de las tecnologías y procesos relacionados con la gestión de la información en la organización, debe ser considerada una actividad necesaria e imprescindible, sobre todo, en aquellos casos donde deba asegurarse la utilización eficiente y segura de la información que, en definitiva, formará parte de su inteligencia y de su potencial utilización a favor del negocio.

14.1.3 Política de seguridad y auditoria

En el módulo anterior, tuvimos oportunidad de mencionar la importancia que tenía para una organización, el contar con una adecuada Política de Seguridad, que regulase en forma clara y precisa, todos y cada uno de los aspectos relacionados con la seguridad de la información. Los controles de auditoria, no escapan a dicha afirmación y por ende, deben ser documentados y previstos con anterioridad.

Cuando se encuentra bien definida, una adecuada política de seguridad, representa un excelente punto de partida para el auditor de Sistemas de Información, puesto que, en principio, su trabajo consistirá en corroborar por medio de una serie de evaluaciones previamente estipuladas, si las normas y procedimientos definidos en ella oportunamente, se encuentran operativos y siguen siendo puntos de control válidos. Así mismo, la existencia de una política de auditoria en la organización, suele ser un instrumento fundamental, no sólo para el auditor encargado de llevar a cabo la misma, sino también para la organización auditada, quien debería trabajar en pro de satisfacer los objetivos de la auditoria, puesto que, idealmente, éstos deberán ser consistentes con los propios objetivos de negocio de la organización. Las normas ISO 17799, en su sección "Controles de auditoria de sistemas", menciona que "*Los requerimientos y actividades de auditoria que involucran verificaciones de los sistemas operacionales deben ser cuidadosamente planificados y acordados a fin de minimizar el riesgo de discontinuidad de los procesos de negocio*". Al mismo tiempo enuncia una serie de puntos a ser contemplados al momento de llevar a cabo esta tarea.

ISO 17799 Controles de auditoria de sistemas

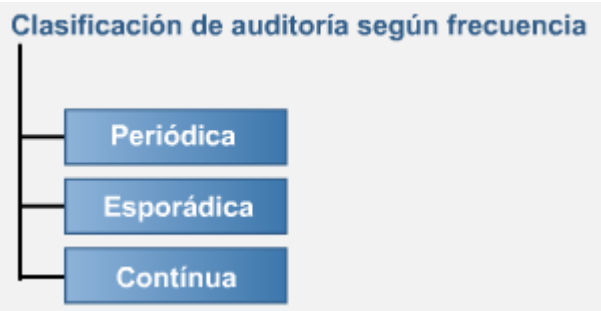
Las actividades y requerimientos de auditoría que involucran chequeos de los sistemas operacionales debieran ser planeados y acordados cuidadosamente para minimizar el riesgo de interrupciones en los procesos comerciales.

Se deberían observar los siguientes puntos:

- se debieran acordar los requerimientos de auditoría con la gerencia apropiada;
- se debiera acordar y controlar el alcance de los chequeos;
- los chequeos debieran limitarse a un acceso sólo-de-lectura al software y data;
- sólo se debiera permitir un acceso diferente al sólo-de-lectura para copias aisladas de los archivos del
- sistema, los cuales se pueden borrar cuando termina la auditoría,
- o se les puede dar la protección apropiada si existe la obligación de mantener dichos archivos en concordancia con los requerimientos de la documentación de auditoría;

14.1.4 La auditoría continúa

Si bien es cierto que de acuerdo a la frecuencia con la que se practique una auditoría, ésta puede ser referida como Periódica, Esporádica o Continua, en función de como se haya definido oportunamente su práctica en relación a los objetivos planteados como resultado de la misma; la última de estas opciones suele ser aquella que con mayor frecuencia, suele ser la escogida, cuando de auditar un Sistema de Información se trata.



Y esto no es casualidad, los Sistemas de Información, suelen poseer características dinámicas que hacen que los cambios se encuentren a la orden del día, propiciando muchas veces, que controles previamente especificados, dejen de ser válidos, de la misma forma en que circuitos administrativos oportunamente definidos carezcan de sentido al cambiar su aspecto práctico, debido muchas veces al componente humano actuante en la organización.

Pero no sólo las auditorías de un “gran” Sistema de Información se ven relacionadas con los cambios frecuentes. Aplicando este mismo concepto a la auditoría puntual de un sistema de cómputo, por ejemplo en instancias de un “Test de Penetración”, nos encontramos con una situación similar, debido a lo cual, como resultado del test realizado, podremos ofrecer al propietario del sistema, una fotografía de cómo se encuentra su sistema al momento de realizado el test, aunque dicha fotografía puede no ser importante, si al día siguiente se cambia la configuración del sistema previamente auditado, ya sea accidental o intencionalmente. Respecto a esto último, proyectos como el OSSTMM (Open Source Security Testing Methodology Manual) de ISECOM (Institute for Security and Open Methodologies), plantean el testeo metodológico y en forma continua al momento de ejecutar el análisis de seguridad de un sistema objetivo, practicando más de una “instantánea” en diferentes momentos.

En resumen, la auditoría continua, brindará a usted los elementos necesarios como para mantener sus controles al corriente, evitando que cambios imprevistos en los Sistemas de Información o en sus controles asociados, repercutan en forma negativa respecto del negocio y su esquema de Tecnología de la Información.

14.1.5 Auditoría interna versus auditoría externa

En indicadores anteriores, hemos catalogado a la auditoría de acuerdo a su frecuencia (Periódica, Esporádica o Continua). Pero ésta no es la única categorización válida. El término de auditoría, suele ser frecuentemente utilizado refiriendo junto a él, su ámbito de aplicación, el cual se encuentra, íntimamente relacionado con sus objetivos. Desde este punto de vista, las Auditorias de Gestión, Organizativas y Financieras, suelen abocarse a escenarios puntuales, de la misma forma en que lo hace la Auditoría Informática, tema tratado en esta unidad. A su vez, cualquiera sea el tipo de auditoría, ésta puede ser ejercitable tanto por personas pertenecientes a la empresa como independientes de ella, permitiendo de esta forma clasificarlas como interna o externa dependiendo de quien la realice

A continuación, mencionaremos algunas de las principales características, de cada una de éstas:

- **Auditoría Interna:** Generalmente, solemos referirnos con el término de "Auditoría Interna", a aquella que se realiza con recursos materiales y humanos pertenecientes a la empresa u organización auditada. Una de sus características principales, radica en que por lo general, ésta es creada por expresa decisión de la empresa con sus recursos internos, y puede eventualmente, ser disuelta en cualquier momento.
- **Auditoría Externa:** Ésta es realizada por personas ajenas a la empresa u organización auditada. Por lo general, suele obtenerse un mayor grado de objetividad, debido a la distancia entre auditados y auditores. Habitualmente es contratada como un servicio. Dicha contratación, puede o no ser requisito o exigencia, respecto de las leyes, normas o reglas del mercado en el que se encuentre la organización contratante.

Principales objetivos de la auditoria interna:

- Revisiones continuas, estipuladas como parte de un plan estratégico
- Determinación de la utilidad de los procedimientos, así como su nivel de cumplimento
- Custodia y contabilización de los activos (Hardware, Software)
- Control de la divulgación de los procedimientos, desde el nivel estratégico hacia el nivel operativo
- Verificación de la información recibida por la dirección

Principales objetivos de la auditoria externa

- Auditar área específicas que la auditoria interna no puede abarcar
- Medición de la magnitud de un error ya conocido, detección de errores supuestos o confirmación de la ausencia de errores
- Propuesta de sugerencias, en tono constructivo para ayudar a la dirección
- Contrastar los informes elaborados por la auditoría interna
- Control de las actividades de investigación y desarrollo donde participen agentes externos de la empresa
- Obtener una visión externa de la empresa por un organismo ajeno a la misma
- Cumplir con un requerimiento de norma, procedimiento, ley o política relacionada con el negocio

14.2 RIESGO Y CONTROL

Cualquiera sea el tamaño de una organización, con frecuencia ésta deberá enfrentar, diversos tipos de riesgos, sean los mismos de origen interno o externo. Teniendo este punto en claro, la evaluación, administración y control de dicho riesgo, deberá ser considerada parte integral de todo planeamiento de auditoría.

Cuando hablamos de Evaluación del Riesgo, solemos referirnos al proceso de identificación y análisis de los riesgos y vulnerabilidades a los cuales se encuentran sometidos los sistemas de información en particular, y todo recurso informático en general.

Algunos autores, afirman que La Administración de Riesgos es una “aproximación científica” al comportamiento del riesgo, anticipando posibles pérdidas accidentales, por medio del diseño e implementación de procedimientos y controles, que minimicen la ocurrencia de incidentes, o el impacto financiero que los mismos pudieran generar. Una correcta Evaluación del Riesgo, sentará las bases necesarias, a la hora de trabajar en la posterior gestión o administración de los mismos.

Las Actividades de Control por su parte, deben estar integradas en el proceso de Evaluación del Riesgo. Una vez que estos fueran analizados, deberán establecerse los métodos y procedimientos de control necesarios, los cuales a su vez deberán ser cumplidos correcta y oportunamente. Las Actividades de Control establecidas, permitirán entonces, garantizar que las medidas necesarias para hacer frente a los riesgos que amenazan la consecución de los objetivos de negocio, dispuestos por la dirección de la organización, han sido adoptadas. Al mismo tiempo, los hitos de control establecidos, cerrarán el círculo previamente establecido, al ser factibles de ser revisados mediante prácticas de auditoría.

Características:

- Análisis de riesgos
- Reflejar los cambios en los requerimientos y prioridades de la empresa
- Implementación de controles
- Considerar nuevas amenazas y vulnerabilidades
- Comprobar si los controles son efectivos

14.2.1 Elementos del riesgo

A lo largo del tiempo, varios estudios se han publicado respecto de la forma correcta en que los Elementos del Riesgo deben ser definidos. Si bien es factible encontrar diferencias en dichos trabajos de campo, todos ellos coinciden en que el riesgo suele encontrarse relacionado básicamente, con la amenaza a los procesos y activos; lo cual incluye tanto los activos físicos como los de información, y las debilidades o vulnerabilidades en ellos encontradas. Al mismo tiempo, el riesgo se establece teniendo en cuenta la probabilidad de que una amenaza se concrete, de hecho, cuando hablamos de riesgo, en rigor de verdad nos estamos refiriendo precisamente, a la combinación entre la probabilidad de que una amenaza se concrete, y la frecuencia u ocurrencia con ella relacionada.

14.2.2 Proceso de evaluación de riesgos

Debido a la naturaleza dinámica de los factores intervinientes en los sistemas de información, la evaluación de riesgos no debe ser nunca considerada, como una tarea a cumplir de una vez para siempre. Por el contrario, debe ser un proceso continuo, una actividad básica de la organización, tal

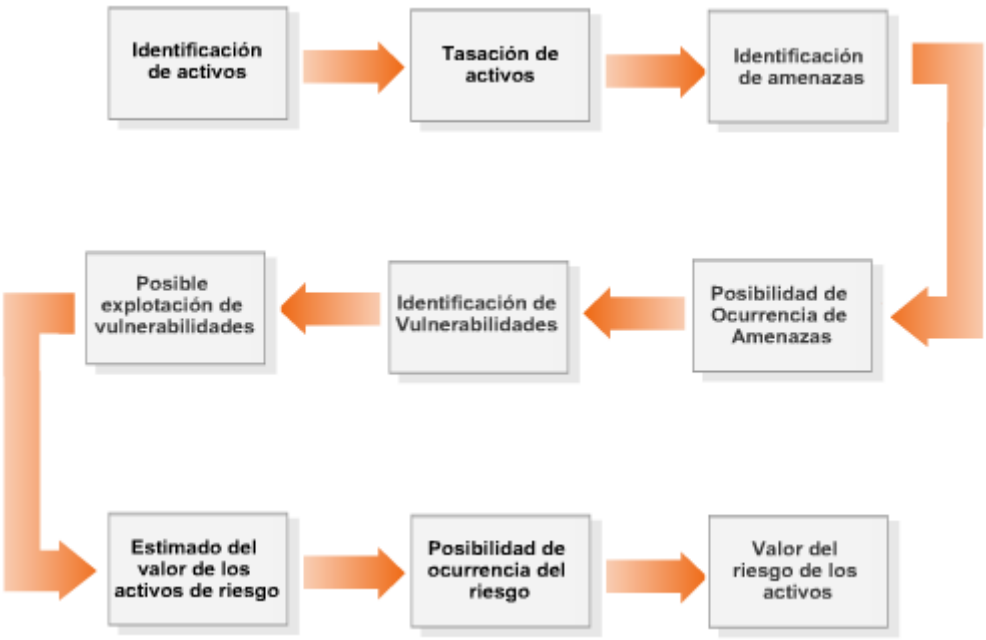
como lo es la evaluación continua de la utilización de los sistemas de información o la mejora continua de los procesos.

Varias son las metodologías posibles a la hora de realizar una evaluación de riesgos efectiva. A continuación, mencionaremos brevemente, alguno de los puntos mencionados en CobiT, en su item “P09 (Planeación & Organización) Evaluación de Riesgos”, los cuales apuntan a establecer una serie de objetivos de control, o directrices, a ser utilizados como marco de referencia a la hora de determinar la forma en la que los riesgos deberán ser administrados.

- **Enfoque de Evaluación de Riesgos:** Deberá establecerse un enfoque general, en el cual se defina claramente el alcance, los límites y la metodología a utilizar. Del mismo modo las responsabilidades y habilidades requeridas en el proceso, deberán ser especificadas en esta etapa. Identificar las relaciones entre la organización y su entorno, entender la organización, sus objetivos, estrategias, capacidades y habilidades, así como identificar todos aquellos objetos (áreas, procesos, proyectos, etc.) de la organización a los cuales se podría aplicar un Análisis de Riesgos, son aspectos fundamentales de esta etapa.
- **Identificación de Riesgos:** El propósito final de esta etapa es proveer los mecanismos necesarios para recopilar la información relacionada con los elementos esenciales de riesgos, tales como activos, amenazas, elementos vulnerables, protecciones, consecuencias y probabilidades de amenaza. Es importante recordar, que la administración de riesgos, no está dirigida exclusivamente a evitarlos. Su enfoque está en identificar, evaluar, controlar y “dominar” los riesgos. Administración de riesgos también significa tomar ventaja de las oportunidades y tomar riesgos basados en decisiones informadas y análisis de resultados.
- **Medición de Riesgos:** Tal como se encuentra especificado en CobiT, “El enfoque de la evaluación de riesgos deberá asegurar que el análisis de la información de identificación de riesgos genere como resultado una medida cuantitativa y/o cualitativa del riesgo al cual está expuesta el área examinada. Asimismo, deberá evaluarse la capacidad de aceptación de riesgos de la organización”.
- **Plan de Acción contra Riesgos:** En esta etapa, se deberá proporcionar la definición del plan de acción contra los riesgos identificados oportunamente, para asegurar la existencia de los controles y medidas de seguridad necesarias a fin de mitigar los riesgos en forma continua.
- **Aceptación de Riesgos:** Llegada esta instancia, la organización deberá definir y formalizar, cuál es el nivel de riesgo residual que asumirá, dependiendo de la oportuna identificación y medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y del resultado económico de dichas evaluaciones.

Objetivos del análisis de riesgos:

- Identificar, evaluar y manejar los riesgos de la seguridad
- Estimar la exposición de un recurso a una amenaza determinada
- Determinar cual combinación de medidas de seguridad proporcionará un nivel de seguridad razonable a un costo aceptable
- Tomar mejores decisiones en seguridad informática
- Enfocar recursos y refuerzos en la protección de los activos



Proceso de evaluación de riesgos

14.2.3 Objetivos de control

Un objetivo de control es una definición del resultado o propósito que se desea alcanzar, implantando procedimientos de control en una actividad particular dentro de las tecnologías de la información. Es de suma importancia, que estos controles tengan como objetivo el desarrollo de políticas claras y buenas prácticas para la seguridad y el control de la tecnología de la información, a partir de la perspectiva de los objetivos y necesidades de la empresa u organización.

A fin de cumplir con los objetivos de negocio propuestos, es fundamental que una organización incorpore todos aquellos objetivos de control necesarios a la hora de asegurar que el plan o marco general de control previamente establecido, es practicable. Muchas veces, dicho marco general de control, suele encontrarse superditado al ámbito de Control Interno.

Por lo general, solemos referirnos al Control Interno, como las políticas, procedimientos, prácticas y estructuras organizativas que permiten garantizar que los objetivos de negocio sean alcanzados razonablemente mediante el uso de las tecnologías de la información, y que eventos no deseables serán prevenidos o detectados y corregidos.

Una vez mas, modelos de control generales como COSO (The Committee of Sponsoring Organizations of the Treadway Commission), o específicos para las áreas relacionadas con las Tecnologías de Información como CobIT, presuponen algunas de las mejores opciones a la hora de establecer un marco de referencia para la evaluación de riesgos y el control, dentro de una organización.

14.2.4 Tipos de control

Tradicionalmente se han definido los controles internos como cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos. De acuerdo a su tipo, generalmente solemos referirnos a los controles como Preventivos, De Detección y Correctivos. A continuación, enumeraremos brevemente, las características principales de cada uno de ellos:

- **Control Preventivo:** Dentro de esta categoría, se encuentran todos aquellos controles que apuntan a evitar un evento o incidente, descartando problemas antes que los mismos aparezcan, monitoreando la operación en general y el ingreso de datos en particular, prediciendo problemas potenciales a fin de hacer ajustes antes que éstos ocurran o impidiendo que un error, omisión o acto malicioso sea llevado a cabo.
- **Control de Detección:** Cuando fallan los controles preventivos, entran en acción los controles de detección. Éstos son los encargados de detectar que un error, omisión o acto malicioso ha ocurrido y actuar en consecuencia por medio alertas y reportes.
- **Control Correctivo:** Los controles correctivos, apuntan directamente a minimizar la amenaza, solucionando problemas que pueden haber sido descubiertos por los controles de detección, intentando siempre que sea posible modificar o corregir los procesos o procedimientos necesarios, a fin de que la eventual ocurrencia reiterada sobre un mismo evento, pueda ser prevenida. Al mismo tiempo, parte de la función de los controles correctivos, radica en identificar las causas o motivos del evento o incidente.

14.2.5 Relación entre riesgo y control

El riesgo al que se enfrentan todas y cada una de las empresas y organizaciones, se encuentra íntimamente relacionado entre otras cosas, con el alcance de las Actividades de Control que hayan sido oportunamente implementadas.

Como hemos visto en los indicadores anteriores, técnicas aplicadas a la definición, evaluación y administración del riesgo, requieren de elementos de control, a la hora de establecer prácticas confiables. Una correcta evaluación del riesgo, sin el conjunto de controles necesarios a fin de asegurar que los mecanismos asociados a su mitigación, se encuentren operativos, significará que la organización no cuenta con una protección efectiva, y consecuentemente con ello, probablemente sea incapaz en cierto momento, de alcanzar los objetivos de negocio dispuestos por la dirección de la organización.

Por último, debemos recordar que las prácticas de evaluación y administración del riesgo, así como la definición y seguimiento de los controles implementados en la organización, requieren de mantenimiento continuo, de forma tal, que los mismos sean adaptados a las circunstancias actuales, reflejando la realidad de los procesos y operaciones.

14.3 ESCENARIO Y ELEMENTOS CLAVES

Cualquier auditoría, suele encontrarse íntimamente relacionada con el ámbito de su aplicación, el cual incluye no sólo “cosas”, sino personas y la tarea que ellas realizan. Desde este punto de vista, varios son los elementos que deben ser identificados como Claves a la hora de comenzar los trabajos de auditoría en una organización.

Por lo general, las personas actúan diferente al saberse auditados, lo cual puede provocar un cambio transitorio en su trabajo, el cual poco tiene que ver con los procedimientos y prácticas realizadas a diario. Éste es un punto que deberá ser tenido en cuenta especialmente, por ejemplo a la hora de realizar auditorías remotas de sistemas, o test de penetración controlados. La mayoría de las veces, será aconsejable que las únicas personas informadas de la realización de este tipo de operaciones, sean los responsables de la contratación o los directivos, y no los empleados o personas involucradas en forma directa con los sistemas a auditar. De este modo, se logrará obtener resultados más reales, entre los cuales se deben incluir por ejemplo, la respuesta por parte de los administradores responsables. Por otra parte, aspectos tales como: La relación entre el auditor y el auditado, la independencia por parte de la auditoría, la ética profesional y los recursos al alcance del grupo encargado de llevarla a la práctica, forman parte de los lineamientos principales, que de acuerdo a su importancia, serán mencionados en los próximos indicadores

14.3.1 Relación entre el auditor y el auditado

Un aspecto clave a fin llevar a cabo una auditoría exitosa, tanto sea, desde el punto de vista del auditor o del cliente que solicita la auditoría, es aquel que regula, cuál debe ser específicamente la relación entre auditor y auditado. En tal respecto, suele decirse que la relación entre los miembros del equipo de auditoría y el cliente debe ser de confidencialidad y discreción. Los miembros del equipo de auditoría no deben transferir, sin aprobación expresa del cliente y, cuando corresponda, sin la aprobación del auditado, información o documentos obtenidos durante la auditoría, ni el informe final, a terceras partes, excepto que sea requerido por ley.

Un aspecto fundamental, es aquel que se refiere a la independencia misma, que las partes deberán comprender y adoptar en la práctica de sus funciones. Sin dicha independencia, una auditoría podría carecer de sentido.

Es de esperar que las funciones de análisis y revisión que el auditor informático lleve a cabo en el transcurso de su labor, puedan chocar con la psicología del auditado, debido a diversos factores tanto técnicos como psicológicos. Generalmente, el auditor deberá prever como parte de su trabajo, la posibilidad de encontrar reticencia por parte del auditado, lo cual es comprensible y, deberá ser tenido en cuenta a la hora de obrar correctamente.

En todo momento, el auditor deberá tener en claro, que en su posición, sólo deberá limitarse a emitir un juicio global o parcial basado en hechos y situaciones incontrovertibles, careciendo de poder para modificar la situación analizada por él mismo. Al mismo tiempo, tanto en sus relaciones con el auditado como con terceras personas deberá en todo momento, actuar conforme a las normas implícitas o explícitas de dignidad requeridas por su profesión.

El auditor deberá facilitar e incrementar la confianza del auditado en base a una actuación de transparencia en su actividad profesional, sin alardes científico-técnico que, por su incomprensión, pueden restar credibilidad a los resultados obtenidos y a las directrices aconsejadas.

14.3.2 Independencia del auditor

Otro factor tan importante como la relación entre auditor y auditado, a la hora de llevar a cabo una auditoría, cualquiera sea su alcance, es la independencia necesaria por parte del auditor o auditoría actuante, en relación al auditado o el objeto de la auditoría. Como norma general, en todo asunto relacionado con la Auditoría, el auditor debe mantener independencia de criterio. Dicha independencia, debe concebirse como la libertad profesional que le asiste al auditor para expresar su opinión libre de presiones (políticas, religiosas, familiares, etc.), subjetividades (sentimientos personales e intereses de grupo), tendencias, y conflictos de intereses a lo largo del proceso. Sólo de esta forma se podrá asegurar la objetividad del proceso de auditoría, de sus hallazgos y de sus conclusiones. Pero el auditor no solo debe "ser" independiente, sino también "parecerlo", es decir, cuidar su imagen ante el auditado a fin de evitar cualquier tipo de situación indebida, que pueda resultar contraproducente para el proceso de auditoría y la obtención de los objetivos fijados por el solicitante del mismo. Un aspecto fundamental de toda auditoría, radica en que ésta, no posee carácter ejecutivo, ni son vinculantes sus conclusiones. Debido a ello toda decisión deberá quedar a cargo de la empresa, debiendo el auditor liberarse de dicha responsabilidad.

La *Asociación de Auditoría y Control de Sistemas*, creó este código de ética profesional para guiar la conducta profesional y personal de los miembros de la asociación y/o los poseedores de la designación CISA:

Los auditores de Sistemas Certificados deberán:

- Apoyar el establecimiento y cumplimiento apropiado de procedimientos estándares y controles en los sistemas de información

- Cumplir con los estándares de auditoría de sistemas de información adoptador por la Asociación de Auditoría de sistemas de Información
- Dar servicios a sus empleadores, accionistas, clientes y público en general en forma diligente, leal y honesta y no formar parte de actividades impropias o ilegales
- Mantener la confidencialidad de la información obtenida en el curso de sus tareas. Dicha información no debe ser usada en beneficio propio ni ser entregada a terceros
- Realizar sus tareas en forma objetiva e independiente, y rechazar la realización de actividades que amenacen o parezcan amenazar su independencia
- Mantener competencia en los campos relacionados a la auditoría de sistemas de información a través de la participación en actividades de desarrollo profesional
- Obtener suficiente material y documentación de sus observaciones que le permita respaldar sus recomendaciones y conclusiones
- Informar a las partes que correspondan, los resultados del trabajo de auditoría realizado.
- Dar apoyo a la educación y el conocimiento de clientes, gerentes y público en general sobre la auditoría de sistemas de información
- Mantener altos estándares de conducta y personalidad tanto en las actividades profesionales como personales

14.3.3 Recursos de Auditoría

Probablemente, una de las partes más importantes dentro del planeamiento de una auditoría, muy especialmente aquellas relacionadas con los sistemas de información, radica en el personal que deberá participar en ella y sus características asociadas. Varios puntos deberán ser cubiertos a la hora de seleccionar los recursos humanos correctos, aunque sin lugar a dudas, algunos de los más importantes son aquellos que se encuentran relacionados con: el seguimiento de estrictas políticas de capacitación, el alto sentido de moralidad implícito en las tareas a realizar y en su carácter personal, y las características técnicas a incluir en cada uno de los perfiles requeridos al momento de conformar un equipo eficiente, al cual sea posible exigirle la optimización de recursos (eficiencia) y se le retribuya o compense justamente por su trabajo.

Conocimientos, práctica profesional y capacitación que debe tener el personal que intervendrá en la auditoría, son algunos de los objetivos que deberán encontrarse relacionados con el “objeto” de la auditoría. Algunos equipos de trabajo, podrían requerir elementos con habilidades específicas (Por ejemplo, al realizar una auditoría de código). Por otra parte, se deberá planificar y solicitar, la asignación de recursos de la propia organización a ser auditada, los cuales deberán contar con el suficiente nivel, como para poder coordinar el desarrollo de la auditoría, proporcionar toda la información que se solicite y programar las reuniones y entrevistas requeridas. Éste es un punto muy importante ya que, de no tener el apoyo de la alta dirección, ni contar con un grupo multidisciplinario en el cual estén presentes una o varias personas del área a auditar, sería casi imposible obtener información en el momento y con las características deseadas.

Perfiles Profesionales de los auditores informáticos

Profesión	Actividades y conocimientos deseables
Informático Generalista	Con experiencia amplia en ramas distintas. Deseable que su labor se haya desarrollado en Explotación y en Desarrollo de Proyectos. Conocedor de Sistemas.
Experto en Desarrollo de Proyectos	Amplia experiencia como responsable de proyectos. Experto analista. Conocedor de las metodologías de Desarrollo más importantes.
Técnico de Sistemas	Experto en Sistemas Operativos y Software Básico. Conocedor de los productos equivalentes en el mercado. Amplios conocimientos de Explotación.
Experto en Bases de Datos y Administración de las mismas.	Con experiencia en el mantenimiento de Bases de Datos. Conocimiento de productos compatibles y equivalentes. Buenos conocimientos de explotación
Experto en Software de Comunicación	Alta especialización dentro de la técnica de sistemas. Conocimientos profundos de redes. Muy experto en Subsistemas de teleproceso.
Experto en Seguridad Informática	Alta especialización el la implementación de soluciones de seguridad informática.
Experto en Explotación y Gestión de CPD´S	Responsable de algún Centro de Cálculo. Amplia experiencia en Automatización de trabajos. Experto en relaciones humanas. Buenos conocimientos de los sistemas.
Experto en Programación	Responsable de realizar auditorias de código fuente.
Técnico de Organización	Experto organizador y coordinador. Especialista en el análisis de flujos de información.
Técnico de evaluación de Costes	Economista con conocimiento de Informática. Gestión de costes.

14.3.4 Riesgos de Auditoría

Todo profesional, en facultad de auditor, debe ser conciente de los riesgos que su propio trabajo representa, a nivel personal y/o profesional, al llevar a cabo su tarea. Entre los mas importantes, se encuentran:

- **Riesgo Profesional** Es el riesgo a que está expuesto el auditor frente a la posibilidad de emitir una opinión errónea o un informe equivocado o que no satisfaga a su cliente. Éste, de materializarse, puede provocar en el auditor daño en su imagen o prestigio profesional, personal o incluso en su patrimonio.
- **Riesgo Inherente** (RI) Está dado por la posibilidad de omisiones, errores o irregularidades significativas del objeto sometido a examen. Es aquel propio de la naturaleza del objeto auditado y está influenciado tanto por factores internos como por externos. Aquel que no se puede eliminar, siempre estará presente en toda empresa.
- **Riesgo de Control** (RC) Corresponde a la posibilidad que se materialicen los riesgos inherentes y que éstos no se hayan detectado, controlado o evitado por el sistema de control interno diseñado para tales efectos.
- **Riesgo de Detección** (RD) Es la posibilidad que los procedimientos de auditoría no detecten los errores, o irregularidades existentes en el objeto auditado (situaciones tampoco detectadas por el sistema de control interno). Esto puede originarse en el alcance de las pruebas, la oportunidad en que fueron efectuadas y la calidad con que fueron aplicadas.
- **Riesgo de Auditoría** (RA) Es la posibilidad que una vez efectuado el examen de auditoría,

permanezcan situaciones relevantes no informadas o errores significativos en el objeto auditado. La materialización de este riesgo implica la emisión de un informe incorrecto o incompleto. A fin de precaverse del riesgo asociado a su labor profesional, el auditor debe explicitar formalmente los objetivos de la revisión. Además debe efectuarse una adecuada planificación, ejecución y control del trabajo de tal modo de reducir este riesgo a niveles aceptables. A menudo, éste suele definirse como la combinación de las categorías individuales de riesgos de auditoría, determinados para cada objetivo de control. El mismo puede ser cuantificable o no cuantificable y suele estar representado por la siguiente formula: RA=RI*RC*RD.

14.3.5 Selección y prueba de controles claves

Gran parte del éxito de la implementación de controles y posterior auditoría, se encuentra relacionado con la oportuna selección y prueba de una serie de controles, que habiendo sido identificados como claves, representen un porcentaje importante de la seguridad del esquema general, propuesto a una empresa u organización. Muchas veces, deberá prestarse una atención especial, sobre aquellos controles que apuntan a proteger, bienes u objetos, de mayor valor para la compañía. De la misma forma, deberán ser considerados claves, aquellos controles utilizados a la hora de supervisar a su vez, controles de capas relacionadas con el ambiente de control en si mismo. Esto evitará, supervisar cada vez, controles de bajo nivel, y centrarse en aquellos que de no existir, tendrían incidencia en el resto.

Es importante hacer notar, que debido a las características intrínsecas asociadas con los complejos sistemas de información, utilizados hoy día por las organizaciones, se deberá contar con personal con conocimientos y experiencia en áreas específicas a fin de evaluar qué pruebas y controles son punibles de ser considerado claves en cada caso.

14.3.6 Muestreos

Por lo general, el dictamen del auditor suele basarse en evidencia. Precisamente una de las técnicas por las cuales, es posible recopilar dicha evidencia de auditoría, es el muestreo. El muestreo, cualquiera sea su forma, consiste en la aplicación de pruebas de cumplimiento o sustantivas a una muestra suficientemente representativa de la población total, bien se trate esta, de una serie de transacciones o de un conjunto de partidas que forman el saldo de una cuenta.

La utilización de técnicas de muestreo, es especialmente útil, en aquellos casos donde el tiempo y los costos, impiden una verificación total del ambiente a auditar. A continuación, mencionaremos algunos conceptos relacionados con las técnicas de muestreo en general:

- Frecuentemente solemos referirnos a “muestra” como un subconjunto de puntos, tomados de un contexto general.
- Las técnicas de muestreo, suelen ser frecuentemente utilizadas, a la hora de inferir características relativas a una población, basadas en los resultados del examen de las características de una muestra de la población.
- Muestreo Estadístico: Objetivo para determinar el tamaño de la muestra y para elegir los criterios. El auditor decide cuantitativamente el grado de aproximación con que la muestra debe representar a la población (en %).
- Muestreo No Estadístico: Utiliza el juicio del auditor para determinar el método de muestreo y el número de “cosas” que serán examinadas de una población.

Para que un método de muestreo, sea adecuado, la mayoría de las veces el auditor requerirá de un

plan de actividades que considere entre otros, los siguientes aspectos principales:

- Definir la población o universo.
- Elegir el método de muestreo.
- Determinar los objetivos del muestreo.
- Establecer los procedimientos de muestreo estadístico.

14.3.7 Relación entre evidencia y hallazgo

Sin lugar a dudas, uno de los aspectos más importantes en todo proceso de auditoría, es aquel que se encuentra relacionado con la recolección de evidencia y los hallazgos a partir de ésta . ¿Pero a qué nos estamos refiriendo cuando hablamos de evidencia y hallazgo?

En el ámbito de auditoría, solemos utilizar el término de *Evidencia* o *Evidencia de Auditoría*, para referirnos ha: información verificable, registros o declaraciones de hechos. La evidencia de auditoría, puede ser cualitativa o cuantitativa, y a menudo es utilizada por el auditor para determinar si se cumplen los criterios de auditoría.

Por lo general, la evidencia de auditoría está basada en el examen de documentos, procesos, sistemas de información, observación de actividades y condiciones, documentos de soporte de operaciones, declaraciones de funcionarios y empleados, sistemas internos de información y transmisión de instrucciones, manuales, procedimientos o documentación de sistemas, obtención de confirmaciones de terceras personas ajenas a la entidad, sistemas de control interno en general, resultados existentes de mediciones y documentos técnicos u otros medios dentro del alcance de la auditoría.

Por su parte, deberemos utilizar el término de hallazgo, para referirnos a los resultados de la evaluación de la evidencia reunida durante la auditoría, comparada con los criterios de auditoría acordados. Generalmente, los hallazgos de auditoría suelen ser la fuente de información inicial, a la hora de redactar el informe de auditoría.

Por último, es importante recordar, que un principio básico de auditoría, es aquel que enuncia que, el dictamen del auditor, debe estar basado en evidencia, la cual, como comentáramos en indicadores anteriores, suele ser obtenida mediante técnicas de muestreo. Por tanto, una decisión importante para los auditores, será la determinación de la cantidad y el tipo de evidencia que deben reunir; siendo un aspecto importante de esta decisión la respuesta a la pregunta ¿Qué tan grande debe ser la muestra seleccionada? En tal sentido, entre los factores que deben ser tomados en cuenta por el auditor al planear los tamaños de las muestras, se incluyen los siguientes: Control Interno; Importancia y Riesgo de Auditoría. No necesariamente, grandes muestras proveerán mayor cantidad de hallazgos.

14.3.8 Técnicas de documentación

Probablemente uno de los elementos más importantes con los que cuenta el profesional, a la hora de llevar a cabo una auditoría, respecto de un sistema de información, sea sin lugar a duda la gestión documental. A lo largo del proceso de auditoría, muchos serán los documentos que deberán ser recopilados, revisados y generados. Por este motivo, será de vital importancia que los mismos se encuentren correctamente clasificados e incluyan toda aquella información adicional, que pueda resultar valiosa al auditor practicante, en instancias posteriores. Ejemplos de dicha información, pueden ser: marcas de "*Time Stamp*", origen o destino del documento, documentos relacionados, técnica a partir de la cual se haya posibilitado el registro, etc.

Pero como hemos mencionado, la tarea del auditor, no sólo se encontrará circunscripta a la obtención de documentación previamente realizada, sino que por el contrario, muchas veces será necesario utilizar diversas técnicas, con el propósito de generar su propia documentación. A continuación,

enumeraremos algunas de las más utilizadas:

- Registro de entrevistas personales.
- Cuestionarios Personalizados.
- Entrevistas.
- Diagramas de Flujo.
- Organigramas
- Checklist o Listas de Verificación.
- Etc.

14.3.9 Técnicas de Auditoría asistidas por computadora (CAATS)

A menudo, el auditor requerirá de otras herramientas además de las manuales (inspección, observación, investigación o indagación, confirmación, cálculo y revisión analítica), a la hora de llevar a cabo un plan de auditoría efectivo. Las CAATS (Computer Assisted Audit Techniques) o Técnicas de Auditoria Asistidas por Computadora, se refieren precisamente, al conjunto de utilidades o programas de computación y datos relacionados, que el auditor utiliza como parte de los procedimientos de auditoría, a efectos de procesar datos de significancia en un sistema de información. Entre las funciones principales de este tipo de herramientas, se encuentran:

- Pruebas de detalles de transacciones y balances (Recálculos de intereses, extracción de ventas por encima de cierto valor, etc.)
- Procedimientos analíticos, por ejemplo identificación de inconsistencias o fluctuaciones significativas.
- Pruebas de controles generales, tales como configuraciones en sistemas operativos, procedimientos de acceso al sistema, comparación de códigos y versiones, etc.
- Programas de muestreo para extractar datos.
- Programas de Verificación por Oposición.
- Pruebas de control en aplicaciones.
- Recálculos.
- Programas de Simulación Paralela.
- Etc.

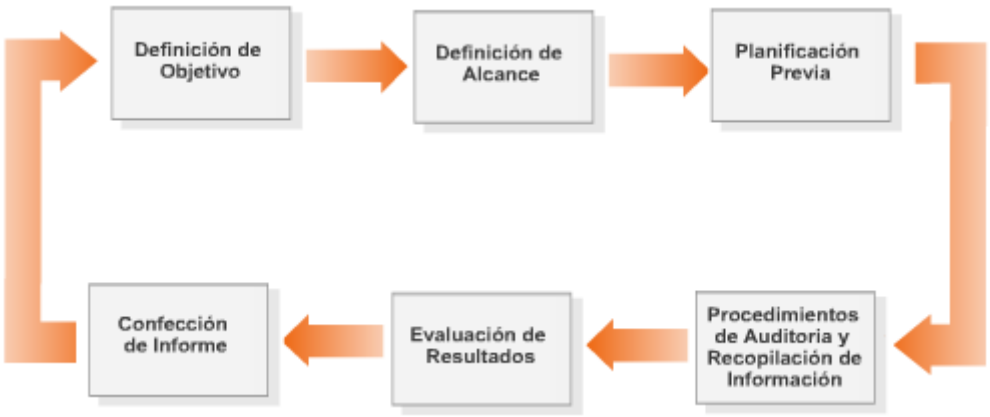
Si bien es cierto que hoy día en el mercado, es posible obtener herramientas CAATS específicas (IDEA, ACL, etc.), muchas veces, funciones de asistencia con el objeto de analizar datos o reportar hallazgos, podrán ser perfectamente realizadas, utilizando diversos recursos informáticos tradicionales como por ejemplo: software de utilidades, comandos SQL, opciones y reportes integrados en los sistemas a auditar, desarrollos a medida, etc. Según ISACA (Information Systems Audit and Control Association) por ejemplo, las CAATS suelen ser clasificadas en cuatro categorías:

1. Software de Análisis de Datos.
2. Software o Utilidades de evaluación de la seguridad de la red.
3. Software o Utilidades de evaluación de la seguridad en Sistemas Operativos y DBMS.
4. Herramientas de testeo y auditoría de código

En resumen, las CAATS pueden consistir en paquetes de programas comerciales específicos, programas escritos a medida para un propósito puntual de auditoría, programas de utilerías o programas de administración del sistema incluidos con el mismo. Independientemente de la fuente de los programas, el auditor deberá verificar su validez para fines de auditoría antes de su uso.

14.4 FASES DE UN PROGRAMA DE AUDITORÍA

Como probablemente haya notado a lo largo de esta unidad, la Auditoría de Sistemas de Información persigue a nivel general, los mismos objetivos propuestos por la Auditoría Tradicional. Si partimos de la base, de que ambas centran su atención en la salvaguarda de los activos y la integridad de los datos, al tiempo que procuran asegurar aspectos tales como la eficacia y eficiencia en los procesos de negocio, veremos que las coincidencias son notables. Por su parte, el proceso de Auditoría de Sistemas de Información, se puede concebir como una fuerza que ayuda a las organizaciones a conseguir mejorar estos objetivos. Por ende, la definición de un programa de auditoría tendiente a llevar a los hechos estos lineamientos generales, deberá ser considerada un requerimiento esencial dentro del esquema de negocio.



Fases de un programa de auditoría

Solemos referirnos a un programa de auditoría, como un conjunto documentado de procedimientos, diseñados para alcanzar los objetivos de auditoría planificados. Como tal, éste se encuentra generalmente dividido en una serie de fases claramente identificadas, a partir de las cuales se es factible organizar la totalidad de las tareas involucradas.

Si bien es cierto, que dependiendo de los objetivos planteados y del alcance esperado, muchos de los elementos envueltos en un programa de auditoría podrían variar las fases principales del mismo, suelen tener la particularidad de permanecer inalterables más allá de estos, debido principalmente a la naturaleza de su existencia. En los próximos indicadores, desarrollaremos cada una de estas fases principales, haciendo hincapié en su función específica dentro del programa de auditoría.

14.4.1 Objetivo y Alcance

Las fases de fijación de Objetivo y Alcance respectivamente, forman parte de las tareas iniciales, en todo programa de auditoría. A fin de poder avanzar en las fases posteriores, será esencial relevar los requerimientos realizados por quien ha solicitado la auditoría (Cliente, Directores, Gerente, etc.) con el objeto de formalizar los mismos y someterlos a posterior revisión por parte del solicitante.

Gran parte del éxito del proyecto, sin dudas se encontrará basado en las decisiones tomadas a lo largo de estas etapas. Objetivos mal definidos, o alcance mal estipulado, traerán aparejado no sólo el fracaso del programa de auditoría, sino también un impacto económico negativo, dado por las

perdidas sufridas por falta de control en el momento oportuno, y el esfuerzo mal orientado por parte del grupo de auditoría.

Entre las tareas principales que el analista deberá realizar en el transcurso de estas dos etapas iniciales, se encuentran: la identificación del objetivo principal de la auditoría (sujeto, área, sistema, etc.), el propósito de la auditoría, los sistemas o procesos específicos, la función o unidad de la organización que debe ser incluida en la revisión, etc.

Sólo por poner un ejemplo, podríamos convenir en que un objetivo probable a ser auditado, sea determinar qué cambios producidos en el código fuente de un programa, ocurren en un entorno bien definido y controlado; en cuyo caso la declaración del alcance, podría estar dado por el hecho de limitar dicha revisión, a tan sólo una aplicación del sistema o a un tiempo limitado.

En resumen, puesto que el objetivo y especialmente el alcance de toda auditoría, expresa los límites de la misma, el analista deberá esmerarse en formalizar un acuerdo sumamente preciso con el cliente sobre las funciones, las materias y los procesos o sistemas a auditar. Sólo de esta forma, será posible trabajar en forma acotada y en función de objetivos concretos.

14.4.2 Planificación previa

Producto de la correcta ejecución de las tareas previstas en las etapas de fijación de Objetivo y Alcance, el analista encarará la Planificación del Programa de Auditoría, con la documentación respaldatoria necesaria, a la hora de planificar en forma efectiva, aspectos tales como por ejemplo, los recursos que deberá incorporar al equipo de auditoría, atendiendo específicamente a las capacidades técnicas o de especialización que sean requeridas en cada caso.

Al mismo tiempo, se deberá identificar a lo largo de esta etapa, toda aquella información, que relacionada con el objetivo y alcance de la auditoría, deberá formar parte del conjunto de elementos a ser probados o revisados, como por ejemplo: organigramas funcionales, flujogramas de información, políticas, normas y procedimientos, documentos de auditorías anteriores, documentación de códigos fuentes, definición de controles a ser auditados, instalaciones físicas a revisar, equipamiento relacionado, etc.

Al igual que lo sucedido en etapas anteriores, los errores producidos al momento de planificar un programa de auditoría, pueden ser críticos. Por este motivo, deberá asignarse el tiempo necesario a las tareas incluidas en esta etapa, con el fin de ahorrar tiempo en fases posteriores.

Sin lugar a dudas, uno de los principales objetivos, de la fase de planificación, se encuentra íntimamente relacionado con el dimensionamiento general de proyecto, y el conocimiento por parte del grupo de trabajo de las características generales del objeto de la auditoría, en relación al mundo que lo rodea, referido generalmente como contexto (la organización, el sistema de información, el espacio físico, etc.). Este último es de suma importancia, puesto que muchas veces, los recursos tanto físicos como humanos, requeridos al momento de llevar a cabo las tareas de auditoría, se encuentran condicionados por el contexto de aplicación.

Por último, un aspecto sumamente importante a tener en cuenta a la hora de planificar una auditoría, es el relacionado con las leyes y regulaciones vigentes en el ámbito de aplicación. Muchas veces, será función del analista, conocer las reglamentaciones vigentes en el segmento de mercado al cual pertenece el auditado.

14.4.3 Procedimientos de auditoría y recopilación de información

Una vez concluidas las fases de definición de objetivo, alcance y planificación, el analista podrá comenzar con la ejecución de las tareas, de acuerdo a lo establecido en la documentación obtenida como cierre de la etapa de planificación.

Como norma general, se suele identificar al menos dos tipos de pruebas a realizar como parte de los

procedimientos de auditoría, éstas son referidas como “pruebas de cumplimiento” o “pruebas sustantivas”, las de cumplimiento se hacen para verificar que los controles funcionan de acuerdo a las políticas y procedimientos establecidos y las pruebas sustantivas verifican si los controles establecidos por las políticas o procedimientos son eficaces.

La recopilación de material de evidencia, por su parte, debe ser visto como un paso clave en el proceso de auditoría, el auditor de sistemas debe tener conocimientos acertados, respecto de la forma de recopilar la evidencia examinada.

En concordancia con los conceptos encima mencionados, el analista deberá entonces en esta fase, identificar y seleccionar el enfoque de auditoría a utilizar a la hora de verificar y probar los controles, realizar las entrevistas previstas con aquellas personas que hayan sido identificadas como clave en la etapa de planificación, obtener y revisar las normas, políticas y procedimientos previamente identificadas, chequear las listas de verificación diseñadas, desarrollar las herramientas de auditoría y metodología para probar y verificar los diferentes controles oportunamente identificados, hacer uso de CAATS (Computer Assisted Audit Techniques) y cualquier otra tarea que habiendo sido previamente planificada, requiera ser ejecutada a fin de obtener la evidencia necesaria a la hora de pasar a la fase de evaluación de resultados.

A fin de que los trabajos realizados en esta etapa sean plausibles de convertirse en elemento probatorio, el profesional a cargo deberá seguir una estricta política de documentación, la cual podría tener forma de guía, a fin de que sea posible registrar, todos y cada uno de los pasos de auditoría y para señalar la ubicación del material de evidencia.

14.4.4 Evaluación de los resultados

Finalmente, luego de haber concluido exitosamente las fases anteriores, el profesional a cargo utilizará el conjunto de información o evidencia de auditoría recolectada a lo largo del proceso, a fin de evaluar los resultados y determinar los hallazgos correspondientes.

Dichos hallazgos y conclusiones, deberán estar siempre respaldados por el análisis apropiado, el cual a su vez deberá estar basado en la correcta interpretación de la evidencia recolectada. A tal efecto, el analista involucrado con la evaluación de resultados, deberá poseer el acabado conocimiento de la materia auditada a fin de evitar la interpretación errónea de la información analizada, hecho que de suceder, podría resultar en graves perjuicios para las partes.

Si bien es cierto que muchas veces, los métodos involucrados en la evaluación de resultados, dependerá en gran parte de la organización, estos a menudo se encontrarán relacionados con la identificación de aquellas áreas, procedimientos, sistemas y procesos, en donde se carezca de controles, o los mismos hayan probado no ser suficientes de acuerdo a los objetivos de negocio planteados al momento de sugerir la auditoría. Finalmente, el criterio del auditor o grupo de auditores intervinientes, tomará partido a la hora de, definir los controles a implementar, modificar los procedimientos para los cuales se hayan detectado deficiencias y por último elegir o determinar la materialidad de las observaciones o hallazgos de auditoría, a fin de juzgar cuales observaciones son dependientes a diversos niveles de la gerencia y por tanto califican para ser informadas según corresponda.

14.4.5 Informe

A menudo, el informe de auditoría es considerado el producto final del trabajo del auditor de sistemas, y como tal, es de gran importancia que el mismo cumpla con las pautas de estilo y diseño requeridos al momento de realizar una presentación de calidad.

Como hemos visto a lo largo de esta unidad, la auditoria contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones. El objetivo del informe de auditoría, se encuentra relacionado precisamente, con la formalización por escrito, de todas aquellas sugerencias y

planes de acción, que producto del proceso de auditoría, aparecen como necesarios a fin de eliminar las disfunciones y debilidades antedichas; estas sugerencias plasmadas en el Informe final, generalmente reciben el nombre de Recomendaciones.

Es necesario comentar, que por lo general, el informe final requerirá de la redacción previa de borradores e informes parciales previos al informe final, con el objeto de contrastar las opiniones del grupo de auditores entre si, y eventualmente las personas auditadas. Este proceso se realiza con el objeto de descubrir fallos de apreciación, o al solo efecto de unificar criterios entre los miembros del equipo de trabajo.

Por su parte, si bien es cierto que no existe una plantilla obligatoria a la hora de confeccionar el informe de auditoría, deberán ser tenidos en cuenta, una serie de lineamientos generales en cuanto a su estructura. A modo de ejemplo, enumeraremos a continuación algunas de las secciones principales que deberán formar parte del mismo:

- Elementos de ubicación (Fechas de comienzo de la auditoría y confección del informe, identificación personal de los miembros del grupo de auditoría y de cada uno de los entrevistados, responsabilidad y puesto de trabajo que ostente, etc.).
- Carta de introducción o presentación.
- Definición de objetivos y alcance de la auditoría.
- Enumeración de temas considerados (A modo de introducción general).
- Cuerpo expositivo (Por cada tema considerado: situación actual, hallazgos, tendencias, puntos débiles y amenazas, recomendaciones y plan de acción, etc.).
- Conclusión global del auditor expresando una opinión sobre los controles y procedimientos revisados.

14.5 LEYES, REGLAMENTACIONES Y NORMATIVAS

Cada vez con más frecuencia, las organizaciones incorporan como parte de sus procedimientos de administración de sistemas, reglamentaciones y normativas específicas a fin de adecuar su operatoria, a aquellos lineamientos generales que apuntan a transmitir lo que oportunamente fuera considerado alguna de las mejores prácticas en relación a la informática en general y al manejo de información en particular.

Ya sea que usted se desempeñe como administrador de sistemas, analista de seguridad, consultor, o auditor en sistemas de información; muchos de los proyectos que encarará a lo largo de su carrera profesional, se encontrarán relacionados de una u otra forma con aquellas leyes, reglamentaciones y normativas, aplicables a su actividad o lo que también es probable con regulaciones propias del segmento de negocio en donde se desempeñe, que requerirán de su entero conocimiento, a fin de aplicarlas en forma eficaz y oportuna

En los próximos indicadores, tendremos oportunidad de presentar brevemente, algunas de las leyes, reglamentaciones y normativas, que encontrándose íntimamente relacionadas con las tecnologías de la información, suelen a menudo, ser consideradas las de mayor importancia. Como profesional en seguridad informática, será parte de su responsabilidad, el conocer, aplicar y transmitir a sus clientes, la necesidad y las ventajas, que suele traer aparejada la implementación y/o adecuación, de los procedimientos seguidos por la organización, a las leyes y normativas vigentes; así como también, los beneficios económicos que la puesta en marcha de las mismas implica, al encontrarse estas relacionadas con la concreción en forma segura, de los objetivos de negocio pautados por la dirección de la empresa.

Procesar información respecto de las personas implica una responsabilidad que debe estar orientada a conjugar los intereses de las empresas usuarias de bases de datos con el derecho a la privacidad

de la gente. Este es un concepto fundamental, que debe ser tenido en cuenta por el profesional de seguridad informática en todo momento. Claro está que en un mundo tendiente a informatizar aspectos que involucran los datos de millones de personas, existe la necesidad de regular y poner límites al uso que se hará de los mismos.

14.5.1 Firma Digital

Tal como lo mencionáramos en capítulos anteriores (Criptografía), desde el punto de vista conceptual, la Firma Digital, es básicamente una herramienta tecnológica, que permite garantizar la autoría e integridad de los documentos digitales, permitiendo que éstos gocen de una característica que únicamente era propia de los documentos en papel. Desde el punto de vista informático, una Firma Digital, puede ser vista como un grupo de datos asociados a un mensaje digital. Técnicamente hablando, el esquema de Firma Digital se basa en la utilización combinada de Criptografía Asimétrica o de Clave Pública y de Funciones de Hash o Resumen.

Un aspecto importante respecto a la firma digital, es que debe ser considerado un instrumento con características técnicas y normativas. Lo que significa, que existen procedimientos técnicos que permiten la creación y verificación de firmas digitales, y documentos normativos que respaldan el valor legal que dichas firmas poseen.

14.5.2 Propiedad intelectual

La era de la información, no sólo ha significado avances maravillosos relacionados con la informática y las comunicaciones, junto a ellos, varios han sido los inconvenientes a los que fue necesario hacer frente. Sin lugar a dudas, en el plano legal, uno de los más importantes ha sido el tema de la propiedad intelectual. Ahora bien, desde el punto de vista del analista de seguridad, al menos dos puntos importantes, deberán ser tenidos en cuenta respecto del alcance y aplicación de esta ley en relación a su trabajo. En primer lugar, puesto que la ley pena la utilización de software sin licencia, resultará imprescindible, tener en cuenta las restricciones de la misma, a la hora de realizar, supervisar o auditar instalaciones de programas de computadora patentados. Este hecho, no sólo ayudará a combatir la piratería en general, sino que también protegerá a su cliente u organización, de ser víctima del contagio de virus o troyanos distribuidos en software pirata, o de una eventual acción legal, por no contar con las licencias correspondientes.

En segundo término, puesto que tanto la neutralización de los medios técnicos aplicados para proteger el software, como la copia y distribución de software propietario, también se encuentran regulados y penados por esta ley, el profesional deberá incluir entre sus puntos de control, procedimientos tendientes a identificar y eventualmente corregir desviaciones en tal sentido.

14.5.3 Delito Informático

El 25 de enero de 1998, al cumplirse el primer aniversario del crimen del fotógrafo José Luis Cabezas, la página principal del sitio de la Corte Suprema de Justicia de Argentina, fue hackeada. Aparecían allí imágenes del fotógrafo asesinado y una proclama pidiendo el esclarecimiento de los hechos. La página tenía la firma del grupo Hacker argentino "X-Team". Dos años más tarde, el 19 de enero de 2001, era detenido en el Aeropuerto Internacional de Ezeiza, el “pirata informático” Wence, aparente líder del grupo “X-Team” y acusado de ser responsable entre otros, del hecho anteriormente citado. La denuncia era por daños y presunta asociación ilícita, este último, un delito no excarcelable. Sucede que para las leyes argentinas, el hacking no existe en la jurisprudencia actual. Finalmente, el 20 de Marzo de 2002, el Juez a cargo de la causa, establecía en su fallo, que una página web no puede asimilarse al concepto de cosa (definición que si se encuentra contemplada en el código penal actual) en tanto y en cuanto, por su naturaleza, no es un objeto corpóreo ni puede ser detectado

materialmente, motivo por el cual, dejaba sin efecto la denuncia, declarando el sobreseimiento de todos y cada uno de los implicados en la causa

14.5.4 ISO 17799

ISO / IEC 17799, es un modelo internacional, a través del cual se propone un estándar relacionado con cómo las empresas deberían conducir el manejo de sus requerimientos de información de seguridad. Dicho de otra forma, es una guía o código de buenas prácticas para la gestión de la seguridad de la información. Claro está que no es la única, existen otras tales como la ISO 13335 e ISO 15408, aunque sin lugar a dudas ISO 17799, gracias a algunas de sus características principales, se ha convertido en un estándar de facto.

La ISO 17799 como tal, se encuentra basada en el estándar Británico BS 7799-1:1999, del cual toma gran parte de los conceptos en él esbozado. En ella se involucra la totalidad de los activos de un sistema de información: el hardware, el software, la estructura de los datos y el personal. Además, desde su título mismo es mandataria en algo que debe realizarse: “Gestión de la Seguridad de la Información”, entendiéndose como gestión, el hecho de administrar, redactar políticas, normas y procedimientos, implementarlas y verificar su cumplimiento (Ese cumplimiento podría ser en el futuro, oportunamente verificado por alguna entidad, tal como sucede con las normas de calidad ISO 9000, objeto de una certificación).

La norma ISO 17799, se compone de diez ítems o temáticas generales, a la vez que identifica más de cien controles potenciales. Cada punto es desarrollado con el objeto de alcanzar todos y cada uno de los principales temas relacionados con la seguridad de la información, que suelen estar presentes en una organización. Objetivos, lineamientos generales y buenas prácticas, son parte integral de los mismos.

En la actualidad, la ISO/IEC 17799, se encuentra ganando mercado a nivel mundial, en forma constante, imponiéndose como el estándar más ampliamente implementado e internacionalmente aceptado. Gobiernos tales como los de Gran Bretaña, y países tales como Australia, Brasil, Japón, y Suecia, suelen contarse entre sus adeptos.

Por último, un aspecto importante de ISO 17799, radica en la identificación que en ella se realiza, respecto de los “factores de éxito decisivos” (critical success factors) que una organización debe lograr si desea tener éxito implementando seguridad de la información.

14.5.5 COBIT

Hace ya algunos años, los profesionales de IT, comenzaron a verse en la necesidad de conocer varias normas de control diferentes (DTI, NIST, etc.), cada una de ellas con una función u orientación específica, a la hora de organizar sus departamentos relacionados con las tecnologías de la información. El inconveniente detrás de ello, pasaba porque ninguna de las normas, proporcionaba un modelo de control completo y utilizable (específicamente sobre IT), como soporte para los procesos de negocio.

Atentos a esta necesidad, la “Information Systems Audit And Control Association” (ISACA), en conjunto con un grupo de empresas, desarrolló, tomando como referencia la publicación en los EE.UU de los modelos de control generales de COSO, un marco de referencia genuino, para la definición de objetivos de control aplicados a las Tecnologías de Información, que recibiría el nombre de “COBIT: Objetivos de Control para la Información y Tecnologías Afines”.

El COBIT se compone de un conjunto de 34 objetivos de control de alto nivel, uno para cada uno de los procesos de TI, agrupados en cuatro dominios principales:

- Planeamiento y Organización.

- Adquisición e Implementación.
- Entrega (de Servicio)
- Monitoreo.

Tal como se menciona en el resumen ejecutivo de este marco de referencia, esta estructura cubre todo y cada uno de los aspectos de la información y de la tecnología que la soporta. Dirigiendo estos 34 objetivos de control de alto nivel, el propietario de procesos de negocio podrá asegurar que se proporciona un sistema de control adecuado para el ambiente de tecnología de información. Pero el COBIT no sólo estipula objetivos de control, a su vez, cada uno de ellos se incluye como parte de la entrega, una serie de guías imprescindibles, a la hora de revisar o auditar el cumplimiento de los objetivos propuestos.

14.6 METODOLOGÍA OSSTMM

El Manual de la Metodología Abierta de Comprobación de la Seguridad (OSSTMM, Open Source Security Testing Methodology Manual) es uno de los estándares profesionales más completos y comúnmente utilizados en Auditorías de Seguridad para revisar la Seguridad de los Sistemas desde Internet. Incluye un marco de trabajo que describe las fases que habría que realizar para la ejecución de la auditoría. Se ha logrado gracias a un consenso entre más de 150 expertos internacionales sobre el tema, que colaboran entre sí mediante Internet. Se encuentra en constante evolución y actualmente se compone de las siguientes fases:

Seguridad de la Información, Revisión de la Inteligencia Competitiva, Seguridad de los Procesos, Seguridad en las tecnologías de Internet, Seguridad en las Comunicaciones, Seguridad Inalámbrica, Seguridad Física

Este documento de metodología de testeo de seguridad, Es un conjunto de reglas y lineamientos para CUANDO, QUE y CUALES eventos son testeados. Esta metodología cubre únicamente el testeo de seguridad externo, es decir, testear la seguridad desde un entorno no privilegiado hacia un entorno privilegiado, para evadir los componentes de seguridad, procesos y alarmas y ganar acceso privilegiado. Está también dentro del alcance de este documento proveer un método estandarizado para realizar un exhaustivo test de seguridad de cada sección con presencia de seguridad (por ejemplo, seguridad física, seguridad inalámbrica, seguridad de comunicaciones, seguridad de la información, seguridad de las tecnologías de Internet, y seguridad de procesos) de una organización. Dentro de este método abierto y evaluado por expertos, para realizar exhaustivos testeos de seguridad, alcanzamos un estándar internacional en testeos de seguridad, que representa una línea de referencia para todas las metodologías de testeo de seguridad tanto conocidas como inexploradas.

14.6.1 ¿Cómo se puede clasificar lo que habitualmente se engloba bajo "Auditorías de Seguridad"?

Para tratar de diferenciar bien las opciones que se puede tener en cuenta a la hora de solicitar este tipo de actividades, se deben considerar al menos tres grandes grupos:

- **Penetration Test**: Se trata de una actividad con objetivo específico y acotado empleando técnicas de Hacking y en general aplicando metodologías de "Caja Negra" (Sin ningún tipo de información, mas allá de la que puede contar cualquier individuo ajeno a la empresa)

  Según la definición de OSSTMM: *Test de seguridad con un objetivo definido que finaliza cuando el objetivo es alcanzado o el tiempo ha terminado.*

- **Diagnóstico o evaluación de Seguridad**: Comprende una actividad más amplia, en general

tanto desde fuera como desde dentro de la empresa, siempre relacionado a actividades eminentemente técnicas, y puede realizar por medio de “Caja Negra o Blanca” (con total conocimiento de la información de la empresa)

Según la definición de OSSTMM: *Una visión general de la presencia de seguridad para una estimación de tiempo y horas hombre.*

- **Auditoría de seguridad**: Comprende a lo anterior y también una visión más amplia en cuanto a planes y políticas de seguridad, revisión de normativas, aplicación de LOPD, procedimientos, planos, inventarios, audiencias, etc. Es decir involucra la visión más amplia a considerar, sin dejar ningún aspecto librado al azar.

  Según la definición de OSSTMM: *Inspección manual con privilegios de acceso del sistema operativo y de los programas de aplicación de un sistema. En los Estados Unidos y Canadá, “Auditor” representa un vocablo y una profesión oficiales, solamente utilizado por profesionales autorizados. Sin embargo, en otros países, una “auditoría de seguridad” es un término de uso corriente que hace referencia a Test de Intrusión o test de seguridad.*

Para completar un poco el enfoque que ISECOM (Institute for Security and Open Methodologies), entidad responsable del proyecto OSSTMM, ofrece sobre estas clasificaciones se presenta a continuación las actividades que pueden ser llevadas a cabo (La misma se presenta textualmente en sus manuales): ISECOM aplica los siguientes términos a los diferentes tipos de sistemas y de testeos de seguridad de redes, basados en tiempo y costo para el Testeo de Seguridad de Internet:

- **Búsqueda de Vulnerabilidades**: se refiere generalmente a las comprobaciones automáticas de un sistema o sistemas dentro de una red.
- **Escaneo de la Seguridad**: se refiere en general a las búsquedas de vulnerabilidades que incluyen verificaciones manuales de falsos positivos, identificación de los puntos débiles de la red y análisis profesional individualizado.
- **Test de Intrusión**: se refiere en general a los proyectos orientados a objetivos en los cuales dicho objetivo es obtener un trofeo, que incluye ganar acceso privilegiado con medios pre-condicionales.
- **Evaluación de Riesgo**: se refiere a los análisis de seguridad a través de entrevistas e investigación de nivel medio que incluye la justificación negocios, las justificaciones legales y las justificaciones específicas de la industria.
- **Auditoría de Seguridad**: hace referencia a la inspección manual con privilegios administrativos del sistema operativo y de los programas de aplicación del sistema o sistemas dentro de una red o redes.
- **Hacking Ético**: se refiere generalmente a los tests de intrusión en los cuales el objetivo es obtener trofeos en la red dentro del tiempo predeterminado de duración del proyecto.
- **Test de Seguridad y su equivalente militar, Evaluación de Postura**, es una evaluación de riesgo con orientación de proyecto de los sistemas y redes, a través de la aplicación de análisis profesional mediante escaneos de seguridad donde la intrusión se usa generalmente para confirmar los falsos positivos y los falsos negativos dentro del tiempo permitido de duración del proyecto.

14.6.2 ¿Es posible respetar algún método que permita repetir esta tarea y obtener índices de evolución?

En este punto es donde se plantea a título de guía lo que propone OSSTMM. Se reitera, no porque sea mejor o peor que cualquier otra que pueda emplear una empresa consultora, sino simplemente

por ser una referencia gratuita y sobre todo porque tiene su punto de partida en respetar la mayoría de los estándares, tal cual lo expresa en sus primeras páginas, estando en plena conformidad con los mismos (ISO-17799 o BS-7799, GAO y FISCAM, NIST,CVE de Mitre, etc.). Resumidamente, esta metodología propone un proceso de evaluación de una serie de áreas que reflejan los niveles de seguridad que posee la infraestructura a auditar, a estos los denominará “Dimensiones de seguridad”, y consisten en el análisis de lo siguiente:

- Visibilidad
- Acceso
- Confianza
- Autenticación
- No repudio
- Confidencialidad
- Privacidad
- Autorización
- Integridad
- Seguridad
- Alarma.

Para un trabajo metódico y secuencial, describe seis secciones que abarcan el conjunto de los elementos que componen todo sistema actual, ellas son:

1. Seguridad de la Información
2. Seguridad de los Procesos
3. Seguridad en las tecnologías de Internet
4. Seguridad en las Comunicaciones
5. Seguridad Inalámbrica
6. Seguridad Física

En cada sección se especifican una serie de módulos a ser evaluados, teniendo en cuenta si aplica o no cada uno de ellos a la infraestructura en cuestión, el resultado de la observación de todos ellos es lo que permitirá “pintar” el mapa de seguridad.

Otro aspecto que trata con bastante detalle es la **Evaluación de riesgo**, teniendo en cuenta que dentro de cada módulo se encuentran los valores adecuados (RAVs) para obtener las métricas finales, lo cual como se recalcó en este texto es uno de los principios que debe tener en cuenta todo auditor si es consciente de las necesidades del cliente.

14.7 SÍNTESIS

En términos resumidos, podemos destacar que:

Una ***auditoría de seguridad informática*** o ***auditoría de seguridad de sistemas de información*** (SI) es el estudio que comprende el análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

Una vez obtenidos los resultados, se detallan, archivan y reportan a los responsables quienes deberán establecer medidas preventivas de refuerzo, siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad.

Los servicios de auditoría constan de las siguientes fases:

- Enumeración de redes, topologías y protocolos
- Identificación de sistemas y dispositivos
- Identificación de los sistemas operativos instalados
- Análisis de servicios y aplicaciones
- Detección, comprobación y evaluación de vulnerabilidades
- Medidas específicas de corrección
- Recomendaciones sobre implantación de medidas preventivas.

Los servicios de auditoría pueden ser de distinta índole:

- ***Auditoría de seguridad interna***. En este tipo de auditoría se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno
- ***Auditoría de seguridad perimetral***. En este tipo de análisis, el perímetro de la red local o corporativa es estudiado y se analiza el grado de seguridad que ofrece en las entradas exteriores
- ***Test de intrusión***. El test de intrusión es un método de auditoría mediante el cual se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada. Es un complemento fundamental para la auditoría perimetral.
- ***Análisis forense***. El análisis forense es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperabilidad del sistema, el análisis se denomina análisis postmortem.
- ***Auditoría de páginas web***. Entendida como el análisis externo de la web, comprobando vulnerabilidades como la inyección de código sql, Verificación de existencia y anulación de posibilidades de Cross Site Scripting (XSS), etc.
- **Auditoría de código de aplicaciones**. Análisis del código tanto de aplicaciones páginas Web como de cualquier tipo de aplicación, independientemente del lenguaje empleado

Realizar auditorías con cierta frecuencia asegura la integridad de los controles de seguridad aplicados a los sistemas de información. Acciones como el constante cambio en las configuraciones, la instalación de parches, actualización de los softwares y la adquisición de nuevo hardware hacen necesario que los sistemas estén continuamente verificados mediante auditoría.

Una auditoría se realiza con base a un patrón o conjunto de directrices o buenas practicas sugeridas. Existen estándares orientados a servir como base para auditorías de informática. Uno de ellos es COBIT (Objetivos de Control de la Tecnologías de la Información), dentro de los objetivos definidos como parámetro, se encuentra el "Garantizar la Seguridad de los Sistemas". Adicional a este estándar podemos encontrar el standard ISO 27002, el cual se conforma como un código internacional de buenas prácticas de seguridad de la información, este puede constituirse como una directriz de auditoría apoyándose de otros estándares de seguridad de la información que definen los requisitos de auditoría y sistemas de gestión de seguridad, como lo es el estándar ISO 27001.

PREGUNTAS Y TIPS

- **¿Cuál es la frecuencia ideal con la que debe practicarse una auditoría?** Continua
- **¿Cómo se denominan las sugerencias plasmadas en el informe final de auditoría?** Recomendaciones
- **¿Cuál es el proyecto que debería ser tenido en cuenta para un testeo metodológico al momento de ejecutar un análisis de seguridad?** OSSTMM
- **¿Qué tipo de auditoría proporciona un mayor grado de objetividad?** Auditoría Externa
- **¿Cómo se denomina al hecho de que una organización defina y formalice el nivel de riesgo residual que asumirá?** Aceptación de riesgo
- **¿Cómo se denomina al proceso de identificación y análisis de riesgos y vulnerabilidades a los cuales se encuentran sometidos los recursos informáticos?** Evaluación de Riesgos
- **¿Cómo se conoce al desarrollo que realizó ISACA, tomando como referencia los modelos de control COSO?** COBIT
- **¿En qué Ley se contemplan casos tales como "Acceso no autorizado", "Daño a datos informáticos", "Violación del correo electrónico?** Delito Informático
- **¿Qué representa un excelente punto de partida para el auditor?** Política de Seguridad
- **¿Cuáles de las siguientes son funciones de CAATS?** Programas de muestreo, Programas de verificación por oposición, Pruebas de detalle de transacciones, Simulación paralela
- **¿Cuáles son funciones a realizar por el auditor informático?** Revisar y juzgar los controles implantados en los circuitos y sistemas informáticos, Revisar y juzgar el nivel de eficacia, utilidad fiabilidad y seguridad de los sistemas utilizados
- **¿Cuáles son técnicas de documentación de auditoría?** Cuestionarios personalizados, Entrevistas, Organigramas, Diagramas de Flujo

CAPÍTULO 15

15.1 INFORMÁTICA FORENSE

La Informática forense permite la solución de conflictos tecnológicos relacionados con seguridad informática y protección de datos. Gracias a ella, las empresas obtienen una respuesta a problemas de privacidad, competencia desleal, fraude, robo de información confidencial y/o espionaje industrial surgidos a través de uso indebido de las tecnologías de la información. Mediante sus procedimientos se identifican, aseguran, extraen, analizan y presentan pruebas generadas y guardadas electrónicamente para que puedan ser aceptadas en un proceso legal.

Según el FBI, la informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional. Desde 1984, el Laboratorio del FBI y otras agencias que persiguen el cumplimiento de la ley empezaron a desarrollar programas para examinar evidencia computacional.

Si bien es cierto que originalmente, la potencia de la informática forense se orientaba específicamente a computadores, la constante evolución de la tecnología ha borrado esos límites de modo tal que sea posible extender un análisis forense más allá de los limites de los computadores tradicionales. Hoy en día, PDAs, teléfonos celulares y otros dispositivos, suelen ser objeto de una investigación forense. Es fundamental remarcar que la "Informática Forense" no aplica sino hasta después de acontecido un incidente.

¿Para qué sirve? Para garantizar la efectividad de las políticas de seguridad y la protección tanto de la información como de las tecnologías que facilitan la gestión de esa información.

¿En qué consiste? Consiste en la investigación de los sistemas de información con el fin de detectar evidencias de la vulneración de los sistemas. Para realizar un adecuado análisis de Informática forense se requiere un equipo multidisciplinar que incluya profesionales expertos en derecho de las TI y expertos técnicos en metodología forense. Esto es así porque se trata de garantizar el cumplimiento tanto de los requerimientos jurídicos como los requerimientos técnicos derivados de la metodología forense.

¿Cuál es su finalidad? Cuando una empresa contrata servicios de Informática forense puede perseguir objetivos preventivos, anticipándose al posible problema u objetivos correctivos, para una solución favorable una vez que la vulneración y las infracciones ya se han producido.

En conclusión, estamos hablando de la utilización de la informática forense con una finalidad preventiva, en primer término. Como medida preventiva sirve a las empresas para auditar, mediante la práctica de diversas pruebas técnicas, que los mecanismos de protección instalados y las condiciones de seguridad aplicadas a los sistemas de información son suficientes. Asimismo, permite detectar las vulnerabilidades de seguridad con el fin de corregirlas. Cuestión que pasa por redactar y elaborar las oportunas políticas sobre uso de los sistemas de información facilitados a los empleados para no atentar contra el derecho a la intimidad de esas personas.

Por otro lado, cuando la seguridad de la empresa ya ha sido vulnerada, la informática forense permite recoger rastros probatorios para averiguar, siguiendo las evidencias electrónicas, el origen del ataque (si es una vulneración externa de la seguridad) o las posibles alteraciones, manipulaciones, fugas o destrucciones de datos a nivel interno de la empresa para determinar las actividades realizadas desde uno o varios equipos concretos.

¿Qué metodologías utiliza la Informática forense? Las distintas metodologías forenses incluyen la recogida segura de datos de diferentes medios digitales y evidencias digitales, sin alterar los datos de

origen. Cada fuente de información se cataloga preparándola para su posterior análisis y se documenta cada prueba aportada. Las evidencias digitales recabadas permiten elaborar un dictamen claro, conciso, fundamentado y con justificación de las hipótesis que en él se barajan a partir de las pruebas recogidas.

¿Cuál es la forma correcta de proceder? Y, ¿por qué? Todo el procedimiento debe hacerse tenido en cuenta los requerimientos legales para no vulnerar en ningún momento los derechos de terceros que puedan verse afectados. Ello para que, llegado el caso, las evidencias sean aceptadas por los tribunales y puedan constituir un elemento de prueba fundamental, si se plantea un litigio, para alcanzar un resultado favorable.

La informática forense está adquiriendo una gran importancia dentro del área de la información electrónica, esto debido al aumento del valor de la información y/o al uso que se le da a ésta, al desarrollo de nuevos espacios donde es usada (por Ej. el Internet), y al extenso uso de computadores por parte de las compañías de negocios tradicionales (por Ej. bancos). Es por esto que cuando se realiza un crimen, muchas veces la información queda almacenada en forma digital. Sin embargo, existe un gran problema, debido a que los computadores guardan la información de forma tal que no puede ser recolectada o usada como prueba utilizando medios comunes, se deben utilizar mecanismos diferentes a los tradicionales. Es de aquí que surge el estudio de la computación forense como una ciencia relativamente nueva.

Resaltando su carácter científico, tiene sus fundamentos en las leyes de la física, de la electricidad y el magnetismo. Es gracias a fenómenos electromagnéticos que la información se puede almacenar, leer e incluso recuperar cuando se creía eliminada. La informática forense, aplicando procedimientos estrictos y rigurosos puede ayudar a resolver grandes crímenes apoyándose en el método científico, aplicado a la recolección, análisis y validación de todo tipo de pruebas digitales.

15.1.1 Objetivos de la Informática Forense

La informática forense tiene 3 objetivos, a saber:

- La compensación de los daños causados por los criminales o intrusos.
- La persecución y procesamiento judicial de los criminales.
- La creación y aplicación de medidas para prevenir casos similares.

Estos objetivos son logrados de varias formas, entre ellas, la principal es la recolección de evidencia.

15.1.2 Usos de la informática forense

Existen varios usos de la informática forense, muchos de estos usos provienen de la vida diaria, y no tienen que estar directamente relacionados con la informática forense:

- *Prosecución Criminal:* Evidencia incriminatoria puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.
- *Litigación Civil*: Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la informática forense.
- *Investigación de Seguros*: La evidencia encontrada en computadores, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.

- *Temas corporativos*: Puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial.
- *Mantenimiento de la ley*: La informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva.

La "*Informática Forense*" ha pasado a convertirse en nuestros días, en un instrumento clave a la hora de combatir el delito, contribuyendo de diversas formas con la investigación de los mismos, ya sea que el "sistema de computo a investigar" sea el fin en sí del delito o solo el móvil del mismo.

Hoy en día, el campo de aplicación de la Informática Forense, puede ser tan puntual como extensivo a la vez. Si bien su objetivo final, es habitualmente el de construir casos, a partir de la investigación de aquellos elementos que podrían haber formado parte en la concreción o intento de un delito, basándose en la obtención y análisis de evidencia, los estadios intermedios de una investigación pueden ser por si mismos objetivos particulares que dependiendo del ámbito pueden transformarse en "el objetivo" en sí mismo.

Desde el punto de vista estrictamente práctico la informática forense se ha convertido en una herramienta imprescindible a la hora de elaborar alegatos y encontrar culpables en investigaciones de delitos tales como: Prácticas Terroristas, Homicidios, Fraudes Financieros, Pornografía Infantil, Discriminación, Evasión de Impuestos, Acoso Sexual, Abuso del uso de Computadores por parte de los Empleados, Espionaje Industrial, etc.

Por su parte y aprovechando tanto la capacidad, metodologías y herramientas, como la experiencia adquirida por los profesionales forenses en materia de recuperación de datos respecto de una unidad de discos dañada (mas allá de cual haya sido el origen del incidente); empresas privadas, gubernamentales e incluso particulares, suelen ser consumidores habituales de este tipo de servicios, haciendo de esta ciencia algo NO exclusivo de la investigación de delitos.

15.1.3 Metodología

Tal como sucede en el resto de las prácticas, los investigadores forenses a menudo suelen llevar adelante sus procesos de investigación siguiendo algún tipo de metodología ampliamente aceptada por la comunidad profesional. A continuación, se describen las principales etapas a menudo asociadas a una metodología efectiva de investigación forense (Identificación, Adquisición, Autenticación, Análisis y Presentación) así como también los principales aspectos relacionados con cada una de ellas:

Identificación: Durante esta parte de la investigación, se busca de alguna forma, determinar a nivel general, la magnitud de la misma, identificando aquellos puntos sobre los cuales se llevara a cabo el trabajo forense y obteniendo en definitiva un resumen de los pasos a seguir. Entre las tareas propias de esta etapa se encuentran:

- Obtención en primera instancia del grado de daño causado a nivel general.
- Identificación de el/los equipos de computo involucrados así como sus características principales.
- Generación de las tareas a realizar así como el orden de las mismas, teniendo en cuenta el tipo de incidente y los dispositivos afectados.
- Obtención de las órdenes necesarias para comenzar con las prácticas forenses, teniendo en cuenta las leyes imperantes en el lugar del incidente, así como las políticas internas de la compañía.

Adquisición: Durante esta etapa, el investigador forense tendrá la responsabilidad de ejecutar el "Plan de Adquisición" elaborado como parte de su trabajo de "Identificación". Generalmente se conoce como "Adquisición", al conjunto de acciones concretas que se deben llevar a cabo, a fin de obtener la evidencia necesaria para el curso de la investigación. Los procesos involucrados en esta etapa, pueden ser tan variados como complejos técnicamente, dependiendo del marco en el que se haya constituido el incidente y su área de influencia.

Una de las tareas más frecuentes, llevada a cabo en esta etapa, es la de "Extracción de Datos", la cual deberá involucrar, todos aquellos dispositivos o componentes (Discos, Memoria RAM, sistemas de LOGS, etc.) de los cuales se presume podría obtenerse evidencia del incidente.

Autenticación: A diferencia de la etapa de "Adquisición", la cual suele representar un reto para el investigador forense en cuanto al elevado skill técnico que debe poseer, en función de diferentes tecnologías, herramientas y sistemas operativos; los procedimientos destinados a la etapa de "Autenticación" de la evidencia suelen requerir precisión y un perfecto entendimiento de lo que significa la tarea en sí misma.

Se entiende por "Autenticar la Evidencia", al proceso de probar que la evidencia presentada en instancias de un litigio, es efectivamente, la evidencia que oportunamente fuera obtenida de la "escena del crimen". Este importante hacer notar, que la autenticación representa un punto fundamental e imprescindible, en toda investigación para la cual se requiera una instancia judicial. En la práctica, esto se traduce como la utilización de herramientas capaces de generar "sumas de verificación" mediante el uso de funciones "hash" como los provistos por los algoritmos MD5 y SHA. La particularidad de este tipo de algoritmos, es que suelen cumplir con propiedades básicas e imprescindibles al momento de autenticar documentos electrónicos.

Análisis: Esta es la etapa donde el investigador forense, en muchos casos en la tranquilidad de su laboratorio, valiéndose de copias forenses validadas, iniciará la exanimación en busca de todos aquellos datos que puedan concluir en evidencia. Algunas tareas propias de esta etapa son:

- Detección de archivos ocultos.
- Recuperación de archivos eliminados.
- Búsquedas por equivalencias de cadena.
- Correlación de Logs.
- Examinación de los "Sellos de Tiempo"
- Examinación de "File Slack", "RAM Slack" y "Drive Slack"
- Examinación de archivos temporales y de intercambio.
- Examinación de cabecera de archivos e identificación de tipo.
- Etc.

Presentación: Desde el punto de vista del Investigador Forense, la etapa de "Presentación" representa el fin de su investigación. En ella, se procede a presentar la evidencia obtenida cumpliendo con las formalidades correspondientes en cada caso, respecto a la confección de informes escritos. Entre las tantas responsabilidades del Investigador Forense durante esta etapa, se encuentran la elaboración de Informe Escrito, la presentación de la Evidencia en soporte magnéticos y eventualmente la exposición ante el ámbito correspondiente.

15.1.4 Características de la evidencia

En líneas generales, solemos referirnos con el término “Evidencia” a cualquier información de valor probatorio y extender esta definición a la “Evidencia Digital”, como cualquier tipo de dato digital que pueda ayudar a demostrar que se ha cometido un ilícito, o bien que permita establecer un vínculo entre el ilícito, la víctima y el criminal.

Las principales características relacionadas con la evidencia digital, son sin lugar a dudas su “Fragilidad” y “Volatilidad”. Así mismo y a diferencia de la evidencia física, los medios electrónicos se caracterizan por ser sumamente sensibles a modificaciones dolosas u accidentales, motivo por lo cual el investigador forense basa su trabajo, tanto en la preservación de la evidencia, así como en su autenticación, de forma tal de asegurar su estado original.

Un aspecto de suma importancia cuando nos referimos a evidencia digital, se encuentra relacionado con los atributos que la misma debe poseer a fin de que esta pueda ser considerada admisible ante una corte. A continuación se mencionan brevemente dichos atributos principales:

- Relevante (Es decir estrechamente relacionada con el crimen bajo investigación)
- Permitida Legalmente (Debe haber sido obtenida de manera legal)
- Confiable (No debe haber sido alterada o modificada en ningún modo)
- Identificada (Debe haber sido claramente etiquetada)
- Preservada (No debe haber sido dañada o destruida)
- Suficiente (Debe ser convincente, no sujeta a interpretaciones personales y concluyentes.

15.1.5 Cadena de custodia

Tal como mencionáramos en indicadores anteriores, toda evidencia debe mantenerse integra y custodiada para ser admisible. En relación a este principio, suele utilizarse el término “Cadena de Custodia”, para referirse a la registración ordenada de todos aquellos eventos relacionados con la evidencia, acontecidos desde su recolección hasta la presentación de la misma.

La cadena de custodia debería ser vista como el seguimiento a dar a la evidencia, con el objeto que esta no vaya a ser alterada, cambiada o extraviada. (A tal efecto, los indicios deben ser etiquetados y la persona que lo recibe deberá entregar a cambio una constancia o cargo).

Adicionalmente, la cadena de custodia supone que la evidencia se mantiene en un lugar seguro al cual solo tiene acceso personal facultado para ello.

Idealmente, una “Cadena de Custodia” bien elaborada debería ser capaz de asegurar y demostrar en cada oportunidad en la que sea necesario, que la evidencia presentada puede ser considerada confiable. A fin de cumplir con su objetivo primario, la cadena de custodia debe ser soportada por un documento generalmente conocido como “Bitácora” o “Log History”, el cual debería ser utilizado a efectos de llevar un historial de todas y cada una de las actividades realizadas durante el proceso de Análisis Forense. A partir de la información obtenida de esta bitácora como parte integral del proceso de cadena de custodia, deberíamos ser capaces de responder mínimamente las siguientes preguntas:

- Quién obtuvo la evidencia?
- Qué era la evidencia?
- Cuándo y dónde se obtuvo la evidencia?
- Quién protegió la evidencia?
- Quién estuvo en control o posesión de la evidencia?

15.1.6 Recomendaciones

A la hora de llevar a cabo una investigación forense, deberían ser tenidas en cuenta algunas recomendaciones de nivel general, con el objeto de no perder de vista algunos de los aspectos más importantes relacionados con dicho proceso. A continuación se mencionan una escueta lista de carácter general:

- Identificar en forma clara toda posible evidencia digital.
- Minimizar el manejo del original (Imágenes forenses).
- Documentar TODO.
- Prestar especial atención a la Cadena de Custodia.
- Cumplir con las reglas de la evidencia.
- Conocer regulaciones y disposiciones legales.
- Estar autorizado para proceder con los análisis.
- No avanzar más allá de nuestros conocimientos.
- Contratar profesionales.
- Contar con el equipo adecuado.
- “Preservar”
- Generar procesos “Repetibles”

15.1.7 La investigación tecnológica

Los investigadores de la computación forense usan gran cantidad de técnicas para descubrir evidencia, incluyendo herramientas de software que automatizan y aceleran el análisis computacional. La evidencia computacional es única, cuando se la compara con otras formas de “evidencia documental”. A diferencia de la documentación en papel, la evidencia computacional es frágil y una copia de un documento almacenado en un archivo es idéntica al original. Otro aspecto único de la evidencia computacional es el potencial de realizar copias no autorizadas de archivos, sin dejar rastro de que se realizó una copia. Esta situación crea problemas concernientes a la investigación del robo de secretos comerciales, como listas de clientes, material de investigación, archivos de diseño asistidos por computador, fórmulas y software propietario.

Debe tenerse en cuenta que los datos digitales adquiridos de copias no se deben alterar de los originales del disco, porque esto invalidaría la evidencia; por esto los investigadores deben revisar con frecuencia que sus copias sean exactas a las del disco del sospechoso, para esto se utilizan varias tecnologías, como por ejemplo *checksums* o hash MD5.

La IOCE (International Organization On Computer Evidence) define los siguientes cinco puntos como los principios para el manejo y recolección de evidencia computacional:

- Sobre recolectar evidencia digital, las acciones tomadas no deben cambiar por ningún motivo esta evidencia.
- Cuando es necesario que una persona tenga acceso a evidencia digital original, esa persona debe ser un profesional forense.
- Toda la actividad referente a la recolección, el acceso, almacenamiento o a la transferencia de la evidencia digital, debe ser documentada completamente, preservada y disponible para la revisión.

- Un individuo es responsable de todas las acciones tomadas con respecto a la evidencia digital mientras que ésta esté en su posesión.
- Cualquier agencia que sea responsable de recolectar, tener acceso, almacenar o transferir evidencia digital es responsable de cumplir con estos principios.

Además definen que los principios desarrollados para la recuperación

estandarizada de evidencia computarizada se deben gobernar por los siguientes atributos:

- Consistencia con todos los sistemas legales.
- Permitir el uso de un lenguaje común.
- Durabilidad.
- Capacidad de cruzar límites internacionales.
- Capacidad de ofrecer confianza en la integridad de la evidencia.
- Aplicabilidad a toda la evidencia forense.

15.1.8 Grabación en medios magnéticos

En general, los medios de almacenamiento magnético se basan directamente en cuatro fenómenos físicos:

- Una corriente eléctrica produce un campo magnético
- Algunos materiales se magnetizan con facilidad cuando son expuestos a un campo magnético débil. Cuando el campo se apaga, el material de desmagnetiza rápidamente. Se conocen como Materiales Magnéticos Suaves.
- En algunos materiales magnéticos suaves, la resistencia eléctrica cambia cuando el material es magnetizado. La resistencia regresa a su valor original cuando el campo magnetizante es apagado. Esto se llama Magneto-Resistencia, o efecto MR. La Magneto-Resistencia Gigante, o efecto GMR, es mucho mayor que el efecto MR y se encuentra en sistemas específicos de materiales de películas delgadas.
- Otros materiales se magnetizan con dificultad (es decir, requieren de un campo magnético fuerte), pero una vez se magnetizan, mantienen su magnetización cuando el campo se apaga. Se llaman Materiales Magnéticos Duros, o Magnetos Permanentes.

Estos cuatro fenómenos son explotados por los fabricantes de cabezas grabadoras magnéticas, que leen y escriben datos, para almacenar y recuperar datos en unidades de disco, de cinta y otros dispositivos de almacenamiento magnético.

Aplicaciones en almacenamiento de datos:

- Cabezas de Escritura : Cabezas usadas para escribir bits de información en un disco magnético giratorio, dependen de los fenómenos A y B para producir y controlar campos magnéticos fuertes.
- Cabezas de lectura : Éstas dependen de los fenómenos A, B y C y son sensibles a los campos magnéticos residuales de los medios de almacenamiento magnetizados (D).
- Medios de Almacenamiento:(Como discos de computador) Los medios de almacenamiento magnético son magnetizados de manera permanente en una dirección (Norte o Sur) determinada por el campo de escritura. Estos medios explotan el fenómeno D.

15.1.9 Escribiendo datos magnéticos

Los computadores almacenan datos en un disco giratorio en la forma de dígitos binarios, o bits transmitidos a la unidad de disco en una secuencia de tiempo correspondiente a los dígitos binarios (bits) uno y cero. Estos bits son convertidos en una onda de corriente eléctrica que es transmitida por medio de cables al rollo de la cabeza de escritura. En su forma más simple, un bit uno corresponde a un cambio en la polaridad de la corriente, mientras que un bit cero corresponde a una ausencia de cambio en la polaridad de la corriente de escritura. Entonces, un disco en movimiento es magnetizado en la dirección positiva (Norte) para una corriente positiva y es magnetizado en la dirección negativa (Sur) para un flujo de corriente negativo. En otras palabras, los unos almacenados aparecen en donde ocurre una inversión en la dirección magnética en el disco, y los ceros residen entre los unos.

Un reloj de regulación está sincronizado con la rotación del disco y existen celdas de bit para cada tick del reloj; algunas de estas celdas de bits representarán un uno (una inversión en la dirección magnética, tal como N cambiando a S o S cambiando a N) y otras representarán ceros (polaridad N constante o S constante). Una vez escritos, los bits en la superficie del disco quedan magnetizados permanentemente en una dirección o la otra, hasta que nuevos patrones sean escritos sobre los viejos. Existe un campo magnético relativamente fuerte directamente sobre la localización de los unos y su fuerza se desvanece rápidamente a medida que la cabeza de grabación se aleja. Un movimiento significativo en cualquier dirección que se aleje de un uno causa una dramática pérdida en la fuerza del campo magnético, lo que implica que para detectar bits de datos de manera confiable, es extremadamente importante que las cabezas de lectura vuelen muy cerca de la superficie del disco magnetizado.

15.1.10 Leyendo datos magnéticos

En la actualidad, las cabezas de lectura leen datos magnéticos mediante resistores magnéticamente sensitivos llamados Válvulas Spin que explotan el efecto GMR. Estas cabezas GMR/Válvula Spin son situadas muy cerca del disco de almacenamiento magnético rotatorio, exponiendo el elemento GMR a los campos magnéticos de bit previamente escritos en la superficie del disco. Si la cabeza GMR se aleja ligeramente del disco (2 o 3 millonésimas de pulgada) la intensidad del campo cae por fuera de un nivel útil, y los datos magnéticos no pueden ser recuperados fielmente. Cuando una corriente atraviesa el elemento GMR, los cambios en la resistencia (correspondientes a los cambios en los estados magnéticos que surgen de los bits escritos N y S) son detectados como cambios en el voltaje. Estas fluctuaciones de voltaje –es decir, la señal- son conducidas a las terminales sensoras del GMR. Sin embargo, el ruido eléctrico está presente en todos los circuitos eléctricos (las cabezas GMR no son la excepción), por lo que la señal combinada con el ruido de un lector GMR son enviados por medio de cables los circuitos electrónicos de la unidad de disco, para decodificar la secuencia de tiempo de los impulsos (y los espacios entre los impulsos) en unos y ceros binarios.

15.1.11 Análisis de discos

La clave de la computación forense es el análisis de discos duros, disco extraíbles, CDs, discos SCSI, y otros medios de almacenamiento. Este análisis no sólo busca archivos potencialmente incriminatorios, sino también otra información valiosa como passwords, logins y rastros de actividad en Internet.

Existen muchas formas de buscar evidencia en un disco. Muchos criminales no tienen la más mínima idea de cómo funcionan los computadores, y por lo tanto no hacen un mayor esfuerzo para despistar a los investigadores, excepto por borrar archivos, que pueden ser recuperados fácilmente. Cuando los usuarios de DOS o Windows borran un archivo, los datos no son borrados en realidad, a menos que se utilice software especial para borrar. Los investigadores forenses, utilizan herramientas especiales

que buscan archivos "suprimidos" que no han sido borrados en realidad, estos archivos se convierten en evidencia. En las siguientes secciones, se explican algunas de las características poco conocidas del almacenamiento de la información en un computador, que son explotadas por los expertos en informática forense para recuperar datos que se creían eliminados.

File Slack: Los archivos son creados en varios tamaños dependiendo de lo que contengan. Los sistemas basados en DOS, Windows 95/98/ME/XP y Windows NT/2000/2003 almacenan los archivos en bloques de tamaño fijo llamados clusters, en los cuales raramente el tamaño de los archivos coinciden perfectamente con el tamaño de uno o muchos clusters.

El espacio de almacenamiento de datos que existe desde el final del archivo hasta el final del cluster se llama "file slack". Los tamaños de los clusters varían en longitud dependiendo del sistema operativo involucrado y, en el caso de Windows 95/98/ME/XP, del tamaño de la partición lógica implicada. Un tamaño más grande en los clusters significan más file slack y también mayor pérdida de espacio de almacenamiento. Sin embargo, esta debilidad de la seguridad del computador crea ventajas para el investigador forense, porque el file slack es una fuente significativa de evidencia y pistas. El file slack, potencialmente contiene octetos de datos aleatoriamente seleccionados de la memoria del computador. Esto sucede porque DOS/Windows escribe normalmente en bloques de 512 bytes llamados sectores. Los clusters están compuestos por bloques de sectores, si no hay suficientes datos en el archivo para llenar el ultimo sector del archivo, DOS/Windows diferencia hacia arriba(los datos) completando el espacio restante con datos que se encuentran en ese momento en la memoria del sistema.

Archivo Swap de Windows: Los sistemas operativos Microsoft Windows utilizan un archivo especial como un "cuaderno de apuntes" para escribir datos cuando se necesita memoria de acceso aleatorio adicional. En Windows 95/98/ME/XP, a estos archivos se les conoce como Archivos Swap de Windows. En Windows NT/2000 se conocen como directorios de página de Windows pero tiene esencialmente las mismas características que los de Win9x. Los archivos de intercambio son potencialmente enormes y la mayoría de los usuarios de PC son inconscientes de su existencia. El tamaño de estos archivos puede extenderse desde 20MB a 200MB, el potencial de estos es contener archivos sobrantes del tratamiento de los procesadores de texto, los mensajes electrónicos, la actividad en Internet (cookies, etc), logs de entradas a bases de datos y de casi cualquier otro trabajo que haya ocurrido durante las últimas sesiones. Todo esto genera un problema de seguridad, porque el usuario del computador nunca es informado de este almacenamiento transparente. Los Archivos Swap de Windows actualmente proporcionan a los especialistas en computación forense pistas con las cuales investigar, y que no se podrían conseguir de otra manera.

Unallocated File Space: Cuando los archivos son borrados o suprimidos en DOS, Win9x, WinNT/2003, el contenido de los archivos no es verdaderamente borrado. A menos que se utilice algún software especial que ofrezca un alto grado de seguridad en el proceso de eliminación, los datos "borrados", permanecen en un área llamada espacio de almacenamiento no-asignado (Unallocated File Space). Igual sucede con el file slack asociado al archivo antes de que éste fuera borrado. Consecuentemente, siguen existiendo los datos, escondidos pero presentes, y pueden ser detectados mediante herramientas de software para el análisis de la computación forense.

15.1.12 Eliminación de datos

Hasta el momento, se ha hablado de la forma de almacenar y leer los datos en un disco de computador, sin embargo pueden darse casos legítimos en donde sea necesario destruir información sin dejar rastro alguno. En este numeral, se describen las prácticas adecuadas para la eliminación de información.

Eliminación de Datos en un Medio Magnético: Borrar de manera definitiva los datos en un medio magnético tiene toda una problemática asociada. Como se vio en una sección anterior, la información es escrita y leída aprovechando las características de magnetización de un material determinado. Sin embargo, y dependiendo del medio usado (unidades de disco, cintas, diskettes, etc.) , el proceso de eliminación total de los datos se ve afectado por diversos factores. El Departamento de Defensa de los Estados Unidos (DoD) cuenta con toda una serie de recomendaciones sobre cómo "sanitizar" un medio magnético, esto es, el proceso por el cual la información clasificada es removida por completo, en donde ni siquiera un procedimiento de laboratorio con las técnicas conocidas a la fecha o un análisis pueda recuperar la información que antes estaba grabada.[28] Aunque en un comienzo los procedimientos a seguir pueden parecer algo paranoicos, la (relativa) facilidad con la que se puede recuperar información que se creía borrada hace necesario tomar medidas extremas a la hora de eliminar datos confidenciales o comprometedores. En enero de 1995, el DoD publicó un documento, el "National Industrial Security Program Operating Manual" (NISPOM), más comúnmente referenciado como "DoD 5220.22-M", que detalla toda una serie de procedimientos de seguridad industrial, entre ellos, cómo eliminar datos contenidos en diferentes medios.

A partir de los lineamientos presentes en 5220.22-M , otro organismo estadounidense, el Defense Scurity Service, publicó una "Matriz de Sanitización y Borrado" que explica de manera práctica los pasos a seguir para remover por completo información sensitiva. En las siguientes secciones se hacen algunas precisiones técnicas, y en el apéndice A se muestra y se explica la Matriz.

Degaussing de Medios Magnéticos: La Matriz de Limpieza y Sanitización es una acumulación de métodos conocidos y aprobados para limpiar y/o sanitizar diversos medios y equipo. Cuando NISPOM fue publicado, el Rango Extendido Tipo II, Tipo III y los degaussers de Propósito Especial no existían. Esto resultaba en la necesidad de destruir todos los medios con un factor de coercividad (cantidad de fuerza eléctrica requerida para reducir la fuerza magnética grabada a cero) mayor que 750 oersteds (unidad que mide la fuerza magnetizante necesaria para producir una fuerza magnética deseada a lo largo de una superficie) y la mayoría de discos magnéticos cuando ya no fueran necesarios como soporte para una misión clasificada. Ahora, la "National Security Agency norteamericana" (NSA) ha evaluado degaussers de cinta magnética que satisfacen los requerimientos del gobierno para sanitizar cintas magnéticas de hasta 1700 oersteds.

Las cintas magnéticas se encuentran divididas en Tipos. La cinta magnética de Tipo I tiene un factor de coercividad que no excede los 350 oersteds y puede ser usada para sanitizar (degauss) todos los medios de Tipo I .La cinta magnética de Tipo II tiene un factor de coercividad entre 350 y 750 oersteds y puede ser usada para sanitizar todos los medios Tipo I y II. La cinta magnética Tipo II de Rango Extendido tiene un factor de coercividad entre 750 y 900 oersteds y puede ser usada para sanitizar todos los medios Tipo I, Tipo II y Rango Extendido. Finalmente, las cintas magnéticas Tipo III, comúnmente conocidas como cintas de alta energía (por ejemplo, cintas de 4 ó 8mm), tiene un factor de coercividad actualmente identificado como entre 750 y 1700 oersteds y puede ser usada para sanitizar todos los tipos de cintas magnéticas.

Para sanitizar (degauss) todos los medios de disco, rígidos o flexibles (por ej., diskettes, Bernoulli, Syquest y unidades de Disco Duro) se deben usar degaussers de Unidad de Disco. Para este tipo de dispositivos la NSA tiene una nueva categoría de degaussers, conocida como Degaussers de Propósito Especial.

DSS, como todas las agencias del DoD, referencia el "Information Systems Security Products and Services Catalog" como guía de sanitización de memoria y medios. NSA publica el "Information Systems Security Products and Services Catalog" entre sus productos y servicios de seguridad para sistemas de información. La lista de productos degausser (DPL) está dedica a los degaussers de discos y cintas magnéticas. La DPL hace un excelente trabajo identificando los fabricantes de degaussers y los diferentes tipos de éstos.

Eliminación de Datos en Cds: Los datos de un CD están almacenados en la parte superior del CD por medio de una capa reflectiva que es leída por un láser. Los CDs ofrecen buenas alternativas para almacenar información por largos periodos de tiempo, pero puede ser necesario destruirlos. Se mencionan algunos medios para hacer esto:

- Retiro de la lámina reflectiva : Se puede retirar la lámina con algún elemento cortante, sin embargo se debe destruir la lámina reflectiva, y aún así pueden quedar algunos rastros de datos en el policarbonato.
- Cortar en pedazos : Con una cortadora industrial de papel, el CD podría ser destruido, sin embargo, la lámina reflectiva podría separarse del CD y no ser cortada correctamente.
- Destruir el CD por medios químicos : Una posible alternativa es introducir el CD en Acetona, lo cual dejaría la lámina superior inservible, sin embargo es posible que la lámina de policarbonato aún contenga algunos rastros de información.
- Destrucción por Incineración : Probablemente es el método más rápido y eficiente, pero es realmente nocivo para el medio ambiente. El humo del policarbonato puede ser perjudicial para la salud de las personas.
- Destrucción por medio de un horno microondas : Introduciendo el CD en un microondas por unos 3 segundos puede destruir gran parte del CD, sin embargo no todas las partes serán destruidas. Este método no se recomienda, especialmente porque puede dañar el horno debido a los campos magnéticos que usa el horno y que pueden causar un cortocircuito debido a que el CD contiene metales.
- Re-escritura : Para los CDs re-escribibles, es posible volverlos a escribir de tal forma que el proceso dañe los datos. Sin embargo, no se sabe si por mecanismos especiales sea posible recuperar la información.
- Rayado Simple : A menos que uno quiera ser realmente precavido, la forma mas fácil de destruir un CD es rayando la parte superior. La razón por la que se debe rayar la parte superior es porque es esta la que mantiene los datos. Si es rayada la parte inferior es fácil recuperar la capa y corregir el problema, utilizando productos comerciales para recuperar CDs.

15.1.13 Pasos para la recolección de evidencia

El procedimiento para la recolección de evidencia varía de país a país, y por lo tanto, un análisis exacto y completo está fuera de los límites de este documento. Sin embargo, existen unas guías básicas que pueden ayudar a cualquier investigador forense:

Hardware: El hardware es uno de los elementos que se deben tener en cuenta a la hora de la recolección de evidencia, debido a que puede ser usado como instrumento, como objetivo del crimen, o como producto del crimen (por Ej. contrabando o robo), es por eso que se deben tener consideraciones especiales. Lo primero que se debe preguntar el investigador es qué partes se deben buscar o investigar.

Cuidados en la Recolección de Evidencia: La recolección de evidencia informática es un aspecto frágil del la computación forense, especialmente porque requiere de prácticas y cuidados adicionales que no se tienen en la recolección de evidencia convencional. Es por esto que:

- Se debe proteger los equipos del daño
- Se debe proteger la información contenida dentro de los sistemas de almacenamiento de información (muchas veces, estos pueden ser alterados fácilmente por causas ambientales, o por un simple campo magnético).

- Algunas veces, será imposible reconstruir la evidencia (o el equipo que la contiene), si no se tiene cuidado de recolectar todas las piezas que se necesiten.

15.1.14 Herramientas de Investigación Forense

En la actualidad existen cientos de herramientas. El uso de herramientas sofisticadas se hace necesario debido a:

- La gran cantidad de datos que pueden estar almacenados en un computador.
- La variedad de formatos de archivos, los cuales pueden variar enormemente, aún dentro del contexto de un mismo sistema operativo.
- 3. La necesidad de recopilar la información de una manera exacta, y que permita verificar que la copia es exacta.
- Limitaciones de tiempo para analizar toda la información.
- Facilidad para borrar archivos de computadores.
- Mecanismos de encriptación, o de contraseñas.

EnCase: EnCase es un ejemplo de herramientas de este tipo. Desarrollada por Guidance Software Inc, permite asistir al especialista forense durante el análisis de un crimen digital. Se escogió mostrar esta herramienta por tratarse del software líder en el mercado, el producto más ampliamente difundido y de mayor uso en el campo del análisis forense.

Algunas de las características más importantes de EnCase se relacionan a continuación:

- ***Copiado Comprimido de Discos Fuente***. Encase emplea un estándar sin pérdida (loss-less) para crear copias comprimidas de los discos origen. Los archivos comprimidos resultantes, pueden ser analizados, buscados y verificados, de manera semejante a los normales (originales). Esta característica ahorra cantidades importantes de espacio en el disco del computador del laboratorio forense, permitiendo trabajar en una gran diversidad de casos al mismos tiempo, examinando la evidencia y buscando en paralelo.
- ***Búsqueda y Análisis de Múltiples partes de archivos adquiridos***. EnCase permite al examinador buscar y analizar múltiples partes de la evidencia. Muchos investigadores involucran una gran cantidad de discos duros, discos extraíbles, discos “zip” y otros tipos de dispositivos de almacenamiento de la información. Con Encase, el examinador puede buscar todos los datos involucrados en un caso en un solo paso. La evidencia se clasifica, si esta comprimida o no, y puede ser colocada en un disco duro y ser examinada en paralelo por el especialista. En varios casos la evidencia puede ser ensamblada en un disco duro grande o un servidor de red y también buscada mediante EnCase en un solo paso.
- ***Diferente capacidad de Almacenamiento***. Los datos pueden ser colocados en diferentes unidades, como Discos duros IDE o SCSI, drives ZIP, y Jazz. Los archivos pertenecientes a la evidencia pueden ser comprimidos o guardados en CD-ROM manteniendo su integridad forense intacta, estos archivos pueden ser utilizados directamente desde el CD-ROM evitando costos, recursos y tiempo de los especialistas.
- ***Varios Campos de Ordenamiento, Incluyendo Estampillas de tiempo***. EnCase permite al especialista ordenar los archivos de la evidencia de acuerdo a diferentes campos, incluyendo campos como las tres estampillas de tiempo (cuando se creó, último acceso, última escritura), nombres de los archivos, firma de los archivos y extensiones.
- ***Análisis Compuesto del Documento***. EnCase permite la recuperación de archivos internos y

meta-datos con la opción de montar directorios como un sistema virtual para la visualización de la estructura de estos directorios y sus archivos, incluyendo el slack interno y los datos del espacio unallocated.

- ***Firmas de archivos, Identificación y Análisis***. La mayoría de las gráficas y de los archivos de texto comunes contiene una pequeña cantidad de bytes en el comienzo del sector los cuales constituyen una firma del archivo. EnCase verifica esta firma para cada archivo contra una lista de firmas conocida de extensiones de archivos. Si existe alguna discrepancia, como en el caso de que un sospechosos haya escondido un archivo o simplemente lo haya renombrado, EnCase detecta automáticamente la identidad del archivo, e incluye en sus resultados un nuevo ítem con la bandera de firma descubierta, permitiendo al investigador darse cuenta de este detalle.
- ***Análisis Electrónico Del Rastro De Intervención***. Sellos de fecha, sellos de hora, registro de accesos y la actividad de comportamiento reciclado son a menudo puntos críticos de una investigación por computador. EnCase proporciona los únicos medios prácticos de recuperar y de documentar esta información de una manera no invasora y eficiente. Con la característica de ordenamiento, el análisis del contenido de archivos y la interfaz de EnCase, virtualmente toda la información necesitada para un análisis de rastros se puede proporcionar en segundos.
- ***Soporte de Múltiples Sistemas de Archivo***. EnCase reconstruye los sistemas de archivos forenses en DOS, Windows (todas las versiones), Macintosh (MFS, HFS, HFS+), Linux, UNIX (Sun, Open BSD), CD-ROM, y los sistemas de archivos DVDR. Con EnCase un investigador va a ser capaz de ver, buscar y ordenar archivos desde estos discos concurridos con otros formatos en la misma investigación de una manera totalmente limpia y clara.
- ***Vista de archivos y otros datos en el espacio Unallocated***. EnCase provee una interfaz tipo Explorador de Windows y una vista del Disco Duro de origen, también permite ver los archivos borrados y todos los datos en el espacio Unallocated. También muestra el Slack File con un color rojo después de terminar el espacio ocupado por el archivo dentro del cluster, permitiendo al investigador examinar inmediatamente y determinar cuándo el archivo reescrito fue creado. Los archivos Swap y Print Spooler son mostrados con sus estampillas de datos para ordenar y revisar.
- ***Integración de Reportes***. EnCase genera el reporte del proceso de la investigación forense como un estimado. En este documento realiza un análisis y una búsqueda de resultados, en donde se muestra el caso incluido, la evidencia relevante, los comentarios del investigador, favoritos, imágenes recuperadas, criterios de búsqueda y tiempo en el que se realizaron las búsquedas.
- ***Visualizador Integrado de imágenes con Galería***. EnCase ofrece una vista completamente integrada que localiza automáticamente, extrae y despliega muchos archivos de imágenes como .gif y .jpg del disco. Seleccionando la "Vista de Galería" se despliega muchos formatos de imágenes conocidas, incluyendo imágenes eliminadas, en el caso de una vista pequeña. El examinador puede después escoger las imágenes relevantes al caso e inmediatamente integrar todas las imágenes en el reporte de EnCase. No es necesario ver los archivos gráficos usando software de terceros, a menos que el formato de archivo no sea muy conocido y todavía no sea soportado por EnCase.

15.1.15 RFC 3227: Pautas para la recolección y archivo de evidencia

Este documento especifica las mejores prácticas corrientes de Internet para la comunidad de Internet y la discusión de pedido y sugerencias para los mejoramientos.

Un "incidente de seguridad" como se define en RFC 2828, es un evento de seguridad de sistemas importante, en el cual la política de seguridad del sistema no se cumple o no se obedece. El propósito de este documento es proveer a los administradores de un sistema pautas sobre la recolección y

archivo de reevidencia importante para dicho incidente de seguridad.

Dicha recolección representa un esfuerzo considerable por parte del administrador del sistema. En los últimos años se han realizado grandes progresos para acelerar la reinstalación del Sistema Operativo y facilitar la reversión de un sistema a un estado "conocido" haciendo de este modo, la "Opción fácil" aun mas atractiva. Mientras tanto, poco se ha realizado para suministrar formas fáciles para archivar la evidencia (la opción difícil). Además las capacidades de memoria y de disco en aumento y el uso más difundido de cautela y de tácticas de cubrir huellas por parte de los atacantes han exacerbado el problema.

Si la recolección de evidencia se realiza correctamente, es mucho mas útil para aprehender al atacante y representa una oportunidad mucho mayor en ser admitida como hecho en un juicio.

Deberías utilizar esta pautas como una base para formular tus procedimientos de recolección de evidencia de sitio y deberías incorporar tus procedimientos de sitio en una documentación de manejo de incidente. Las pautas en este documento pueden no ser apropiadas en todas las jurisdicciones. Una vez que hayas formulado tus procedimiento de recolección de evidencia de sitio, deberías tener la aplicación de la ley para tu jurisdicción confirmando que son adecuados.

Principios directrices durante la recolección de evidencia

- Adherir a la política de seguridad de sitio y comprometer al personal de aplicación de la ley y manejo de incidente apropiados.
- Capturar la imagen tan exacta del sistema como sea posible.
- Conservar notas detalladas. Estas deberían incluir fechas y horarios. Si es posible generar un copia automática. (por ejemplo, sobre los sistema Unix, se puede utilizar el programa "Script", sin embargo, el archivo output que se genera no debería ser para medios, es decir parte de la evidencia). Las notas y las impresiones deberían ser firmadas y fechadas.
- Notar la diferencia entre el sistema real y el UTC. Para cada marca de tiempo provista, indicar si se utiliza UTC y hora local.
- Estar preparado para testificar (tal vez años más tarde) trazando todas las acciones que tomaste y en que momentos. Las notas detalladas serán vitales.
- Minimizar los cambios a los datos a medida que los van recolectando. Esto no esta limitado a los cambios de contenido, tu deberías evitar la actualización de archivos o tiempos de acceso de directorio.
- Borrar caminos externos para cambiar.
- Cuando te enfrentes a una elección entre recolección y análisis, tu deberías hacer la recolección primeo y el análisis después.
- Aunque escasamente necesita establecerse, tus procedimientos deberían ser implementables. Como con cualquier aspecto de un política de respuesta a un incidente, los procedimiento deberían ser evaluados para asegurar la viabilidad, particularmente en una crisis, Si es posible los procedimientos debería ser automatizados por razones de velocidad y precisión. Ser metódicos.
- Para cada dispositivo, debería adoptarse un enfoque metódico que siga las directivas establecidas de tu procedimiento de recolección. La velocidad será a menudo critica, por eso donde exista un numero de dispositivos que requieran examen puede ser apropiado extender el trabajo entre tu equipo para recolectar la evidencia en paralelo. Sin embargo, en una recolección de sistema simple debería realizarse paso por paso.
- Proceder desde lo volátil a lo menos volátil
- Deberías hacer una copia a nivel de bit de los medios del sistema. Si deseas hacer un análisis

forense, deberías hacer una copia a nivel de bit de tu copia de evidencia para tal fin, ya que tu análisis alterará casi seguramente el tiempos de acceso de los archivos.

- Evitar hacer forensics sobre la copia de evidencia.

Orden de volatilidad

Cuando recolectes la evidencia deberías proceder desde los volátil a lo menos volátil. Aquí hay un ejemplo de orden de volatilidad para un sistema típico.

- Registros, Cache.
- Tabla de ruta. ARP Cache, Tabla de Proceso, Núcleo de estadísticas, memoria
- Sistema de Archivo temporarios
- Disco
- Datos de monitoreo y log's remotos que es relevante al sistema en cuestión
- Configuración física, topología de red.
- Medio de Archivos.

Cosas para evitar

- Es demasiado fácil destruir la evidencia, aún desapercibidamente.
- No cerrar hasta que hayas completado la recolección de evidencia.
- Se puede perder mucha evidencia y el atacante puede haber alterado los startup/shutdown scripts/services para destruir evidencia.
- No confíes en los programas sobre el sistema. Conduce tu evidencia reuniendo programas a partir de medios protegidos apropiadamente (ver abajo)
- No ejecutes programas que modifiquen el tiempo de acceso de los archivos sobre el sistema (por ejemplo: "tar" o "xcopy")
- Cuando elimines los caminos externos para el cambio, observa que simplemente desconectando o filtrando desde la red puede accionar "deadman switches" que detectan cuanto están fuera de la red y limpian la evidencia.

Consideraciones privadas

Respetar las reglas de privacidad y las directivas de tu compañía y de tu jurisdicción legal. En particular, asegúrate de que ninguna información recolectada junto con la evidencia que estás buscando está disponible a cualquiera que normalmente no tuviera acceso a esta información. Esto incluye acceso a archivos log (que pueden revelar modelos de comportamiento del usuario) así como también archivos de datos personales.

No te entrometas en la privacidad de la gente sin una justificación convincente. En particular, no recolectes información de áreas a las que tu normalmente no tienes porque acceder (tales como almacenamiento de archivos personal) al menos que tengas indicios suficientes de que existe un incidente real.

Asegúrate de que tengas el apoyo de los procedimientos establecidos de tu compañía en seguir los pasos que tú haces para recolectar la evidencia de un incidente.

Consideraciones Legales

La Evidencia de computadora necesita ser:

- *Admisible*: debe estar de acuerdo con ciertas reglas legales antes de ser puesta ante una corte.
- *Auténtica*: Debe ser posible ligar positivamente el material de evidencia al incidente.
- *Completa*: Debe contar la historia completa y n solamente una perspectiva particular.
- *Confiable*: No debe existir nada acerca de cómo la evidencia fue recolectada y posteriormente manejada que ponga en duda acerca de su autenticidad y veracidad.
- *Creíble*: Debe ser fácilmente creíble y comprensible por una corte.

Herramientas necesarias

Deberías tener los programas que necesitas para realizar la recolección de evidencia y análisis forense en medios de solo lectura (por Ej. Un CD). Deberías tener preparado un set de herramientas para cada uno de los sistemas operativos que manejes antes de tener que usarlo.

Tu test de herramientas debería incluir lo siguiente:

- Un programa para procesos de examen (por Ej. "ps")
- Programas para estado de sistemas de examen (por Ej. "showrev", "ifconfig", "netsat", "arp").
- Un programa para hacer copias bit-a-bit (por Ej. "dd", "SafeBack").
- Programas para generar sumas de control y Firmas (por Ej. "shalsum", a cheksum-enabled "dd", "safeBack", "pgp").
- Programas para generar imágenes esenciales y para examinarlas (por Ej. "goore", "gdb").
- Escritura/manuscritos para la recolección de evidencia automatizada (por Ej. The Coroner's toolkit (FAR 1999)

15.2 ANÁLISIS FORENSE EN LINUX

La ciencia forense es metódica y se basa en acciones premeditadas para reunir pruebas y analizarlas. La tecnología, en caso de análisis forense en sistemas informáticos, son aplicaciones que hacen un papel importante en reunir la información y pruebas necesarias. La escena del crimen es el ordenador y la red a la cual éste está conectado. El objetivo de un análisis forense informático es realizar un proceso de búsqueda detallada para reconstruir a través de todos los medios el log de acontecimientos que tuvieron lugar desde el momento cuando el sistema estuvo en su estado integro hasta el momento de detección de un acceso no autorizado.

Esa tarea debe ser llevada acabo con máxima cautela, asegurándose que se conserva intacta, a la mayor medida posible, la información contenida en el disco de un sistema comprometido, de forma similar que los investigadores policiales intentan mantener la escena del crimen intacta, hasta que se recogen todas las pruebas posibles.

El trabajo de un investigador forense es necesario para ofrecer un punto de partida fundamental para los investigadores policiales, ofreciéndoles pistas sólidas, así como pruebas para su uso posterior.

Los ordenadores y las redes pueden verse involucrados en un crimen informático siendo las herramientas utilizadas para cometer el crimen, las víctimas del crimen o ser utilizadas para propósitos incidentales relacionados con el crimen. El Análisis Forense de Sistemas comprende el proceso de extracción, conservación, identificación, documentación, interpretación y presentación de

las evidencias digitales de forma que sean legalmente aceptadas en cualquier proceso legal, proporcionando las técnicas y principios que facilitan la investigación del delito.

Linux es un entorno ideal en el cual realizar tareas de análisis forense pues está dotado de gran variedad de herramientas que facilitan todas las etapas que se deben llevar a cabo en la realización de un análisis exhaustivo de un sistema comprometido.

Otra ventaja de GNU/Linux para investigadores forenses es la capacidad del interfaz "loopback", que permite montar un fichero que contiene una imagen del disco (obtenida con *dd*) dentro del sistema de ficheros de la estación de análisis

Los pasos para empezar la investigación de un incidente son diferentes en cada caso. El investigador debe tomar decisiones basándose en su experiencia y el "sexto sentido" para llegar al fondo del asunto. No es necesario seguir pasos determinados, ni su orden es importante a veces.

Puede que algunos pasos básicos sean más de lo que hace falta y también puede ser que estos sean insuficientes para solucionar el problema. Los pasos básicos pueden concluir en localizar todas las huellas y eventos que se produjeron. Y en supuestos los pasos básicos no han desvelado la situación, se debe recurrir a llevar acabo un análisis profundo o de-compilación de las aplicaciones encontradas durante la búsqueda. Estas aplicaciones pueden ser escritas totalmente desde cero y protegidas, pero en la mayoría de los casos son aplicaciones utilizadas de forma común, que circulan por la red, estén o no estén protegidas. Cuando hablamos de protección de ficheros podemos hablar sobre técnicas de confusión, ofuscación y compresión (Ver apéndice A para detalles).

Una vez que el Administrador del sistema tenga sospechas de que su sistema haya sido violado, y que no existan pruebas que indiquen lo contrario como por ejemplo resultados de chequeos de integridad realizados por por alguna herramienta como Tripwire o AIDE (Advanced Intrusion Detection Environment), tiene que considerar que efectivamente el sistema ha sido violado. Desde aquél momento, es necesario tener máximo cuidado para evitar que se produzca cualquier alteración de la "escena del crimen".

Hay varios tipos de pruebas que oculta el sistema, con diferentes niveles de volatilidad, en lugares como registros del procesador, estructura de datos en la memoria, swap, estructuras de datos de red, contadores, procesos de usuario en memoria y stacks, cache del file system, el file system y etc.

Será muy difícil o casi imposible de reunir toda esa información en el preciso momento que el intruso está operando, por lo tanto necesitamos prescindir de ella y reunir aquella información, que se recoge con mayor facilidad antes de llegada de un especialista forense que determinará el método de entrada, actividad de intrusos, identidad y origen de intrusos, duración de compromiso, posiblemente lo bastante para localizarles). En otras palabras ¿Cómo? ¿Qué? ¿Quién? ¿De dónde? ¿Cuando?

La opción más fácil es de evitar que las cosas no cambien - cerrar el sistema o suspender su funcionamiento. Normalmente los sistemas Unix se cierran con el comando shutdown. Eso se hace para asegurarse que todos los servicios han finalizado de forma limpia, todos los ficheros cache y buffers de sistemas están flusheados y los usuarios están notificados. Este procedimiento es perfecto para sistemas intactos, pero en un sistema afectado, esa acción, lo más seguro que borre alguna información de interés. Hubo casos cuando los intrusos programaban sistemas para eliminar algunos ficheros en la máquina cuando el interfaz de red se deshabilitase (es decir, cuando el cable de conexión haya sido desconectado) o cuando el procedimiento de un shutdown normal haya sido activado.

Para prevenir esas modificaciones del sistema de ficheros es mejor sacar el cable de electricidad del enchufe (Sí, sí, lo has leído bien). Hay que estar informados que puede ser que alguna información en la memoria o información del cache no guardada en el disco puede ser eliminada como estado de red, procesos ejecutándose en la memoria, accesos a memoria kernel, contenido de registros swap, etc.

Para ello antes de sacar el cable del enchufe puede hacer lo siguiente; ejecutar varios comandos antes de apagar de forma "bruta" el sistema. Se debe hacerlo en una sesión script.

```
script -a fichero
```

También se pueden utilizar algunas herramientas para obtener información de utilidad:

- **last, w, who** - Obtener el listado de usuarios actuales en el sistema, logins anteriores, etc.
- **ls** - Obtener el listado largo (ls -lat) de ficheros en lugares sospechosos, los home directories, directorio /dev, directorio /root, etc.
- **ps** - Obtener el listado largo de todos los procesos incluidos aquellos sin ttys (e.g., ps auxwww y ps elfwww -- añadir más flags w si el listado se acorta).
- **lsof** - Obtener un listado completo de descriptores de ficheros, que puede mostrar algunos backdoors, sniffers, eggdrop IRC bots, redireccionadores de puertos para VNC, etc.
- **find** - Identificar todos ficheros corrientes, directorios modificados desde la fecha de último acceso no autorizado, o que pertenecen al usuario desde cuya cuenta se sospecha que fue originado el ataque. La utilidad "***find***" modifica el i-node "last accessed" con el timestamp actual, entonces no debe utilizar esta utilidad para barrer el sistema de ficheros, si todavía quiere saber cuales son los ficheros accedidos por el atacante si el sistema de ficheros está montado en modo lectura y escritura.
- **ltrace, strace, truss (SunOS 5)** - Ver últimos accesos a ficheros de configuración de "rootkit", ejemplo: Examinar el fichero /bin/ls trucado.
- **nc (NetCat)** – Permite transferir vía red la información del equipo afectado a otro sistema en el cual realizar el análisis. Ej.

  En el sistema de análisis de ejecutará: `nc –l –p puerto > fichero de salida`

  En el sistema comprometido se ejecutará: `cat /etc/passwd | nc maquina de análisis puerto –w 2`
- **mount** – Muestra los sistemas de archivos que se encuentran “montados”
- **fdisk** – muestra las particiones existentes en cada unidad de disco, estén o no “montadas” en ese momento
- **dd** – Permite crear imágenes (copias bit a bit) de los sistemas de archivos. Ej. `dd if=/dev/fd0 of=/tmp/disco.img`

  La ejecución del comando `dd if=/dev/zero of=/dev/fd0` permite inicializar completamente el dispositivo sobre el que se va a almacenar la imagen.

Si no hay seguridad de que las utilidades comunes estén mostrando la verdadera situación, se debe utilizar aplicaciones alternativas. Los módulos de kernel cargables (LKM) o librerías dinámicas, pueden estar alteradas para proporcionar información falsa. En estos casos se debe utilizar binarios compilados de forma estática desde un toolkit como Fire Biatchux o descargados de la web de incident-responce.org.

Se debe cuestionar permanentemente la información que el servidor está proporcionando. Sería aconsejable y mucho más fácil y seguro si simplemente el disco duro fuese extraído de la máquina afectada y fuese montado en modo sólo lectura en una estación de análisis similar al servidor atacado.

Se debe también considerar montar el disco como noexec y nodev para asegurarse que no pueda ser ejecutada ninguna aplicación desde el disco duro comprometido y que se ignoren los ficheros de dispositivos en el directorio /dev. Ej. `mount –o ro,noexec,nodev /dev/hda1 /t`

Si no disponemos de un equipo dedicado para el análisis, ni decidimos llevarlo por la vía oficial, pero tenemos el interés de conocer los detalles del ataque y el equipo tiene un CD-ROM, existen herramientas forenses que permiten el estudio post-mortem "en situ". Un buen ejemplo de herramienta de este tipo es Fire-Biatchux que permite tener de forma instantánea un entorno de análisis seguro,

proporcionando copias íntegras de todos los binarios necesarios de GNU/Linux y Solaris para llevar acabo la investigación.

Análisis con Autopsy

Autopsy es un frontal Web que permite realizar operaciones de análisis forense sirviendo como interfaz gráfico del popular juego de herramientas forenses The Sleuth Kit (TSK). TSK es un referente en el mundo del análisis forense mediante la línea de mandatos, y que permite a los investigadores lanzar auditorías forenses no intrusivas en los sistemas a investigar. Probablemente la mayor concentración de uso de TSK la tengamos en dos tipos de análisis: análisis genérico de sistemas de archivos y líneas temporales de ficheros.

TSK tiene una larga historia, ya que emplea el mismo código que The Coroner's Toolkit (TCT), de Wietse Venema y Dan Farmer, y puede ser empleado en plataformas Linux, Mac OS X, CYGWIN, OpenBSD, FreeBSD y Solaris. Es posible su instalación en Windows, aunque es poco frecuente, ya que la mayoría de suites forenses suelen estar disponibles como live CDs de Linux, aprovechando no sólo la abundancia de aplicaciones libres, sino la integración de las mismas.

Para facilitar la labor de los investigadores, TSK y Autopsy suelen ir de la mano, lo que hace que no sea necesario invocar constantemente la línea de comandos cuando queremos inspeccionar una imagen.

Una vez el disco ha sido sacado de la máquina, debe ser almacenado de forma segura para poder ser utilizado como prueba a posteriori en un juicio. Si no se almacena de forma correcta, no será la primera vez que la investigación no pueda seguir o las pruebas se declaren nulas por parte de un juez o jurado por contaminación o tratamiento indebido.

Es necesario tomar notas de lo que se hace con el disco duro, y a que hora, almacenándolo en una ubicación segura como por ejemplo una caja fuerte. Es recomendable que siempre que se trabaje con el medio original esté acompañado por un colega, para que conste a los efectos legales y su testimonio pueda ser confirmado por alguien con un nivel de conocimientos similar.

Las copias deben ser hechas bit-por-bit, es decir será necesario hacer imágenes del disco. La investigación debe ser llevada sobre una copia y nunca sobre el disco original. Se debe hacer tres copias del disco duro original. Sobre todas las copias y original se debe llevar acabo una verificación criptográficas - un checksum MD5.

Esté analizando el sistema con las herramientas forenses específicas o no, se debe de seguir los mismos pasos básicos siempre para prepararse para el análisis completo del sistema.

- En algunos casos es necesario fotografiar el equipo afectado antes de mover cualquier detalle del mismo. Eso puede ser necesario como prueba del incidente en casos que posiblemente puedan acabar en una sala de juicio. En otros casos será necesario documentar los detalles de todos los componentes del sistema como valores ID de los dispositivos SCSI, por ejemplo y etc.
- Empezar haciendo apuntes detallados en el cuaderno. Tener bien detallados apuntes con la fecha y hora del inicio y fin de cualquier trabajo realizado será muy útil durante y al final del análisis. Es importante que todos los hechos pertinentes al caso durante la preparación, recuperación y análisis de las pruebas sobre un ataque, estén perfectamente documentados. Estas notas servirán como base para poder desarrollar un informe detallado de incidencia que se debe preparar una vez terminado el análisis. Este documento deberá servir como una prueba del incidente o ataque. Siempre que se realiza cualquier apunte al cuaderno, el asistente debe tener un completo conocimiento y entendimiento de lo que ha sido apuntado.

- ¡Haga 3 imágenes del disco duro entero y trabaje con copias, y no con el original! En el peor caso que tenga que trabajar con el disco original correría el riesgo de hacer una pequeña equivocación que eliminaría las huellas de forma parcial o total. El original debe ser almacenado en una caja fuerte para estar totalmente seguros que el contenido del dispositivo no esté alterado o eliminado. Para ello generaríamos verificaciones de integridad MD5, las imprimiremos en etiquetas y éstas las pegaremos en el original y en las copias. La etiqueta del original debe contener la fecha y hora de extracción del disco del sistema comprometido, y la fecha y hora de almacenamiento del disco en la caja fuerte. Las etiquetas de las 3 copias deben tener letras de alfabeto griego (como ejemplo).
- A la hora de verificar los MD5 del disco y de la/s cintas si al menos un único byte ha sido modificado a la hora de realizar la duplicación o backup, el checksum no coincidirá. Eso puede estar causado por un sector dañado en el disco duro o en la cinta, puede que haya hecho una copia del sistema "vivo" (no montado read-only), o haya hecho la copia de una partición incorrecta.

The Coroner's Toolkit

The Coroner's Toolkit (o el "TCT") es un suite de aplicaciones escritas por Dan Farmer y Wietse Venema para un curso organizado por IBM sobre un estudio forense de equipos comprometidos.

Las aplicaciones más importantes del suite son:

- **grave-robber** - Una utilidad para capturar información sobre inodes, para luego pueda ser procesada por el programa mactime del mismo toolkit.
- **unrm y lazarus** - Herramientas para la recuperación de archivos borrados (logs, RAM, swap, etc.). Estas aplicaciones identifican y recuperan la información oculta en los sectores del disco duro.
- **mactime** - El programa para visualizar los ficheros/directorios su timestamp MAC (Modification, Access, y Change).

De todas esas herramientas, las más útiles y interesantes son grave-robber y mactime. unrm y lazarus son buenas si se tiene mucho tiempo y espacio libre en el disco, ya que el programa necesita identificar información en los sectores del disco para recuperar los ficheros (logs, fuentes, etc..) borrados por los intrusos.

La función más básica de grave-robber es de escanear algunas o todas sistemas de ficheros con función stat() para obtener información de los inodes. Grave-robber crea en la carpeta /data un directorio llamado como el nombre del host de la máquina y allí almacena los inodes, dentro del fichero body. El programa mactime luego ordena los resultados y los muestra: según el tiempo, cual de los tres timestamps corresponde, muestra el tipo de fichero, tamaño y a quién pertenece junto con el path.

Desde el listado, podremos sacar algunas conclusiones sobre la actividad que ha ejercido el intruso/los intrusos durante el tiempo que estuvieron dentro del sistema. Eso puede incluir instalación de caballos de Troya, backdoors, sustitución de ficheros legítimos del sistema operativo, descarga de herramientas, modificación de las librerías del sistema o instalación de rpm's/deb's/pkg's etc. También podemos ver desde aquí la creación de directorios ocultos, ejecución de los comandos de sistema operativo, compilación y ejecución de aplicaciones. Toda esa información que nunca se almacena de forma directa, puede ser extraída de la información que da mactime.

15.3 ANÁLISIS FORENSE EN WINDOWS

Un plan de respuesta a incidentes ayuda a estar preparado y a saber cómo se debe actuar una vez se haya identificado un ataque. Constituye un punto clave dentro de los planes de seguridad de la información, ya que mientras que la detección del incidente es el punto que afecta a la seguridad del sistema, la respuesta define cómo debe reaccionar el equipo de seguridad para minimizar los daños y recuperar los sistemas, todo ello garantizando la integridad del conjunto.

El plan de respuesta a incidentes suele dividirse en varias fases, entre las que destacan:

1) respuesta inmediata, para evitar males mayores, como reconfigurar automáticamente las reglas de los cortafuegos o inyectar paquetes de RESET sobre conexiones establecidas
2) investigación, para recolectar evidencias del ataque que permitan reconstruirlo con la mayor fidelidad posible
3) recuperación, para volver a la normalidad en el menor tiempo posible y evitar que el incidente se repita de nuevo
4) creación de informes, para documentar los datos sobre los incidentes y que sirvan como base de conocimiento con posterioridad, para posibles puntos de mejora y como información para todos los integrantes de la organización. De manera adicional, se hacen necesarios los informes por posibles responsabilidades legales que pudieran derivarse.

Suelen distinguirse dos tipos de evidencia. La primera, conocida como volátil, comprende la información que desaparece cuando un sistema informático pierde la alimentación eléctrica. Por consiguiente, en esta categoría se incluye tanto la memoria RAM , los procesos activos y usuarios conectados, así como la información de la red y aplicaciones a la escucha en todos los puertos en el momento de la interrupción. El segundo tipo de evidencia es la de disco, que puede ser capturada sin necesidad de tener la máquina encendida, simplemente con acceso físico al disco.

Dada su fragilidad, y que puede perderse con mucha facilidad, este tipo de evidencia es la primera que debe ser recogida. Por tanto, en la medida de lo posible, la máquina objeto del análisis no debería ser apagada o reiniciada hasta que se haya completado el proceso. Si se ha ensayado con anterioridad o es realizado por un especialista, no debería llevar más de unos pocos minutos.

La teoría señala que la herramienta perfecta para esta tarea no debería apoyarse en absoluto en el sistema operativo objeto del análisis, pues éste podría haber sido fácilmente manipulado para devolver resultados erróneos. Sin embargo, a pesar de que tales herramientas existen, como la tarjeta PCI Tribble, son herramientas hardware, que necesitan estar instaladas en la máquina antes de la intrusión, ataque o análisis de la misma. Evidentemente, este escenario sólo es factible para máquinas que procesan información especialmente sensible, cuyo hardware puede ser fácilmente controlado.

En el resto de casos, la inmensa mayoría, hay que conformarse con utilizar herramientas software y limitar el proceso de recolección de información a los mínimos pasos posibles, con el fin de generar el menor impacto posible sobre la máquina analizada.

Existen varias distribuciones especializadas en análisis forense, pero quizá las más adecuadas sean Helix, de la empresa e-fense, especializada en análisis forense (www.e-fense.com) y Back–Track, orientada también a pruebas de intrusión (www.remote-exploit.org/backtrack.html). Ambas son de libre distribución y directamente utilizables tanto en entornos Windows como Unix, por lo que sólo es necesario introducir el CD en la unidad y comenzar a trabajar. Se distribuyen en forma de CD autoarrancable (Live CD), de forma que también es posible cargar un Sistema Operativo nuevo, absolutamente confiable, para realizar la segunda parte del proceso de recogida de evidencias.

Otra opción, exclusiva para entornos Microsoft, es el kit gratuito Forensic Acquisition Utilities (FAU)

disponible en www.gmgsystemsinc.com/fau. FAU contiene binarios compilados estáticamente, de forma que hagan el mínimo uso posible del sistema, el cual, debe recordarse, ha sido comprometido y no es fiable.

15.3.1 Sistema de Archivos

Los sistemas de archivos (filesystem en inglés), estructuran la información guardada en una unidad de almacenamiento (normalmente un disco duro de una computadora), que luego será representada ya sea textual o gráficamente utilizando un gestor de archivos. La mayoría de los sistemas operativos poseen su propio sistema de archivos.

Lo habitual es utilizar dispositivos de almacenamiento de datos que permiten el acceso a los datos como una cadena de bloques de un mismo tamaño, a veces llamados sectores, usualmente de 512 bytes de longitud. El software del sistema de archivos es responsable de la organización de estos sectores en archivos y directorios y mantiene un registro de qué sectores pertenecen a qué archivos y cuáles no han sido utilizados. En la práctica, un sistema de archivos también puede ser utilizado para acceder a datos generados dinámicamente, como los recibidos a través de una conexión de red (sin la intervención de un dispositivo de almacenamiento).

Los sistemas de archivos tradicionales proveen métodos para crear, mover, renombrar y eliminar tanto archivos como directorios, pero carecen de métodos para crear, por ejemplo, enlaces adicionales a un directorio o archivo (enlace duro en Unix) o renombrar enlaces padres (en Unix).

El acceso seguro a sistemas de archivos básicos puede estar basado en los esquemas de lista de control de acceso o capacidades. Las listas de control de acceso hace décadas que demostraron ser inseguras, por lo que los sistemas operativos experimentales utilizan el acceso por capacidades. Los sistemas operativos comerciales aún funcionan con listas de control de acceso.

Generalmente un sistema de archivos tiene directorios que asocian un nombre de archivo a cada archivo, usualmente conectando el nombre de archivo a un índice en una tabla de asignación de archivos de algún tipo —como FAT en sistemas de archivos MS-DOS o los inodos de los sistemas Unix.

La estructura de directorios suele ser jerárquica, ramificada o "en árbol", aunque en algún caso podría ser plana. En algunos sistemas de archivos los nombres de archivos son estructurados, con sintaxis especiales para extensiones de archivos y números de versión. En otros, los nombres de archivos son simplemente cadenas de texto y los metadatos de cada archivo son alojados separadamente.

En los sistemas de archivos jerárquicos, usualmente, se declara la ubicación precisa de un archivo con una cadena de texto llamada "ruta" —o path en inglés—. La nomenclatura para rutas varía ligeramente de sistema en sistema, pero mantienen por lo general una misma estructura. Una ruta viene dada por una sucesión de nombres de directorios y subdirectorios, ordenados jerárquicamente de izquierda a derecha y separados por algún carácter especial que suele ser una barra ('/') o barra invertida ('\') y puede terminar en el nombre de un archivo presente en la última rama de directorios especificada.

NTFS (New Technology File System) es un sistema de archivos diseñado específicamente para Windows NT (incluyendo las versiones Windows 2000, Windows 2003, Windows XP y Windows Vista), con el objetivo de crear un sistema de archivos eficiente, robusto y con seguridad incorporada desde su base. También admite compresión nativa de ficheros, cifrado (esto último sólo a partir de Windows 2000) e incluso transacciones (sólo a partir de Windows Vista). Está basado en el sistema de archivos HPFS de IBM/Microsoft usado en el sistema operativo OS/2, y también tiene ciertas influencias del formato de archivos HFS diseñado por Apple.

Todo lo que tiene que ver con los ficheros, se almacena en forma de metadatos. Esto permitió una

fácil ampliación de características durante el desarrollo de Windows NT. un ejemplo lo hallamos en la inclusión de campos de indexado añadidos para posibilitar el funcionamiento de Active Directory.

Los nombres de archivo son almacenados en Unicode (UTF-16), y la estructura de ficheros en árboles-B, una estructura de datos compleja que acelera el acceso a los ficheros y reduce la fragmentación, que era lo más criticado del sistema FAT.

Se emplea un registro transaccional (journal) para garantizar la integridad del sistema de ficheros (pero no la de cada archivo). Los sistemas que emplean NTFS han demostrado tener una estabilidad mejorada, que resultaba un requisito ineludible considerando la naturaleza inestable de las versiones más antiguas de Windows NT. Sin embargo, a pesar de lo descrito anteriormente, este sistema de archivos posee un funcionamiento prácticamente secreto, ya que Microsoft no ha liberado su código como hizo con FAT.

Gracias a la ingeniería inversa, aplicada sobre el sistema de archivos, se desarrolló controladores como el NTFS-3G que actualmente proveen a sistemas operativos GNU/Linux, Solaris, MacOS X o BSD, entre otros, de soporte completo de lectura y escritura en particiones NTFS.

15.3.2 Tipos de Inicio de sesión

Los sucesos de inicio de sesión en un sistema Windows se generan en los controladores de dominio para la actividad de cuentas de dominio y en los equipos locales para la actividad de cuentas locales. Si están habilitadas ambas categorías de directiva, los inicios de sesión que utilizan una cuenta de dominio generan un suceso de inicio o cierre de sesión en la estación de trabajo o servidor, y generan un suceso de inicio de sesión de cuenta en el controlador de dominio. La categoría de inicio de sesión en Windows registrará la entrada con un evento ID 528 (Inicio de sesión) que contendrá una serie de datos importantes, como son el tipo de entrada y el ID de inicio de sesión. También podría devolver un ID 529 que se refiere al fallo de inicio de sesión. Dependiendo del inicio de sesión que hagamos en la máquina, ya sea a través de recursos compartidos, de forma remota o de forma física, Windows registrará ese inicio de sesión con una numeración u otra. Algunos tipos de inicio de sesión son:

- Tipo 2. Interactivo. Entrada a un sistema desde la consola (teclado)
- Tipo 3. Red. Entrada al sistema a través de la red. Por ejemplo con el comando net use, recursos compartidos, impresoras, etc.
- Tipo 4. Batch. Entrada a la red desde un proceso por lotes o script programado.
- Tipo 5. Servicio. Cuando un servicio arranca con su cuenta de usuario.
- Tipo 7. Unlock. Entrada al sistema a través de un bloqueo de sesión.
- Tipo 10. Remote Interactive. Cuando accedemos a través de Terminal Services, Escritorio Remoto o Asistencia Remota.

15.3.3 Estructura de la papelera de reciclaje

Al contrario de lo que se piensa mucha gente, cuando un archivo se borra de una computadora, realmente no se borra. Los archivos se modifican por decirlo de alguna manera, para que el sistema operativo no los vea. Windows utiliza un almacén para los archivos eliminados llamado Papelera de Reciclaje. La existencia de este almacén permite que un usuario pueda recuperar la información, si ésta ha sido borrada accidentalmente por ejemplo. Cuando Windows da orden de eliminar cierto archivo o directorio, la información se guarda en expedientes, por si el usuario se arrepiente y quiere recuperar sus datos. El archivo que contiene esta información se llama INFO2 y reside en el directorio de la Papelera de Reciclaje, es decir, está dentro de la Papelera. Es necesario explicar cómo funciona la Papelera de Reciclaje antes de que discutamos las estructuras del archivo INFO2. Cuando un usuario suprime un archivo a través del explorador de Windows, una copia del archivo se mueve al

almacén de la Papelera de Reciclaje. La localización de este directorio es distinta, dependiendo de la versión de Windows que tengamos. En versiones NT/XP/2003, el archivo INFO2 se encuentra en el siguiente directorio: `C:\Recycler\<USER SID>\INFO2`, Windows 95/98/ME en `C:\Recycled\`

Un ejemplo en de la estructura de dos usuarios en un Windows XP:

- C:\RECYCLER\S-1-5-21-1417001333-343818398-1801674531-1004
- C:\RECYCLER\ S-1-5-21-1417001333-343818398-1801674531-500

Si entramos en la carpeta del usuario en la ruta C:\RECYCLER\S-1-5-21-1417001333-343818398-1801674531-500> Y ejecutamos ***Rifiuti*** (Herramienta de análisis forense para la papelera de reciclaje. También está disponible para Linux), `rifiuti INFO2>e:\analisis.txt` Automáticamente se genera el archivo "*analisis.txt*" donde podremos saber: la fecha y hora de eliminación, la ruta de donde se eliminaron, y el tamaño de todos los archivos que se enviaron a la papelera de reciclaje

Cuando eliminamos un fichero, Windows lo renombra siguiendo este parámetro:

D <Unidad raíz del sistema> <número> .Extensión del archivo

Es decir, que si nosotros quisiésemos eliminar el archivo Contabilidad.doc y lo mandásemos a la Papelera de Reciclaje, Windows lo renombraría de la siguiente manera: DC1.Doc. Si borrásemos otro archivo, a éste nuevo archivo se le pondría el número 2, y así sucesivamente.

Si al menos un archivo se ha movido a la Papelera de Reciclaje, el archivo INFO2 existirá. Cuando se vacía la Papelera de Reciclaje, el contenido del archivo INFO2 se limpiará, y el número se establecerá de nuevo a 1. Es decir, el archivo INFO2 se suprime y se crea un nuevo y vacío INFO2.

15.3.4 Archivo de registro

Windows define al registro como una base de datos jerárquica central utilizada en todas las versiones de Windows, con el fin de almacenar información necesaria para configurar el sistema para uno o varios usuarios, aplicaciones y dispositivos hardware. El registro contiene información que Windows utiliza como referencia constantemente, como por ejemplo los perfiles de usuario, las aplicaciones instaladas, los parches o HotFixes instalados, etc... Los archivos del registro de Windows se almacenan en archivos binarios, es decir, que si abrimos estos ficheros con un editor de texto, como puede ser notepad, no podremos leerlo. El registro se puede manipular desde muchos medios, tanto en línea de comandos como por la propia interfaz gráfica de Windows. Evidentemente la forma más fácil de manipular el registro es de forma gráfica. Sólo tendríamos que ejecutar la herramienta regedit. Viene a reemplazar los obsoletos Win.ini y System.ini , aunque estos todavía siguen siendo usados por los programas de 16 bits.

Esta base es consultada durante el arranque y luego varias veces en una sesión típica. Allí se establece desde qué programa abrirá cada tipo de archivo o los parámetros de la conexión con Internet hasta el color de fondo del Escritorio y el mapa del teclado. Las versiones 95 y 98 usan un Registro prácticamente idéntico, pero la forma en que corrigen sus errores y lo preservan es muy diferente. El 95 guardaba una sola copia de respaldo del Registro con cada arranque exitoso, en dos archivos llamados user.da0 y system.da0 (es un cero, no una letra O). El 98 convoca al programa scanreg.exe en cada inicio para detectar y corregir errores y crear un backup con cada arranque exitoso. Sin embargo, estas copias se guardan ahora como archivos .cab en la carpeta Sysbckup de Windows. Todavía más importante, almacena cinco copias buenas de cinco arranques sucesivos (lo que normalmente equivale a cinco días). El primero se llama rb000.cab y el más reciente, rb004.cab . Los .cab son archivos comprimidos, como los .zip , y se puede ver o extraer su contenido con la interfaz de Windows o con programas como el WinZip. El 98 puede guardar más de cinco copias de respaldo. Si quiere aumentar este valor -es aconsejable- busque el archivo scanreg.ini y eleve el valor

de MaxBackupCopies a, por ejemplo, 10.

El Registro está organizado en una estructura jerárquica compuesta por subárboles con sus respectivas claves, subclaves y entradas. Las claves pueden contener subclaves y éstas, a su vez, pueden contener otras subclaves. Generalmente, la mayor parte de la información del Registro se almacena en disco y se considera permanente, aunque en determinadas circunstancias hay datos que se almacenan en claves llamadas volátiles, las cuales se sobrescriben cada vez que se inicia el sistema operativo. Toda información relativa al sistema operativo y al PC se encuentra recogida en los archivos del sistema del registro de Windows, los cuales se localizan en %systemroot %\system32\config, y atienden a los nombres siguientes:

- SECURITY
- SOFTWARE
- SYSTEM
- SAM
- DEFAULT

El registro de Windows se crea durante la instalación del sistema operativo. Está formado por seis apartados, llamados HKEYS (llaves), perfectamente estructurados y donde se guarda importante información de cada aplicaciín o dispositivo conectado a nuestro ordenador, además de todas las claves de acceso. Los apartado son:

- HKEY_LOCAL_MACHINE: Es la llave más importante, contiene las versiones de los controladores utilizados por nuestro hardware.

  HKEY_LOCAL_MACHINE\SAM Archivos asociados: sam y sam.log

  HKEY_LOCAL_MACHINE\SECURITY Archivos asociados: Security y Security.log

  HKEY_LOCAL_MACHINE\SOFTWARE Archivos asociados: Software y Software.log

  HKEY_LOCAL_MACHINE\SYSTEM Archivos asociados: System y Sistem.log
- HKEY_CURRENT_CONFIG: Más información sobre configuración de hardware, redes y seguridad. Archivos asociados: System y System.log
- HKEY_CLASSES_ROOT: Contiene los tipos de archivos utilizados y su asociación con cada programa en concreto, los directorios dónde están instalados y los comandos de apertura.
- HKEY_DYN_DATA: En este apartado se guarda la información de los dispositivos ´plug and play´ (los que Windows reconoce e instala) como la tarjeta de sonido, vídeo, ratón o el monitor.
- HKEY_USERS: Contiene la información de usuario, como el modo en que tenemos configurado que se presenten las carpetas, los salvapantallas, sonido, etc. Archivos asociados: Ntuser.dat y Ntuser.dat.log
- HKEY_CURRENT_USERS: El mismo tipo de información que el anterior pero, guarda las configuraciones de varios usuarios.

15.3.5 Logs del sistema

Los ficheros Log de una máquina, sea la que sea, son una fuente de información importantísima en un análisis forense. Empezaremos con estos ficheros. Los sistemas Windows basados en NT tienen su principal fuente de Log en los archivos de sistema siguientes:

- SysEvent.Evt. Registra los sucesos relativos al sistema

- SecEvent.Evt. Registra los sucesos relativos a la seguridad
- AppEvent.Evt. Registra los sucesos relativos a aplicaciones

Estos ficheros se encuentran en el directorio %systemroot%\system32\config. Si están auditadas las opciones de inicio de sesión, cambio de directivas y permisos, nos centraremos con especial atención en el archivo Log SecEvent.Evt. Para visualizar este fichero podremos utilizar la herramienta de Windows eventvwr.msc, comúnmente llamada Visor de Sucesos. Abriremos con esta herramienta el archivo SecEvent.Evt, que es el encargado de almacenar los sucesos relativos a la seguridad, tales como ingresos en la máquina, cambio de directivas, etc... Por ejemplo, podríamos buscar todo acceso físico a la máquina, cambio de directivas y creación de cuentas de usuario. Eso nos podría dar una idea de quién toca el sistema. Por ejemplo, el evento 624 es el referido por Windows para un suceso de creación de cuenta de usuario. Otro ejemplo de suceso, sería el relativo al inicio de sesión. Windows almacena este suceso con el identificador 528.

Windows tiene distintos archivos Log para auditar los posibles sucesos y/o errores que puedan surgir en la vida útil del sistema operativo. Algunos de ellos son:

- WindowsUpdate.log (Log de Windows Update)
- memory.dump (Archivos de volcado de memoria)
- Archivos de registro de Windows (Software, System, etc)

En términos resumidos, el Visor de eventos es una útil herramienta para visualizar los logs del sistema.

15.3.6 Ntuser.dat y archivos de registro

Dado que Windows utiliza como referencia toda la información que se encuentra en el registro, un analista forense puede utilizar como referencia esta gran base de datos para recabar información sobre la máquina. En la base de datos de registro que se encuentra en el sistema Windows, podremos averiguar:

- Versión del Sistema Operativo
- Ruta de instalación
- Clave de Producto
- Tipo de Procesador de la máquina
- Aplicaciones Instaladas
- HotFix y parches instalados
- Servicios corriendo en la máquina
- Configuración y enumeración de los adaptadores de red

Podemos utilizar varias herramientas para analizar el registro. Algunas de ellas son:

- WRR (Windows Registry Recovery de MiTec)
- Comando nativo XP FC (Compara ficheros)
- Access Data Registry Viewer
- Windows Registry File Viewer

- Windiff (Herramienta para comparar ficheros)

Una vez abierto estos archivos de sistema que referencian al registro de Windows (SECURITY, SYSTEM, SOFTWARE, SAM, DEFAULT) con alguna de estas aplicaciones, podremos movernos por sus distintas ramas, y poder así analizar los datos que contienen estos ficheros.

15.3.7 Archivo de paginación

El archivo de paginación (Pagefile.sys) es un archivo que Windows utiliza como si fuera memoria RAM (Memoria de acceso aleatorio). Este archivo está situado en la raíz del disco duro y por defecto lo marca como oculto. El archivo de paginación y la memoria física conforman la memoria virtual. De manera predeterminada, Windows almacena el archivo de paginación en la partición de inicio, que es la partición que contiene el sistema operativo y sus archivos auxiliares. El tamaño predeterminado o recomendado del archivo de paginación es igual a 1,5 veces la cantidad total de memoria RAM. Para visualizar el contenido del archivo de paginación, podemos utilizar una herramienta de SysInternals, llamada Strings.exe.

Esta herramienta busca cadenas de texto (ASCII o Unicode) en archivos. Podemos conjugar esta herramienta con la herramienta nativa de Windows findstr. Esta herramienta busca patrones de texto en archivos utilizando expresiones regulares. Por ejemplo, podríamos buscar información relativa a conversaciones de Messenger, buscando cadenas de texto que contengan las palabras MSNMSGR o MSNSLP. El comando resultante: strings C:\pagefile.sys | findstr /i MSNMSGR

15.3.8 Recopilando información

La evidencia digital, por su naturaleza, es bastante frágil. Ésta puede ser alterada, dañada y/o destruida, principalmente por un mal manejo y/o recogida de estos datos. Por estas razones (intentamos hacer) tanto hincapié en la recogida y manejo de estos datos. La falta de este principio, puede ocasionar que estas evidencias sean inutilizables o no válidas en un proceso judicial, por no decir que podemos llegar a una conclusión inexacta. Debemos recopilar las evidencias que nos encontremos de tal forma que las protejamos y mantengamos su fiabilidad.

El primer paso que vamos a realizar será una captura de los datos físicos de la máquina, es decir, recoger diversos datos como:

Dueño de la máquina (Organización), Tipo de BIOS, Uptime del sistema (Time to live), Directorios del sistema, Número de tarjetas de red, Número de servipacks o updates del sistema, Ubicación del archivo de paginación, Tipo de procesador, Fabricante y modelo del sistema, Número de procesadores, Tamaño de la memoria RAM, Versión del sistema operativo, etc.

El segundo paso que vamos a realizar será recopilar información acerca de los servicios que hay corriendo en la máquina con sus estadísticas. En este punto voy a utilizar el comando nativo de Windows net y el comando SC. Con el comando net statistics vamos a recabar información acerca de los bytes recibidos por el sistema, el número de inicios de sesión fallidos, las cuentas de uso fallidas, etc… Toda esta información la almacenaremos en un archivo de texto con fecha y hora incluida para su posterior análisis. El comando resultante podría ser el siguiente:

```
Net statistics Workstation >Estadisticas.txt &date /t >>Estadisticas.txt
&time /t >>Estadisticas.txt
```

El comando SC me va a permitir conseguir una lista de los servicios que actualmente están corriendo en la máquina. Aunque SC posee muchos comandos para poder regular su salida, un comando resultante válido podría ser el siguiente:

```
SC query >ServiceOpen.txt &date /t >>ServiceOpen.txt &time /t >>ServiceOpen.txt
```

El tercer paso que vamos a realizar será la recopilación de supuestos procesos maliciosos, puertos de escucha, identificación de aplicaciones no autorizadas y la finalización de procesos legítimos. Para saber cuantas conexiones tengo abiertas puedo utilizar el comando nativo de Windows netstat. Utilizaré la opción –a para conocer todas las conexiones y puertos de escucha, y la juntaré con la opción -b para conocer el ejecutable que crea la conexión necesaria para llegar al TCP/IP. El comando resultante fechado para su posterior análisis quedaría:

```
netstat –ab >Conexiones.txt &date /t >>Conexiones.txt &time /t Conexiones.txt
```

Para saber los procesos que tenemos actualmente corriendo en nuestro sistema utilizaremos la aplicación nativa de Windows tasklist, o en su defecto pslist (sysinternals). También utilizaremos la herramienta Fport. Ambas herramientas (tasklist, pslist) permiten realizar esta operación en local como en remoto. El comando resultante quedaría:

```
Tasklist >Procesos.txt &date /t >>Procesos.txt &time /t >>Procesos.txt
```

También vamos a recopilar información sobre los servicios que dependen de los procesos que están en funcionamiento. Tasklist también contempla esta situación. El comando sería:

```
Tasklist /SVC >ProcesosYServicios.txt &date /t >>ProcesosYServicios.txt &time /t >>ProcesosYServicios.txt
```

Muchas veces cuando en el sistema hay determinados rootkits, virus o troyanos, éste no nos muestra una salida “coherente”, de ahí a que siempre que podamos utilicemos aplicaciones que sean lo menos intrusivas en el sistema. Si somos un poco “paranoicos” en ese tema, para ver los puertos abiertos en un sistema podemos utilizar la herramienta fport. Por regla general, no nos debemos fiar de un sistema en el que haya corriendo este tipo de virus. Básicamente fport nos muestra la misma salida que si ejecutásemos el comando nativo netstat con el filtro –a y –n. También puede identificar puertos desconocidos que estén abiertos, con sus correspondientes procesos y PID. También podríamos recabar información sobre los módulos que cargan estos proceso

Podemos averiguar por ejemplo qué DLL están asociadas a un determinado proceso.Así tendremos un control más exhaustivo sobre los procesos. Para recabar esta información podemos utilizar la herramienta de sysinternals ListDLLS.exe. Por ejemplo, si quisiésemos averiguar qué DLL dependen del proceso con PID 1548utilizaríamos la siguiente sintaxis:

```
ListDLLS.exe 1548 >DLL1548.txt &date /t >>DLL1548.txt &time /t>>DLL1548.txt
```

El cuarto paso que vamos a realizar será una recopilación de los últimos accesos a ficheros, clasificados por fechas. Esta lista nos servirá de referencia a la hora de realizar el análisis, y podremos comprobar qué ficheros se modificaron en el día o los días en los que el sistema estuvo comprometido. Podremos utilizar varias herramientas destinadas a tal fin, pero vamos utilizar sólo dos. En una primera instancia podremos utilizar el comando nativo de Windows DIR, con algunas reglas para que nos muestre los ficheros modificados conforme a la fecha. Podríamos utilizar el siguiente comando:

```
DIR /t: a /a /s /o: d c:\ >Directory.txt &date /t >>Directory.txt &time /t >>Directory.txt
```

- /t:a Nos muestra el campo del último acceso (Fecha)
- /a Muestra todos los ficheros

- /s Muestra todos los archivos del directorio especificado, incluidos los subdirectorios
- /o Lista los archivos indicados
- d Muestra los más antiguos primero (Por fecha y hora)

En varias ocasiones esta lista puede ser larguísima y el fichero puede ocuparnos unos cuantos megas. La herramienta que vamos a describir a continuación puede ayudarnos a buscar archivos en fechas concretas. La herramienta en sí se llama MacMatch.exe. Ésta herramienta básicamente buscará ficheros modificados en un intervalo de tiempo, que lógicamente se lo daremos nosotros.

En párrafos anteriores, hemos podido comprobar cómo funciona el archivo de registro de Windows, y cómo podemos sacar información de ellos. Para auditar los sucesos relativos a los inicios de sesión, el archivo de seguridad del visor de sucesos nos mostrará todos los sucesos auditados, como inicios de sesión fallidos, inicios de sesión correctos, alguna operación con privilegios, etc. Si tuviésemos que mirar uno a uno todos esos sucesos en un entorno de producción, prácticamente nos sería casi imposible de terminar, debido a la longitud del fichero. Aquí es donde actúa la herramienta NtLast. Por medio de esta herramienta podremos averiguar de forma sencilla todos y cada uno de los sucesos del sistema.

15.3.9 Analizando una pantalla azul (BSOD)

Cuando Windows encuentra una sentencia que pueda llegar a comprometer el sistema, éste se para. Esta sentencia se llama KeBugCheckEx. Esta llamada al sistema la podríamos llamar fallo de sistema, error de kernel, STOP, etc. y toma 5 argumentos:

- **Código de STOP**: Si hemos configurado nuestro sistema para que nos vuelque el contenido de la memoria, éste nos generará un archivo para su posterior análisis. Estos archivos se dividen en Small Memory Dump, Kernel Memory Dump, Complete Memory Dump. En muchos casos, la información que viene contenida en un MiniDump, no es suficiente para analizar en profundidad un error. Hace años el espacio en disco podría ser un problema para almacenar este tipo de datos, pero hoy en día esto ya no es un problema. Si queremos analizar mejor el error, configurar el sistema para generar o un volcado de memoria completo (Complete Memory Dump) o un volcado del Kernel (Kernel Memory Dump).

En la suite de aplicaciones llamadas “Sysinternals Suite” de Microsoft se encuentran todas estas utilidades entes mencionadas, incluso hay más de 60 que se pueden usar desde linea de comando.

15.3.10 Alternate Data Streams (ADS)

Hablando desde el punto de vista NTFS, un fichero no es más que un conjunto de data streams. Un stream por ejemplo, puede contener información acerca del nivel de acceso a ese fichero (directivas ACL, permisos, etc.), otro stream contendrá los datos del fichero en sí almacenados en el contenedor. Si el fichero es un acceso directo o link, un stream puede contener la dirección en donde se ubica el fichero original, etc. Si por ejemplo leyésemos un fichero en un sistema de archivos que no fuese NTFS, ej: FAT16 o FAT32, el sistema leería tan sólo el stream que contiene los datos del fichero. Aunque muchos piensen que es una falla o Bug del sistema, lo cierto es que ADS no es más que un feature (característica) del sistema, y generalmente se usa para mantener información asociada a un fichero. Microsoft tiene amplia documentación sobre ADS, en el que se incluye tutoriales, scripts para creación de ADS, etc. Por defecto cualquier usuario del sistema puede usar esta característica. Tan sólo se limita a aquellos ficheros en los que tengamos permiso de escritura. Es decir, un Administrador, podrá añadir un ADS en prácticamente todos los ficheros del sistema, mientras que un

usuario se limitará sólo a los ficheros y directorios en donde tenga acceso de escritura (Por defecto su perfil). Por defecto ADS sólo está limitado a volúmenes NTFS como hemos visto. A través de red local (LAN) podremos mandar ficheros con ADS, siempre y cuando los volúmenes intermedios tengan el sistema de archivos NTFS. La limitación teórica es mandar un ADS a través de Internet. Teóricamente no podemos mandar un fichero con ADS (sea malicioso o no), ya que nuestro cliente de correo, el medio (Internet) y el destinatario, sólo mandaría el stream con los datos, sin procesar los demás.

15.4 RESPUESTA A INCIDENTES DE SEGURIDAD TI

¿Qué preparación tiene su departamento o administrador de tecnologías de la información (TI) para tratar con incidentes de seguridad? Muchas organizaciones aprenden a responder a incidentes de seguridad sólo después de sufrir ataques. Para entonces, los incidentes a menudo pasan a ser mucho más costosos de lo necesario. La respuesta apropiada a un incidente debe ser una parte esencial de la directiva de seguridad general y de la estrategia de mitigación de riesgos. El hecho de responder a los incidentes de seguridad tiene ventajas directas evidentes. No obstante, también pueden existir ventajas financieras indirectas. Por ejemplo, puede que su compañía de seguros le ofrezca descuentos si puede demostrar que su organización es capaz de controlar los ataques rápidamente y de manera rentable. O, si se trata de un proveedor de servicios, un plan formal de respuesta a incidentes puede ayudarle a aumentar su negocio, ya que muestra que se toma en serio el proceso de seguridad de la información.

Este sección presenta un proceso y procedimientos recomendados para responder a intrusiones identificadas en entornos de red pequeños o medianos. Se explica el valor de formar un equipo de respuesta a incidentes de seguridad con funciones explícitas para los miembros del equipo, así como la forma de definir un plan de respuesta a incidentes de seguridad.

Para responder correctamente a cualquier incidente, se necesita lo siguiente:

- Minimizar la cantidad y gravedad de los incidentes de seguridad.
- Crear un CSIRT principal (Computer Security Incident Response Team, Equipo de respuesta a incidentes de seguridad informática).
- Definir un plan de respuesta a incidentes.
- Contener los daños y minimizar los riesgos.

Los administradores de sistemas pasan mucho tiempo con los entornos de red y están muy familiarizados con las redes. Documentan los entornos y crean copias de seguridad. Debe existir un proceso de auditoría ya implementado para supervisar el rendimiento y la utilización. Debe haberse alcanzado cierto nivel de conciencia antes de implementar un equipo de respuesta a incidentes. Por más detalles que se conozcan del entorno de red, el riesgo de ataques persiste. Toda estrategia de seguridad sensata debe incluir detalles sobre la forma de responder a diferentes tipos de ataque.

En la mayoría de los ámbitos de la vida, es mejor prevenir que curar, y la seguridad no es una excepción. Siempre que sea posible, se deseará evitar que, en primer lugar, se produzcan incidentes de seguridad. No obstante, resulta imposible evitar todos los incidentes de seguridad. Cuando se produce un incidente de seguridad, se debe garantizar que se minimice su repercusión. Para minimizar la cantidad y repercusión de los incidentes de seguridad, debe seguir estas pautas:

- Establecer claramente y poner en práctica todas las directivas y procedimientos. Muchos incidentes de seguridad están provocados accidentalmente por el personal de TI, que no ha seguido o no ha entendido los procedimientos de administración de cambios, o bien no ha configurado correctamente los dispositivos de seguridad, como pueden ser los firewall o los

sistemas de autenticación. Las directivas y los procedimientos se deben probar exhaustivamente para garantizar que son prácticos y claros, y que ofrecen el nivel de seguridad apropiado.

- Obtener compatibilidad administrativa para las directivas de seguridad y el control de incidentes.
- Evaluar de forma regular las vulnerabilidades del entorno. Las evaluaciones deben ser realizadas por un experto en seguridad con la autoridad necesaria (con derechos de administrador de los sistemas) para llevar a cabo estas acciones.
- Comprobar con regularidad todos los sistemas y dispositivos de red para garantizar que tienen instaladas las revisiones más recientes.
- Establecer programas de formación sobre la seguridad tanto para el personal de TI como para los usuarios finales. La mayor vulnerabilidad de cualquier sistema es el usuario carente de experiencia. El gusano ILOVEYOU aprovechó de forma eficaz esa vulnerabilidad entre el personal de TI y los usuarios finales.
- Se deben enviar pancartas de seguridad que recuerden a los usuarios sus responsabilidades y restricciones, junto con la advertencia de que se pueden emprender acciones legales en caso de infracción. Estas pancartas facilitan el hecho de reunir pruebas y procesar a los atacantes. Se debe buscar asesoramiento legal para asegurarse de que la redacción de las pancartas de seguridad es apropiada.
- Desarrollar, implementar y poner en práctica una directiva que requiera contraseñas seguras. Para obtener más información sobre contraseñas, consulte el apartado "Aplicación del uso de contraseñas seguras en las organizaciones" del kit de orientaciones sobre seguridad.
- Supervisar y analizar con regularidad el tráfico de red y el rendimiento del sistema.
- Comprobar con regularidad todos los registros y mecanismos de registro, incluidos los registros de eventos del sistema operativo, los registros específicos de aplicación y los registros de sistema de detección de intrusiones.
- Comprobar los procedimientos de restauración y copia de seguridad. Debe saber dónde se almacenan las copias de seguridad, quién tiene acceso a ellas y los procedimientos para la restauración de datos y la recuperación del sistema. Asegúrese de que las copias de seguridad y los medios se comprueban con regularidad mediante la restauración selectiva de datos.
- Crear un CSIRT para abordar los incidentes de seguridad. Para obtener más información sobre los CSIRT, consulte la siguiente sección de este documento.

El CSIRT es crucial para tratar con los incidentes de seguridad del entorno. El equipo debe estar formado por un grupo de personas responsables de abordar los incidentes de seguridad. Los miembros del equipo deben haber definido claramente sus tareas para asegurar que no quede ningún área de la respuesta sin cubrir. El hecho de reunir un equipo antes de que se produzca cualquier incidente es muy importante para la organización e influirá positivamente en la manera de tratar los incidentes. Un equipo adecuado realizará las siguientes tareas:

- Supervisar los sistemas en busca de infracciones de seguridad.
- Servir como punto central de comunicación, tanto para recibir los informes de incidentes de seguridad, como para difundir información esencial sobre los incidentes a las entidades correspondientes.
- Documentar y catalogar los incidentes de seguridad.
- Aumentar el nivel de conciencia con respecto a la seguridad dentro de la compañía para ayudar a evitar que se den incidentes en la organización.

- Posibilitar la auditoría de sistemas y redes mediante procesos como la evaluación de vulnerabilidades y pruebas de penetración.
- Obtener más información sobre las nuevas vulnerabilidades y estrategias de ataque empleadas por los atacantes.
- Investigar acerca de nuevas revisiones de software.
- Analizar y desarrollar nuevas tecnologías para minimizar los riesgos y vulnerabilidades de seguridad.
- Ofrecer servicios de consultoría sobre seguridad.
- Perfeccionar y actualizar continuamente los sistemas y procedimientos actuales.

Al crear un CSIRT, debe preparar al equipo para tratar con los incidentes. Para preparar al equipo, debe seguir estas pautas:

- Formarlos en el uso adecuado y la ubicación de las herramientas de seguridad críticas. También ha de estudiar el hecho de facilitarles equipos portátiles preconfigurados con estas herramientas para asegurar que no se malgasta tiempo en la instalación y configuración de las herramientas, de modo que puedan responder a los incidentes. Estos sistemas y las herramientas asociadas deben estar protegidos adecuadamente cuando no se usen.
- Reunir toda la información de comunicación pertinente. Debe asegurarse de que cuenta con los nombres y números de teléfono de contacto de las personas de la organización a las haya que avisar (incluidos los miembros del CSIRT, los responsables de mantener todos los sistemas y los encargados de las relaciones con los medios). También necesita los detalles del proveedor de servicios de Internet (ISP) y las autoridades locales y nacionales. Hable con la asesoría legal para contactar con las autoridades locales pertinentes antes de que se produzca un incidente. Esto le ayudará a asegurarse de que entiende los procedimientos apropiados para comunicar los incidentes y reunir pruebas. Debe informar a la asesoría legal de cualquier contacto con las autoridades.
- Colocar toda la información del sistema de emergencia en una ubicación central y sin conexión, como una carpeta física o un equipo sin conexión. Esta información de emergencia incluye las contraseñas de los sistemas, las direcciones IP, la información sobre la configuración de los enrutadores, las listas de conjuntos de reglas del firewall, copias de las claves de entidad emisora de certificados, los nombres y números de teléfono de contacto, los procedimientos de extensión, etc. Esta información debe estar disponible con facilidad y se debe mantener en un lugar seguro. Un método para proteger y hacer esta información fácilmente disponible consiste en cifrarla en un equipo portátil de seguridad dedicado, guardado en una caja fuerte con acceso limitado a ciertos individuos, como el coordinador del CSIRT, o el director del departamento informático o tecnológico.

La pertenencia y estructura ideal del CSIRT depende del tipo de organización y de la estrategia de administración de riesgos. No obstante, como regla general, el CSIRT debe pertenecer en parte o totalmente al equipo de seguridad de la organización. El equipo principal está compuesto por profesionales responsables de coordinar una respuesta a cualquier incidente. El número de miembros del CSIRT dependerá normalmente del tamaño y la complejidad de la organización. No obstante, debe asegurarse de que cuenta con suficientes miembros para cubrir adecuadamente todas las tareas del equipo en cualquier momento.

Establecimiento de las funciones en el equipo

Coordinador de equipo del CSIRT. El CSIRT debe tener a alguien a cargo de sus actividades. Generalmente, el coordinador de equipo del CSIRT será responsable de las actividades del CSIRT y coordinará las revisiones de sus acciones. Esto quizás acarree cambios en las directivas y procedimientos para el control de futuros incidentes.

Coordinador de incidentes del CSIRT. En caso de que se produzca un incidente, se debe designar un individuo responsable de coordinar la respuesta. El coordinador de incidentes del CSIRT es propietario del incidente o del conjunto de incidentes de seguridad relacionados. Toda comunicación acerca del evento se coordina a través del coordinador de incidentes: al hablar con cualquiera que no pertenezca al CSIRT, representará a todo el equipo. El coordinador de incidentes puede variar según la naturaleza del incidente y, a menudo, no se trata del coordinador de equipo del CSIRT.

Miembros asociados al CSIRT. Aparte del equipo del CSIRT principal, se debe contar con varias personas concretas que traten y respondan a incidentes concretos. Los miembros asociados provienen de varios departamentos diferentes de la organización. Deben especializarse en áreas afectadas por incidentes de seguridad que el CSIRT principal no trata directamente. Los miembros asociados pueden implicarse directamente en un incidente o servir de punto de entrada para delegar la responsabilidad a alguien más apropiado dentro de su departamento. En la siguiente tabla se muestran algunas sugerencias con respecto a los miembros asociados y sus funciones.

Todos los miembros del entorno de TI deben saber cómo actuar en caso de incidente. El CSIRT realizará la mayoría de las acciones en respuesta a un incidente, pero todo el personal de TI debe saber cómo informar de incidentes internamente. Los usuarios finales deben informar de cualquier actividad sospechosa al personal de TI directamente o a través de un personal de asistencia, no directamente al CSIRT. Cada miembro del equipo debe revisar el plan de respuesta a incidentes detalladamente. El hecho de que el plan sea fácilmente accesible para todo el personal de TI ayudará a garantizar que, cuando se produzca un incidente, se seguirán los procedimientos correctos.

Para elaborar un plan satisfactorio de respuesta a incidentes se deben seguir estos pasos:

- Realizar una evaluación inicial.
- Comunicar el incidente.
- Contener el daño y minimizar el riesgo.
- Identificar el tipo y la gravedad del ataque.
- Proteger las pruebas.
- Notificar a los organismos externos, si corresponde.
- Recuperar los sistemas.
- Compilar y organizar la documentación del incidente.
- Valorar los daños y costos del incidente.
- Revisar las directivas de respuesta y actualización.

Estos pasos no son puramente secuenciales, sino que se suceden a lo largo del incidente. Por ejemplo, la documentación comienza al principio y continúa durante todo el ciclo de vida del incidente;

las comunicaciones también se producen durante todo el incidente.

Algunos aspectos del proceso se desarrollan junto a otros. Por ejemplo, como parte de la evaluación inicial, se hará una idea de la naturaleza general del ataque. Es importante usar esta información para contener el daño y minimizar el riesgo tan pronto como sea posible. Si actúa con rapidez, podrá ahorrar tiempo y dinero, y salvar la reputación de la organización.

No obstante, hasta que conozca mejor el tipo y la gravedad del ataque, no podrá contener el daño ni minimizar el riesgo de forma realmente efectiva. Una respuesta excesiva podría causar aún más daño que el ataque inicial. Al llevar a cabo estos pasos de manera conjunta, obtendrá la mejor unión entre acciones rápidas y efectivas.

Muchas actividades podrían indicar un posible ataque a su organización. Por ejemplo, cuando un administrador de red realiza labores de mantenimiento del sistema, puede parecer que alguien está iniciando alguna forma de ataque. En otros casos, un sistema mal configurado puede llevar a varios falsos positivos en el sistema de detección de intrusiones, lo que dificulta la identificación de los verdaderos incidentes.

Como parte de su evaluación inicial, debe realizar las siguientes acciones:

- Tomar medidas para determinar si está tratando con un incidente verdadero o un falso positivo.
- Hacerse una idea general del tipo y la gravedad del ataque. Debe reunir al menos suficiente información para su investigación adicional y para empezar a contener los daños y minimizar el riesgo.
- Registrar las acciones minuciosamente. Estos registros se usarán más adelante para documentar el incidente (ya sea real o falso).

Cuando sospeche que hay un incidente de seguridad, debe comunicar rápidamente la infracción al resto del CSIRT principal. El coordinador de incidentes, junto con el resto del equipo, debe identificar rápidamente con quién debe contactar fuera del CSIRT principal. Así se garantiza que se puede mantener un control y una coordinación de incidentes adecuada, al tiempo que se minimizan los daños. Tenga en cuenta que los daños pueden producirse de muchas formas y que un titular en el periódico que describa una infracción de seguridad puede ser mucho más destructivo que muchas intrusiones en el sistema. Por este motivo y para evitar que los atacantes estén avisados, sólo se debe informar a aquellos implicados en la respuesta a incidentes hasta que el incidente esté totalmente controlado. Basándose en cada situación concreta, el equipo determinará a quién se debe informar acerca del incidente. Podría tratarse de cualquiera, desde personas concretas hasta toda la compañía y los clientes externos. La comunicación externa debe estar coordinada con el representante legal.

Al actuar rápidamente para reducir los efectos reales y potenciales de un ataque, puede marcar la diferencia entre un ataque de menor o mayor importancia. La respuesta exacta dependerá de la organización y de la naturaleza del ataque al que se enfrente. No obstante, se sugieren las siguientes prioridades como punto de partida:

1. Proteger la vida humana y la seguridad de las personas. Por supuesto, esta debe ser siempre la máxima prioridad.
2. Proteger la información secreta y confidencial. Como parte de su plan de respuesta a incidentes, debe definir claramente qué información es secreta o confidencial. Esto le permitirá establecer prioridades a sus respuestas de protección de datos.
3. Proteger otra información, como datos científicos, sobre propiedad o del ámbito directivo. Puede que otra información de su entorno también sea valiosa. Debe proteger en primer lugar los datos más valiosos antes de pasar a otros menos útiles.
4. Proteger el hardware y software contra el ataque. Esto incluye protegerlos contra la pérdida o

la modificación de los archivos de sistema y contra daños físicos al hardware. Los daños en los sistemas pueden tener como consecuencia un costoso tiempo de inactividad.

5. Minimizar la interrupción de los recursos informáticos (incluidos los procesos). Aunque el tiempo de producción sea muy importante en la mayoría de los entornos, el hecho de mantener los sistemas en funcionamiento durante un ataque puede tener como consecuencia problemas más graves en el futuro. Por este motivo, la minimización de la interrupción de los recursos informáticos debe ser generalmente una prioridad relativamente baja.

Existen varias medidas que se pueden tomar para contener el daño y minimizar el riesgo en el entorno. Como mínimo, debe llevar a cabo las siguientes acciones:

- Intentar evitar que los atacantes sepan que conoce sus actividades. Puede resultar difícil, porque algunas respuestas esenciales pueden alertar a los atacantes. Por ejemplo, si hay una reunión de emergencia del CSIRT o solicita un cambio inmediato de todas las contraseñas, algún atacante interno puede saber que está al corriente de un incidente.
- Comparar el costo de dejar sin conexión los sistemas en peligro y los sistemas relacionados con el riesgo de continuar funcionando. En la inmensa mayoría de los casos, debe desconectar el sistema de la red inmediatamente. No obstante, puede tener contratos de servicio en funcionamiento que requieran que los sistemas estén disponibles, incluso con la posibilidad de sufrir daños adicionales. En estas circunstancias, puede decidir mantener un sistema conectado con conectividad limitada para reunir pruebas adicionales durante un ataque en proceso. A veces, el daño y el alcance de un incidente pueden ser tan extensos que tenga que tomar medidas que apelen a las cláusulas penales especificadas en sus contratos de nivel de servicio. En todo caso, es muy importante que las acciones que lleve a cabo en caso de incidente se traten de antemano y se describan en el plan de respuesta para que se puedan tomar medidas inmediatas cuando ocurra un ataque.
- Determinar los puntos de acceso usados por el atacante e implementar las medidas adecuadas para evitar futuros accesos. Las medidas pueden incluir la deshabilitación de un módem, la adición de entradas de control de acceso en un enrutador o firewall, o el aumento de las medidas de seguridad físicas.
- Considere la opción de volver a crear un sistema con discos duros nuevos (se deben eliminar los discos duros existentes y almacenarlos, ya que se pueden usar como prueba si decide procesar a los atacantes). Asegúrese de que cambia las contraseñas locales. También debería cambiar las contraseñas de las cuentas de servicio y administrativas en todo el entorno.

Para poder recuperarse de forma eficaz de un ataque, debe determinar la gravedad de la situación de peligro que han sufrido los sistemas. Esto determinará cómo contener y minimizar el riesgo, cómo recuperarse de él, en qué momento y a quién comunicar el incidente, y si se debe intentar obtener una indemnización legal.

Debe intentar:

- Determinar la naturaleza del ataque (puede ser diferente a lo que sugiere la evaluación inicial).
- Determinar el punto de origen del ataque.
- Determinar la intención del ataque. ¿Estaba el ataque dirigido específicamente a su organización para conseguir información concreta o fue un ataque aleatorio?
- Identificar los sistemas puestos en peligro.
- Identificar los archivos a los que se ha tenido acceso y determinar su grado de confidencialidad.

Al realizar estas acciones, podrá determinar las respuestas apropiadas para su entorno. Un buen plan de respuesta a incidentes resumirá los procedimientos específicos que ha de seguir hasta obtener más información sobre el ataque. Generalmente, la naturaleza de los síntomas del ataque determinará el orden en el que deberá seguir los procedimientos definidos en el plan. Ya que el tiempo es de suma importancia, los procedimientos que requieran menos tiempo tendrán prioridad ante los que consuman más tiempo. Para ayudar a determinar la gravedad del ataque, debe llevar a cabo estas acciones:

- Ponerse en contacto con otros miembros del equipo de respuesta para informarles de sus conclusiones, hacer que comprueben sus resultados, determinar si están al corriente de actividades relacionadas o ataques potenciales, y ayudar a determinar si el incidente es un falso positivo. A veces, lo que quizás parezca ser un incidente verdadero en la evaluación inicial, resultará un falso positivo.
- Determinar si se ha usado hardware no autorizado en la red o si hay signos de acceso no autorizado a través de controles de seguridad físicos puestos en peligro.
- Examinar los grupos clave (administradores de dominio, administradores, etc.) en busca de entradas no autorizadas.
- Buscar software de evaluación o de detección de vulnerabilidades de seguridad. A menudo, se pueden encontrar utilidades de violación en los sistemas en peligro durante la recopilación de pruebas.
- Buscar procesos o aplicaciones no autorizados en ejecución o configurados para ejecutarse usando las carpetas de inicio o las entradas del Registro.
- Buscar espacios en blanco, o la ausencia de los mismos, en los registros del sistema.
- Revisar los registros del sistema de detección de intrusiones en busca de signos de intrusión, qué sistemas pueden estar afectados, los métodos de ataque, el tiempo y la duración del ataque, así como el grado de los posibles daños.
- Examinar otros archivos de registro en busca de conexiones inusuales, auditorías de seguridad correctas no habituales, inicio de sesión fallidos, intentos de inicio de sesión en cuentas predeterminadas, actividad fuera del horario laboral, cambios de permisos en los archivos, directorios y recursos compartidos, y permisos de usuario elevados o cambiados.
- Comparar los sistemas con comprobaciones de integridad del sistema y los archivos realizadas con anterioridad. Esto le permite identificar las adiciones, supresiones, modificaciones y modificaciones del permiso y control realizadas en el sistema de archivos y el Registro. Puede ahorrar mucho tiempo al responder a los incidentes si identifica exactamente qué ha sufrido peligro y qué áreas hay que recuperar.
- Buscar datos confidenciales, como los números de tarjeta de crédito y empleado o los datos del cliente, que se puedan haber cambiado de ubicación o escondido para modificarlos o recuperarlos en el futuro. Puede que también deba comprobar si en los sistemas hay información no empresarial, copias ilegales de software y mensajes de correo electrónico u otros registros que puedan ayudar en una investigación. Si existe la posibilidad de infringir la privacidad u otras leyes al buscar en un sistema durante la investigación, debe contactar con su asesoría jurídica antes de continuar.
- Comparar el rendimiento de los sistemas sospechosos con sus niveles de rendimiento de línea de base. Por supuesto, se presupone que las líneas de base se han creado y actualizado adecuadamente.

Al determinar qué sistemas se han puesto en peligro y cómo, generalmente comparará los sistemas con una línea de base registrada con anterioridad del mismo sistema antes de sufrir estos ataques. El hecho de asumir que una instantánea reciente del sistema es suficiente para la comparación puede ponerle en una situación difícil si la instantánea anterior proviene de un sistema que ya ha sido

atacado. En entornos Windows las herramientas como EventCombMT, DumpEL y Microsoft Operations Manager (MOM) pueden ayudarle a determinar el nivel de ataques que ha sufrido un sistema. Los sistemas de detección de intrusiones de terceros avisan de los ataques de antemano y otras herramientas muestran los cambios en los archivos de los sistemas.

En muchos casos, si el entorno ha sufrido un ataque intencionado, puede que desee poner una denuncia contra los autores. Para conservar esta opción, debe reunir pruebas que se puedan usar contra ellos, incluso si finalmente se decide no llevar a cabo tal acción. Es muy importante realizar copias de seguridad de los sistemas en peligro tan pronto como sea posible. Realice copias de seguridad de los sistemas antes de realizar cualquier acción que pueda afectar a la integridad de los datos en los medios originales.

Alguien cualificado en el análisis forense informático debe hacer al menos dos copias de seguridad completas bit a bit del sistema entero con medios totalmente nuevos. Al menos se debe realizar una copia de seguridad en un medio que admita una sola escritura pero múltiples lecturas, como CD-R o DVD-R. Esta copia de seguridad se debe usar sólo para propósitos legales y se debe proteger en lugar seguro hasta que se necesite.

La otra copia de seguridad se puede usar para la recuperación de datos. No se debe tener acceso a estas copias de seguridad a menos que sea con propósitos legales, de modo que se deben proteger físicamente. Asimismo, necesitará documentar la información acerca de las copias de seguridad: quién realizó las copias de seguridad de los sistemas, cuándo, cómo se protegieron y quién tenía acceso a ellas.

Una vez que se hayan realizado las copias de seguridad, debe eliminar los discos duros originales y almacenarlos en una ubicación físicamente segura. Estos discos se pueden usar como prueba forense en un juicio. Los discos duros nuevos se deben usar para restaurar el sistema.

En ocasiones, la ventaja de conservar los datos puede que no iguale a los costos de retrasar la respuesta y la recuperación del sistema. Los costos y las ventajas de conservar los datos se deben comparar con los de una recuperación más rápida para cada evento.

Para sistemas muy grandes, puede que no sea posible realizar copias completas de todos los sistemas en peligro. En lugar de esta operación, debe realizar copias de seguridad de todos los registros y de las partes seleccionadas y violadas del sistema.

Si es posible, realice también copias de seguridad de los datos de estado del sistema. Pueden pasar meses o años hasta que se celebre un juicio, de modo que es importante tener archivados todos los detalles del incidente para su uso en el futuro.

A menudo, el aspecto legal más difícil de procesar un crimen informático es reunir pruebas de forma que se adapten a las leyes de presentación de pruebas de la jurisdicción en cuestión. De ahí que el componente más importante del proceso forense sea la documentación detallada y completa sobre cómo se procedió con los sistemas, quién y cómo lo hizo, para aportar pruebas confiables. Firme y ponga fecha a cada página de la documentación.

Una vez que cuente con copias de seguridad comprobadas y funcionales, puede borrar los sistemas infectados y volverlos a crear. Esto le permitirá empezar a trabajar de nuevo. Las copias de seguridad ofrecen la prueba crítica y definitiva necesaria para emprender acciones legales. Se debe usar una copia de seguridad distinta a la forense para restaurar los datos.

Después de contener el incidente y reunir los datos necesarios para un posible juicio, debe plantearse si debe comunicárselo a los organismos externos adecuados. Toda comunicación externa se debe coordinar con el representante legal. Entre los organismos a los que puede acudir se encuentran los siguientes: autoridades competentes locales y nacionales, organismos externos de seguridad y expertos en virus. Los organismos externos pueden ofrecer ayuda técnica, una resolución más rápida e información derivada de incidentes similares para ayudarle a recuperarse completamente del incidente y evitar que se vuelva a producir en el futuro.

En sectores y tipos de infracciones concretos, quizás tenga que notificar la situación a los clientes y al público general, especialmente si los clientes pueden verse directamente afectados por el incidente.

Si el evento causó una repercusión financiera considerable, puede que desee informar del incidente a las autoridades competentes.

Para compañías e incidentes de un perfil superior, puede que los medios de comunicación se vean implicados. La atención de los medios a un incidente de seguridad no suele ser deseable, pero a menudo resulta inevitable. La atención de los medios puede permitir a su organización tomar una postura proactiva en la comunicación del incidente. Como mínimo, los procedimientos de respuesta a incidentes deben definir claramente a los individuos autorizados a hablar con los representantes de los medios.

Normalmente, el departamento de relaciones públicas de la organización hablará con los medios. No debe intentar negar a los medios que se ha producido un incidente, porque hacerlo probablemente dañará su reputación más que la admisión proactiva y las respuestas visibles. Esto no significa que deba notificar a los medios cada incidente independientemente de su naturaleza o gravedad. Debe valorar la respuesta apropiada a los medios según el caso.

La forma de recuperar el sistema dependerá generalmente del alcance de la infracción de seguridad. Deberá determinar si puede restaurar el sistema existente dejando intacto todo lo posible, o si es necesario volver a crear completamente el sistema.

Para restaurar los datos se asume, por supuesto, que cuenta con copias de seguridad limpias, realizadas antes de que ocurriera el incidente. El software de integridad de archivos puede ayudar a señalar el primer daño en aparecer. Si el software le avisa sobre un archivo modificado, sabrá que la copia de seguridad que hizo antes de la alerta es adecuada y que debe conservarla para su uso cuando vuelva a crear el sistema en peligro.

Un incidente podría dañar los datos almacenados varios meses antes de su descubrimiento. Por lo tanto, es muy importante que, como parte del proceso de respuesta a incidentes, determine la duración del incidente. (El software de integridad del sistema y archivos, junto con los sistemas de detección de intrusiones, puede ayudarle en esta tarea.) En algunos casos, la última o incluso las últimas copias de seguridad pueden no ser adecuadas para recuperar un estado apropiado, de modo que debe archivar con regularidad copias de seguridad de los datos en una ubicación externa.

El CSIRT debe documentar minuciosamente todos los procesos al tratar con un incidente. Se debe incluir una descripción de la infracción y detalles de cada acción tomada (quién llevó a cabo la acción, cuándo lo hizo y por qué motivos). Se debe avisar a todas las personas implicadas con acceso durante el proceso de respuesta.

Después, se debe organizar la documentación cronológicamente, comprobar que está completa, y firmarla y revisarla con la directiva y los representantes legales. Asimismo, deberá proteger las pruebas recopiladas en la fase de protección de pruebas. Debe plantearse la presencia de dos personas durante todas las fases, que puedan aprobar cada paso. Esto ayudará a reducir la probabilidad de que las pruebas se consideren no admisibles y de que se modifiquen después.

Recuerde que el atacante puede ser un empleado, contratista, empleado temporal u otra persona de la organización. Sin documentación completa y detallada, la identificación de un atacante interno será muy difícil. Una documentación apropiada también le proporciona la mejor oportunidad de procesar legalmente a los atacantes.

Al determinar los daños que sufre la organización, debe considerar tanto los costos directos como los indirectos. El daño y los costos del incidente constituirán una prueba importante y necesaria si decide emprender acciones legales. Entre ellos, se pueden contar los siguientes:

- Costos debidos a la pérdida de la ventaja competitiva por la divulgación de información confidencial o de propietario.
- Costos legales.

- Costos laborales por el análisis de las infracciones, la reinstalación del software y la recuperación de datos.
- Costos relacionados con el tiempo de inactividad del sistema (por ejemplo, productividad de los empleados perdida, ventas perdidas, sustitución del hardware, del software y de otras propiedades).
- Costos relacionados con la reparación y posible actualización de las medidas de seguridad físicas dañadas o ineficaces (cierres, paredes, cajas, etc.).
- Otros daños derivados, como la pérdida de la reputación o de la confianza del cliente.

Una vez que se hayan finalizado las fases de documentación y recuperación, debe revisar el proceso minuciosamente. Determine con su equipo qué pasos se siguieron correctamente y qué errores se cometieron. En casi todos los casos, descubrirá que debe modificar algunos procesos para controlar mejor futuros incidentes.

Encontrará debilidades en su plan de respuesta a incidentes. Este análisis posterior tiene como objetivo encontrar oportunidades de mejora, que iniciarán un nuevo proceso de planificación de la respuesta a incidentes.

CAPÍTULO 16

16.1 SEGURIDAD EN GNU/LINUX

Ante todo Linux es un sistema multiusuario real. Puede haber varios usuarios distintos trabajando a la vez cada uno desde su terminal. El sistema tiene la obligación de proteger a unos usuarios frente a otros y protegerse a sí mismo. Linux es una excelente estación de trabajo aislada, pero lo habitual es que cada máquina linux esté conectada a una red y además esté prestando servicios de red. El sistema tiene la obligación de garantizar los servicios que presta.

Además, con la generalización de las conexiones con Internet y el rápido desarrollo del software, la seguridad se está convirtiendo en una cuestión cada vez más importante. Ahora, la seguridad es un requisito básico, ya que la red global es insegura por definición. Mientras sus datos estén almacenados en un soporte informático, mientras sus datos vayan desde un sistema X a otro sistema Y a través de un medio físico, Internet, por ejemplo, puede pasar por ciertos puntos durante el camino proporcionando a otros usuarios la posibilidad de interceptarlos, e incluso alterar la información contenida. Incluso algún usuario de su sistema puede modificar datos de forma maliciosa para hacer algo que nos pueda resultar perjudicial. Con el acceso masivo y barato a Internet se han reducido notablemente los costes de un atacante para asaltar un sistema en red, a la vez que ha aumentado paralelamente el número de potenciales atacantes. Resumiendo, a nadie le gustaría que desconocidos abran su correo privado, que miren en sus cajones, que se hagan copias de las llaves de su escritorio o de la tarjeta de crédito. Pues todo esto es aplicable en la misma medida a las redes telemáticas.

También queremos remarcar el carácter dinámico de la seguridad de los sistemas en red. Continuamente aparecen nuevos métodos para conseguir accesos indebidos o comprometer el correcto funcionamiento de la red. Esto obliga a estar actualizado permanentemente, y consultar las publicaciones electrónicas que informan de los últimos sucesos detectados. Evidentemente, estas publicaciones informan principalmente sobre actividades que ya se han llevado a cabo, por lo que esperamos que no sea el primero en sufrirlas. Pero también se puede encontrar información sobre debilidades detectadas antes de que se lleven a cabo. Por todo esto, este curso no pretende proporcionar una lista actualizada de programas o servicios potencialmente inseguros o de programas que afectan a la seguridad (denominados exploits). Como continuamente aparecen nuevos programas para comprometer la seguridad de las redes y de las comunicaciones, lo que sí haremos será indicar los lugares más habituales donde buscar una información actualizada de ese tipo, y algunos métodos generales para prevenir que esos programas tengan éxito en su sistema.

Primero, tenga en cuenta que ningún sistema es "completamente" seguro. El único sistema seguro es aquel que no está conectado en red, que está apagado y encerrado bajo llave.

Desde esta perspectiva, partimos de que todo lo único que puede hacer es aumentar la dificultad para que alguien pueda comprometer la seguridad de su sistema. Tampoco todos los usuarios tienen las mismas necesidades de seguridad en sus entornos. Por ejemplo, los usuarios domésticos de Linux, no necesitan demasiado trabajo para mantener alejados a los crackers ocasionales, mientras que para los usuarios muy especializados de Linux, como por ejemplo servidores de Internet, bancos, compañías de telecomunicaciones, etc., se necesita un trabajo mucho más detallado para garantizar la seguridad en los términos previstos.

También tenemos que tener en cuenta que existe una relación inversa entre seguridad y funcionalidad. Tiene que decidir dónde está el equilibrio entre la facilidad de uso de su sistema y su seguridad. Por ejemplo, puede necesitar que cualquiera que llame por el módem a su sistema, y nuestro módem tenga que devolver la llamada a su número de casa. Este mecanismo garantiza un mayor nivel de seguridad, pero si alguien no está en casa, le hace más difícil conectarse. Otra forma de aumentar la seguridad sería no tener conexión con Internet, pero seguro que no es eso lo que queremos.

También existe una relación inversa entre el nivel de seguridad y el número de servicios distintos que presta un sistema. Cada servicio prestado por un sistema puede ser susceptible de ser utilizado contra el propio equipo servidor, como puede ser el caso de bloqueos intencionados, conocidos como ataque de denegación de servicio (DoS). Pero un sistema servidor que no presta servicios es menos servidor.

En el caso de administrar un instalación mediana o grande conviene establecer una "Política de Seguridad" que fije el nivel de seguridad que requiere ese sitio y que sistema de comprobación se realiza. Puede encontrar un ejemplo muy conocido de política de seguridad en el RFC 2196.

Como probablemente sabrá, las fuentes del núcleo de linux son abiertas. Cualquiera puede obtenerlas, analizarlas y modificarlas. El modelo de desarrollo abierto, que siguen tanto Linux como la mayoría de las aplicaciones que se ejecutan sobre él, conduce a altos niveles de seguridad. Es cierto que cualquiera puede acceder al código fuente para encontrar las debilidades, pero no es menos cierto que el tiempo que tarda en aparecer la solución para cualquier debilidad se mide más fácilmente en horas que en días.

Gracias a esto, Linux es conocido por su alto nivel de estabilidad que parte del propio núcleo del sistema operativo (lo que propiamente es Linux).

Servicios en Linux

Linux tiene disponible todos los servicios habituales en una red:

- Bases de datos.
- Servicios de internet.
- Servicio de ficheros e impresión.
- Utilidades necesarias para mantener el nivel de seguridad requerido.

Pero además hay que reseñar que cada servicio funciona sin afectar al resto de los servicios. Ud. puede modificar la dirección IP de su equipo, las rutas, añadir, parar o reiniciar un servicio concreto sin que el resto de los servicios se vean afectados. Sólo es necesario detener el equipo para realizar operaciones con el hardware, como añadir un disco duro, o utilizar un nuevo núcleo. No tendrá, pues, la necesidad de tener que ser Ud. mismo el atacante de su propio sistema, a diferencia de lo que ocurre en otros sistemas operativos.

Normalmente querrá garantizar que el sistema permanece en funcionamiento de forma adecuada. Querrá garantizar que nadie pueda obtener o modificar una información a la que no tiene derecho legítimo. Y también querrá garantizar unas comunicaciones seguras. Una buena planificación ayuda bastante a conseguir los niveles de seguridad que pretendemos. Antes de intentar asegurar su sistema debería determinar contra qué nivel de amenaza quiere protegerse, qué riesgo acepta o no y, como resultado, cómo de vulnerable es su sistema. Debería analizar su sistema para saber qué está protegiendo, por qué lo está protegiendo, qué valor tiene y quiénes tienen responsabilidad sobre sus datos y otros elementos.

¿Qué está en juego si alguien entra en su sistema? Desde luego será distinto para un usuario en casa con un enlace PPP dinámico que para las compañías que conectan su máquina a Internet u otra gran red.

¿Cuanto tiempo me llevaría recuperar/recrear cualquier dato que se ha perdido? Una inversión en tiempo ahora puede ahorrar diez veces más de tiempo con posterioridad si tiene que recrear los datos

que se perdieron. ¿Ha verificado su estrategia de copias de respaldo, y ha verificado sus datos últimamente?

La seguridad pretende que los sistemas informáticos que utiliza una entidad se mantengan en funcionamiento según los requisitos de la política establecida por la propia entidad. Cada entidad define una serie de servicios que pretende obtener de una red de ordenadores para prestarlos a unos usuarios legítimos.

En particular, en Linux tendremos que proteger ciertos ficheros que contienen información sobre los usuarios (`/etc/passwd`, `/etc/shadow`), los ficheros de configuración del sistema (los contenidos en `/etc`), el acceso al sistema para que se realice según marca la política prevista y la correcta utilización de los recursos para evitar abusos (p.e. si un usuario tiene sólo una cuenta de correo, que no pueda abrir una shell en el sistema). A todo esto habrá que sumar la protección de los distintos servicios que presta.

16.1.1 Seguridad Física

Las primeras medidas de seguridad que necesita tener en cuenta son las de seguridad física de sus sistemas. Hay que tomar en consideración quiénes tienen acceso físico a las máquinas y si realmente deberían acceder.

El nivel de seguridad física que necesita en su sistema depende de su situación concreta. Un usuario doméstico no necesita preocuparse demasiado por la protección física, salvo proteger su máquina de un niño o algo así. En una oficina puede ser diferente.

Linux proporciona los niveles exigibles de seguridad física para un sistema operativo:

- Un arranque seguro
- Posibilidad de bloquear las terminales
- Por supuesto, las capacidades de un sistema multiusuario real.

Cuando alguien inicia el sistema operativo Linux se encuentra con una pantalla de login: el sistema está pidiendo que se identifique. Si es un usuario conocido, podrá iniciar una sesión y trabajar con el sistema. Si no lo es, no tendrá opción de hacer absolutamente nada. Además, el sistema registra todos los intentos de acceso (fallidos o no), por lo que no pasarán desapercibidos intentos repetidos de acceso no autorizado. LILO (Linux Loader) es el encargado de cargar el sistema operativo en memoria y pasarle información para su inicio. A su vez, Vd. puede pasarle parámetros a LILO para modificar su comportamiento.

Por ejemplo, si alguien en el indicador de LILO añade *init single*, el sistema se inicia en modo monousuario y proporciona una shell de root sin contraseña. Si en su entorno de trabajo cree necesario evitar que alguien pueda iniciar el sistema de esta forma, debería utilizar el parámetro *restricted* en el fichero de configuración de LILO (habitualmente */etc/lilo.conf*). Este parámetro le permite iniciar normalmente el sistema, salvo en el caso de que se hayan incluido argumentos en la llamada a LILO, que solicita una clave. Esto proporciona un nivel de seguridad razonable: permite iniciar el sistema, pero no manipular el arranque. Si tiene mayores necesidades de seguridad puede incluir la opción *password*. De esta forma necesitará una clave para iniciar el sistema. En estas condiciones, sólo podrá iniciar el sistema quien conozca la clave.

Puede encontrar más detalles en las páginas del manual lilo y lilo.conf. Para ello, introduzca en la línea de comandos las siguientes órdenes:

```
# man lilo
```

```
# man lilo.conf
```

16.1.2 Seguridad local

Linux es un sistema operativo multiusuario real: puede haber varios usuarios trabajando simultáneamente con él, cada uno en su terminal. Esto obliga a tener en cuenta medidas de seguridad adicionales. Además, según hablan las estadísticas, el mayor porcentaje de violaciones de un sistema son realizadas por usuarios locales. Pero no sólo hay que protegerse de las violaciones intencionadas, sino que el sistema debe protegernos de operaciones accidentales debidas a decuidos o ignorancia de los usuarios.

En este aspecto de la seguridad, Linux dispone de todas las características de los sistemas Unix: un control de acceso a los usuarios verificando una pareja de usuario y clave; cada fichero y directorio tienen sus propietario y permisos.

Por otro lado, la meta de la mayoría de los ataques es conseguir acceso como root, lo que garantiza un control total sobre el sistema. Primero se intentará conseguir acceso como usuario "normal" para posteriormente ir incrementando sus niveles de privilegio utilizando las posibles debilidades del sistema: programas con errores, configuraciones deficientes de los servicios o el descifrado de claves cifradas. Incluso se utilizan técnicas denominadas "ingeniería social", consistentes en convencer a ciertos usuarios para que suministren una información que debiera ser mantenida en secreto, como sus nombres de usuario y contraseñas.

En este apartado de seguridad local pretendemos dar unas ideas generales de los riesgos existentes, mecanismos para su solución y unas directrices de actuación que deberían convertirse en hábitos cotidianos.

Cuentas de Usuarios y Grupos: Cada usuario del sistema está definido por una línea en el fichero /etc/passwd y cada grupo por otra línea en el fichero /etc/group. Cada usuario pertenece a uno o varios grupos y cada recurso pertenece a un usuario y un grupo. Los permisos para un recurso se pueden asignar al propietario, al grupo y a otros (resto de los usuarios). Ahora bien, para mantener un sistema seguro, pero funcional, tendremos que realizar las combinaciones necesarias entre el propietario y grupo de un recurso con los permisos de los propietarios, grupos y otros. Por ejemplo, la unidad de disco flexible tiene las siguientes características:

```
brw-rw-r-- 1 root floppy 2,0 may 5 1998 /dev/fd0
```

- Propietario: root con permiso de lectura y escritura.
- Grupo: floppy con permiso de lectura y escritura.
- Otros: resto de los usuario con permiso de lectura.

Cuando queramos que un usuario pueda escribir en la unidad de disco, sólo tendremos que incluirlo en el grupo floppy. Cualquier otro usuario que no pertenezca al grupo floppy (salvo root) sólo podrá leer el disquete.

El administrador tiene que conocer las necesidades de cada uno de sus usuarios y asignarle los mínimos privilegios para que pueda realizar su trabajo sin resultar un peligro para otros usuarios o el sistema. Más abajo veremos otro mecanismo para poder utilizar un recurso sobre el cual no tenemos privilegios.

No se asuste. Los valores que traen por defecto las distribuciones de Linux son suficiente para mantener el sistema seguro.

Otro peligro potencial para el sistema es mantener cuentas abiertas que se han dejado de utilizar. Estas cuentas pueden constituir un buen refugio para un potencial atacante y pasar desapercibidas sus acciones.

Seguridad de las claves: La seguridad de una sola cuenta puede comprometer la seguridad de todo el sistema. Esto es una realidad ante la que debemos protegernos.

Por un lado tenemos que asegurarnos de que nuestros usuarios utilizan claves sólidas:

- No deben ser una palabra conocida.
- Deberían contener letras, números y caracteres especiales.
- Deben ser fáciles de recordar y difíciles de adivinar.

Para comprobar que este requisito se verifica en nuestro sistema, podemos usar los mismos mecanismos que utilizan los atacantes. Existen varios programas que van probando varias palabras de diccionario, claves habituales y combinaciones de caracteres, que son cifrados con el mismo algoritmo que usa el sistema para mantener sus claves; después son comparadas con el valor de la clave cifrada que queremos averiguar hasta que el valor obtenido de un cifrado coincide con una clave cifrada. Posteriormente notificaremos al usuario que su clave es débil y le solicitaremos que la modifique. Usando este mecanismo, al menos podemos garantizar que no estaremos en inferioridad de condiciones con respecto a los atacantes locales. Un conocido programa para realizar el descifrado de claves es John the Ripper. Por otro lado, las claves cifradas se almacenan en el fichero `/etc/passwd`. Cualquier usuario del sistema tiene permiso de lectura sobre este fichero. Lo que es peor, agujeros en los navegadores permiten que se puedan leer ficheros arbitrarios de una máquina (evidentemente, que el usuario de navegador tenga permiso para leer), de manera que lleguen hasta un hacker que cree páginas web que exploten estos agujeros. Entonces puede parecer a primera vista que nos encontramos con un grave agujero de seguridad. El atacante, una vez obtenido el fichero `/etc/passwd` no tiene más que ejecutar su programa revientaclaves favorito y sentarse a esperar hasta que empiecen a aparecer nombres de usuario con sus respectivas contraseñas, algo que suele pasar muy rápidamente. Con suerte, si el administrador es ingenuo o dejado, incluso dará con la clave del root, abriéndosele así las puertas a la máquina objetivo. Para solucionar esta vulnerabilidad, podemos recurrir a contraseñas en la sombra (*shadow passwords*), un mecanismo consistente en extraer las claves cifradas del fichero `/etc/passwd` y situarlas en otro fichero llamado `/etc/shadow`, que sólo puede leer el root y dejar el resto de la información en el original `/etc/passwd`. El fichero `/etc/shadow` sólo contiene el nombre de usuario y su clave, e información administrativa, como cuándo expira la cuenta, etc. El formato del fichero `/etc/shadow` es similar al siguiente:

```
usuario : clave : ultimo : puede : debe : aviso : expira : desactiva : reservado
```

usuario: El nombre del usario.

- clave: La clave cifrada
- ultimo: Días transcurridos del último cambio de clave desde el día 1/1/70
- puede: Días transcurridos antes de que la clave se pueda modificar.
- tiene: Días transcurridos antes de que la clave tenga que ser modificada.
- aviso: Dias de aviso al usuario antes de que expire la clave.
- expira: Días que se desactiva la cuenta tras expirar la clave.
- desactiva: Días de duración de la cuenta desde el 1/1/70.
- reservado: sin comentarios.

Un ejemplo podría ser:

```
julia : gEvm4sbKnGRlg : 10627 : 0 : 99999 : 7 : -1 : -1 : 134529868
```

El paquete de Shadow Passwords se puede descargar desde cualquiera de los siguientes sitios, con instrucciones para su instalación:

- ftp://i17linuxb.ists.pwr.wroc.pl/pub/linux/shadow/shadow-current.tar.gz
- ftp://ftp.icm.edu.pl/pub/Linux/shadow/shadow-current.tar.gz
- ftp://iguana.hut.fi/pub/linux/shadow/shadow-current.tar.gz
- ftp://ftp.cin.net/usr/ggallag/shadow/shadow-current.tar.gz
- ftp://ftp.netural.com/pub/linux/shadow/shadow-current.tar.gz

Para activar contraseñas en la sombra, tiene que ejecutar `pwconv` como *root*; acción que creará su fichero `/etc/shadow`.

El bit SUID/SGID: En muchas ocasiones un proceso necesita ejecutarse con unos privilegios mayores (o menores) que el usuario que lo lanzó. Por ejemplo, un usuario puede modificar su propia clave con el mandato `passwd`, pero esto implica modificar el fichero `/etc/passwd`, y para esto un usuario "de a pie" no tiene permiso. ¿Cómo se soluciona? Pues activando el bit SUID del comando `passwd` (notese que cuando esto sucede, la `x` de ejecutable pasa a ser una `s`):

```
ls -la /usr/bin/passw*
-r-sr-xr-x 1 root bin 15613 abr 27 1998 /usr/bin/passwd
```

Esto quiere decir que cuando se ejecute, el proceso correspondiente va a tener los privilegios del propietario del comando (es decir, el root), no del usuario que lo lanzó. En otras palabras, el proceso generado por `passwd` pertenece a root. A primera vista, esto puede parecer una seria brecha de seguridad. Y lo es. Si el programa funciona correctamente, no tiene por qué dar problemas; pero pequeños defectos en el programa pueden ser utilizados por alguien para tratar de ejecutar otro código distinto con los privilegios de este proceso. El método suele ser el desbordamiento de la pila (buffer overflow).

Cualquier atacante que haya entrado en un sistema de forma ilegítima intentará dejar una shell con el bit SUID para mantener ese nivel de privilegio cuando vuelva a entrar en el sistema.

SGID es lo mismo que SUID, pero aplicado al grupo.

Así pues, tenga cuidado con los programas con el bit SUID/SGIG. Puede encontrarlos con

```
root# find / -type f \( -perm -04000 -o -perm -02000 \) -print
```

Tenga en cuenta que algunos programas (como `passwd`) tienen que tener el bit SUID. Compruebe en los lugares habituales, (que indicamos en la sección correspondiente) que ninguno de los programas propiedad del *root* o SUID que utiliza en su sistema, tiene un fallo de seguridad conocido que pueda ser explotado.

Nunca debe permitir que quede una shell SUID corriendo en el sistema. Si el root deja desatendida la consola durante unos instantes (recuerde, debe utilizar siempre `xlock`), un intruso podría escribir lo siguiente:

```
# cp /bin/sh /tmp/cuenta-root
# chmod 4755 /tmp/cuenta-root
```

creándose una versión SUID de la shell `sh`. En el futuro, cuando el atacante ejecute ese programa, `cuenta-root`, ¡se convertirá en *root*! Si lo escondiera en un directorio oculto, la única forma de encontrarlo sería escaneando el sistema completo como se ha explicado antes.

Seguridad del root: Los peores destrozos de un sistema es probable que no vengan de ningún *Cracker*, o de un malévolo intruso. En muchísimas más ocasiones ha sido el propio administrador el

que ha destrozado el sistema. Sí, el *root*. ¿Por qué? Por descuido, por exceso de confianza, por ignorancia. Evitar este problema no es difícil. Siguiendo unas fáciles normas, podrá protegerse de Ud. mismo:

- No use la cuenta de *root* por norma. Evítela. Intente primero cualquier acción como un usuario normal, y si ve que no tiene permiso, piense porqué y use el comando `su` si es necesario.
- Ejecute los comandos de forma segura verificando previamente la acción que va a realizar. Por ejemplo si quiere ejecutar `rm borrar.*`, ejecute primero `ls borrar.*` y si es lo que pretende modifique el mandato y ejecútelo.
- Ciertos mandatos admiten una opción (-i) para actuar de forma interactiva. Actívela, si no lo está ya añadiendo estas líneas a su fichero de recursos par la shell:
    - `alias rm='rm -i'`
    - `alias cp='cp -i'`
    - `alias mv='mv -i'`

  Siempre puede evitar estas preguntas, a veces incordiosas, con el mandato `yes`, cuando esté seguro de la operación que está realizando:

```
$ yes s|rm borrar.*
```

- Como ya deben saber, el directorio actual no está, por defecto, en la ruta de búsqueda de ejecutables (PATH). Esto garantiza que no lanzaremos, sin darnos cuenta, un ejecutable que esté en el directorio actual llamado, por ejemplo `ls`.
- Evite que la clave del *root* viaje por una red sin cifrar. Utilice `ssh` u otro canal seguro.
- Limite los terminales desde los que se puede conectar *root*. Es preferible limitarlo a la consola del sistema. Esto se puede decidir en `/etc/securetty`. Si necesita una sesión remota como root, entre como usuario normal y luego use *su*.
- Actúe de forma lenta y meditada cuando sea *root*. Sus acciones podrían afectar a un montón de cosas. ¡Piénselo antes de teclear!

Hay herramientas como `sudo` que permiten a ciertos usuarios utilizar comandos privilegiados sin necesidad de ser *root*, como montar o desmontar dispositivos. Además registra las actividades que se realizan, lo que ayuda a determinar qué hace realmente este usuario.

16.1.3 Seguridad del sistema de archivos

Una norma básica de seguridad radica en la asignación a cada usuario sólo de los permisos necesarios para poder cubrir las necesidades de su trabajo sin poner en riesgo el trabajo de los demás.

¿Como se puede poner en riesgo el correcto funcionamiento del sistema?: Podemos apuntar algunas ideas: violando la privacidad de la información, obteniendo unos privilegios que no le corresponden a un usuario, haciendo un uso desmedido de los recursos o modificando información legítima contenida en una máquina, como pueden ser el contenido de una página web o una base de datos.

¿Cómo podemos mantener un almacenamiento seguro?: La respuesta no puede ser concreta, pero sí que se pueden tomar ciertas medidas que garanticen un mínimo de seguridad y funcionalidad. Si Ud. va a administrar un sistema Linux para dar servicio a diversos usuarios, debería tener algunas nociones sobre sistemas de ficheros, que pasamos a explicar a continuación.

El árbol de directorios: Para quienes no estén familiarizados con las características del sistema de almacenamiento de información en sistemas Unix, hay que indicar que se organizan en un único árbol de directorios. Cada soporte, disco, partición, disquete o CD tiene su propia organización lógica, un sistema de ficheros. Para poder usar uno de estos soportes tenemos que "montarlo" en un directorio existente. El contenido de la partición nos aparecerá como el contenido del directorio. Un primer criterio para mantener un sistema seguro sería hacer una correcta distribución del espacio de almacenamiento. Esto limita el riesgo de que el deterioro de una partición afecte a todo el sistema. La pérdida se limitaría al contenido de esa partición. No hay unas normas generales aplicables; el uso al que vaya destinado el sistema y la experiencia son las bases de la decisión adecuada, aunque sí podemos dar algún consejo:

- Si el sistema va a dar servicio a múltiples usuarios que requieren almacenamiento para sus datos privados, sería conveniente que el directorio `/home` tuviera su propia partición.
- Si el equipo va a ser un servidor de correo, impresión, etc., el directorio `/var` o incluso `/var/spool` podrían tener su propia partición.
- Algunos directorios son necesarios en la partición raíz. Contienen datos que son necesarios durante el proceso de arranque del sistema. Son `/dev/`, `/etc`, `/bin`, `/sbin`, `/lib`, `/boot`.
- El directorio `/usr/local` contiene los programas compilados e instalados por el administrador. Resulta conveniente usar una partición propia para proteger estos programas personalizados de futuras actualizaciones del sistema. Este criterio también se puede aplicar al directorio `/opt`.

Permisos: Linux, como sistema multiusuario, asigna un propietario y un grupo a cada fichero (y directorio) y unos permisos al propietario, al grupo y al resto de los usuarios. La forma más rápida de comprobar esta característica es usar el comando `ls -la`. Así nos aparece el tipo de fichero, el propietario, el grupo, los permisos e información adicional. Por supuesto, el sistema de ficheros tiene que admitir esta característica, como es el caso del sistema de ficheros *ext2* (Linux nativo). En los sistemas de ficheros pensados para entornos monousario, como *msdos* o *vfat*, no tenemos esta característica, por lo que son inseguros y su uso no es aconsejable bajo Linux.

Es conveniente tener claros los permisos que se pueden asignar a un fichero o directorio. Puede que algunas aplicaciones no funcionen bien si algún fichero no tiene el permiso o el propietario correctos, bien por falta de permisos o bien por exceso. Algunas aplicaciones son un poco quisquillosas en este aspecto. Por ejemplo, *fetchmail* es un programa que podemos usar para recoger el correo de un servidor pop (por ejemplo). Este programa se configura en el fichero `.fetchmailrc`, donde tendremos que indicar la clave que usamos en el servidor; pues bien, si este fichero tiene permiso de lectura para otro usuario que no sea el propietario, `fetchmail` no funcionará. Otras aplicaciones, como por ejemplo *inn* (un servidor de noticias de Internet) tampoco funcionará si el propietario de sus ficheros es otro usuario distinto a `news`. Todo esto está perfectamente documentado en cada uno de los programas, por lo que es conveniente leer la documentación que aporta y las páginas del manual.

Permisos de ficheros y directorios: Como decíamos anteriormente, tenemos que asegurarnos de que los ficheros del sistema y los de cada usuario sólo son accesibles por quienes tienen que hacerlo y de la forma que deben. No sólo hay que protegerse de ataques o miradas indiscretas, también hay que protegerse de acciones accidentales. En general, cualquier sistema UNIX divide el control de acceso a ficheros y directorios en tres elementos: `propietario`, `grupo` y `otros`. Tanto el propietario como el grupo son únicos para cada fichero o directorio. Eso sí, a un grupo pueden pertenecer múltiples usuarios. `Otros` hace referencia a los usuarios que ni son el propietario ni pertenecen al grupo. Todas estas características se almacenan en el sistema de ficheros, en particular en un `i-nodo`, que es un elemento que describe las características de un fichero en disco (salvo su nombre).

Permisos en Unix

Propiedad: Qué usuario y grupo posee el control de los permisos del i-nodo. Se almacenan como dos valores numéricos, el uid (user id) y gid (group id).

Permisos: Bits individuales que definen el acceso a un fichero o directorio. Los permisos para directorio tienen un sentido diferente a los permisos para ficheros. Más abajo se explican algunas diferencias.

- **Lectura (r):**
    - **Fichero**: Poder acceder a los contenidos de un fichero
    - **Directorio**: Poder leer un directorio, ver qué ficheros contiene
- **Escritura (w)**:
    - **Fichero**: Poder modificar o añadir contenido a un fichero
    - **Directorio**: Poder borrar o mover ficheros en un directorio
- **Ejecución(x)**:
    - **Fichero**: Poder ejecutar un programa binario o guion de shell
    - **Directorio**: Poder entrar en un directorio

Estos permisos se pueden aplicar a:

- **usuario (u)**: El propietario del fichero
- **grupo (g)**: El grupo al que pertenece el fichero
- **otros (o)**: El resto de los usuarios del sistema

Además tenemos otros bits de permisos que no podemos pasar por alto cuando estamos tratando de temas de seguridad.

Sticky bit: El sticky bit tiene su significado propio cuando se aplica a directorios. Si el sticky bit está activo en un directorio, entonces un usuario sólo puede borrar ficheros que son de su propiedad o para los que tiene permiso explícito de escritura, incluso cuando tiene acceso de escritura al directorio. Esto está pensado para directorios como /tmp, que tienen permiso de escritura global, pero no es deseable permitir a cualquier usuario borrar los ficheros que quiera. El sticky bit aparece como 't' en los listados largos de directorios.

drwxrwxrwt 19 root root 8192 Jun 24 14:40 tmp

Attributo SUID: (Para Ficheros): Este bit describe permisos al identificador de usuario del fichero. Cuando el modo de acceso de ID de usuario está activo en los permisos del propietario, y ese fichero es ejecutable, los procesos que lo ejecutan obtienen acceso a los recursos del sistema basados en el usuario que crea el proceso (no el usuario que lo lanza). Por ejemplo /usr/bin/passwd es un ejecutable propiedad de root y con el bit SUID activo. ¿Por qué? Este programa lo puede usar cualquier usuario para modificar su clave de acceso, que se almacena en

```
-rw-r--r-- 1 root root 1265 Jun 22 17:35 /etc/passwd
```

pero según los permisos que observamos en este fichero, sólo root puede escribir y modificar en él. Entonces sería imposible que un usuario pudiera cambiar su clave si no puede modificar este fichero. La solución para este problema consiste en activar el bit SUID para este fichero:

```
-r-s--x--x 1 root root 10704 Apr 14 23:21 /usr/bin/passwd
```

de forma que cuando se ejecute, el proceso generado por él es un proceso propiedad de root con todos los privilegios que ello acarrea.

¿Piensa que esto puede ser un riesgo para la seguridad? Efectivamente lo podría ser si no mantenemos un mínimo de atención, ya que en este tipo de programas se pueden producir desbordamientos de búfer que comprometan su sistema. Recuerde siempre lo siguiente:

- No asignar el bit SUID salvo cuando sea estrictamente necesario.
- Comprobar que cualquier programa con est bit activo no tiene ningún desbordamiento de buffer (conocido).
- No asignarlo jamás si el programa permite salir a la shell.

Atributo SGID: (Para ficheros): Si está activo en los permisos de grupo, este bit controla el estado de "poner id de grupo" de un fichero. Actúa de la misma forma que SUID, salvo que afecta al grupo. El fichero tiene que ser ejecutable para que esto tenga algún efecto.

Atributo SGID: (Para directorios): Si activa el bit SGID en un directorio (con "chmod g+s directorio"), los ficheros creados en ese directorio tendrán puesto su grupo como el grupo del directorio. A continuación se describen los significados de los permisos de acceso individuales para un fichero. Normalmente un fichero tendrá una combinación de los siguientes permisos:

-r-------- Permite acceso de lectura al propietario

--w------- Permite modificar o borrar el fichero al propietario

---x------ Permite ejecutar este programa al propietario, (los guiones de shell también requieren permisos de lectura al propietario)

---s------ Se ejecutará con usuario efectivo ID = propietario

-------s-- Se ejecutará con usuario efectivo ID = grupo

-rw------T No actualiza "instante de última modificación". Normalmente usado para ficheros de intercambio (swap)

---t------ No tiene efecto. (antes sticky bit)

A continuación se describen los significados de los permisos de acceso individuales para un directorio. Normalmente un directorio tendrá una combinación de los siguientes permisos:

dr-------- Permite listar el contenido pero no se pueden leer los atributos.

d--x------ Permite entrar en el directorio y usar en las rutas de ejecución completas.

dr-x------ Permite leer los atributos del fichero por el propietario.

d-wx------ Permite crear/borra ficheros.

d------x-t Previene el borrado de ficheros por otros con acceso de escritura. Usado en /tmp

d---s--s-- No tiene efecto

Los ficheros de configuración del sistema (normalmente en /etc) es habitual que tengan el modo 640 (-rw-r-----), y que sean propiedad del root. Dependiendo de los requisitos de seguridad del sistema, esto se puede modificar. Nunca deje un fichero del sistema con permiso de escritura para un grupo o para

otros. Algunos ficheros de configuración, incluyendo /etc/shadow, sólo deberían tener permiso de lectura por root, y los directorios de /etc no deberían ser accesibles, al menos por otros.

SUID Shell Scripts: Los scripts de shell SUID son un serio riesgo de seguridad, y por esta razón el núcleo no los acepta. Sin importar lo seguro que piense que es su script de shell, puede ser utilizado para que un Cracker pueda obtener acceso a una shell de root.

Enlaces: Los sistemas de ficheros de tipo Unix permiten crear enlaces entre ficheros. Los enlaces pueden ser `duros` o `simbólicos`. El primer caso consiste en asignar más de un nombre a los mismos datos en disco. Un enlace duro no consume más espacio adicional que el que pueda representar el nuevo nombre que le damos a unos datos y sólo es válido para ficheros que estén en el mismo sistema de ficheros, es decir, la misma partición. Los enlaces simbólicos son ficheros que apuntan a otro fichero o directorio. Crean un nuevo fichero pequeño que contiene la ruta del fichero destino.

Tripwire: Una forma cómoda de detectar ataques locales (y también de red) en su sistema es ejecutar un programa que verifique la integridad de la información almacenada en los ficheros, tal como *Tripwire*. El programa *Tripwire* ejecuta varios cheksums de todos los binarios importantes y ficheros de configuración y los compara con una base de datos con valores de referencia aceptados como buenos. Así se detecta cualquier cambio en los ficheros.

Es buena idea instalar *tripwire* en un disquete y protegerlo físicamente. De esta forma no se puede alterar *tripwire* o modificar su base de datos. Una vez que *tripwire* se ha configurado, es buena idea ejecutarlo como parte de de los deberes habituales de administración para ver si algo ha cambiado. Incluso puede añadir una entrada a *crontab* para ejecutar *tripwire* desde su disquete todas las noches y enviar por correo los resultados y verlos por la mañana, algo como esto:

```
MAILTO=gonzalo
15 05 * * * root /usr/local/bin/tripwire
```

que le enviará por correo un informe cada mañana a las 5:15 am.

Tripwire puede ser una de la mejores herramientas para detectar intrusos antes de que tenga otro tipo de noticias de ellos. Como son muchos los ficheros que se modifican en su sistema, debería tener cuidado para discernir lo que es la actividad de un Cracker y lo que es la actividad normal del sistema.

Limitar el espacio: Una ataque posible a cualquier sistema es intentar consumir todo el espacio del disco duro. Una primera protección contra este ataque es separar el árbol de directorios en diversos discos y particiones. Pero esto puede no ser suficiente y por eso el núcleo del sistema proporciona la posibilidad de controlar el espacio de almacenamiento por usuario o grupo.

Lo primero que tendríamos que hacer es asegurarnos de que nuestro núcleo tiene soporte para las cuotas de usuarios.

```
# dmesg | grep quotas
VFS: Diskquotas version dquot_6.4.0 initialized
```

En caso contrario, el núcleo no ha sido compilado con soporte para el sistema de cuotas para usuarios. En este caso será necesario compilar un nuevo núcleo Linux. El resto del procedimiento de instalación se puede realizar utilizando la documentación existente. Ahora es necesario editar el

fichero `/etc/fstab` y añadir `usrquota` o `grpquota` en la partición o particiones en las que nos interese limitar el espacio de almacenamiento. El siguiente ejemplo establece el sistema de cuotas para el uso del directorio `/home` montado en la partición `/dev/hda3`:

```
/dev/hda3 /home ext2 defaults,usrquota 1 2
```

Ahora podemos recopilar la información de las particiones donde se haya definido el sistema de cuotas. Podemos usar el comando:

```
/sbin/quotachek -av

Scanning /dev/hda3 [/home] done
Checked 215 directories and 2056 files
Using quotafile /home/quota.user
Updating in-core user quotas
```

Al ejecutar este comando también se crea un fichero llamado `quota.user` o `quota.grp` en la partición o particiones afectada(s).

```
# ls -la /home/quota.user

-rw------- 1 root root 16224 Feb 04 14:47 quota.user
```

Ya está activo el sistema de cuotas y la próxima vez que se inicie el sistema, se activarán automáticamente en todas las particiones que se hayan definido. Ya no será necesario volver a ejecutar manualmente este comando, ya que el sistema lo hara de forma automática al comprobar y montar cada uno de los sistemas de ficheros desde el fichero `/etc/rc.d/rc.sysinit`. El siguiente paso es definir la cuotas para cada usuario. Para ello existen dos métodos. El primero consiste en editar la quota de cada usuario. Por ejemplo, para editar la cuota del usuario *antonio*, se ejecuta desde el usuario *root* el comando:

```
# edquota -u antonio

Quotas for user antonio:
/dev/hda3: blocks in use:15542,limits (soft=0,hard=0)
inodes in use: 2139, limits (soft = 0, hard = 0)
```

El sistema de cuotas de Linux permite limitar el número de bloques y el número de i-nodos que un usuario puede tener. Los valores a modificar son los límites que están puestos entre paréntesis (que ahora valen 0). Ahí se puede especificar cualquier cantidad (en Kbytes). Por ejemplo, para limitar la cuota de disco del usuario *antonio* a 1 Mb, se pondría lo siguiente:

```
Quotas for user antonio:
/dev/hda7:blocks in use:18542,limits (soft=1024,hard=1024)
inodes in use: 1139, limits (soft = 0, hard = 0)
```

El límite soft es un límite de aviso y el límite hard es un límite insalvable, es decir, el sistema ya no le asigna más espacio. De una forma análoga, podríamos modificar la cuota de espacio asignada al grupo users con:

```
# edquota -g users
```

Normas prácticas: Aunque sea necesario tener claros los conceptos y dedicarle algo de tiempo a una correcta planificación, tampoco los pelligros expuestos tienen por qué asustar a nadie. Todas las distribuciones de Linux traen unos valores por defecto que son más que razonables para cubrir unas necesidades normales.

- **nosuid, nodev, noexec**.

  Salvo casos excepcionales, no debería haber ninguna razón para que se permita la ejecución de programas SUID/SGID en los directorios *home* de los usuarios. Esto lo podemos evitar usando la opción `nosuid' en el fichero `/etc/fstab` para las particiones que tengan permiso de escritura por alguien que no sea el *root*. También puede ser útil usar `nodev' y `noexec' en las particiones de los directorios personales de los usuarios y en `/var`, lo que prohíbe la creación dispositivos de bloque o carácter y la ejecución de programas.

- **Sistemas de ficheros en red**

  Si exporta sistemas de archivos vía NFS, esté seguro de configurar `/etc/exports` con los accesos lo más restrictivos posibles. Esto significa no usar plantillas, no permitir acceso de escritura a *root* y montar como sólo lectura siempre que sea posible.

- **umask**

  Configure la máscara de creación de ficheros para que sea lo más restrictiva posible. Son habituales *022*, *033*, y la más restictiva *077*, y añadirla a `/etc/profile`.

  El comando *umask* se puede usar para determinar el modo de creación de ficheros por defecto en su sistema. Es el complemento octal a los modos de fichero deseado. Si los ficheros se crean sin ningún miramiento de estado de permisos, el usuario, de forma inadvertida, podrá asignar permisos de lectura o escritura a alguien que no debería tenerlos. De forma típica, el estado de umask incluye *022*, *027* y *077*, que es lo más restrictivo. Normalmente *umask* se pone en */etc/profile* y por tanto se aplica a todos los usuarios del sistema. Por ejemplo, puede tener una línea parecida a la siguiente:

  ```
  # Pone el valor por defecto de umask del usuario
  umask 033
  ```

  Esté seguro de que el valor *umask* de *root* es *077*, lo cual desactiva los permisos de lectura, escritura y ejecución para otros usuarios, salvo que explícitamente use *chmod(1)*.

  Si está usando , y utiliza su esquema de creación de idetificador de grupos y usuarios (*User Private Groups*), sólo es necesario usar *002* para *umask*. Esto se debe a que al crear un usuario se crea un grupo exclusivo para ese usuario.

- **Limitar recursos**

  Ponga el límites al sistema de ficheros en lugar de 'ilimitado' como está por defecto. Puede controlar el límite por usuario utilizando el módulo *PAM* de límite de recursos y */etc/pam.d/limits.conf*. Por ejemplo, los límites para un grupo `users' podría parecer a esto:

  ```
  @users hard core 0
  @users hard nproc 50
  @users hard rss 5000
  ```

  Esto dice que se prohiba la creación de ficheros *core*, restringe el número de procesos a 50, y restringe el uso de memoria por usuario a 5M.

- **wtmp, utmp**

  Los ficheros `/var/log/wtmp` y `/var/run/utmp` contienen los registros de conexión de todos los usuarios de su sistema. Se debe mantener su integridad, ya que determinan cuándo y desde dónde entró en su sistema un usuario o un potencial intruso. Los ficheros deberían tener los permisos `644`, sin afectar a la normal operación del sistema.

- **Sticky bit**

  El `sticky bit` se puede usar para prevenir borrados accidentales o proteger un fichero para sobreescritura. También previene que alguien cree enlaces simbólicos a un fichero, que ha sido el origen de ataques basados en el borrado de los ficheros `/etc/passwd` o `/etc/shadow`. Vea la página del manual de `chattr(1)` para tener más información.

- **SUID y SGID**

  Los ficheros `SUID` y `SGID` de su sistema son potenciales riesgos de seguridad y deberían ser controlados. Como estos programas garantizan privilegios especiales al usuario que los ejecuta, es necesario estar seguro que no hay instalados programas inseguros. Un truco favorito de los *crackers* es explotar programas con el bit `SUID`, y entonces dejar un programa `SUID` como puerta trasera para entrar la próxima vez, incluso aunque el agujero original ya esté tapado.

  Encuentre todos los programas `SUID/SGID` de su sistema y mantener la pista de lo que son, para que esté prevenido de cualquier cambio que podría indicar un potencial intruso. Use el siguiente comando para localizar todos los progrmas *SUID/SGID* en su sistema:

  ```
  root# find / -type f \( -perm -04000 -o -perm -02000 \)
  ```

  Incluso podría crear una base de datos de progrmas `SUID` con

  ```
  root# find / -type f \( -perm -04000 -o -perm -02000 \)>/var/suid
  ```

  y posteriormente verificar si ha aparecido alguno nuevo con el siguiente guión:

  ```
  for fich in `find / -type f \( -perm -04000 -o -perm -02000 \)`
  do
  if ! grep $fich /var/suid
  then
  echo "$fich es un nuevo fichero con SUID"
  fi
  done
  echo "Actualiza la base de datos si es necesario"
  ```

  Puede eliminar los permisos `SUID` o `SGIG` de un programa con `chmod(1)`, y siempre puede devolverlo a su estado original si piensa que es absolutamente necesario.

- **Permisos de escritura**

  Los ficheros con permiso de escritura global, particularmente los del sistema, pueden ser un agujero de seguridad si un cracker obtiene acceso a su sistema y los modifica. Además, los directorios con permiso de escritura global son peligrosos, ya que permiten a un cracker añadir y borrar los ficheros que quiera. Para localizar los ficheros con permiso de escritura global, use el siguiente comando:

  ```
  root# find / -perm -2 -print
  ```

  y esté seguro de saber por qué tienen esos permisos de escritura. En el curso normal de una operación los ficheros tendrán permisos de escritura, incluidos algunos de `/dev` y enlaces simbólicos.

- **Ficheros extraños**

  Los ficheros sin propietario también pueden ser un indicio de que un intruso ha accedido a su sistema. Puede localizar los ficheros de su sistema que no tienen propietario o que no pertenecen a un grupo con el comando:

  ```
  root# find / -nouser -o -nogroup -print
  ```

- **Ficheros peligrosos**

La localización de ficheros `.rhosts` debería ser uno de los deberes regulares de la administración de su sistema, ya que estos ficheros no se deberían permitir en sus sistema. Recuerde que un cracker sólo necesita una cuenta insegura para potencialmente obtener acceso a toda su red. Puede localizar todos los ficheros `.rhosts` de su sistema con el siguiente comando:

```
root# find /home -name .rhosts -print
```

- **Permisos**

  Finalmente, antes de cambiar permisos en cualquier sistema de ficheros, esté seguro de que entiende lo que hace. Nunca cambie permisos de un fichero simplemente porque parezca la forma fácil de hacer que algo funcione. Siempre debe determinar porqué el fichero tiene esos permisos y propietario antes de modificarlos.

16.1.4 Seguridad del núcleo

Linux tiene la gran ventaja de tener disponible el código fuente del núcleo; en realidad Linux propiamente dicho es sólo el núcleo. Esto nos permite la posibilidad de crear núcleos a medida de nuestras necesidades. Y parte de nuestras necesidades será la mejora de la seguridad.

Para compilar el núcleo primero tendremos que configurar las opciones que nos interesen. Los fuentes del núcleo se guardan habitualmente en el directorio /usr/src/linux, y una vez situados en él, tendremos que ejecutar «make menuconfig» (o «make xconfig» si estamos en modo gráfico). Así nos aparecen todas las opciones de configuración. Dentro de ellas nos vamos a fijar en las que están relacionadas con la seguridad, viendo una breve explicación de lo que hacen y cómo se usan. Como el núcleo controla las características de red de su sistema, es importante que el núcleo tenga las opciones que garanticen la seguridad y que el propio núcleo no pueda ser comprometido. Para prevenir algunos de los últimos ataques de red, debe intentar mantener una versión del núcleo actualizada.

Una de las características más interesantes del núcleo Linux es la posibilidad de realizar enmascaramiento de direcciones. Con esta técnica podremos dar acceso a Internet a una red local con direcciones privadas de forma transparente, es decir, sin ningún tipo de modificación en la configuración de las aplicaciones clientes, a diferencia de los proxies clásicos. Consiste en que el sistema Linux que posee la conexión hacia el exterior recibe las peticiones de conexión desde los equipos de la red local que tienen direcciones no válidas para Internet. El equipo Linux rehace la petición poniendo su propia dirección IP y modificando el puerto al que tiene que responder el equipo remoto. Cuando Linux recibe la respuesta del equipo remoto, mira el puerto al que va destinado y vuelve a rehacer el paquete para enviarlo al equipo concreto de la red local que solicitó la conexión. De esta forma podemos mantener un nivel aceptable de protección para los equipos de la red local, ya que sólo podrán recibir respuestas a peticiones que ellos mismos originaron.

Opciones de compilación

IP: Drop source routed frames (CONFIG_IP_NOSR): Esta opción debería estar activada. Source routed frames contienen la ruta completa de sus destinos dentro del paquete. Esto significa que los enrutadores a través de los que circula el paquete no necesitan inspeccionarlo, y sólo lo reenvían. Esto podría ocasionar que los datos que entran a su sistema puedan ser un exploit potencial.

IP: Firewalling (CONFIG_IP_FIREWALL): Esta opción es necesaria si va a configurar su máquina como un cortafuegos, hacer enmascaramiento o desea proteger su estación de trabajo con línea telefónica de que alguien entre a través de su interfaz PPP. Con esta opción activa podremos usar el

filtrado de paquetes en el propio núcleo del sistema, decidiendo el tráfico que llega o sale de nuestro equipo.

IP: forwarding/gatewaying (CONFIG_IP_FORWARD): Si activa reenvío IP (IP forwarding), su Linux esencialmente se convierte en un encaminador (router). Si su máquina está en una red, podría estar enviando datos de una red a otra, y quizás saltándose un cortafuegos que esté puesto allí para evitar que esto suceda. A los usuarios con un puesto aislado y conexión telefónica les interesará desactivar esta característica. Otros usuarios deberían pensar en las implicaciones de seguridad de hacer esto en su caso concreto. Las máquinas que actúen como cortafuegos tendrán que activar esta característica y usarla junto al software cortafuegos. Puede activar y desactivar el reenvío IP (IP forwarding) dinámicamente usando el siguiente comando:

```
root# echo 1 > /proc/sys/net/ipv4/ip_forward
```

y desactivarlo con el comando:

```
root# echo 0 > /proc/sys/net/ipv4/ip_forward
```

Ese fichero (y muchos otros ficheros de `/proc`) aparecerá con longitud cero, pero en realidad no es un fichero en el sentido clásico, sino que son datos guardados en memoria.

IP: firewall packet logging (CONFIG_IP_FIREWALL_VERBOSE): Esta opción le suministra información sobre los paquetes que su cortafuegos recibe, como remitente, destinatario, puerto, etc. Así podremos rastrear los orígenes de los posibles intentos de ataque.

IP: always defragment (CONFIG_IP_ALWAYS_DEFRAG): Generalmente esta opción está desactivada, pero si está construyendo un host cortafuegos o para enmascaramiento, deberá activarla. Cuando se envían paquetes de un host a otro, no siempre se envían como simples paquetes de datos, sino que se fragmentan en varios trozos. El problema es que los números de puerto sólo se almacenan en el primer fragmento. Esto significa que alguien puede insertar información en el resto de los paquetes para su conexión que se supone que no deberían estar allí.

IP: syn cookies (CONFIG_SYN_COOKIES): El ataque SYN es un ataque de denegación de servicio (denial of service, DoS) que consume todos los recursos de su máquina forzando un reinicio. No podemos encontrar ninguna razón por la que no debiera activar esto.

Dispositivos del núcleo: Hay algunos dispositivos de bloque y carácter disponibles en Linux que también le resultarán utiles para mantener la seguridad de sus sistema.

Los dos dispositivos */dev/random* y */dev/urandom* los proporciona el núcleo para generar datos aleatorios en cualquier instante. Por ejemplo, se utilizan para iniciar un número de secuencia para conexiones TCP/IP.

Ambos, */dev/random* y */dev/urandom*, deberían ser suficientemente seguros como para generar claves PGP, SSH y otras aplicaciones donde son un requisito números aleatorios seguros para generar claves válidas para una sesión. Los atacantes no deberían ser capaces de determinar el siguiente número dada cualquier secuencia de números con este origen. Se han dedicado muchos esfuerzos para garantizar que los números que se obtienen de esta fuente son pseudoaleatorios en todos los sentidos de la palabra pseudoaleatorio.

La única diferencia es que */dev/random* suministra bytes aleatorios y le hace esperar para que se

acumulen más. Observe que en algunos sistemas puede bloquear durante un rato a la espera de que se genere una nueva entrada de usuario al sistema. Por tanto debe tener cuidado al usar */dev/random*. (Quizás lo mejor que puede hacer es usarlo cuando esté generando información sensible de claves e indicarle al usuario que pulse una tecla repetidas veces hasta que indique por la pantalla "*Ya es suficiente*").

/dev/random tiene gran calidad de entropía, midiendo tiempos entre interrupciones, etc. Bloquea hasta que hay disponibles suficientes bits de datos aleatorios.

/dev/urandom es parecido, no es tan seguro, pero suficiente para la mayoría de las aplicaciones. Puede leer los dispositivos usando algo parecido a lo siguiente:

```
root# head -c 6 /dev/urandom | uuencode -
```

Esto imprimirá seis caracteres aleatorios en la consola, válidos para la generación de una clave.

16.1.5 Seguridad de Red

La seguridad de las conexiones en red merecen en la actualidad una atención especial, incluso por medios de comunicación no especializados, por el impacto que representan los fallos ante la opinión pública. El propio desarrollo tanto de Linux, como de la mayoría del software que lo acompaña, es de fuentes abiertas. Podemos ver y estudiar el código. Esto tiene la ventaja de que la seguridad en Linux no sea una mera apariencia, sino que el código está siendo escrutado por muchas personas distintas que rápidamente detectan los fallos y los corrigen con una velocidad asombrosa. Si además comprendemos los mecanismos que se siguen en las conexiones en red, y mantenemos actualizados nuestros programas, podemos tener un nivel de seguridad y una funcionalidad aceptables. Tampoco tienen las mismas necesidades de seguridad un equipo doméstico, con conexiones esporádicas a Internet, que un servidor conectado permanentemente y que actúe como pasarela entre una intranet e Internet. Para describir las pautas de actuación seguras iremos examinando cómo actúan las conexiones y cómo podemos protegerlas.

Inetd: Para atender las solicitudes de conexión que llegan a nuestro equipo existe un demonio llamado **inetd** que está a la escucha de todos los intentos de conexión que se realicen a su máquina. Cuando le llega una solicitud de conexión irá dirigida a un puerto (número de servicio, quizás sea más claro que puerto), por ejemplo, el 80 sería una solicitud al servidor de páginas web, 23 para telnet, 25 para smtp, etc. Los servicios de red que presta su máquina están descritos en `/etc/inetd.conf` (y en `/etc/services` los números de puertos). Por ejemplo, en `/etc/inetd.conf` podemos encontrar las siguientes líneas:

```
(...)
pop-3 stream tcp nowait root /usr/sbin/tcpd ipop3d
# imap stream tcp nowait root /usr/sbin/tcpd imapd
(...)
```

Esto quiere decir que, cuando llegue una solicitud de conexión al puerto 110 (pop3) se ejecutará el programa `/usr/sbin/tcpd ipop3d`. Sin embargo, el servicio imap está deshabilitado (está comentado con un # delante), por lo que el sistema no le responde.

TCP Wrapper: El siguiente paso es `/usr/sbin/tcpd`, que es el **tcp_wrapper**: un servicio que

verifica el origen de las conexiones con su base de datos `/etc/hosts.allow` (equipos autorizados) y `/etc/hosts.deny` (equipos a los que se les deniega la conexión). **tcpd** anota todos los intentos de conexión que le llegan en `/var/log/secure` para que tenga la posibilidad de saber quién intenta conectarse a su máquina y si lo consigue. Si **tcpd** autoriza la conexión, ejecuta **ipop3d** que es el programa que realmente atiende la conexión, ante el cual se tiene que validar el usuario mediante una clave. Observe que ya llevamos tres niveles de seguridad: prestar un servicio, autorizar un conexión y validar un usuario.

También hay que asegurarse de que el programa **ipop3d** no tenga ninguna vulnerabilidad, es decir, que esté actualizado. Existen numerosos medios para estar al día de las vulnerabilidades que aparecen. Una buena lista de correo o una revista electrónica tal vez sean la forma más rápida de conocer los incidentes, las causas y las soluciones. Posiblemente la mejor lista de correo para el mundo Unix sea Bugtraq (busque en forums).

Pero esto no es todo, además puede filtrar las conexiones que le lleguen desde el exterior para que ni siquiera alcancen a los **tcp_wrappers**. Por ejemplo, en el caso de conexiones a Internet por módem:

```
ipchains -A input -j DENY -s 0/0 -d $4/32 23 -p tcp -i ppp0 -l
```

poniendo la anterior línea en el fichero `/etc/ppp/ip-up` (y `ipchains -F input` en `ip-down`) estaríamos añadiendo (`-A`) un filtro de entrada (`input`), que deniega (`-j DENY`) desde cualquier sitio de internet (`-s 0/0`) dirigidas a nuestro equipo (`-d $4/32`) al puerto telnet (`23`) por tcp (`-p tcp`) que lleguen desde internet (en este caso `-i ppp0`) y que además las anote en el registro de incidencias (`-l`) (`$4` es la dirección IP que obtenemos dinámicamente).

El mecanismo de filtrado de conexiones se realiza en el núcleo del sistema operativo y si ha sido compilado con estas opciones. Normalmente lo está. Este filtrado se realiza a nivel de red y transporte: cuando llega un paquete por un interfaz de red se analiza siguiendo los filtros de entrada. Este paquete puede ser aceptado, denegado o rechazado, en este último caso se avisa al remitente. Si los filtros de entrada aceptan el paquete, pasa al sistema si era su destino final o pasa por los filtros de reenvío o enmascaramiento, donde se vuelve a repetir una de las acciones. Por último, los paquetes que proceden del propio sistema o los que han sido aceptados por los filtros de reenvío o enmascaramiento pasan al filtro de salida. En cualesquiera de estos filtros se puede indicar que lo anote en el registro de incidencias.

Registro y conocimiento de incidencias: A parte de todo esto, puede conocer las incidencias que ocurren durante el funcionamiento del sistema. Por un lado conviene familiarizarse con los procesos que se ejecutan habitualmente en una máquina. Es una buena costumbre ejecutar periódicamente `ps axu`. Cualquier cosa extraña debiéramos aclararla. Puede matar cualquier proceso con la orden `kill -9 pid` (o `killall -9 nombre_proceso`). Pero en caso de ataque activo, lo mejor es desconectar de la red inmediatamente, si es posible, claro está.

Después tenemos los registros de incidencias (las ubicaciones pueden ser diferentes dependiendo del sistema, pero no radicalmente distintas) de `/var/log`.

Trabajando en modo texto se puede hacer en una consola virtual (como *root*)

```
tail -f /var/log/messages
```

y

```
tail -f /var/log/secure
```

Y de esta forma podemos ir viendo las incidencias del sistema. Conviene también familiarizarse con las anotaciones que aparecen habitualmente para diferenciarlas de las que puedan presentar un

problema. En modo gráfico hay un programa llamado ktail que le muestra las incidencias de una forma similar a la anterior.

Comunicaciones seguras: Por último, nos interesará mantener unas comunicaciones seguras para garantizar la privacidad e integridad de la información. Actualmente existen las herramientas necesarias para cada necesidad.

Podemos usar cifrados simétricos como pgp y gpg para documentos, correo electrónico y comunicaciones sobre canales inseguros

Podemos crear canales de comunicación seguros de distinto tipo:

- SSH (Secure Shell), stelnet: SSH y stelnet son programas que le permiten efectuar conexiones con sistemas remotos y mantener una conexión cifrada. Con esto evitamos, entre otras cosas, que las claves circulen por la red sin cifrar.
- Cryptographic IP Encapsulation (CIPE): CIPE cifra los datos a nivel de red. El viaje de los paquetes entre hosts se hace cifrado. A diferencia de SSH que cifra los datos por conexión, lo hace a nivel de socket. Así un conexión lógica entre programas que se ejecutan en hosts diferentes está cifrada. CIPE se puede usar en tunnelling para crear una Red Virtual Privada. El cifrado a bajo nivel tiene la ventaja de poder hacer trabajar la red de forma transparente entre las dos redes conectadas en la RVP sin ningún cambio en el software de aplicación.
- SSL: En su estado actual proporciona los siguientes servicios:
    - Cifrado de datos: la información transferida, aunque caiga en manos de un atacante, será indescifrable, garantizando así la confidencialidad.
    - Autenticación de servidores: el usuario puede asegurarse de la identidad del servidor al que se conecta y al que posiblemente envíe información personal confidencial.
    - Integridad de mensajes: se impide que modificaciones intencionadas o accidentales en la información mientras viaja por Internet pasen inadvertidas.
    - Opcionalmente, autenticación de cliente: permite al servidor conocer la identidad del usuario, con el fin de decidir si puede acceder a ciertas áreas protegidas.

16.1.6 Preparación para la seguridad

La seguridad es un proceso continuo, que requiere tener previsto hasta lo imprevisible. Tener unos buenos hábitos y tomar unas pequeñas precauciones nos ayudarán mucho.

Determinar los servicios activos: Desactive todos los servicios que no vaya a prestar, en particular revise los ficheros /etc/inittab, /etc/inetd.conf y los demonios que se lanzan durante el arranque. Si no está realmente seguro de lo que hace, mejor no haga nada; las distribuciones más modernas incorporan unos mínimos de seguridad aceptables para un usuario medio. No tiene sentido tener abierto un servicio del que no va a hacer uso ningún usuario legal. Puede que esté consumiendo recursos de su sistema para ofrecer a algún atacante la posibilidad de violarlo. Puede usar un analizador de puertos para ver qué parte de su sistema es visible desde el exterior. Existen utilidades como SATAN, Nessus o nmap que realizan esta labor. Trinux es una minidistribución de Linux totalmente portable que se puede llevar en 2 ó 3 disquetes y se ejecuta por completo en RAM, puediéndose usar desde cualquier equipo para la red. Se arranca desde el disquete y no utiliza el disco duro para nada. Contiene las últimas versiones de algunas herramientas muy prácticas enfocadas a la seguridad en redes. Nos permitirá analizar el tráfico de la red, analizar puertos e incluso ver el contenido de los paquetes que circulan por la red.

Proteger los ficheros importantes: Existe un parche para el núcleo Linux que impide que ciertos ficheros puedan ser modificados, incluso por el propio root. El núcleo parcheado de esta forma puede

garantizarnos la integridad de la información almacenada incluso en el caso de que alguien consiguiera privilegios de root en nuestro sistema. Este parche se puede obtener, junto con la información necesaria para su instalación, en LIDS. Si no queremos aplicar el parche, sí que deberíamos vigilar los permisos de ficheros y directorios.

Software actualizado: La gran mayoría del sofware que acompaña a Linux es de código fuente público, como el propio núcleo. Esto es una garantía de seguridad en sí. Cientos de expertos analizan minuciosamente el código para detectar alguna pega que poder publicar en las listas de correo sobre seguridad más prestigiosas, y se corrigen con gran rapidez. De esta forma nos garantizamos un software de calidad y no una mera seguridad aparente. Esto por otro lado nos obliga a ir sustituyendo las versiones defectuosas por otras corregidas y que mejoran las prestaciones. En cualquier sistema operativo, mantener un software que ha demostrado tener fallos supone asumir un riesgo innecesario. Para estar actualizado consulte los recursos de información sobre seguridad en Linux.

Prevenir pérdidas de información: Existen acontecimientos de los que nos puede resultar muy difícil protegernos como son los desastres naturales, únicamente podremos seguir una serie de pasos para evitar que su incidencia sea lo menor posible. La mejor solución es mantener un buen conjunto de copias de seguridad sobre toda la información necesaria del sistema. Hay que pensar que las copias de seguridad no sólo nos protegen de desastres naturales, también de los desastres que pueda ocasionar algún intruso en nuestro sistema, de cualquier ataque a la disponibilidad o integridad de la información del sistema. Si los datos tienen un tamaño inferior a 650Mb, puede ser una buena opción grabarlos en un CD, bien permanente (ya que es más difícil de falsificar con posterioridad, y si están almacenados de forma adecuada pueden durar mucho tiempo) o regrabable. Las cintas y otros medios sobre los que se puede escribir deberían protegerse tan pronto como se completa la copia y se verifica para evitar la falsificación. Tenga cuidado y almacene su copia de seguridad en un sitio seguro. Una buena copia de seguridad le asegura que tiene un buen punto desde el que restaurar su sistema. Hay que insistir en la seguridad de las copias de seguridad. Si las copias de seguridad no están almacenadas en un sitio seguro, puede que el posible intruso no tenga necesidad de idear métodos sofisticados para obtenerla, si le basta con copiar o sustraer un CD.

Características de las copias de seguridad: Cuando se realice una copia de seguridad es conveniente seleccionar un método que garantice la conservación de las características de la información como son derechos y permisos. Si realizamos una copia de seguridad de una forma o sobre un soporte que no contemple esta posibilidad, si tenemos que restaurar los datos sobre el sistema el resultado sobre la seguridad y funcionalidad globales puede ser impredecible.

Secuencia de Copias: Es necesario tener un política de copias de seguridad adecuada a las características de la entidad que estamos gestionando. Quizás el mejor método es el de rotación de cintas. Pasamos a verlo con un ejemplo. Un ciclo de seis cintas es fácil de mantener. Esto incluye cuatro cintas para la semana, una cinta para cada Viernes y una cinta para para los Viernes impares. Se realiza una copia incremental cada día, y una copia completa en la cinta adecuada de cada Viernes. Si hace algún cambio importante o añade datos importantes a su sistema también sería adecuado efectuar una copia.

Copiar las Bases de Datos del Sistema: Existe cierta información del sistema que es imprescindible para su correcto funcionamiento. Es conveniente tener una copia de estos ficheros en una ubicación segura. En particular resulta conveniente tener una copia del contenido del directorio /etc. También hay que mantenerla en lugar seguro, ya que tiene copias de los ficheros /etc/passwd y /etc/shadows, entre otros que puedan contener claves de usuarios que no están cifradas.

También en cada sistema se puede tener una base de datos de las aplicaciones que hay instaladas en

el servidor. Cada distribución dispone de alguna herramienta que nos realiza el mantenimiento de la base de datos a la mism vez que instala o desinstala aplicaciones. La pérdida de esta base de datos nos haría perder el control sobre qué aplicaciones tenemos instaladas.

En muchas situaciones también será necesario tener copia de seguridad de los ficheros de registro de incidencias, para tener constancia de las distintas actividades del sistema.

Consejos

- Suscribirse a las listas de correo de alertas de seguridad para estar actualizado.
- Prestar atención a los ficheros de registro.
- Actualizar el software inseguro.
- Verificar regularmente la integridad de los ficheros con algún software como tripwire.
- Tener unas copias de seguridad adecuadas.
- Utilizar PGP o GnuPG para garantizar la autenticidad y la privacidad.
- Verificar con periodicidad los puertos de los equipos.
- Revisar periódicamente las cuentas de usuario.
- Asignar cuotas de uso de recursos del sistema.
- Mantener los terminales seguros.
- Asegurarse de tener claves sólidas.
- Mantener el sistema de ficheros con propietarios y permisos adecuados.
- Instalar cortafuegos.

En resumen

Ahora, una vez vistas las características generales de seguridad, lo que queda es aplicar el sentido común. Tenemos que ver nuestra situación y respondernos a una serie de preguntas:

- ¿Qué queremos proteger?
- ¿Qué valor tiene lo que queremos proteger?
- ¿Qué coste tiene la seguridad?
- ¿De quién nos queremos proteger?
- ¿Cuáles son los puntos débiles de nuestro sistema?

Las posibles respuestas a estas preguntas nos proporcionan un abanico de posibilidades demasiado amplio como para poderlo tratar todo.

Lo primero que tenemos que determinar es lo que queremos proteger. No será lo mismo una estación de trabajo personal aislada con conexiones a Internet esporádicas que un servidor web con conexión permanente o un cortafuegos.

También tendremos que considerar el coste de lo que queremos proteger: posible coste económico, tiempo de restauración o instalación, prestigio, perdida de clientes, etc. También el coste de la seguridad en unos términos parecidos a los anteriores. Sería absurdo que invirtiéramos más en protección que el coste de lo protegido.

También hay que considerar que existe una relación inversa entre seguridad y funcionalidad. Cuanto

más seguro hacemos un sistema, menos funcional resulta, ofreciendo menos servicios y más limitaciones de acceso. Esto también constituye otro coste adicional: facilidad de uso.

Después de saber qué y de qué tenemos que protegernos, de quiénes y cuáles son sus posibles objetivos, y viendo los servicios que necesariamente hay que prestar o usar, obtendremos un esquema elemental de nuestra situación y de las medidas que tenemos que tomar.

16.1.7 ¿Qué hacer en caso de ruptura?

Ahora vamos a ver qué se puede hacer en caso de haber sufrido o estar sufriendo un ataque. No es una situación agradable, y aunque siempre sería preferible que no hubiera sucedido, conviene tener en mente una serie de normas que nos permitan una actuación rápida y certera que disminuya las consecuencias del incidente. Como norma general hay que conservar la calma. No conviene tomar medidas apresuradas que puedan aumentar el impacto del ataque.

Vamos a distinguir una serie de situaciones posibles y cómo se debe actuar. Una vez visto esto nos queda aplicar el sentido común.

Detección de un ataque activo: Nos ponemos en situación: acabamos de detectar un ataque que está actualmente en curso. El ataque puede ser de diversa naturaleza. Dejaremos aparte los casos genéricos como detectar alguien manipulando físicamente el ordenador.

Ataque local: Cuando detectamos un ataque local tendremos que verificar la identidad del atacante. No conviene sacar conclusiones precipitadas y culpar a alguien de atacar el sistema cuando sólo puede que sea una negligencia a la hora de seleccionar una clave o abandonar abierta una consola. Hay que verificar el origen de la conexión, los registros del sistema y los procesos que tiene activos. Tendremos que comprobar si son los habituales y qué es lo que se sale de lo normal. Después nos dirigiremos a esa persona, por teléfono o personalmente, para preguntar qué está haciendo y pedir que cese en la actividad. Si no tiene una conexión activa y no tiene idea de lo que le estamos diciendo, habrá que profundizar en la investigación porque cabe la posibilidad de que alguien haya utilizado esa cuenta de forma ilegítima. Si reconoce el incidente, que le informe de los mecanismos que ha utilizado, las acciones que ha realizado y actúe en consecuencia. Nunca se precipite para hacer acusaciones. Recopile todas las pruebas que haya detectado en los registros, procesos, modificaciones de información, etc. Sea rápido, pero seguro. Está en juego su sistema y su prestigio.

Ataque en red: Si el ataque se produce a través de la red podemos tener distintas situaciones. En general puede ser conveniente espiar un poco al intruso para obtener más pruebas y después desconectar el interfaz de red si es posible. Si no fuera posible desconectar el interfaz, deberíamos usar algún filtro para las conexiones procedentes de la dirección del atacante. Programas como ipchains (o ipfwadm en su caso) pueden realizar esta labor. Si desconectamos el interfaz o denegamos (no rechazar) los paquetes procedentes de esa dirección el intruso lo podría interpretar como un error de red, más que una detección del ataque. Si no se pudiera limitar el acceso a las direcciones que usa el intruso, intente cerrar la cuenta del usuario. Observe que cerrar una cuenta no es una cosa simple. Tiene que tener en cuenta los ficheros .rhosts, el acceso FTP y otras posibles puertas traseras.

En general no es aconsejable apagar el sistema. Por supuesto, nunca apagarlo en caliente; esto podría hacernos perder la información que tenemos en memoria. En Linux podemos ver la lista de procesos que hay en ejecución y matar aquellos que puedan estar dañando al sistema.

¿Somos el destino del ataque o somos un punto intermedio?: Se puede dar la situación que nuestra máquina no sea el destino final del ataque. Puede que el intruso la haya utilizado como punto

intermedio para atacar a otros sistemas e intentar dificultar el seguimiento de las pistas. En este caso, además de limitar las acciones del atacante deberíamos notificarlo al administrador del destino del ataque y conservar todas las pruebas existentes por si se pudieran reclamar judicialmente. En cualquier caso, si queremos dar validez legal a las pruebas obtenidas, sería conveniente la intervención judicial.

Es habitual que durante los próximos minutos el atacante vuelva a intentar continuar con sus acciones, tal vez usando una cuenta diferente y/o una dirección de red distinta.

El ataque ha concluido: Ha detectado un compromiso que ya ha ocurrido o bien lo ha detectado mientras ocurría y ha echado al atacante fuera de su sistema. Ahora viene la parte más dura del incidente: tratar de dejar el sistema mejor que estaba antes de que ocurriera.

Tapar el agujero: Determine los medios que usó el atacante para acceder a su sistema. Deberá analizar cuidadosamente los ficheros de registro del sistema. En ellos debería haber una información valiosa para seguir la pista de las actividades del intruso en nuestra máquina. Las causas más habituales son una mala configuración de algún servicio, un programa defectuoso o la negligencia de algún usuario con respecto a su clave de acceso.

Compruebe por los cauces más conocidos, que se pueden consultar en la página sobre recursos de seguridad bajo Linux, la existencia de algún nuevo «exploit» que pueda ser la causa u otros fallos que tenga que corregir.

Si no elimina al atacante, probablemente volverá. No sólo a su máquina, sino a cualquiera otra de la red. Durante sus incursiones ha podido utilizar algún «sniffer», y disponer de información suficiente para tener acceso a otras máquinas locales.

Si sospecha que el atacante ha obtenido copias de los ficheros /etc/passwd, /etc/shadow, /etc/ppp/pap-secrets, /etc/ppp/chap-secrets o cualquier otro fichero que contenga datos de usuarios y claves, sería conveniente modificarlas todas. Si tiene distintos usuarios en su máquína, oblígueles a cambir su clave. En general es preferible cambiar siempre las claves despues de un incidente, una vez que sepamos que lo hacemos de una forma segura.

Verifique si se han modificado las limitaciones al acceso a distintas herramientas de administración remota como linuxconf. Puede que el atacante trate de abrir alguna puerta trasera para continuar aprovechándose de nuestras máquinas.

En algunos casos puede interesar antes de nada, hacer alguna copia de todo el disco duro para seguir investigando el incidente en otra máquina distinta que no esté conectada a la red y no perder una información que puede ser valiosa.

Evaluación de los efectos del ataque: El siguiente paso que hay que realizar es la evaluación de los efectos que ha tenido el ataque. Tiene que tener en mente la naturaleza del ataque para evaluar los efectos. Si ha sido una denegación de servicio es probable que el atacante no haya tenido acceso a la información local. Si tenía instalado algún programa, estilo Tripwire, que verifica la integridad, su trabajo ahora sería más cómodo. En caso contrario tendrá que verificar todos sus datos importantes. Verifique las fechas de creación de los ficheros binarios y si detecta alguna incongruencia con la fecha de instalación puede empezar a sospechar. Si tiene la posibilidad, compare los tamaños de los ficheros con otro sistema «limpio» y por supuesto, no trate de verificar los programas ejecutándolos como root.

Unas buena alternativa es volver a instalar el sistema. Guarde los ficheros de configuración para tener una funcionalidad idéntica a la previa al ataque. En Linux, los ficheros de configuración se almacenan en modo texto por lo que no son susceptibles de contener caballos de Troya. Eso sí, debería verificar que las configuraciones son las originales y no han sido manipuladas por el atacante. Reinstale el sistema y utilice las copias de seguridad para reponer los datos de los usuarios. Hay que tener

especial cuidado con las copias de seguridad. Tiene que estar seguro de que las copias de seguridad que está utilizando son previas a cualquier ataque. No se arriesgue a restaurar unas copias de seguridad que pudieran tener algún caballo de Troya; tenga un cuidado especial con los ficheros binarios que restaura.

Avisar: Si cree que ha sido objeto de un ataque que no está documentado, debería notificarlo a alguna organización de seguridad como CERT o similar para que se pueda solucionar lo antes posible y evitar que otros sistemas lo puedan padecer. Y aunque sea un hecho documentado con anterioridad, no dude en pedir consulta a alguna de la múltiples lista de correo que tratan temas de seguridad en general y de Linux en particular. En España resulta especialmente recomendada la lista CERT-ES de RedIris. Si ha conseguido información sobre el atacante, se lo debería notificar al administrador del dominio del intruso. Puede buscar este contacto con whois, con la base de datos del Internic o en RedIris. Podría enviarles un mensaje de correo con todos los registros relacionados con el incidente, fechas y horas. Si conoce alguna otra información sobre su intruso, podría mencionarla también. En ciertas situaciones, tras enviar el correo podría llamar por teléfono al administrador del sistema que originó el incidente. Si el admininistrador localiza a su atacante, podría hacerle las cosas mucho más fáciles. Los buenos Hackers con frecuencia usan sistemas intermedios. Algunos (o muchos) puede que ni sepan que han sido comprometidos. Intentar seguir la pista de un cracker hasta su origen puede ser difícil. Siendo educado con los administradores, le puede facilitar la obtención de la ayuda necesaria. De todas formas, esperamos que la lectura de este capítulo sea totalmente innecesaria, si ha seguido unas normas adecuadas de seguridad.

APÉNDICE A: Herramientas

Kismet: Kismet es un sniffer, un husmeador de paquetes, y un sistema de detección de intrusiones para redes inalámbricas 802.11. Kismet funciona con cualquier tarjeta inalámbrica que soporte el modo de monitorización raw, y puede rastrear tráfico 802.11b, 802.11a y 802.11g. El programa corre bajo Linux, FreeBSD, NetBSD, OpenBSD, y Mac OS X. El cliente puede también funcionar en Windows, aunque la única fuente entrante de paquetes compatible es otra sonda.

Kismet se diferencia de la mayoría de los otros sniffers inalámbricos en su funcionamiento pasivo. Es decir que lo hace sin enviar ningún paquete detectable, permitiendo detectar la presencia de varios puntos de acceso y clientes inalámbricos, asociando unos con otros.

Kismet también incluye características básicas de Sistemas de detección de intrusos como detectar programas de rastreo inalámbricos incluyendo a NetStumbler, así como también ciertos ataques de red inalámbricos.

Kismet tiene tres partes diferenciadas. Una Sonda que puede usarse para recoger paquetes, que son enviados a un servidor para su interpretación. Un servidor que puede o bien ser usado en conjunción con una sonda, o consigo mismo, interpretando los datos de los paquetes, extrapolando la información inalámbrica, y organizándola. El cliente se comunica con el servidor y muestra la información que el servidor recoge.

Airmon: Antes de empezar a capturar tráfico debemos poner nuestra tarjeta en modo monitor, con esta aplicación lo hacemos.

Airodump: Se usa para capturar datos trasmitidos a través del protocolo 802.11 y en particular para la captura y recolección de IVs (vectores iniciales) de los paquetes WEP con la intención de usar aircrack. Si existe un receptor GPS conectado al ordenador, airodump muestra las coordenadas del AP.

Aireplay: Es una herramienta para la creación de peticiones ARP

Aircrack: Aircrack es un programa crackeador de claves 802.11 WEP y WPA/WPA2-PSK. Aircrack puede recuperar la clave WEP una vez que se han capturado suficientes paquetes encriptados con airodump. Este programa de la suite aircrack lleva a cabo varios tipos de ataques para descubrir la clave WEP con pequeñas cantidades de paquetes capturados, combinando ataques estadísticos con ataques de fuerza bruta. Para crackear claves WPA/WPA2-PSK, es necesario usar un diccionario.

Para “romper” claves WEP se pueden utilizar múltiples técnicas:

- Ataques FMS (Fluhrer, Mantin, Shamir) - son técnicas estadísticas
- Ataques Korek - tambien técnicas estadísticas
- Fuerza bruta

Cuando se usan técnicas estadísticas para crackear claves WEP, cada byte de la clave es tratado de forma individual. Usando matemáticas estadísticas, la posibilidad de que encuentres un byte determinado de la clave crece algo más de un 15% cuando se captura el vector de inicialización (IV) correcto para ese byte de la clave. Esencialmente, ciertos IVs “revelan” algún byte de la clave WEP. Esto es básicamente en que consisten las técnicas estadísticas.

Usando una serie de pruebas estadísticas llamadas FMS y ataques Korek, se van acumulando posibilidades o votos (votes) para cada byte de la clave WEP. Cada ataque tiene un número diferente

de votos asociado con él, por lo que la probabilidad de cada ataque varia matemáticamente. Cuantos más votos tengamos de un byte o valor particular, mayor probabilidad hay de que sea el correcto.

MACchanger: Es una utilidad que permite ver y modificar (fake) la MAC address.

Microsoft Baseline Security Analyzer: Permite explorar múltiples sistemas, a fin de identificar falta de actualizaciones y errores comunes de configuración, en sistemas operativos y aplicaciones de Windows de uso corriente(IIS, SQL Server, etc.)

Software Update Services (SUS): Se trata de una herramienta fundamental a la hora de mantener el nivel de actualización de parches para el conjunto de sistemas Windows, en instalaciones con un gran numero de equipos conectados a la LAN

Qchain: Permite al administrador, instalar por medio de scripting, varios parches simultáneos, sin necesidad de realizar múltiples booteos

Nikto: Es una secuencia de comandos en Perl, que utiliza la librería Libwhisker para las funciones HTTP/Socket. Su función es la de examinar servidores Web en busca de múltiples problemas, incluyendo configuraciones erróneas, archivos y secuencias de comando inseguras o predeterminadas y aplicaciones anticuadas.

Netcat: Ha sido bautizada la “navaja suiza” debido a sus múltiples utilidades. En su nivel más básico, es capaz de leer y escribir datos a través de conexiones de red utilizando los protocolos TCP y UDP

Achilles: Es un servidor proxy, que actúa como “una persona en el medio” (man in the middle) durante una sesión HTTP. Un proxy de HTTP típico pasa paquetes hacia y desde el explorador de Web cliente y un servidor de Web. Achilles intercepta los datos en una sesión HTTP en cualquier dirección y le da la habilidad al usuario de alterar los datos antes de ser transmitidos.

BACK TRACK: es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática. Deriva de la unión de dos grandes distribuciones orientadas a la seguridad, el Auditor + WHAX. WHAX es la evolución del Whoppix (WhiteHat Knoppix), el cual pasó a basarse en la distribución Linux SLAX en lugar de Knoppix.

Incluye larga lista de herramientas de seguridad listas para usar, proporciona en un par de minutos acceso a más de 300 herramientas de todo tipo entre las que destacan numerosos scanners de puertos y vulnerabilidades, archivos de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless.

Fue incluida en la famosa lista Top 100 Network Security Tools del 2006 disponible en SecTools.Org. Es una de las más conocidas y apreciadas distribuciones GNU/Linux orientadas a profesionales de la seguridad, con un enfoque especial hacia la realización de tests de penetración. Para dar una idea de su popularidad, baste decir que ocupa el puesto 32 en el famoso ránking de Insecure.org.

WIFISLAX: es una distribución GNU/Linux con funcionalidades de LiveCD y LiveUSB pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general.

Deriva del inicio de varios desarrollos sin éxito de otras distribuciones cono Knoppix, Debian y finalmente Slax. Tras realizar un destacable trabajo, se utilizaron funcionalidades de antiguas versiones de BackTrack, debido a que esta última, nace de la unión de dos grandes distribuciones orientadas a la seguridad, el Auditor + WHAX.

WiFiSlax incluye larga lista de herramientas de seguridad y auditoría listas para ser utilizadas, entre las que destacan numerosos scanners de puertos y vulnerabilidades, herramientas para creación y diseño de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless, además de añadir una serie de útiles lanzadores muy intuitivos.

Wifislax es un CD de arranque que contiene al sistema operativo Linux. Puede hacer correr Linux directamente desde el CDROM sin instalación. Aunque lleva incorporado herramientas de instalación en el disco duro o en llaveros USB, o una emulación en Windows. Wifislax esta basado básicamente y principalmente en SLAX (basado en la distribución Slackware Linux), pero debido al gran trabajo realizado por los autores del BackTrack hemos trabajado directamente sobre este ultimo live CD, así pues catalogar al Wifislax como una live CD podría incluso considerarse como erróneo. También están disponibles todos los scripts y códigos fuente, los cuales pueden ser utilizados para construir tu propio live CD.

Esta distribución de seguridad, contiene entre otros Asistencia Chipset, Herramientas Wireless, Suite Aircrack y aircrack-ng, estudio de cifrado (WEP, WPA y WPA2), nmap, amap, lanzadores para asistencia de conexión, herramientas bluetooth, etc.

WifiWay: Es un live CD que, basado en el sistema operativo Linux, puede ser ejecutado sin necesidad de instalación directamente desde el CDROM o también desde el disco duro como LiveHD, además de poderse instalar en memorias USB o en disco duro.

Wifiway es un Linux live cd diseñado por www.seguridadwireless.net y www.wifiway.org esta pensada y diseñada para la auditoría de seguridad del estándar 802.11. (WiFi, BlueTooth y RFID) y ademas con soporte internacional. Deriva del inicio de varios desarrollos, algunos muy éxitosos como es el caso de WiFiSlax. Se debe destacar que Wifiway no está basada en otras distribuciones si no que es Linux From Scratch.

Linux From Scratch o LFS es una colección de documentos que nos indican los pasos para compilar una distribución GNU/Linux desde cero. El proyecto se diferencia de otras distribuciones en que no consta de paquetes y scripts pre ensamblados para una instalación automática del sistema, sino que sus usuarios son provistos simplemente con paquetes de código fuente y un manual de instrucciones para el armado de un sistema GNU/Linux propio.

Debido al inmenso trabajo que demanda la instalación de este sistema en comparación a otras distribuciones, los usuarios que deciden hacer uso de LFS son principalmente aficionados que desean aprender sobre el funcionamiento interno de un sistema GNU/Linux y ensamblar un sistema a su medida. Linux From Scratch es también utilizado como base de varias distribuciones, usualmente alejadas de su espíritu original de "metadistribución".

Wifiway incluye una larga lista de herramientas de seguridad y auditoría inalámbrica listas para ser utilizadas, especializadas en la auditoría Wireless, además de añadir una serie de útiles lanzadores muy intuitivos.

Una característica de esta distribución es que hace uso de un script (airoway.sh) que simplifica y acelera el proceso de una auditoría Wireless.

Zabbix: Es una aplicación open source que nos permite monitorizar nuestros servidores vía web. Permite un acceso centralizado a toda la información obtenida de nodos de nuestra red. Encuentra automáticamente, mediante un rango de IPs, servicios y SNMP, y empieza a monitorizarlos automáticamente. Tiene una buena escalabilidad, ha sido testeado contra 5000 servidores y

dispositivos. Permite una administración sencilla, guardándose los datos en BD (Oracle, MySQL, PostgreSQL o SQLite). Monitorización en tiempo real, mandando avisos mediante email, SMS o Jabber. Zabbix resume en sus objetivos principales su eficacia y potencia:

- Interfaz amigable
- Hacer las cosas simples
- Utilizar los mínimos recursos
- Reaccionar rápidamente
- Documentar cualquier aspecto del software

Zabbix es capaz de monitorizar numerosos parámetros en una red, así como indicarnos la salud, rendimiento e integridad de sus equipos. Utiliza un mecanismo de notificaciones extremadamente flexible y nos ofrece un excelente catálogo de informes y gráficas perfectos para el análisis de nuestros equipos, ya sea a nivel de software o hardware.

IPCop: Es una distribución Linux que implementa un cortafuegos (o firewall) y proporciona una simple interfaz web de administración basándose en una computadora personal. Originalmente nació como una extensión (fork) de la distribución SmoothWall cuyo desarrollo había estado congelado bastante tiempo.

IPCop tiene como objetivos ser un cortafuegos sencillo, con pocos requerimientos hardware orientado a usuarios domésticos o a pequeñas empresas (SOHO), administrado a través de una interfaz web, con funcionalidades basicas y avanzadas, yendo (a manera de ejemplo) desde el simple filtrado de paquetes hasta la asignación de ancho de banda fijo a cada puesto de trabajo o la configuración de redes virtuales VPN. IPCop se actualiza desde el Interfaz Web de manera muy sencilla, incluyendo actualizaciones del Kernel.

IPCop está capado y solo tiene instaladas las herramientas justas para su función como firewall, limitando el daño que podría hacer un intruso que comprometiera el sistema. Si se desea ampliar la funcionalidad existen extensiones, comunes con SmoothWall, que permiten instalar todo tipo de utilidades como por ejemplo instalar Nmap para escanear IPs.

La distribución Linux se puede bajar desde el sitio oficial en inglés, consiste de una imagen ISO de menos de 100Mb la cual puede ser grabada en un CD e instalada en cualquier PC que tenga al menos dos interfaces de red.

Topologías de red soportadas: Permite la implementación de diferentes topologías de red, ya sea desde la simple LAN que sale a internet, hasta la creación de una zona desmilitarizada (DMZ), soportando también la inclusión de una red inalámbrica.

Las diferentes zonas las divide en colores, siendo:

- Roja (o Red) = zona de Internet,
- Verde (green) = Red de Área Local (LAN) cableada,
- Naranja (Orange) = zona desmilitarizada (DMZ, para la granja de servidores),
- Azul (Blue) = zona inalámbrica (Wireless).

SmoothWall: Smoothwall es una distribución Linux que tiene como objetivo proporcionar un cortafuegos o Firewall de fácil administración e instalación, administrable a través de una interfaz web.

Squid: Squid es un popular programa de software libre que implementa un servidor proxy y un

demonio para caché de páginas web, publicado bajo licencia GPL. Tiene una amplia variedad de utilidades, desde acelerar un servidor web, guardando en caché peticiones repetidas a DNS y otras búsquedas para un grupo de gente que comparte recursos de la red, hasta caché de web, además de añadir seguridad filtrando el tráfico. Está especialmente diseñado para ejecutarse bajo entornos tipo Unix.

Squid ha sido desarrollado durante muchos años y se le considera muy completo y robusto. Aunque orientado a principalmente a HTTP y FTP es compatible con otros protocolos como Internet Gopher. Implementa varias modalidades de cifrado como TLS, SSL, y HTTPS.

OSSIM: Es una distribución de productos open source integrados para construir una infraestructura de monitorización de seguridad. Su objetivo es ofrecer un marco para centralizar, organizar y mejorar las capacidades de detección y visibilidad en la monitorización de eventos de seguridad de la organización.

PuTTY: Es un cliente SSH, Telnet, rlogin, y TCP raw con licencia libre. Disponible originariamente sólo para Windows, ahora también está disponible en varias plataformas Unix, y se está desorrollando la versión para Mac OS clásico y Mac OS X. Otra gente ha contribuido con versiones no oficiales para otras plataformas, tales como Symbian para teléfonos móviles. Es software beta escrito y mantenido principalmente por Simon Tatham, open source y licenciado bajo la Licencia MIT.

Quarkbase (www.quarkbase.com) es la última herramienta online en aparecer cuyo cometido es realizar una completa analítica de la url que introducimos en su campo correspondiente. Para ello nos encontramos con la página inicial, bastante sencilla, pero que una vez introducida la url, nos aparece una página más completa estructurando su información en diferentes apartados.

Lo primero que nos encontraremos en la página de la información de cualquier url es su captura y un resumen del mismo. Más abajo nos encontramos con datos introductorios, donde además, nos darán una serie de enlace de sitios similares. Le sigue la popularidad social, donde ya empezaremos a obtener una serie de número y gráficas, que también encontraremos en el apartado de tráfico, donde además obtendremos una serie de gráficas de Alexa.

La información de las personas que están tras una url, los enlaces entrantes desde diferentes fuentes, y la información técnica, son los últimos apartados que podemos conocer de una url.

Gracias a Quarkbase podemos conocer mucho más de cualquier sitio web, información que en su mayor parte han sido obtenidas a través de Zoominfo, CrunchBase, Bloglines, Dmoz y Dealipedia.

AbouThiSite (www.aboutthisite.com), un servicio de reciente aparición que nos mostrará una serie de datos sobre cualquier url que le indiquemos. Basta con que le indiquemos una url para que nos muestre la información general, donde conoceremos quien está detrás de la url junto con otros datos como el pagerank, número de visitas diarias o la ip del servidor donde está alojado.

Además, también obtendremos una paleta de colores donde conoceremos el porcentaje de cada tono de color usado en el diseño de la página a la que pertenece la url. Sabremos asimismo si valida las normas del W3C o el set de caracteres utilizado.

Pero si lo que queremos saber es la ubicación del servidor, también nos lo indica a través de un mapa de Google Maps así como los datos que la acompañan. Por último podremos conocer los vecinos, tal y como también hace MyIpNeighbors. Para quien aún no lo entienda, sobre la ip del servidor conoceremos otros sitios web que comparten el mismo servidor web que la url que estamos analizando. También nos mostrará una captura de la web a la que pertenece la url.

GreatDB (www.greatdb.com) es una utilidad que recopila en una sola interfaz varias herramientas

para saber todo acerca de cualquier sitio web con tan solo ingresar su URL: Whois, Alexa, blacklinks, paginas indexadas por Google y Yahoo, Screenshots de Internet Archive's Wayback, entre muchas otras. Podemos averiguar, la antigüedad, el lenguaje, las 5 palabras clave, etc.

EventReporter de Adiscon permite a los administradores combinar funciones de informe de registro de sucesos y alerta de UNIX y Windows en un único entorno. Es compatible con el protocolo syslog estándar de UNIX para la integración con sistemas basados en este sistema operativo, así como con el protocolo simple de transferencia de correo (SMTP) para el reenvío de alertas. EventReporter incluye un agente que se puede configurar para recopilar sucesos de seguridad de varios equipos, filtrarlos y, a continuación, colocarlos en una base de datos. En función del suceso de seguridad, se podrá reenviar estos sucesos por correo electrónico, iniciar aplicaciones y crear mensajes de red, entre otros.

GFI LANguard Security Event Log Monitor (SELM) de GFI. LANguard realiza la detección de intrusiones basada en los registros de sucesos y lleva a cabo la administración de éstos en toda la red. Asimismo, almacena y analiza los registros de sucesos de todos los equipos de red y alerta en tiempo real acerca de los problemas de seguridad, ataques y otros sucesos críticos. Security Event Log Monitor puede almacenar los registros de sucesos en una base de datos central y ofrece reglas e informes personalizados para el análisis forense.

Systrack 3 de Lakeside Software, Inc. Emite alarmas de registro de suceso prácticamente en tiempo real a través de Event Log Monitor. Event Log Monitor inspecciona de forma periódica todos los registros de sucesos de un equipo con el fin de determinar si ocurrió algo nuevo desde la última inspección. Systrack 3 filtra los sucesos recién descubiertos y realiza la acción pertinente. Estos filtros pueden utilizar la configuración predeterminada, la configuración definida por el usuario o una combinación de ambas. Las cadenas de caracteres específicos en las propiedades de los sucesos, como el nombre de una estación de trabajo o un usuario, pueden desencadenar alarmas de registro de sucesos. Un suceso también puede ejecutar una secuencia de comandos o reiniciar el equipo. Los filtros también pueden generar capturas del protocolo simple de administración de redes (SNMP), mensajes emergentes de Windows o alertas de correo electrónico.

TCP Wrappers: es un software de domino público desarrollado por Wietse Venema (Universidad de Eindhoven, Holanda). Su función principal es: proteger a los sistemas de conexiones no deseadas a determinados servicios de red, permitiendo a su vez ejecutar determinados comandos ante determinadas acciones de forma automática. Con este paquete podemos monitorear y filtrar peticiones entrantes a distintos servicios TCP-IP, como: SYSTAT, FINGER, FTP, RLOGIN, RSH, REXEC, TFTP, TALK. El software está formado por un pequeño programa que se instala en el "/etc/inetd.conf". Una vez instalado, se pueden controlar los accesos mediante el uso de reglas y dejar una traza de todos los intentos de conexión tanto admitidos como rechazados (por servicios, e indicando la máquina que hace el intento de conexión). El programa utiliza el syslogd (puerto 514 udp) para mandar esa información; por defecto utilizará la salida de mail, la cual estará indicada en el archivo de configuración de syslogd (/etc/syslog.conf) con la línea mail.debug. Esto se puede cambiar en los fuentes del programa y se puede re-dirigir a otro lugar mediante el uso de las variables de usuario que deja libres el syslogd (LOCAL_0,...LOCAL_7, estas variables vienen definidas en el archivo /usr/include/syslog.h). Una vez modificados los fuentes, se deberá indicar al syslogd donde debe dejar la información de esa variable local.

En referencia al control de conexiones a distintos servicios, el software utiliza dos archivos de información (hosts.allow, hosts.deny) situados en el directorio "/etc". Es en estos archivos donde se definirán las reglas que deben utilizarse para el filtrado de los paquetes. El filtrado se puede realizar teniendo en cuenta tanto a máquinas como a servicios o una mezcla de ambos. En el caso de las máquinas hay varias formas de hacerlo. Por ejemplo se le puede indicar que sólo se conecten las

máquinas pertenecientes al mismo dominio (esto se puede ampliar a los que tengan el mismo rango de direcciones IP, para evitar que máquinas no definidas en el DNS no puedan conectarse), o sólo aquéllas cuyos nombres sean especificados de forma explícita.

Netlog: Este software de dominio público diseñado por la Universidad de Texas, es una herramienta que genera trazas referentes a servicios basados en IP (TCP, UDP) e ICMP, así como tráfico en la red (los programas pueden ejecutarse en modo promiscuo) que pudiera ser "sospechoso" y que indicara un posible ataque a una máquina (por la naturaleza de ese tráfico). El paquete está formado por el siguiente conjunto de programas:

- *Tcplogger:* Este programa escucha todos los servicios sobre TCP, dejando una traza de cada servicio en un archivo de trazas, indicando la hora, la máquina origen y el puerto de esa conexión.
- *Udplogger:* Es semejante al anterior, pero para los servicios sobre UDP.
- *Icmplogger:* Se encarga de trazar el tráfico de icmp.
- *Etherscan*: Es una herramienta que monitorea la red buscando ciertos protocolos con actividad inusual, como puedan ser conexiones tftp - en este caso, si se han realizado con éxito nos indica qué archivos se han llevado -, comandos en el puerto de sendmail (25 tcp) como vrfy, expn, algunos comandos de rpc como rpcinfo, peticiones al servidor de NIS (algunas herramientas utilizan este tipo de servidores para obtener el archivo de password, ej: ypx), peticiones al demonio de mountd, etc. Etherscan se ejecuta en modo promiscuo en la máquina utilizando (al igual que las anteriores) el NIT (Network Interface Tap de SunOs 4.1.x), y también el "Packet Filtering Interface" para realizar esas capturas.
- *Nstat*: Esta herramienta que originariamente fue diseñada para obtener estadísticas de uso de varios protocolos, se puede utilizar para detectar cambios en los patrones de uso de la red, que nos puedan hacer sospechar que algo raro está pasando en la misma. Esta herramienta viene acompañada por dos utilidades que nos permiten analizar la salida que origina nstat, a saber: nsum, nload. La primera de ellas, nos da información de ciertos periodos de tiempo. La segunda, es un programa awk que produce una salida que puede ser vista de forma gráfica por herramientas como xvgr. Para concluir este apartado, podemos decir que esta herramienta es muy útil para detectar ciertos tipos de ataques, tal como hemos reflejado anteriormente (con etherscan), así como dar una idea de qué tipo de protocolos están viajando por la red. Además, tiene la ventaja de que al estar en modo promiscuo, con sólo tenerlo en una máquina del segmento se puede tener monitoreado todo el segmento en el que esté conectado.

Argus: Es una herramienta de dominio público que permite auditar el tráfico IP que se produce en nuestra red, mostrándonos todas las conexiones del tipo indicado que descubre. Este programa se ejecuta como un demonio, escucha directamente la interfaz de red de la máquina y su salida es mandada bien a un archivo de trazas o a otra máquina para allí ser leída. En la captura de paquetes IP se le puede especificar condiciones de filtrado como protocolos específicos, nombres de máquinas, etc. A la hora de leer esa información disponemos de una herramienta que incluye el software (llamado ra) y que nos permite también realizar filtros de visualización. Una característica de esta herramienta es la posibilidad de filtrar paquetes de acuerdo a las

listas de acceso de los routers CISCO. Es posible por tanto decirle que nos capture aquellos paquetes que no cumplen las reglas de la lista de acceso definida para esa interfaz del router. Como en el caso anterior (netlog) es posible ejecutar el comando en modo promiscuo (si lo que queremos es auditar todo nuestro segmento). Este programa divide las transacciones en cuatro grupos: TCP, UDP/DNS, MBONE, ICMP.

Tcpdump: Es un software de dominio público que imprime las cabeceras de los paquetes que pasan

por una interfaz de red. Este programa es posible ejecutarlo en modo promiscuo con lo que tendremos las cabeceras de los paquetes que viajan por la red. Tanto en la captura como en la visualización de la información, es posible aplicar filtros por protocolo (TCP, UDP, IP, ARP, RARP...), puertos (en este caso el puerto puede ser un número o un nombre especificado en el archivo/etc/services), direcciones fuente, direcciones destino, direcciones de red, así como realizar filtros con operadores (=, <, >, !=, and, not, ...). En la última versión, es posible ver también los paquetes de datos.

SATAN (Security Administrator Tool for Analyzing Networks): Es un software de dominio público creado por Dan Farmer que chequea máquinas conectadas en red y genera información sobre el tipo de máquina, qué servicios da cada máquina y avisa de algunos fallos de seguridad que tengan dichas máquinas. Una de las ventajas de SATAN frente a otros paquetes, es que utiliza una interfaz de WWW (como Mosaic, Netscape,..), va creando una base de datos de todas las máquinas chequeadas y las va relacionando entre ellas (de forma que si encuentra una máquina insegura, y chequea otra máquina que está relacionada con ésta, automáticamente esta segunda quedará marcada también como insegura). Además, tiene la posibilidad de poder chequear las máquinas con tres niveles ("light", normal y "heavy"). Una vez realizado el chequeo de la máquina se genera una salida en formato html, y en el caso de encontrar fallos, da una pequeña explicación sobre el fallo en concreto. Cuando existe algún documento sobre ese fallo recogido en el CERT (advisory) tiene un enlace a ese documento, para que sobre la marcha pueda ser consultado. Asimismo, en el caso de que el fallo de seguridad sea debido a versiones antiguas de software da la posibilidad (mediante un enlace) de instalar una versión nueva de ese software. Algunos de los servicios chequeados por SATAN son: finger, NFS, NIS, ftp, DNS, rexd, así como tipo de sistema operativo, versión de sendmail, etc. La base de datos generada por SATAN puede ser luego consultada por varios campos: tipo de sistema operativo, tipo de servicio (servidores de NIS, ftp, NFS, X, etc). SATAN ha sido diseñado como una herramienta de seguridad para ayudar a administradores de sistemas y redes, pero también puede ser utilizada para atacar a sistemas y descubrir la topología de la red de una organización. SATAN es capaz de chequear máquinas por subredes, con lo que quedan al descubierto todas las máquinas que se encuentran conectadas en dicha subred.

ISS (Internet Security Scanner): Es una herramienta de la cual existe versión de dominio público que chequea una serie de servicios para comprobar el nivel de seguridad que tiene esa máquina. ISS es capaz de chequear una dirección IP o un rango de direcciones IP (en este caso se indican dos direcciones IP e ISS chequeará todas las máquinas dentro de ese rango). El programa viene acompañado de dos utilidades que son ypx y strobe. La primera, nos permite la transferencia de mapas NIS a través de la red y la segunda, chequea y describe todos los puertos TCP que tiene la máquina que chequeamos. Como podemos ver, con la primera herramienta es posible la transferencia de los archivos de "password" en aquellas máquinas que hayan sido configuradas como servidores de NIS. ISS se puede ejecutar con varias opciones y la salida se deja en un archivo. Además, si ha podido traerse el archivo de "password" de la máquina chequeada, creará un archivo aparte con la dirección IP de la máquina.

Courtnet: Este software de dominio público sirve para identificar la máquina origen que intenta realizar ataques mediante herramientas de tipo SATAN. El programa es un script perl que trabaja conjuntamente con tcpdump. Courtney recibe entradas desde tcpdump y controla la presencia de peticiones a nuevos servicios del stack TCP/IP (las herramientas de este tipo realizan ataques, chequeando de forma ordenada todos los puertos TCP y UDP que tiene el sistema, para poder ver qué servicios tiene instalados dicha máquina). Si se detecta que se está produciendo un continuo chequeo de estos puertos en un breve intervalo de tiempo, Courtney da un aviso. Este aviso se manda vía syslog. Courtney puede generar dos tipos de alarmas dependiendo del ataque que se esté produciendo (normal o "heavy", las herramientas como SATAN dispone de distintos grados de chequeo de la máquina). Esta herramienta necesita el intérprete de PERL y el tcpdump.

Gabriel: Software desarrollado por "Los Altos Technologies Inc" que permite detectar "ataques" como los generados por SATAN. Gabriel identifica el posible ataque y de forma inmediata lo notifica al administrador o responsable de seguridad. La notificación se puede realizar de varias formas (e-mail, cu, archivo de trazas). Este programa existe, en este momento, para SunOs y Solaris, y está formado por un cliente y un servidor. El cliente se instala en cualquier máquina de la red, recoge la información que se está produciendo y la envía al servidor vía syslog. Estos clientes además envían de forma regular información al servidor para indicarle que están en funcionamiento.

Tcplist: Es un pequeño programa de dominio público que nos informa acerca de todas las conexiones TCP desde o hacia la máquina donde lo estamos ejecutando.

Nocol (Network Operations Center On-Line): Es un conjunto de programas de monitoreo de sistemas y redes. El software es un conjunto de agentes que recogen información y escriben la salida en un formato que se puede, luego, procesar. Cada dato procesado recibe el nombre de evento y cada evento tiene asociado una gravedad.

Netflow Analyzer: es una herramienta de monitorización de ancho de banda basado en tecnología web. Permite analizar la utilización de ancho de banda y ofrece visibilidad completa sobre routers y switches Cisco. Gracias a sus informes detallados y gráficos en tiempo real, NetFlow Analyzer proporciona información muy completa sobre el tráfico de red, sin necesidad de utilizar sondas.

APÉNDICE B: Definiciones

DEF CON es una de las más viejas convenciones de Hackers. Se lleva a cabo generalmente en la última semana del mes de julio o la primera semana de agosto en Las Vegas. La primera reunión de DEF CON tuvo lugar en Las Vegas, en junio de 1993. Los *Def Con Goons* organizan y controlan el evento. La mayoría de los asistentes son profesionales de la seguridad informática, Crackers, y Hackers con intereses comunes como la programación, las computadoras y la seguridad.

ECHELON es considerada la mayor red de espionaje y análisis para interceptar comunicaciones electrónicas de la historia. Controlada por la comunidad UKUSA (Estados Unidos, Canadá, Gran Bretaña, Australia, y Nueva Zelanda), ECHELON puede capturar comunicaciones por radio y satélite, llamadas de teléfono, faxes y e-mails en casi todo el mundo e incluye análisis automático y clasificación de las interceptaciones. Se estima que ECHELON intercepta más de tres mil millones de comunicaciones cada día. A pesar de haber sido presuntamente construida con el fin de controlar las comunicaciones militares y diplomáticas de la Unión Soviética y sus aliados, se sospecha que en la actualidad ECHELON es utilizado también para encontrar pistas sobre tramas terroristas, planes del narcotráfico e inteligencia política y diplomática. Sus críticos afirman que el sistema es utilizado también para el espionaje económico y la invasión de privacidad en gran escala. La existencia de ECHELON fue hecha pública en 1976 por Winslow Peck.

Los miembros de esta alianza de habla inglesa son parte de la alianza de inteligencia UKUSA, que lleva reuniendo inteligencia desde la Segunda Guerra Mundial. El sistema está bajo la administración de la NSA (National Security Agency). Esta organización cuenta con 100.000 empleados tan sólo en Maryland (Estados Unidos) (otras fuentes hablan de 380.000 empleados a escala mundial), por lo que es probablemente la mayor organización de espionaje del mundo. La información es enviada desde Menwith Hill (Reino Unido) por satélite a Fort Meade en Maryland (EEUU).

A cada estado dentro de la alianza UKUSA le es asignado una responsabilidad sobre el control de distintas áreas del planeta. La tarea principal de Canadá solía ser el control del área meridional de la antigua Unión Soviética. Durante el período de la guerra fría se puso mayor énfasis en el control de comunicaciones por satélite y radio en centro y Sudamérica, principalmente como medida para localizar tráfico de drogas y secuaces en la región. Los Estados Unidos, con su gran cadena de satélites espías y puertos de escucha controlan gran parte de Latinoamérica, Asia, Rusia asiática y el norte de China. Gran Bretaña intercepta comunicaciones en Europa, Rusia y África. Australia examina las comunicaciones de Indochina, Indonesia y el sur de China, mientras que Nueva Zelanda barre el Pacífico occidental.

Varias fuentes afirman que estos estados han ubicado estaciones de intercepción electrónica y satélites espaciales para capturar gran parte de las comunicaciones establecidas por radio, satélite, microondas, móviles y fibra óptica. Las señales capturadas son luego procesadas por una serie de superordenadores, conocidas como diccionarios, las cuales han sido programadas para buscar patrones específicos en cada comunicación, ya sean direcciones, palabras, frases o incluso voces específicas. Según algunas fuentes el sistema dispone de 120 estaciones fijas y satélites geoestacionarios. Estos podrían filtrar más del 90% del tráfico de internet. Las antenas de Echelon pueden captar ondas electromagnéticas y trasmitirlas a un lugar central para su procesamiento. Se recogen los mensajes aleatoriamente y se procesan mediante los diversos filtros buscando palabras clave. Este procedimiento se denomina "Control estratégico de las telecomunicaciones".

OWASP (acrónimo de Open Web Application Security Project, en inglés ‘Proyecto de seguridad de aplicaciones web abiertas’) es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. La Fundación OWASP es un organismo sin ánimo de lucro que apoya y gestiona los proyectos e infraestructura de OWASP. La comunidad OWASP está formada por empresas, organizaciones educativas y particulares de todo mundo. Juntos constituyen una comunidad de seguridad informática que trabaja para crear artículos, metodologías,

documentación, herramientas y tecnologías que se liberan y pueden ser usadas gratuitamente por cualquiera.

OWASP es un nuevo tipo de entidad en el mercado de seguridad informática. Estar libre de presiones corporativas facilita que OWASP proporcione información imparcial, práctica y redituable sobre seguridad de aplicaciones informática. OWASP no está afiliado a ninguna compañía tecnológica, si bien apoya el uso informado de tecnologías de seguridad. OWASP recomienda enfocar la seguridad de aplicaciones informáticas considerando todas sus dimensiones: personas, procesos y tecnologías.

Los documentos con más éxito de OWASP incluyen la Guía OWASP y el ampliamente adoptado documento de autoevaluación OWASP Top 10. Las herramientas OWASP más usadas incluyen el entorno de formación WebGoat, la herramienta de pruebas de penetración WebScarab y las utilidades de seguridad para entornos .NET OWASP DotNet. OWASP cuenta con unos 50 capítulos locales por todo el mundo y miles de participantes en las listas de correo del proyecto. OWASP ha organizado la serie de conferencias AppSec para mejorar la construcción de la comunidad de seguridad de aplicaciones web.

SANS Institute: El Instituto SANS (SysAdmin Audit, Networking and Security Institute) es una institución con ánimo de lucro fundada en 1989, con sede en Bethesda (Maryland, Estados Unidos) que agrupa a 165.000 profesionales de la seguridad informática (consultores, administradores de sistemas, universitarios, agencias gubernamentales, etc.)

Sus principales objetivos son:

- Reunir información sobre todo lo referente a seguridad informática (sistemas operativos, routers, firewalls, aplicaciones, IDS, etc.)
- Ofrecer capacitación y certificación en el ámbito de la seguridad informática

Igualmente, el SANS Institute es una universidad formativa en el ámbito de las tecnologías de seguridad. Es una referencia habitual en la prensa sobre temas de auditoría informática.

ITIL: Desarrollada a finales de 1980, la Biblioteca de Infraestructura de Tecnologías de la Información (ITIL) se ha convertido en el estándar mundial de de facto en la Gestión de Servicios Informáticos. Iniciado como una guía para el gobierno de UK, la estructura base ha demostrado ser útil para las organizaciones en todos los sectores a través de su adopción por innumerables compañías como base para consulta, educación y soporte de herramientas de software. Hoy, ITIL es conocido y utilizado mundialmente. Pertenece a la OGC, pero es de libre utilización.

ITIL fue desarrollada al reconocer que las organizaciones dependen cada vez más de la Informática para alcanzar sus objetivos corporativos. Esta dependencia en aumento ha dado como resultado una necesidad creciente de servicios informáticos de calidad que se correspondan con los objetivos del negocio, y que satisfagan los requisitos y las expectativas del cliente. A través de los años, el énfasis pasó de estar sobre el desarrollo de las aplicaciones TI a la gestión de servicios TI. La aplicación TI (a veces nombrada como un sistema de información) sólo contribuye a realizar los objetivos corporativos si el sistema está a disposición de los usuarios y, en caso de fallos o modificaciones necesarias, es soportado por los procesos de mantenimiento y operaciones. ITIL fue producido originalmente a finales de 1980 y constaba de 10 libros centrales cubriendo las dos principales áreas de Soporte del Servicio y Prestación del Servicio. Estos libros centrales fueron más tarde soportados por 30 libros complementarios que cubrían una numerosa variedad de temas, desde el cableado hasta la gestión de la continuidad del negocio. A partir del año 2000, se acometió una revisión de la biblioteca. En esta revisión, ITIL ha sido reestructurado para hacer más simple el acceder a la información necesaria para administrar sus servicios. Los libros centrales se han agrupado en dos, cubriendo las áreas de Soporte del Servicio y Prestación del Servicio, en aras de eliminar la duplicidad y mejorar la navegación. El material ha sido también actualizado y revisado para un enfoque conciso y claro.

CCNA (Cisco Certified Network Associate) es una certificación entregada por la compañía Cisco Systems a las personas que hayan rendido satisfactoriamente el examen correspondiente sobre infraestructuras de red e Internet. Está orientada a los profesionales que operan equipamiento de networking. Hay un curso preparatorio, del mismo nombre, ofrecido en las academias de networking Cisco en todo el mundo. Existen distintos niveles de certificación en la línea de operación, recientemente se lanzaron unas certificaciones entre nivel técnico y profesional llamadas concentraciones y hasta ahora sólo hay concentraciones en redes inalámbricas, voz sobre Ip y seguridad pero todas son de nivel CCNA, es decir, uno puede estar certificado como CCNA en redes inalámbricas por ejemplo. El siguiente nivel es el CCNP ("Cisco Certified Network Professional").

CCNP (Cisco Certified Network Professional) es el nivel intermedio de certificación de la compañía. Para obtener esta certificación, se han de superar varios exámenes, clasificados según la empresa en 4 módulos. Esta certificación, es la intermedia de las certificaciones generales de Cisco, no está tan valorada como el CCIE, pero si, mucho más que el CCNA.

CCIE: El Certificado Cisco de Experto en Internet (CCIE) es el nivel de Cisco más alto de la certificación profesional. CCIE es una certificación de nivel avanzado para los profesionales que tienen “el entrenamiento, la experiencia y la confianza para abordar los problemas más desafiantes de su campo.” El CCIE “certifica así las habilidades de establecimiento de una red de un individuo en el nivel experto.” CCIE es un programa aparte que, hasta principios del 2009, no tenía un programa oficial de entrenamiento. Para certificar al nivel experto no es prerrequisito haber certificado otros niveles (CCNA, CCNP o equivalentes), pero tener una certificación de Cisco de nivel avanzado, tal como CCNP (Certificado Cisco de Profesional de Red), CCDP (Certificado Cisco de Profesional de Diseño), CCIP (Certificado Cisco de Profesional de Internet), o CCSP (Certificado Cisco de profesional en Seguridad) serían deseables antes de tomar el CCIE.

CompTIA: La Asociación de la industria de tecnología de cómputo (Computing Technology Industry Association(CompTIA)) es una organización sin fines de lucro fundada en 1982 y que se dedica a la certificación de profesionales para la industria de tecnologías de información. Los exámenes de certificación de CompTIA son administrados a través de los centros de pruebas Pearson VUE y Prometric. Además de certificaciones, CompTIA proporciona membresías corporativas. Entre sus certificaciones más conocidas tenemos:

- **CompTIA Network+:** La certificación Network+ sirve para demostrar las habilidades como un técnico de red: entender el hardware de red, instalación y Resolución de problemas. Network+ sirve para prepararse y continuar con las certificaciones de Microsoft y las certificaciones de Cisco.
- **CompTIA Server+:** La certificación Server+ se enfoca en servidores específicos de algún hardware y sistemas operativos.
- **CompTIA Security+:** es una certificación que trata sobre seguridad informática; la temática está relacionada con criptografía y control de acceso. Actualmente, y de acuerdo a CompTIA, hay más de 23,000 personas en el mundo que se han certificado con esta modalidad.
- **CompTIA Linux+:** La certificación Linux+ prueba los conocimientos de los sistemas operativos Linux, desde su instalación y uso hasta las aplicaciones de software libre, open source y licencias. El examen Linux+ está enfocado a los profesionales de tecnologías de la información que han tenido una experiencia de entre seis y doce meses en la utilización de Linux. El examen se compone de distintas áreas: instalación, administración, configuración, seguridad, documentación y hardware. La prueba consiste en un examen de opción múltiple que se hace en una computadora, una pregunta seguida de cuatro posibles respuestas, al menos una (pero probablemente más) respuesta correcta. Los tópicos de los exámenes incluyen métodos de instalación, configuración del cargador de arranque, manejo de paquetes (Debian y RPM),

navegación de directorios por medio del intérprete de comandos, utilizando bash, consideraciones de seguridad, administración de sistemas incluyendo configuración de TCP/IP, montaje de sistemas de archivos (NFS, SMB ó ext3) y manipulación de archivos de configuración para los servicios más comunes en Linux.

LPI: El Linux Professional Institute (LPI) o Instituto Profesional Linux es una organización sin ánimo de lucro que otorga certificaciones profesionales de Linux a administradores de sistema, así como, programadores. El instituto aplica los exámenes en casi todos los países del mundo y proporciona una amplia gama de certificaciones, LPIC, para profesionales. Es un miembro fundador del Desktop Linux Consortium y es conocido en todo el mundo como la primera organización en impulsar y apoyar el uso de Linux, Código abierto y Software Libre. Se constituye formalmente como una organización sin ánimo de lucro en octubre de 1999 siendo sus fundadores Chuck Mead, Dan York y algunos otros. Su sede se encuentra cerca de Toronto, Ontario Canadá. Las certificaciones LPI -en inglés, LPI Certificación (LPIC)- han sido diseñadas para certificar la capacitación de los profesionales de las Tecnologías de la Información usando el Sistema Operativo Linux y herramientas asociadas a este sistema. Ha sido diseñado para ser independiente de la distribución y siguiendo la Linux Standard Base y otros estándares relacionados. El programa LPI se basa en realización de encuestas para establecer un nivel de certificación basado en el puesto de trabajo a desempeñar utilizando para ello procesos de Psicometría para garantizar la relevancia y calidad de la certificación. Los programas de certificación LPI están actualmente en revisión; la intención es actualizarlos para así poder acompañar la evolución de las Tecnologías de la Información. Para ello se está en permanente contacto con la industria del sector donde se realizan estudios y evaluaciones para determinar los perfiles idóneos del profesional Linux. Luego de establecer los nuevos objetivos de la certificación, se elaborarán los nuevos exámenes que comenzarán a tener vigencia a partir del 1º de Abril del 2009

MCP (Microsoft Certified Professional): Es una Certificación de competencias ofrecida por Microsoft, que acredita las destrezas de profesionales y técnicos en la aplicación de las tecnologías de este fabricante en soluciones de negocios para la empresa. La MCP certifica destrezas, conocimientos y experiencia en, al menos, una herramienta Microsoft de las áreas de Desarrollo de Aplicaciones, Administración de Bases de Datos y Administración de Infraestructura de Red. Los candidatos a MCP deben aprobar un examen de certificación Microsoft para validar y dimensionar su eficiencia y expertise. Los exámenes de certificación requeridos para esta credencial deben ser rendidos en los centros Prometric instalados alrededor del mundo. Completando una serie de exámenes MCP definidos dentro de un currículo determinado, están disponibles una serie de certificaciones de destrezas orientadas a los roles como:

- Microsoft Certified Systems Administrator (MCSA)
- Microsoft Certified Application Developer (MCAD)
- Microsoft Certified Database Administrator (MCDBA)
- Microsoft Certified Systems Engineer (MCSE)
- Microsoft Certified Solution Developer (MCSD)

CEH (Certified Ethical Hacker): Certified Ethical Hacker es una certificación profesional promovida por el Consorcio Internacional de Consultas de Comercio Electrónico. Un Hacker ético es el nombre adoptado para la realización de pruebas de penetración o intrusión a redes informáticas. Un hacker ético usualmente es un empleado o persona perteneciente a una organización, el cual intenta introducirse a una red informática o un sistema informático, utilizando métodos y técnicas Hacker, pero su propósito principal es la búsqueda y resolución de vulnerabilidades de seguridad que permitieron la intrusión. La Certificación de Hacker Ético CEH actualmente se encuentra en su versión 6.

CISSP (Certified Information Systems Security Professional) es una certificación de alto nivel profesional otorgada por la (ISC)2 (International Information Systems Security Certification Consortium, Inc), con el objetivo de ayudar a las empresas a reconocer a los profesionales con formación en el área de seguridad de la información. CISSP es considerada como una de las credenciales de mayor representatividad en el ámbito de la seguridad informática a nivel mundial. Para mayo del 2006, había registrados 38384 CISSPs en el mundo. Los aspirantes a obtener la certificación CISSP deben cumplir con los siguientes requerimientos:

- Aprobar el examen para CISSP: Este examen consta de 250 preguntas de selección simple y 6 horas de duración, en el cual se evalúa el manejo que tiene el candidato sobre cada uno de los 10 dominios de conocimiento que conforman el Common Body of Knowledge (CBK).
- Demostrar experiencia mínima de 5 años en al menos dos de los 10 dominios del CBK.
- Adherirse al Código de Ética de la ISC2.
- En caso de ser seleccionado para tal fin, el aspirante debe someterse y pasar un proceso de auditoría.

Con el objetivo de mantener su estado de CISSP, aquellos profesionales certificados deben realizar cierta cantidad de actividades cuya finalidad primordial es asegurar que el profesional se ha mantenido activo en el área de la seguridad. Cada una de estas actividades reciben cierta cantidad de créditos (CPE) de los cuales el profesional debe reunir 120 cada 3 años. Si el CISSP no reúne los 120 CPEs en el tiempo definido, debe entonces volver a tomar y aprobar el examen si desea mantener su certificación.

SSCP: La certificación *Systems Security Certified Practitioner* (Profesional Certificado en Seguridad de Sistemas) es una certificación neutral para técnicos en seguridad computacional entregada por el consorcio (ISC)2: International Information Systems Security Certification Consortium. Las siete áreas generales que cubre esta certificación están contenidas en el "SSCP Common Body of Knowledge" Los siete campos son: Controles de Acceso; Análisis y Monitoreo; Criptografía; Código Malintencionado; Redes y Telecomunicaciones; Riesgo, Respuesta y Recuperación y Operaciones de Seguridad y Administración.

Conexiones Dedicadas Privadas ("Leased Lines"): Tal y como su nombre lo implica los circuitos son alquilados completos y son privados, un caso común es: Si una oficina en cierta ciudad requiere acceso las 24 horas a otra información que resida en otra ciudad o país. Sus velocidades oscilan desde 56Kbps hasta (800 veces mayor) 45 Mbps (T3) . En ocasiones la atracción a este tipo de conexión también se debe a los ahorros de telefonía que pueden generar oficinas de la misma empresa.

Conexiones Dedicadas Compartidas ("Packet Switched"): Este tipo de conexión, similar a la anterior, es compartida por varios usuarios o empresas que envían su información a un sólo punto para realizar la transmisión, el ejemplo más claro de esto es el Backbone de Internet. A este tipo de conexión pertenecen las tecnologías de Frame Relay, ATM, Cable Coaxial y Satelital.

Conexiones Intermitentes ("Circuit-Switched Connections"): Este tipo de conexión establece un circuito permanente temporal , como el mencionado anteriormente, la diferencia estriba en que este circuito debe de ser establecido y eliminado cada vez que se requiera la comunicación. El ejemplo clásico es el de una llamada telefónica por módem o conexión vía ISDN.

Conexiones T1: Las líneas T1 son una opción popular para las empresas y para los ISP. Es una línea de teléfono dedicada que soporta transferencias de 1,544 mbps. En realidad una línea T1 consiste de 24 canales individuales, cada uno soporta 64kbits por segundo. Cada anal puede ser configurado para transportar voz o datos. La mayoría de las compañías permiten comprar sólo uno o un par de canales individuales. Esto es conocido como acceso fraccional T1.

Bonded T1: Una bonded T1 son dos o más líneas T1 que han sido unidas juntas para incrementar el ancho de banda. Si una línea T1 provee 1,5 mbps, dos líneas T1 proveerán 3 mbps (o 46 canales de voz o datos). Las líneas T1 permiten velocidades de 1,544 mbps. Un T1 fraccionado permite 64 kbps por canal. Una Bonded T1, permite velocidades de hasta 3 mbps.

Conexiones T3: Las líneas T3 son conexiones dedicadas de teléfono con transferencia de datos de entre 43 y 45 mbps. En realidad una línea T3 consiste de 672 canales individuales, cada uno soporta 64 kbps. Las líneas T3 son utilizadas principalmente por los ISP para conectarse al backbone de internet. Un T3 típico soporta una velocidad de 43 a 45 mbps.

Conexiones E1: E1 es un formato de transmisión digital; su nombre fue dado por la administración de la (CEPT). Es una implementación de la portadora-E. El formato de la señal E1 lleva datos en una tasa de 2,048 millones de bits por segundo y puede llevar 32 canales de 64 Kbps * cada uno, de los cuales treinta y uno son canales activos simultáneos para voz o datos en SS7 (Sistema de Señalización Número 7). En R2 el canal 16 se usa para señalización por lo que están disponibles 30 canales para voz o datos. E1 lleva en una tasa de datos algo más alta que el T-1 (que lleva 1544 millones de bits por segundo) porque, a diferencia del T-1, no hace el bit-robbing y los ocho bits por canal se utilizan para cifrar la señal. E1 y el T-1 se pueden interconectar para uso internacional.

Un enlace E1 opera sobre dos juegos separados de cable, usualmente es un cable coaxial. Una señal nominal de 2,4 voltios es codificada con pulsos usando un método que evita períodos largos sin cambios de polaridad. La tasa de línea es de 2,048 Mbit/s (full duplex, o sea, 2,048 Mbit/s descarga y 2,048 Mbit/s carga) el cual esta abierto en 32 segmentos de tiempo (llamados Time Slots), cada uno tiene un turno direccionado de 8 bit. De esa manera cada casilla envía y recibe un número de 8 bits muestreado 8000 veces por segundo (8 x 8000 x 32 = 2.048.000). Esto es ideal para llamadas telefónicas de voz, en donde la voz es muestreada en un número de 8 bit a esa tasa de datos y es reconstruida en el otro extremo.

Una casilla de tiempo (TS0) es reservado para efectos de segmentación, y transmite alternadamente un patrón arreglado. Esto permite al receptor detectar el inicio de cada trama y encontrar cada canal en el turno. Los estandares permiten que se realice un chequeo de redundacia cíclica a través de todos los bit transmitidos en cada segmento, para detectar si el circuito está perdiendo bits (información), pero esto no siempre es usado en una sola trama.

Una casilla de tiempo (TS16) es usualmente reservada para propósitos de señalización, para controlar la configuración de la llamada y desmonte de acuerdo a varios protocolos estandar de telecomunicaciones. Esto incluye señalización de canales asociados (Channel Associated Signaling - CAS) en donde un juego de bits es usado para replicar la apertura y cerrada del circuito (como si se descolgara y se marcara en un teléfono analógico).

Sistemas más recientes usan señalización de canal común (Common Channel Signaling - CCS) como ISDN o sistema de señalización número 7 (SS7 - Signalling System 7), el cual envía pequeños mensajes codificados con más información de la llamada, incluyendo Identificador de llamada (Caller ID), tipo de transmisión requerida etc.

WDM: (del inglés Wavelength Division Multiplexing) es una tecnología que multiplexa varias señales sobre una sola fibra óptica mediante portadoras ópticas de diferente longitud de onda, usando luz procedente de un láser o un LED.

Este término se refiere a una portadora óptica (descrita típicamente por su longitud de onda) mientras que la multiplexación por división de frecuencia generalmente se emplea para referirse a una portadora de radiofrecuencia (descrita habitualmente por su frecuencia). Sin embargo, puesto que la longitud de onda y la frecuencia son inversamente proporcionales, y la radiofrecuencia y la luz son ambas formas de radiación electromagnética, la distinción resulta un tanto arbitraria.

El dispositivo que une las señales se conoce como multiplexor mientras que el que las separa es un demultiplexor. Con el tipo adecuado de fibra puede disponerse un dispositivo que realice ambas funciones a la vez, actuando como un multiplexor óptico de inserción-extracción.

Los primeros sistemas WDM aparecieron en torno a 1985 y combinaban tan sólo dos señales. Los sistemas modernos pueden soportar hasta 160 señales y expandir un sistema de fibra de 10 Gb/s hasta una capacidad total 25.6 Tb/s sobre un solo par de fibra.

CWDM: El multiplexado por división aproximada de longitud de onda (CWDM) es un sistema que pertenece a la familia de multiplexion por divisiòn de longitud de onda (WDM), se utilizó a principios de los años 80 para transportar señal de video (CATV) en conductores de fibra multimodo, fue estandarizado por la ITU-T (internacional Telecommunication Union – Telecommunication sector), cuya norma es: ITU-T G.694.2 en el año 2002

Dentro de la familia WDM existen 4 sistemas, DWND de ultra larga distancia, DWDM de larga distancia, DWDM metropolitana y CWDM, las 3 primeras utilizan componentes ópticos más complejos, de mayores distancias de transmisión y más caros que CWDM, la cual esta desarrollada especialmente para zonas metropolitanas, ofreciendo anchos de banda relativamente altos a un coste mucho más bajo esto debido a los componentes ópticos de menor complejidad, limitada capacidad y distancia, por lo cual es la más competitiva a corta distancia.

DWDM: DWDM es el acrónimo, en inglés, de Dense wavelength Division Multiplexing, que significa Multiplexación por división en longitudes de onda densas. DWDM es una técnica de transmisión de señales a través de fibra óptica usando la banda C (1550 nm).

DWDM es un método de multiplexación muy similar a la Multiplexación por división de frecuencia que se utiliza en medios de transmisión electromagnéticos. Varias señales portadoras (ópticas) se transmiten por una única fibra óptica utilizando distintas longitudes de onda de un haz láser cada una de ellas. Cada portadora óptica forma un canal óptico que podra ser tratado independientemente del resto de canales que comparten el medio (fibra óptica) y contener diferente tipo de trafico. De esta manera se puede multiplicar el ancho de banda efectivo de la fibra óptica, así como facilitar comunicaciones bidireccionales. Se trata de una técnica de transmisión muy atractiva para las operadoras de telecomunicaciones ya que les permite aumentar su capacidad sin tender más cables ni abrir zanjas. Para transmitir mediante DWDM es necesario dos dispositivos complementarios: un multiplexador en lado transmisor y un demultiplexador en el lado receptor. A diferencia del CWDM, en DWDM se consigue mayor números de canales ópticos reduciendo la dispersión cromática de cada canal mediante el uso de un láser de mayor calidad, fibras de baja dispersión o mediante el uso de módulos DCM "Dispersion Compensation Modules". De esta manera es posible combinar más canales reduciendo el espacio entre ellos. Actualmente se pueden conseguir 40, 80 o 160 canales ópticos separados entre si 100 GHz, 50 GHz o 25 GHz respectivamente.

El primer sistema WDM en combinar dos señales portadoras hizo su aparición alrededor de 1985. A principios del siglo 21, la tecnología permite combinar hasta 160 señales con un ancho de banda efectivo de unos 10 gigabits por segundo. Ya las operadoras están probando los 40 Gbit/s. No obstante la capacidad teórica de una sola fibra óptica se estima en 1.600 Gbit/s. De manera que es posible alcanzar mayores capacidades en el futuro, a medida que avance la tecnología.

Fibra Oscura: es la denominación popular que se atribuye a los circuitos de fibra óptica, que han sido desplegados por algún operador de telecomunicaciones, pero no están siendo utilizados. La

conectividad por la fibra se comercializa en bruto, de manera que es el propio cliente quien aplica la tecnología de transmisión que más se adecúa a sus necesidades, mejorando así el rendimiento obtenido puesto que se evitan conversiones innecesarias de protocolos.

Cuando un operador de telecomunicaciones despliega su red de fibra óptica tiene que hacer una gran inversión para construir las canalizaciones y tender los cables de fibra óptica. Si en un futuro fuese necesario ampliar la capacidad de una red ya existente, sería necesario reabrir las zanjas y tender cables adicionales. Dado lo costoso de esta operación, resulta más atractivo sobredimensionar la red inicial instalando más cables de fibra óptica de los que son necesarios.

Los cables de fibra pueden contener diferentes números de fibras: 8,16,32,64,128,256 etc. Debido al sobredimensionamiento, no todas las fibras se emplean. Los que quedan sin uso reciben el nombre de fibra oscura. En último término, algunos de estos cables nunca llegan a ser utilizados, es decir, nunca se transmite luz a través de ellos. De ahí la denominación de fibra oscura.

Existen grandes compañías que disponen de diversas sedes alejadas entre sí por distancias considerables, y que tienen necesidad de grandes anchos de banda para intercomunicar dichas sedes. Las operadoras de telecomunicaciones pueden cubrir estas necesidades concretas alquilando sus circuitos de fibra oscura a estas compañías.

La fibra oscura es una opción cara de telecomunicaciones, pero existen casos en los que resulta rentable. Por ejemplo, grandes bancos y organizaciones gubernamentales usan la fibra oscura para interconectar sus centros de procesos de datos con los correspondientes centros de respaldo.

Green Computing: también conocido como Green IT o traducido al español como Tecnologías Verdes se refiere al uso eficiente de los recursos computacionales minimizando el impacto ambiental, maximizando su viabilidad económica y asegurando deberes sociales. No solo identifica a las principales tecnologías consumidoras de energía y productores de desperdicios ambientales sino que ofrece el desarrollo de productos informáticos ecológicos y promueve el reciclaje computacional. Algunas de las tecnologías clasificadas como verdes debido a que contribuyen a la reducción en el consumo de energía o emisión de dióxido de carbono son computación en nube, computación grid, virtualización en centros de datos y teletrabajo.

El término de green computing comenzó a utilizarse después de que la Agencia de Protección Ambiental (EPA, por sus siglas en inglés) de los Estados Unidos desarrollara el programa de Estrella de Energía en el año de 1992, diseñado para promover y reconocer la eficiencia energética de diversas tecnologías como computadoras, monitores y aires acondicionados. La EPA cuenta con una herramienta que funciona en internet con la que se puede realizar una Evaluación Ambiental de Productos Electrónicos (EPEAT) y que sirve para seleccionar y evaluar computadoras de escritorio, laptops y monitores en base a sus características ambientales. Los productos EPEAT están diseñados para reducir el consumo de energía, disminuir las actividades de mantenimiento y permitir el reciclaje de materiales incrementando su eficiencia y tiempo de vida de los productos computacionales.

Virtualización: La virtualización es una tecnología que comparte los recursos de cómputo en distintos ambientes permitiendo que corran diferentes sistemas en la misma máquina física. Crea un recurso físico único para los servidores, el almacenamiento y las aplicaciones. La virtualización de servidores permite el funcionamiento de múltiples servidores en un único servidor físico. Si un servidor se utiliza a un porcentaje de su capacidad, el hardware extra puede ser distribuido para la construcción de varios servidores y máquinas virtuales. La virtualización ayuda a reducir la huella de carbono del centro de datos al disminuir el número de servidores físicos y consolidar múltiples aplicaciones en un único servidor con lo cual se consume menos energía y se requiere menos enfriamiento. Además se logra un mayor índice de utilización de recursos y ahorro de espacio.

Computación en nube: La computación en nube, del inglés cloud computing, es una tecnología que permite ofrecer servicios de computación a través de Internet. La nube es una metáfora de Internet.

Es una forma de computación distribuida que proporciona a sus usuarios la posibilidad de utilizar una amplia gama de recursos en redes de computadoras para completar su trabajo. Los recursos se escalan de forma dinámica y se proporcionan como un servicio a través de Internet. Los usuarios no necesitan conocimientos, experiencia ni control de la infraestructura tecnológica. Al utilizar computación en nube las empresas se vuelven más ecológicas porque disminuyen su consumo de energía al incrementar su capacidad sin necesidad de invertir en más infraestructura. Además se aumenta la tasa de utilización del hardware ya que se comparten los recursos.

En este tipo de computación todo lo que puede ofrecer un sistema informático se ofrece como servicio, de modo que los usuarios puedan acceder a los servicios disponibles "en la nube de Internet"[2] sin conocimientos (o, al menos sin ser expertos) en la gestión de los recursos que usan. Según el IEEE Computer Society, es un paradigma en el que la información se almacena de manera permanente en servidores en Internet y se envía a cachés temporales de cliente, lo que incluye equipos de sobremesa, centros de ocio, portátiles, etc. Esto se debe a que, pese a que las capacidades de las PC han mejorado sustancialmente, gran parte de su potencia es desaprovechada, al ser máquinas de propósito general. La computación en nube es un concepto general que incorpora el software como servicio, tal como la Web 2.0 y otros recientes, también conocidos como tendencias tecnológicas, donde el tema en común es la confianza en Internet para satisfacer las necesidades de cómputo de los usuarios.

Como ejemplos de computación en nube destacan Amazon EC2, Google Apps, eyeOS y Microsoft Azure, que proveen aplicaciones comunes de negocios en línea accesibles desde un navegador web, mientras el software y los datos se almacenan en los servidores.

Computación Grid: La computación grid es una tecnología innovadora que permite utilizar de forma coordinada todo tipo de recursos (entre ellos cómputo, almacenamiento y aplicaciones específicas) que no están sujetos a un control centralizado. En este sentido es una nueva forma de computación distribuida, en la cual los recursos pueden ser heterogéneos (diferentes arquitecturas, supercomputadores, clusters...) y se encuentran conectados mediante redes de área extensa (por ejemplo Internet). Desarrollado en ámbitos científicos a principios de los años 1990, su entrada al mercado comercial siguiendo la idea de la llamada Utility computing supone una revolución que dará mucho que hablar.

El término grid se refiere a una infraestructura que permite la integración y el uso colectivo de ordenadores de alto rendimiento, redes y bases de datos que son propiedad y están administrados por diferentes instituciones. Puesto que la colaboración entre instituciones envuelve un intercambio de datos, o de tiempo de computación, el propósito del grid es facilitar la integración de recursos computacionales. Universidades, laboratorios de investigación o empresas se asocian para formar grid para lo cual utilizan algún tipo de software que implemente este concepto.

Centro de Procesamiento de Datos (CPD): Se denomina centro de procesamiento de datos o CPD a aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización. También se conoce como centro de cómputo (Iberoamérica) o centro de cálculo (España) o centro de datos por su equivalente en inglés data center. Dichos recursos consisten esencialmente en unas dependencias debidamente acondicionadas, computadoras y redes de comunicaciones.

Un CPD es un edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento electrónico. Suelen ser creados y mantenidos por grandes organizaciones con objeto de tener acceso a la información necesaria para sus operaciones. Por ejemplo, un banco puede tener un data center con el propósito de almacenar todos los datos de sus clientes y las operaciones que estos realizan sobre sus cuentas. Prácticamente todas las compañías que son medianas o grandes tienen algún tipo de CPD, mientras que las más grandes llegan a tener varios.

Entre los factores más importantes que motivan la creación de un CPD se puede destacar el garantizar la continuidad del servicio a clientes, empleados, ciudadanos, proveedores y empresas

colaboradoras, pues en estos ámbitos es muy importante la protección física de los equipos informáticos o de comunicaciones implicados, así como servidores de bases de datos que puedan contener información crítica.

INERGEN: es el nombre comercial (y marca registrada) de una gas diseñado para la extinción de incendios. Está indicado para fuego eléctrico y estancias cerradas. Se emplea habitualmente en centros de proceso de datos. El gas INERGEN es una mezcla de elementos gaseosos en la siguiente proporción:

- Nitrógeno: 52%.
- Argón: 40%.
- Dióxido de carbono: 8%.

Es invisible e inodoro.

NOC (Network Operation Center): El Centro de Operaciones de Red es un sistema de operaciones centralizado que permite el monitoreo de todas las unidades de conectividad, de servidores y plataforma de escritorio; así como también la administración y monitoreo de bases de datos e Internet.

SO/IEC 27001: El estándar para la seguridad de la información ISO/IEC 27001 (*Information technology - Security techniques - Information security management systems - Requirements*) fue aprobado y publicado como estándar internacional en octubre de 2005 por *International Organization for Standardization* y por la comisión *International Electrotechnical Commission*.

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido "Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 17799 (actual ISO/IEC 27002) y tiene su origen en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

SkipJack: El Skipjack es un algoritmo de cifrado diseñado por la Agencia de Seguridad Nacional para proteger datos a nivel gubernamental en los Estados Unidos. Inicialmente, su diseño era secreto, la estructura del algoritmo se mantuvo de forma confidencial, sin embargo, debido a problemas que tuvo la NSA para proporcionar toda la cobertura que se requería, el algoritmo se hizo público. Estaba implementado típicamente en hardware de propósito específico.

APENDICE C: Metodología de Análisis de Riesgo

Existen numerosas metodologías disponibles para la realización de análisis de riesgos, ya que es una labor que requiere de bastante dedicación y con una metodología estructurada se facilita la tarea, sobre todo si existe una herramienta que simplifique todo el proceso.

La organización debe escoger aquella que se ajuste a sus necesidades, y si considera varias opciones, inclinarse por la más sencilla. Hay que tener en cuenta que el análisis de riesgos debe revisarse periódicamente, por lo que si se hace con una metodología complicada, esta labor necesitará de una dedicación excesiva.

A continuación se detallarán algunas de las metodologías más reconocidas:

- **Análisis holandés A&K.** Es método de análisis de riesgos, del que hay publicado un manual, que ha sido desarrollado por el Ministerio de Asuntos Internos de Holanda, y se usa en el gobierno y a menudo en empresas holandesas.
- **CRAMM**. Es un método de análisis de riesgos desarrollado por el gobierno británico y cuenta con una herramienta, ya que es un método difícil de usar sin ella. Está basado en las mejores prácticas de la administración pública británica, por lo que es más adecuado para organizaciones grandes, tanto públicas como privadas.
- **EBIOS** Es un juego de guías mas una herramienta de código libre gratuita, enfocada a gestores del riesgo de TI. Desarrollada en un principio por el gobierno francés, ha tenido una gran difusión y se usa tanto en el sector público como en el privado no sólo de Francia sino en otros países. La metodología EBIOS consta de un ciclo de cinco fases:
    - Fase 1. Análisis del contexto, estudiando cuales son las dependencias de los procesos del negocio respecto a los sistemas de información.
    - Fases 2 y 3, Análisis de las necesidades de seguridad y de las amenazas, determinando los puntos de conflicto.
    - Fases 4 y 5, Resolución del conflicto, estableciendo los objetivos de seguridad necesarios y suficientes, con pruebas de su cumplimiento y dejando claros cuales son los riesgos residuales.
- **IT-GRUNDSCHUTZ (Manual de protección básica de TI)** Desarrollado en Alemania por la Oficina Federal de la Seguridad de la Información (BSI en sus siglas alemanas). Este manual proporciona un método para establecer un SGSI en cualquier organización, con recomendaciones técnicas para su implantación. El proceso de seguridad de TI propuesto por esta metodología sigue los siguientes pasos:
    - Iniciar el proceso.
    - Definir los objetivos de seguridad y el contexto de la organización.
    - Establecer la organización para la seguridad de TI.
    - Proporcionar recursos.
    - Crear el concepto de la seguridad de TI.
    - Análisis de la estructura de TI.
    - Evaluación de los requisitos de protección.
    - Modelado.
    - Comprobación de la seguridad de TI.
    - Planificación e implantación.

- Mantenimiento, seguimiento y mejora del proceso.

La metodología incluye listas de amenazas y controles de seguridad que se pueden ajustar a las necesidades de cada organización.

- **MAGERIT** Desarrollado por el Ministerio de Administraciones Públicas español, es una metodología de análisis de riesgos que describe los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación, detalla las tareas para llevarlo a cabo de manera que el proceso esté bajo control en todo momento y contempla aspectos prácticos para la realización de de un análisis y una gestión realmente efectivos. Cuenta con detallados catálogos de amenazas, vulnerabilidades y salvaguardas. Cuenta con una herramienta, denominada PILAR para el análisis y la gestión de los riesgos de los sistemas de información que tiene dos versiones, una completa para grandes organizaciones y otra simplificada para las pequeñas.
- **Manual de Seguridad de TI Austriaco** Consta de dos partes, en la primera se describe el proceso de la gestión de la seguridad de TI, incluyendo el análisis de riesgos y la segunda es un compendio de 230 medidas de seguridad. Es conforme con la Norma ISO/IEC IS 13335 y en parte con la ISO 27002.
- **MARION – MEHARI** El primigenio MARION (Método de Análisis de Riesgos por Niveles), basado en una metodología de auditoría, permitía estimar el nivel de riesgos de TI de una organización. Sustituido por MEHARI, este método de análisis de riesgo cuenta con un modelo de evaluación de riesgos y módulos de componentes y procesos. Con MEHARI se detectan vulnerabilidades mediante auditorías y se analizan situaciones de riesgo
- **Métodos ISF para la evaluación y gestión de riesgos** El Information Security Forum. (ISF) es una importante asociación internacional. Su Estándar de Buenas Prácticas es un conjunto de principios y objetivos para la seguridad de la información con buenas prácticas asociadas a los mismos. El Estándar cubre la gestión de la seguridad a nivel corporativo, las aplicaciones críticas del negocio, las instalaciones de los sistemas de información, las redes y el desarrollo de sistemas. El Estándar contiene:
    - FIRM, una metodología para el seguimiento y control del riesgo. o Una herramienta para la gestión del riesgo. o SARA, otra metodología para analizar el riesgo en sistemas críticos. o SPRINT, una metodología para hacer análisis de impacto en el negocio y analizar el riesgo en sistemas importantes pero no críticos.
    - SARA, otra metodología para analizar el riesgo en sistemas críticos.
    - Una herramienta para la gestión del riesgo
    - SPRINT, una metodología para hacer análisis de impacto en el negocio y analizar el riesgo en sistemas importantes pero no críticos.
- **Norma ISO/IEC IS 27005** La Norma habla de la gestión de los riesgos de la seguridad de la información de manera genérica, utilizando para ello el modelo PDCA, y en sus anexos se pueden encontrar enfoques para la realización de análisis de riesgos, así como un catálogo de amenazas, vulnerabilidades y técnicas para valorarlos.
- **OCTAVE** (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE®), desarrollado en EEUU por el SEI, en un una metodología para recoger y analizar información de manera que se pueda diseñar una estrategia de protección y planes de mitigación de riesgo basados en los riesgos operacionales de seguridad de la organización. Hay dos versiones, una para grandes organizaciones y otra para pequeñas, de menos de 100 empleados.
- **SP800-30 NIST Risk Management Guide for Information Technology Systems** Desarrollado por el NIST estadounidense, es una guía detallada de las consideraciones que deben hacerse para llevar a cabo una evaluación y una gestión de riesgos orientada a la seguridad de los sistemas de información.

Antes de saber qué es un análisis de riesgos y lo que conlleva es importante conocer qué son otro tipo de conceptos muy relacionados con los Análisis de Riesgos y la seguridad de la información. Estos son los más importantes:

- Amenaza: es la causa potencial de un daño a un activo.
- Vulnerabilidad: debilidad de un activo que puede ser aprovechada por una amenaza.
- Impacto: consecuencias de que la amenaza ocurra.
- Riesgo intrínseco: cálculo del daño probable a un activo si se encontrara desprotegido.
- Salvaguarda: Medida técnica u organizativa que ayuda a paliar el riesgo.
- Riesgo residual: Riesgo remanente tras la aplicación de salvaguardas.

El análisis de riesgos se define como la utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

En una organización nunca se podrá eliminar totalmente el riesgo, siempre quedará un cierto nivel de riesgo, por lo que es importante que todos los riesgos residuales sean aceptados por la Dirección.

A continuación haremos una descripción detallada de los pasos con que cuenta nuestra metodología de análisis de riesgo, la cual consideramos el punto central de la definición de una estrategia de seguridad, perfectamente alineada con la visión de la organización, dentro de su entorno de operación. Esta metodología es el resultado de la combinación de diferentes propuestas existentes en la industria, y utiliza métodos tanto cualitativos, como cuantitativos, los primeros permiten agilidad en el proceso y facilidad en la asignación de valores de impacto o riesgo, y los segundos nos permiten la precisión y exactitud, necesarias a la hora de tomar decisiones de tipo financiero, por ejemplo, en el caso de la selección de los controles adecuados, para mitigar un posible evento negativo a la operación y continuidad del negocio.

Entrevistas

Mediante este tipo de aproximación a la organización, se busca entender los diferentes aspectos que la conforman, tanto en el aspecto tecnológico, como en los procesos críticos, los cuales a su vez, son soportados por las aplicaciones y la infraestructura tecnológica.

"*La Empresa*" identificará los siguientes elementos en el marco de la norma de seguridad ISO17799/ISO 27001:

- Descripción de la Organización y sus Objetivo. Entendimiento de la organización, sus áreas funcionales y su ubicación geográfica.
- El levantamiento del detalle topológico de la infraestructura de tecnología existente, en el cual se especificará y detallará la plataforma de hardware, software, comunicaciones y procesos utilizados por XXX.
- Listas de verificación de la Infraestructura Tecnológica: El objetivo de las listas de chequeo es identificar las vulnerabilidades de las plataformas tecnológicas.

Evaluación de riesgo

La evaluación de riesgos identifica las amenazas, vulnerabilidades y riesgos de la información, sobre

la plataforma tecnológica de una organización, con el fin de generar un plan de implementación de los controles que aseguren un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información. Los dos puntos importantes a considerar son:

- La probabilidad de una amenaza
- La magnitud del impacto sobre el sistema, la cual se mide por el nivel de degradación de uno o combinación de alguno de los siguientes elementos: confidencialidad, disponibilidad, integridad.

Determinación de la probabilidad

Con el fin de derivar una probabilidad o una estimación de la ocurrencia de un evento, los siguientes factores deben ser tomados en cuenta:

- Fuente de la amenaza y su capacidad.
- Naturaleza de la vulnerabilidad.

La probabilidad que una vulnerabilidad potencial pueda ser explotada por una fuente de amenaza la podemos clasificar en alta, media-alta, media, media-baja y baja, como se describe a continuación.

Nivel	Definición
Alta=5	La amenaza esta altamente motivada y es suficientemente capaz de llevarse a cabo.
Media-Alta=4	La amenaza está fundamentada y es posible.
Media=3	La amenaza es posible.
Media-Baja=2	La amenaza no posee la suficiente capacidad.
Baja=1	La amenaza no posee la suficiente motivación y capacidad.

Número de ocurrencias del evento en un período de un año

Con el fin de poder determinar la probabilidad de ocurrencia de ciertos eventos, como el caso de una pérdida de potencia, falla en las comunicaciones, utilizamos información obtenida de ciertas publicaciones tecnológicas como Information Week e Infosecurity News. De esta manera se define una escala en la cual, a una probabilidad alta, le asignamos el valor P=5, para una probabilidad media le asignamos el valor P=3 y por último para una probabilidad baja le asignamos el valor P=1, esta asignación se define en proporción directa al numero de veces que el evento puede ocurrir en un periodo de un año. Para el caso P=5 se considera que ocurre al menos dos veces al año.

Identificación de vulnerabilidades

Para la identificación de vulnerabilidades sobre la plataforma de tecnología, se utilizan herramientas como listas de verificación y herramientas de software que determinan vulnerabilidades a nivel del sistema operativo y Firewall:

- Seguridad Física.
    - Monitoreo ambiental
    - Control de acceso

    - Desastres naturales
    - Control de incendios
    - Inundaciones
- Seguridad en las conexiones a Internet.
    - Políticas en el Firewall
    - VPN
    - Detección de intrusos
- Seguridad en la infraestructura de comunicaciones.
    - Routers
    - Switches
    - Firewall
    - Hubs
    - RAS
- Seguridad en Sistema Operacionales(Unix, Windows)
- Correo Electrónico
- Seguridad en las aplicaciones Críticas
    - Se define las aplicaciones que son críticas para la organización y por cada una de ellas se obtendrá una matriz de riesgo. Es importante considerar que las aplicaciones están soportadas por: Sistemas operativos, hardware servidor, redes LAN y WAN, y el Centro de cómputo.
- Búsqueda de vulnerabilidades en su red (Windows y Linux)
- Directorios compartidos, puertos abiertos, cuentas no usadas.
- Revisión de actualizaciones aplicadas en los sistemas operativos.
- Detección de dispositivos USB

Análisis del impacto y el factor de riesgo

El próximo paso en la metodología que estamos describiendo, es poder determinar el impacto adverso para la organización, como resultado de la explotación por parte de una amenaza de una determinada vulnerabilidad, para ello se deben considerar los siguientes aspectos:

- Consecuencias de tipo financiero, es decir pérdidas causadas sobre un activo físico o lógico determinado y las consecuencias que este activo no funcione, y afecte la operación de la compañía.
- La importancia critica de los datos y el sistema (importancia a la organización).
- Sensibilidad de los datos y el sistema.

Identificación de controles

En esta fase se evaluarán las conclusiones de la valoración respecto a ISO17799 y la matriz de riesgo

con el fin de identificar los controles que mitiguen los riesgos encontrados.

Plan de implementación tecnológica

El plan de Implementación tecnológica, se presenta como una herramienta para el control por parte de XXX de las actividades que se deben llevar a cabo para mitigar los riesgos identificados, en la evaluación de riesgo del proyecto en curso y de acuerdo al alcance definido. De esta forma la seguridad hoy en día se ha convertido en la carta de navegación para el tema de la inversión en tecnología, debemos en toda inversión tecnológica considerar aspectos relacionados con la gestión de la seguridad, con el fin de que esta inversión este alineada plenamente con la estrategia del negocio y garantice de manera efectiva y eficiente su continuidad.

Definición de políticas

Se entiende por política, las reglas generales de comportamiento definidas para la interacción entre los usuarios y los activos informáticos. Las políticas son independientes de los ambientes propios de la entidad y representan la base de un modelo de seguridad. Las Políticas de seguridad dependen de la cultura de la organización. Por esta razón las políticas y procedimientos deben estar hechos a la medida, según los requerimientos específicos de cada organización. Para la definición de las políticas y procedimientos se realiza un proceso de validación en conjunto con la organización con el fin de generar políticas y procedimientos que se ajusten a esta. Como punto de partida para la definición de las políticas se tendrá como referencia el análisis de riesgo realizado, los controles del ISO 1 7799/ISO 27001.

Las políticas cubrirán los siguientes temas:

- Seguridad en la Organización:
    - Roles y Responsabilidades de Seguridad de la Información
    - Políticas para la conexión con terceros.
- Clasificación de la Información:
    - Importancia de la información según la organización.
- Seguridad en el recurso Humano:
    - Responsabilidades de seguridad de la información para los diferentes cargos.
    - Entrenamiento a empleados en seguridad de la información como parte de su proceso de inducción y mejoramiento continuo.
- Seguridad física:
    - Seguridad ambiental
    - Control de Acceso físico.
- Administración de las operaciones de cómputo y comunicaciones.
    - Políticas sobre el uso del correo electrónico
    - Políticas sobre el uso de Internet.
    - Políticas sobre el uso de recursos.
- Control de Acceso.

- Desarrollo y mantenimiento de Sistemas.
- Continuidad de Negocio.
- Conformidad con leyes civiles, legales y contractuales.

Las políticas constan de:

- Audiencia
- Introducción
- Definiciones
- Objetivo
- Enunciado de la Política
- Políticas y Procedimientos relacionados
- Roles y responsabilidades
- Violaciones a la política

Definición de procedimientos

Los procedimientos son la descripción detallada de la manera como se implanta una política. El procedimiento incluye todas las actividades requeridas, los roles y responsabilidades de las personas encargadas de llevarlos a cabo.

Los procedimientos a definir son los siguientes: Administración de cuentas de usuario.

- Manejo de Incidentes
- Manejo de Virus
- Administración de cuentas privilegiadas.
- Procedimiento de Control de Cambios.
- Procedimiento de Acceso al edificio.
- Procedimiento de acceso al centro de Cómputo.
- Procedimiento de respaldo

Los procedimientos constan:

- Introducción
- Objetivo
- Alcance
- Responsable de su administración
- Responsables de la implementación y ejecución.
- Responsable del control

Definición de estándares

Es la definición cuantitativa o cualitativa de un valor o parámetro determinado que puede estar incluido en una política o procedimiento.

Algunos de los principales estándares a definir son:

- Longitudes de contraseñas
- Histórico de contraseñas
- Eventos a registrar en logs
- Switches
- Routers
- Firewall
- VPNs
- Sistema Operativo

APÉNDICE D: Una solución de Seguridad

Una solución de seguridad completa de los sistemas de Información requiere algo más que la última tecnología, otros componentes críticos que debe incluir son, como mínimo: una estrategia de seguridad, una gestión de riesgos en línea con las necesidades de negocio de la empresa, un política de seguridad actualizada, una organización que asuma la responsabilidad de la seguridad, un plan de divulgación y unas normas para la implantación de la tecnología.

La política de seguridad misma responderá a la posición que asuma la organización ante las amenazas. Esta posición se traduce en la determinación de una estrategia de seguridad que corresponde a un enfoque en particular para la elección de las reglas y medidas a tomar para proteger la red. Porque una buena estrategia asegura una decisión óptima en cada momento.

Una estrategia bien planificada debe ir acompañada por una serie de recursos informáticos de respaldo, por la implantación de una serie de medidas de seguridad (físicas, lógicas, organizativas), por una organización de emergencia y por unos procedimientos de actuación encaminados a conseguir una restauración progresiva y ágil de los servicios de negocio afectados por una paralización total o parcial de la capacidad operativa de la empresa.

Dependiendo de las características y la finalidad de la empresa, las estrategias de seguridad pueden ir dirigidas a evitar la materialización a ultranza de las amenazas, a minimizar su impacto, a la restauración lo más rápidamente posible de la operatividad del sistema tras un ataque, a la persecución y detección de los responsables del asalto, o bien a una combinación de ellas

Existen algunas estrategias generales que responden a diferentes principios asumidos para llevar a cabo la implementación de una solución de seguridad. Antes de establecer cualquier medida de seguridad es importante comprender algunas estrategias básicas empleadas para la protección de un Sistema de Información.

La defensa a fondo. El fallo de un solo mecanismo de seguridad no debe comprometer por completo toda la seguridad. Esta estrategia se basa en la implementación de varios mecanismos de seguridad y que cada uno de ellos refuerce a los demás. Se trata de no depender solamente de una manera de seguridad sin importar cuán fuerte parezca sino de instalar varios procedimientos que se respalden entre sí. De esta forma se evita que la falla de uno de los mecanismos deje vulnerable al Sistema de Información al completo. Aplicaciones de esta estrategia se pueden ver en otros aspectos de la vida, por ejemplo: una puerta de acceso a una vivienda con más de una cerradura y varios cerrojos.

La idea es hacerle más difícil y costoso a un atacante la tarea de violar la seguridad del sistema de información. Esto se logra con la multiplicidad y redundancia de la protección, es decir, con cada mecanismo respaldando a los demás mecanismos de seguridad y cubriendo aspectos solapados, de forma que si uno de esos mecanismos falla, existen otras barreras más que vencer. Por ejemplo, se pueden aplicar políticas de seguridad de red, junto con políticas de seguridad de hosts y con la seguridad humana (educación en seguridad para los integrantes de la organización y usuarios del sistema de información). Para el caso de la seguridad de red, por ejemplo, con un firewall, es común utilizar una solución de múltiples capas donde puede existir más de un filtro de paquetes, donde uno de ellos es capaz de filtrar aquellos paquetes que deberían haber sido rechazados por el filtro anterior.

Un aspecto importante de esta estrategia es la necesidad de evitar fallas de modo común es decir que los diferentes mecanismos deben ser cuidadosamente configurados para evitar que las fallas de un mecanismo no se propaguen al resto.

Punto de choque. Esta estrategia consiste en depender de un único punto de acceso al sistema. Ya que no existe otro camino, los esfuerzos de control y mecanismos de seguridad se centran y simplifican en monitorear un solo sitio de la red. Este punto debe estar fuertemente defendido contra

todo tipo de ataques y estar listo para responder si los detecta. Hay muchos ejemplos de puntos de choque en la vida cotidiana: los pasos fronterizos, las cajas registradoras de un supermercado, la taquilla de un cine. Esta estrategia se considera como una solución "todo en uno". Como consecuencia, uno de los problemas que presenta es que si un atacante es capaz de traspasar la seguridad de este único punto del acceso tendrá acceso a todos los recursos del sistema. Esta situación puede ser tratada utilizando mecanismos de protección redundantes (defensa a fondo) y así reforzar la seguridad de dicho punto. Adicionalmente, otro de los inconvenientes que puede provocar esta estrategia, es que pueden producirse bajas en el desempeño si se ve superada la capacidad del punto de acceso de registrar los sucesos y controlar todo el tráfico de entrada y salida.

En muchas soluciones para la seguridad de las redes, este punto de choque es implementado por un Firewall perimetral por lo que éste debe tener la capacidad de procesar todo el tráfico que por él pase sin afectar sensiblemente al desempeño de las comunicaciones. La alternativa a este problema es proveer más caminos de acceso a los Sistemas Informáticos, pero estos caminos también deben ser protegidos por algún mecanismo de seguridad, lo que hace más compleja la solución. La estrategia del punto de choque no es útil si existe una forma alternativa de acceder a la red, por lo que estos caminos deben ser cuidadosamente localizados y restringidos del acceso exterior. Un punto de choque es inservible si hay una manera efectiva de que un atacante lo evite. ¿Por qué molestarse en atacar la puerta principal, que está fortificada, si la puerta trasera está totalmente abierta?

El eslabón más débil. Se basa en la idea de que una cadena es tan fuerte como su eslabón más débil. Se deben conocer los puntos débiles de las defensas para, si es posible, eliminarlos o monitorizarlos. Aunque no por esto debe restarse importancia a la seguridad de otros aspectos del sistema. Esta estrategia, aplicada a las redes, establece que un sitio es tan seguro como lo es su enlace más débil. Este enlace suele ser el objetivo de los ataques a la privacidad de una red.

Siempre habrá algún punto que será el más débil de todos, la idea es que ese enlace debe ser lo suficientemente seguro en proporción al riesgo que implica que sea vulnerado. Algunos afirman que el eslabón más débil en la cadena de la seguridad informática es el usuario.

Diversificación de la defensa. Si todos los sistemas son iguales, alguien que sepa entrar en alguno de ellos quizá penetre en todos. Por eso, esta estrategia plantea el uso de diferentes tipos de mecanismos de seguridad de diferentes proveedores para maximizar la seguridad. Esta estrategia puede complementarse con la de defensa a fondo... El objetivo es reducir las posibilidades de fallas comunes en todos los sistemas utilizados para proteger el sistema, debidas a errores propios de los sistemas o de configuración. Esta estrategia tiene la desventaja del posible costo adicional, tanto económico como de tiempo y complejidad, ya que se debe conocer el funcionamiento y manejo de más de un producto. Otra de las posibles desventajas es la incompatibilidad de los sistemas, aunque actualmente existen estándares en varias áreas de la seguridad que hacen posible que diferentes sistemas puedan coexistir en la misma red colaborando para lograr una solución integral. Además, diversos sistemas configurados por la misma persona (o el mismo grupo de personas) pueden compartir problemas comunes, por ejemplo, si el problema es un malentendido sobre como funciona un protocolo específico, todos sus sistemas pueden estar configurados incorrectamente siguiendo ese malentendido... Por eso, adicionalmente estos sistemas pueden ser configurados por distintos administradores de seguridad para evitar que algún error conceptual por parte de los mismos afecte a la protección completa. Aunque se reconoce que utilizar múltiples tipos de Sistemas de Seguridad pueden potencialmente incrementar la seguridad, con frecuencia se concluye que la diversificación de defensas requiere más trabajo de lo que vale, y que las ganancias y mejoras no compensan el costo.

Simplicidad. La simplicidad es una estrategia de seguridad que se basa en dos principios: (1) Mantener las cosas sencillas las hace más fáciles de comprender —Si algo no se entiende, no se puede saber si es seguro o no—, y (2) lo complejo proporciona muchos escondites para que se oculten toda clase de cosas (por ejemplo, es más fácil mantener seguro un apartamento que una mansión). Se sabe que cuanto más grande y complejo es un sistema, más errores tendrá, será más

difícil de utilizar y más costoso de testear. Además, probablemente posea agujeros de seguridad no conocidos que un atacante puede explotar, por más complejos que sean. La simplicidad de los sistemas de seguridad es un factor importante de una sólida defensa de red. Particularmente los sistemas de seguridad de red a nivel de aplicación no deberían tener funcionalidades desconocidas y deberían mantenerse lo más simples posible.

Falla segura. La seguridad absoluta no existe, por tanto, en la medida de lo posible los sistemas deben tener una falla segura, es decir, si van a fallar deben hacerlo de tal forma que nieguen el acceso a un atacante en lugar de dejarlo entrar, o dejen de funcionar si detectan alguna anomalía. La estrategia de falla segura es ampliamente aplicada en la vida diaria. Los dispositivos eléctricos están diseñados para apagarse (detenerse) cuando fallan de alguna forma. Los ascensores están diseñados para frenar si no tienen energía eléctrica. Las puertas eléctricas, por lo general, se abren cuando falla la energía, a fin de que nadie quede atrapado en los edificios.

Menor privilegio. Este es uno de los principios más fundamentales de seguridad. La estrategia consiste en conceder a cada objeto (usuario, programa, sistema, etc.) solo aquellos permisos o privilegios que son necesarios para realizar las tareas que se programó para ellos. El tipo de objeto al cual se apliquen los permisos determinará la granularidad —el grado de detalle— de la seguridad obtenida. Esta estrategia permite limitar la exposición a ataques y limitar el daño causado por ataques particulares. Se basa en el razonamiento de que todos los servicios ofrecidos por una red están pensados para ser utilizados por algún perfil de usuario en particular, y no que todos los usuarios pueden utilizar todos los servicios de la red. De esta forma es posible reducir los privilegios requeridos para varias operaciones sin afectar al servicio prestado a los usuarios del sistema. Esta estrategia es difícil de implementar cuando no está prevista como una característica de diseño en los programas y protocolos que estén siendo utilizados. Debe tenerse cuidado en asegurarse si realmente se está logrando implementar esta estrategia. En cualquier caso, es posible que se termine por implementar algo menos que el mínimo privilegio, o mucho más. Esta consideración esta relacionada con el objeto sobre el cual se aplica la restricción, es decir la granularidad de la protección. Por ejemplo, aplicar la restricción sobre los usuarios, puede restringir el uso de servicios que fueron pensados para todos los usuarios.

Estado a prueba de fallos. Uno de los principios fundamentales en la seguridad es que si un mecanismo de seguridad fallara, debería negarse el acceso a todo usuario, inclusive aquellos usuarios permitidos —ya que no se puede determinar si lo son si la función de autenticación no está funcionando—, es decir debe fallar en un estado seguro. Este principio debe ser considerado al diseñar firewalls de Internet. Los filtros de paquetes y gateways, deben fallar en tal forma que el tráfico desde y hacia Internet sea detenido. La mayoría de las aplicaciones y dispositivos utilizados en una solución firewall, como routers de filtrado de paquetes y servidores proxy, dejan de retransmitir información si fallan. Esta estrategia está apoyada por la implementación de una posición específica con respecto a decisiones de seguridad y políticas. Existen dos posibles posiciones: (1) “Rechazar por defecto”, estableciendo cuales son los servicios que serán permitidos, cualquier otro será rechazado, y (2) “Aceptar por defecto”, estableciendo cuales son los servicios que no son permitidos, cualquier otro será aceptado. Es claro que la posición de rechazar por defecto es una estrategia a prueba de fallos ya que si el mecanismo falla no habrá comunicación se que sea aceptada. Por otro lado, la posición de Aceptar por defecto, asume que todo es permitido a menos que se conozca que es inseguro, en cuyo caso se prohíbe su acceso. Esta posición no es en absoluto una implementación de una estrategia de estado a prueba de fallos.

Participación universal. Más que una estrategia, es un principio que debería cumplir toda solución de seguridad. Se plantea que todo individuo en la organización que posee la red privada debe colaborar en mantener y cumplir las Medidas de Seguridad que permitan ofrecer una protección efectiva sus sistemas. De otra forma, un atacante podría aprovechar la debilidad de aquellos sistemas a cargo de

estas personas para poder llegar al resto de los recursos de la red. Un ejemplo claro de esto sería el caso de alguien que desde su equipo decidiera establecer una conexión telefónica a Internet utilizando un modem, sin ningún tipo de protección. Estaría abriendo una "puerta trasera" a posibles atacantes. Esta colaboración es necesaria ya que al administrador de seguridad de la red no puede estar en todos lados; al menos no debería convertirse en una batalla entre éste y los individuos de la organización.

Seguridad a través de oscuridad. La idea de esta estrategia está basada en mantener oculta la verdadera naturaleza del sistema de seguridad, de esta forma, un atacante lo pasará por alto como una posible víctima. Pero esta suposición es algo ingenua ya que varios estudios han demostrado que el interés de un atacante por un determinado sitio no solo está determinado por el interés que éste tenga sobre la información del sistema. Esta estrategia, aunque puede ser útil en el comienzo de la vida de un sitio, y una buena precaución, es una base pobre para una solución de seguridad a largo plazo ya que la información tiende a filtrarse y los atacantes son habilidosos para obtener información relevante del sitio

Seguridad basada en Hosts. En este modelo, los esfuerzos de protección están enfocados en los sistemas finales de una red privada, es decir que los mecanismos de seguridad son implementados en estos sistemas, y son ellos mismos quienes deciden si aceptar o no los paquetes de una comunicación. Probablemente sea el modelo de seguridad para computadoras mas comúnmente usado en la actualidad, aunque el mayor problema con este modelo es que no es escalable si no se considera un esquema de administración apropiado, por lo que solo es usado en ambientes muy pequeños o donde no existe una red configurada que pueda ofrecer tal tipo de protección. El mayor impedimento para hacer efectiva la seguridad de estos sistemas en ambientes de redes de computadoras actuales es la complejidad y heterogeneidad de esos ambientes. Inclusive si todos los hosts fueran idénticos o si tal heterogeneidad fuera superada, un sitio con un gran número de hosts hace que sea difícil asegurar de forma efectiva a cada uno. Mantener e implementar efectivamente la protección a este nivel requiere una importante cantidad de tiempo y esfuerzo, y es una tarea compleja. En pocas palabras, puede no ser rentable implementar un nivel de seguridad a nivel de hosts para sitios grandes ya que requieran muchas restricciones, y mucho personal de seguridad. Adicionalmente, este modelo presenta un problema importante en cuanto a puntos de ahogo y enlaces débiles: no existe un único punto de acceso ya que existen múltiples conexiones, una para cada host, muchas de las cuales pueden estar débilmente protegidas.

Seguridad basada en la Red. El modelo de seguridad de red se enfoca en controlar el acceso a la red, y no en asegurar los hosts en sí mismos. Este modelo esta diseñado para tratar los problemas identificados en el ambiente de seguridad de hosts, aplicando los mecanismos de protección en un lugar en común por el cual circula todo el tráfico desde y hacia los hosts: los puntos de acceso a la red. Un enfoque de seguridad de red involucra la construcción de firewalls para proteger redes confiadas de redes no confiables, utilizando sólidas técnicas de autenticación, y usando encriptación para proteger la confidencialidad e integridad de los datos a medida que atraviesan la red. La ventaja sobre el modelo de seguridad de hosts es una considerable reducción del costo para proveer la misma o mejor protección, ya que solo se necesita proteger unos pocos puntos de acceso (en muchos casos, uno) lo que permite concentrar todos los esfuerzos en una solución perimetral. Este modelo es escalable en la medida de que la solución perimetral pueda soportar los cambios sin afectar su desempeño. Una desventaja de este modelo es que es muy dependiente de algunos pocos puntos de acceso por lo que pueden producirse reducciones en el desempeño del trafico de entrada y salida de la red; por otro lado, la protección lograda no es flexible y posee un bajo grado de granularidad, es decir, no es posible especializar la protección necesaria para cada host y sistema final de la red privada.

Requerimientos funcionales de una solución de seguridad

El objetivo de una solución de seguridad es "aislar" el segmento de la red local del resto de Internet y controlar el tráfico que llega y sale de ella. De aquí surgen dos aspectos básicos a cubrir por una solución de seguridad para redes, seguridad en tránsito y regulación de tráfico, los cuales, cuando son combinados, ayudan a garantizar que la información correcta sea entregada de forma segura al lugar correcto. Existe también la necesidad de asegurar que los hosts que reciban la información, la procesen apropiadamente, de aquí surge el espectro completo de seguridad de los hosts. La protección de una red contra amenazas no puede ser lograda por una sola tecnología o servicio por lo que es necesario diseñar una estrategia balanceada que permita cubrir los puntos débiles en la seguridad de una red.

Seguridad en tránsito: Todas las comunicaciones entre sitios que forman parte de una red publica son vulnerables a ataques de escuchas, éste riesgo está asociado con la importancia que tiene la información para quien tenga la habilidad de interceptar dicha comunicación. La seguridad en transito enfatiza la necesidad de mantener los datos seguros mientras transitan una red pública como Internet. Así, disponemos de ciertas funciones o servicios que cubren distintos puntos de este aspecto.

Limitar la exposición de la red interna: De esta forma podemos ocultar "todo" lo que sucede dentro de la red de la organización de la red publica, que de otra forma significaría un riesgo en la seguridad de las comunicaciones y los recursos. Mediante este servicio es posible ocultar el esquema de direcciones de la red interior, para evitar que cualquier host no confiable efectúe comunicaciones de forma directa con alguno de los host de nuestra red, así como también asegurar que todo el trafico entre hosts confiables de la red privada que atraviese una red publica se mantenga de esa forma (es decir, solo accesible a aquellos hosts a quienes está destinada la comunicación). Estas funcionalidades pueden ser logradas mediante el uso de la Traducción de Direcciones de Red (NAT) y de Redes Privadas Virtuales (VPN) respectivamente.

Tunneling de Tráfico, Puntos de control y Monitoreo: La transmisión de paquetes entre dos sistemas finales remotos en Internet involucra la intervención de varios sistemas intermedios que pueden tener acceso a la información transmitida si no se considera ningún esquema de privacidad. Un túnel es un tipo especial de conexión entre dos sistemas a través de una red. La conexión establecida es directa y virtual es decir que simulan una conexión por cable directa que comunica dos sistemas. Estas conexiones pueden ser usadas para evitar las limitaciones de una topología ya que un paquete enviado a través de un túnel pasa inadvertido de los nodos que intervienen en la ruta real hasta el destinatario (quien también tiene configurado el túnel). Por ejemplo un túnel puede comunicar dos sitios remotos que estén conectados mediante proveedores de conexión a redes públicas (como un ISP). Este tipo de conexiones proveen de servicios tales como encriptado de datos, autenticación, control de acceso (autorización) e integridad de datos Dos Firewalls conectados mediante túneles ofrecen protección del exterior mientras que el túnel provee conectividad. Si el tráfico del túnel es encriptado, los riesgos son menores y los beneficios son importantes.

Con la utilización de un túnel, un host que se encuentra físicamente en otra red, pertenece virtualmente a nuestra red local con lo que es posible que un servidor ofrezca un servicio más confiable y transparente a sus usuarios. En favor de esto último, las conexiones de túnel existen más allá del tiempo de conexión, es decir, no terminan cuando la transmisión de datos entre los dos sistemas ha finalizado; es una conexión acordada y configurada previa a cualquier transmisión de datos y, en principio, permanente.

Configurados adecuadamente, los túneles permiten forzar el tráfico (de entrada y salida) de un Firewall a través de puntos de control específicos del mismo y de esta forma es posible monitorear la actividad de la red en tales puntos de acceso; utilizando alarmas y habilitando el registro del Firewall

podemos buscar actividades sospechosas para detectar la presencia de intrusos, además de los beneficios ya comentados de utilizar un túnel.

Regulación de Tráfico: Otro de los aspectos importantes acerca de la seguridad de las redes es regular de cerca qué tipos de paquetes pueden viajar entre redes. Si un paquete que puede hacer algo malicioso a un host remoto nunca llega a él, el host remoto no se verá afectado. La regulación del tráfico provee este servicio entre hosts y sitios remotos. Esto sucede en tres áreas básicas de la red: routers, Firewall y hosts. Cada uno provee servicios similares en diferentes puntos de la red. De hecho, la línea que los diferencia es arbitraria y difusa.

Política de Seguridad: La política de seguridad deber ser una de las primeras consideraciones al diseñar una solución de seguridad pues será la que guíe la elección y configuración de la tecnología a utilizar. Y en su definición influye un factor clave: la postura del diseñador, es decir la actitud ante los riesgos que corre la red por su conexión a una red pública. Está afectada por la opinión y habilidades del diseñador y responderá a una filosofía que será más o menos flexible (aceptamos solo aquello que sea seguro -porque lo conocemos-, o rechazar solo aquello que es malo -porque lo conocemos-). No elegir o seleccionar una politica de seguridad, es también en sí misma una política de seguridad: la de permitir todo. Una filosofía apropiada es aquella que no considere que todo es absoluto, es decir, que encuentre un punto intermedio que se ajuste a las necesidades de la organización. Sería deseable que pueda minimizar el peligro y proveer a la vez los beneficios de una conexión de red.

Con esto debe quedar en claro que no existe una fórmula para la política de seguridad de una red privada sino que cada responsable debe diseñarla según el caso, las necesidades, las directivas, las restricciones y otros factores que fundamenten o no una determinada decisión. Tales decisiones son necesariamente dependientes del contexto. Las consideraciones de una política de seguridad están dirigidas por las necesidades estructurales, de negocios o tecnológicas de la organización y pueden involucrar decisiones tales como restringir el tráfico de salida de red que permita a los empleados exportar datos valiosos, restringir el software importado por los empleados sin permiso de la compañía, impedir el uso de un determinado protocolo de comunicación porque no puede ser administrado de forma segura, entre otras. Este es un proceso iterativo que permite modificar la filosofía para ajustarse a las necesidades del momento.

El funcionamiento de un Firewall está fuertemente asociado a la política de seguridad elegida. Definir los límites de comportamiento es fundamental para la operación de un Firewall. Por lo tanto, una vez que se haya establecido y documentado apropiadamente una sólida política de seguridad, el Firewall debe ser configurado para reflejarla y es su trabajo aplicarla como parte de una defensa de perímetro (siguiendo el enfoque tradicional). Consecuentemente se configura un Firewall para rechazar todo, a menos que hayamos elegido explícitamente aceptarlo y correr el riesgo. Tomar el camino opuesto de rechazar solo a los ofensores conocidos es una opción extremadamente peligrosa. Por último, cualquier cambio hecho al Firewall debería se corregido en la política de seguridad y viceversa.

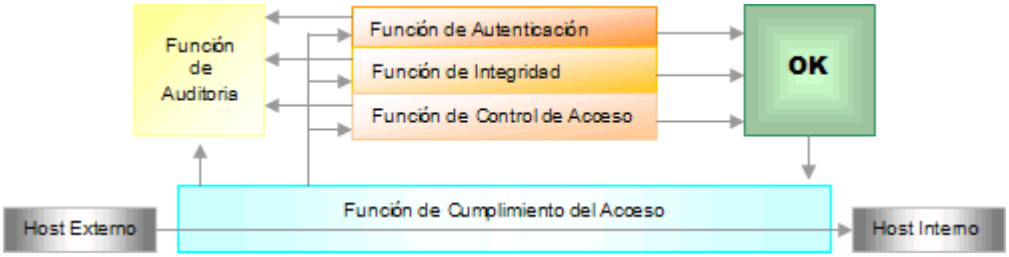
Filtros y listas de acceso: Los filtros son programas que generalmente se encuentran situados en los sistemas que proveen conectividad entre redes, es decir los puntos de acceso a la red, routers, firewalls y gateways (aunque esto no es así para todos los casos). Estos efectúan un análisis para determinar el destino del paquete completo en base a la información contenida en el encabezado de los paquetes que llegan a dichos sistemas y en función de un conjunto de reglas. De aquí podría decidir desechar el paquete, es decir, no permitir que continúe viajando por la red en la dirección original (entrando o saliendo); aceptar el paquete, con lo cual continuaría atravesando la red, o hacer algo más (por ejemplo, redireccionarlo a otro punto de la red).

Las reglas especifican patrones o propiedades en los datos del encabezado de un paquete asociados con la acción a tomar con dicho paquete. Cada paquete que atraviesa el filtro es comparado contra la lista de reglas también conocida como cadena de reglas. Para decidir el destino de un paquete, el filtro busca, a través del conjunto de reglas, alguna que coincida con el contenido del encabezado del

paquete. Una vez encontrada dicha regla, se lleva a cabo la acción indicada por la regla para el paquete. Esta lista de reglas debe ser configurada para reflejar la política de seguridad asumida por la solución de seguridad de la red.

Con la utilización de un filtro es posible bloquear toda comunicación con ciertas partes (sitios) de la red externa para evitar determinados comportamientos no deseables en los sistemas finales de la red privada; permite restringir todas las comunicaciones entrantes a ciertos servicios de la red para evitar el acceso a recursos privados; y habilitar alarmas o avisos que adviertan que paquetes entran, salen o son rechazados. Por lo tanto el filtro de paquetes puede actuar tanto para la entrada como para la salida de paquetes de la red.

Partiendo de la necesidad de implantar estos servicios para una solución Firewall, se ha definido un modelo de referencia que establece los diferentes componentes que deben estar presentes:



Modelo de referencia para Firewalls

- *Función de Auditoría o Monitoreo*: permite el registro de eventos relevantes del sistema, muy útil para la detección de intrusos.
- *Función de Autenticación*: permite la identificación certera de la entidad con la cual se establece una comunicación.
- *Función de Integridad:* asegura que el paquete ha sido recibido tal cual fue enviado y que no ha sido falseado en el transcurso de su transmisión.
- *Función de control de Acceso (filtrado de paquetes):* en base a información dentro del paquete, se verifican las reglas de seguridad para determinar el destino del paquete.
- *Función de cumplimiento del Acceso:* realiza el control final de los datos entrantes derivando la decisión a los módulos apropiados; éste es un servicio de la misma naturaleza que el de control de acceso, solo que a un nivel superior (referido a la aplicación responsable de procesar el paquete).

NAT: Traducción de Direcciones de red: La traducción de direcciones de red (NAT por Network Address Translation) fue creada, inicialmente con el propósito de resolver el problema de escalabilidad de direcciones IP y su agotamiento para la asignación de nuevas números IP; otra ventaja de NAT es que permite ocultar el esquema de direcciones de una red privada al exterior ofreciendo un importante servicio para una solución de seguridad.

La estrategia utilizada por la aplicación de esta tecnología está basada en la distribución topológica de la asignación de futuras direcciones IP de cada espacio de direcciones de red a los distintos dominios de ruteo de tránsito de datos (redes privadas). Las direcciones IP dentro de un red privada no son únicas globalmente, sino que son reusadas en otros dominios, resolviendo así el problema de agotamiento de direcciones.

Cuando un paquete es enviado al exterior de la red, la dirección IP de origen es traducida a una

dirección única globalmente para evitar posibles conflictos con otros espacios de direcciones asignados a otras redes privadas y ocultar el esquema de direcciones de la red local. Para esto, la función de NAT se implementa en cada punto de salida entre la red privada y una conexión a la red pública. Cada dispositivo NAT tiene una tabla de pares de direcciones IP: direcciones locales y direcciones únicas asignadas globalmente para poder realizar el mapeo. Ocurre la operación inversa con las direcciones de los paquetes que provienen del exterior. Con este esquema, es posible que una única dirección IP sea necesaria para representar a un grupo entero de computadoras.

La traducción de direcciones permite a un único dispositivo que interconecte la red privada con la red exterior, por ejemplo un router o un firewall, actuar como agente entre Internet y la red local. NAT puede ser instalado sin grandes cambios a estos dispositivos, lo que lo hace una buena opción con importantes beneficios. NAT es transparente a las sistemas internos y externos y operan en la capa de red sin agregar mucho tiempo de cómputo adicional a las comunicaciones.

La traducción de direcciones puede funcionar de diferentes modos:

- Estática: Mapea una dirección IP no registrada a una dirección IP registrada en un esquema uno a uno. Es útil cuando un dispositivo necesita ser accesible desde el exterior. Por supuesto, esto no es aconsejable si la seguridad es importante.
- Dinámica: Mapea una dirección IP no registrada a una dirección seleccionada dinámicamente de un grupo de direcciones IP registradas.
- Sobrecarga: Es una forma de NAT dinámico que mapea múltiples direcciones IP no registradas a una única dirección IP registrada usando diferentes puertos (seleccionados dinámicamente)
- Solapamiento: Cuando las direcciones usadas en la red interna son direcciones registradas usadas en otra red, el router debe mantener una tabla de búsqueda de éstas direcciones para poder interceptarlas y reemplazarlas con direcciones IP únicas registradas. El router NAT debe traducir las direcciones internas a direcciones únicas registradas así como las direcciones registradas externas a direcciones que sean únicas a la red privada.

Es de principal importancia la traducción dinámica de direcciones: en una red interna se configuran un conjunto de direcciones IP que no han sido asignadas particularmente a esa red, es decir, que no son únicas, por lo que deben considerarse no ruteables. El router que (comúnmente) cumple con la función de NAT, dispone de un rango de direcciones IP únicas globalmente (dirección global interna).

Cuando el router recibe un paquete del interior de la red, almacena la dirección no ruteable del host que lo envió (dirección origen del paquete IP) en la tabla de traducción de direcciones. Luego reemplaza dicha dirección en el paquete recibido por la primer dirección IP única (ruteable) disponible y reenvía el paquete. En la tabla ha quedado registrado el mapeo de la dirección IP real, no ruteable del host de la red con una dirección IP única global.

Cuando el router recibe un paquete de una computadora del exterior de la red, comprueba que la dirección de destino del paquete se encuentre en la tabla de traducción de direcciones (esto ocurrirá si el paquete es una respuesta de un mensaje enviado a esa computadora), luego reemplaza esa dirección con la correspondiente dirección IP real del host de la red privada y reenvía el paquete. De esta forma, la tabla almacenará los mapeos de direcciones internas a direcciones únicas solo cuando se esté realizando una comunicación con un sistema externo. En el caso de no encontrar en la tabla la dirección del destinatario, el paquete es rechazado.

Por otro lado, las direcciones registradas de forma global de otros dispositivos de la red (direcciones globales externas) son traducidas a direcciones privadas no registradas para evitar posibles conflictos de solapamiento de direcciones entre distintos dominios.

Un NAT dinámico ofrece un importante servicio de seguridad, ya que solo son permitidas aquellas

conexiones que se originen en el dominio privado, es decir que una computadora externa no puede iniciar un contacto a menos que un host de la red interna haya iniciado la comunicación (de otra forma es rechazado por el router).

Aunque podemos observar que este esquema no es totalmente seguro, ya que un tercero (no involucrado en la comunicación iniciada en el interior de la red) que intercepte un mensaje enviado desde la red interna puede leer la dirección IP de origen del mensaje y de esta forma sus paquetes serían aceptados por el router. Por esto, un router que realice la función de NAT no es la única solución para un Firewall, sino que es una porción de todas las funciones que debe cumplir un Firewall para ser efectivo (por Ej. puede utilizarse un túnel para comunicar estos paquetes). Un router cumpliendo la función de NAT puede proveer filtrado y registro de tráfico para llevar un control de las comunicaciones que se lleven a cabo.

Encriptación a nivel de enlace: Es la forma de protección criptográfica más transparente tanto para los controladores de los dispositivos como para las aplicaciones.

Esta protección solo afecta a un enlace individual. La ventaja principal es que el paquete es encriptado por completo, incluyendo las direcciones de origen y destino lo que deja fuera de riesgo la comunicación. Aunque el problema es que solo protege un enlace en particular: si un mensaje debe atravesar mas de un enlace, será vulnerable en el nodo intermedio y en el siguiente enlace, si éste no está protegido.

Por lo tanto, el encriptado a nivel de enlace es útil para proteger solo trafico local o unas pocas líneas de enlace muy vulnerables o críticas (como por ejemplo circuitos satelitales).

Encriptación a nivel de transporte y a nivel de red: El Protocolo de Seguridad de la Capa de Red (Network Layer Security Protocol - NLSP) y el Protocolo de Seguridad de la Capa de Transporte (Transport Layer Security Protocol - TLSP) permiten a los sistemas comunicarse de forma segura sobre Internet. Estos son transparentes para la mayor parte de las aplicaciones. La función de encriptado afecta a todas las comunicaciones que ocurran a lo largo de diferentes sistemas. Ambos protocolos están basados en el concepto de id de clave o key-id; éste es transmitido sin encriptar junto con el paquete encriptado. Permite controlar el comportamiento de los mecanismos de encriptado y desencriptado: especifica el algoritmo de encriptado, el tamaño del bloque de encriptado, el mecanismo de control de integridad usado, el período de validez de la clave, etc. Utiliza un mecanismo de administración de claves para intercambiar calves e ids de claves. Ambos protocolos difieren notablemente en la granularidad de la protección.

TLSP está limitado a conexiones individuales tales como circuitos virtuales creados en TCP. Diferentes circuitos entre el mismo par de hosts pueden ser protegidos con diferentes claves. El segmento TCP completo (incluyendo el encabezado) es encriptado. Este nuevo segmento es enviado al protocolo IP, con un identificado de protocolo diferente. Al recibir el paquete, IP envía el paquete a TLSP, que luego de desencriptar y verificar el paquete, lo pasa a TCP

NLSP Ofrece más opciones que TLSP. Puede ser instalado en un router, y proteger así la subred completa. NLSP opera por encapsulación o “tunneling”. En modo túnel, el paquete IP es encriptado y luego es adjuntado a un nuevo paquete IP. La dirección IP en este encabezado puede diferir de aquella del paquete original ofreciendo una defensa contra el análisis de tráfico.

El modo encapsulación es suficiente si los dos sistemas finales de una comunicación NLSP están conectados a la misma red. La creación del nuevo encabezado IP es omitida, el paquete NLSP encriptado es enviado directamente a la capa subyacente.

La granularidad de la protección provista por NLSP depende de donde es situado. Si NLSP se encuentra en un host, se garantiza la seguridad para toda comunicación del mismo, no para un proceso individual. Implementado en un router puede proveer seguridad para todos los mensajes originados en algún lugar de la red protegida. Permite aislar las variables criptográficas en una “caja”.

Estos protocolos no exigen ninguna restricción de comunicación, es decir, cualquier host protegido

puede comunicarse con cualquier otro. Los patrones de comunicación son una cuestión administrativa, estas decisiones son aplicadas por los sistemas de encriptado y los mecanismos de distribución de claves.

La Arquitectura de Seguridad para el Protocolo de Internet (IPsec) provee un marco de seguridad que cubre varios aspectos necesarios para una solución apropiada [RFC-2401].

IPsec – Arquitectura de Seguridad para IP: IPsec está diseñado para proveer seguridad basada en criptografía, de alta calidad e interoperable para Ipv4 e Ipv6. Los servicios de seguridad ofrecidos incluyen control de acceso, integridad en comunicaciones sin conexión, autenticación del origen de datos, protección contra ataques de repetición, confidencialidad mediante encriptado, entre otros. Estos servicios son provistos en la capa IP ofreciendo protección para ésta y las capas superiores. Para ofrecer tales servicios, IPsec utiliza dos protocolos de seguridad de tráfico, AH (Authentication Header) y ESP (Encapsulating Security Payload) además del uso de protocolos y procedimientos de administración de claves criptográficas. El protocolo de administración automática de claves por defecto es IKE. IKE es usado para establecer una política de seguridad compartida y claves autenticadas para servicios que las requieran (como IPsec). Antes del envío de trafico IPsec, cada router/firewall/host debe ser capaz de verificar la identidad de su par. Esto puede ser hecho manualmente entregando claves pre-compartidas en ambos hosts.

El conjunto de protocolos de seguridad utilizados y la forma en que son empleados estará determinado por requerimientos del sistema y de seguridad de los usuarios y aplicaciones.

Los mecanismos utilizados por IPsec están diseñados para ser independientes de los algoritmos empleados. Esta modularidad permite la selección de diferentes conjuntos de algoritmos sin afectar las otras partes del sistema. De todas formas, IPsec propone un conjunto de algoritmos por defecto para ser usados y proveer interoperabilidad en Internet.

AH y ESP: El Encabezado de Autenticación (Authentication Header - AH) de IP provee integridad para comunicación sin conexión y autenticación del origen de datos para datagramas IP y para proveer protección ante ataques de repetición [RFC-2402] [RFC-2406].

AH provee autenticación para la mayor parte de la información del encabezado IP y para los protocolos del nivel superior. No todos los campos del encabezado IP son protegidos ya que son modificados en tránsito.

AH puede ser aplicado solo, en combinación con ESP (Encapsulating Security Payload), o de forma anidada a través del uso del modo túnel. Los servicios de seguridad pueden establecerse entre un par de sistemas finales, entre un par de gateways de seguridad o entre un gateway o un sistema final.

ESP puede ser usado para proveer los mismos servicios de seguridad, y también provee un servicio de encriptación. La principal diferencia entre la seguridad provista por ESP y AH es el alcance de la protección. Específicamente, ESP no protege ningún campo del encabezado IP (excepto en modo túnel, donde los datos encriptados por ESP corresponden a otro paquete IP).

Redes Privadas Virtuales y Firewalls: Es común que un Firewall implemente un servicio VPN, de esta forma, es posible conectar dos redes con protección perimetral mediante túneles de Firewall a Firewall, con lo cual se obtiene una red privada conformada por dos redes remotas.

Existen dos consideraciones en cuanto al acceso por parte de usuarios de una red a los recursos de la otra, dependiendo de la confianza o acuerdo existente: Las comunicaciones entre ambos Firewalls, a través de una VPN pueden ser efectuadas con acceso controlado o acceso abierto.

En conexiones con acceso controlado, la VPN es utilizada solo para ofrecer privacidad entre ambos puntos, ya que no existe una completa relación de confianza entre ambas partes, por lo que la comprobación de autenticidad se lleva a cabo para cada comunicación y el acceso a los recursos de la red es restringido para ciertos servicios. En este caso se utiliza un firewall para controlar el acceso

a la red interna.

En conexiones con acceso abierto, la VPN es configurada para que ambos firewalls tengan un acceso completo a los recursos de la otra red. No se requiere un control de autenticidad ya que se ha acordado previamente este permiso (es decir que no se realiza por no considerarse necesario). En este esquema, el firewall realiza la función de conectividad mediante VPN, por lo que el tráfico es privado, y si agregamos la confianza que resulta de que todos los sitios son administrados por la misma organización, bajo las mismas políticas de seguridad, se podrán permitir todos los servicios de red sobre esta VPN. De esta forma, las transmisiones están bajo la protección del firewall, por lo que el "perímetro" de seguridad de la red se extiende a los sistemas remotos conectados mediante la VPN; todos estos sistemas se encuentran virtualmente en la misma red privada con un perímetro de red virtual.

También es posible establecer una VPN entre un firewall y un sitio remoto simple para proveer acceso privado a usuarios móviles o conexiones hogareñas. De la misma forma que las conexiones anteriores, éstas pueden ser con acceso controlado o abierto. El primero es útil para clientes y socios que necesiten acceso a servicios o sistemas particulares. El segundo es útil para empleados o socios de la organización que necesiten tener acceso a recursos compartidos, como ser, archivos, impresoras, unidades de almacenamiento masivo, etc.; en ambos casos estos servicios o recursos están situados dentro del perímetro de seguridad de la red. Mediante VPNs todas estas operaciones pueden realizarse de forma segura.

Existen varias tecnologías para implementar Redes Privadas Virtuales, la principal es criptografía.

Existe una consideración muy importante para hacer posible el uso global de las VPNs, y es la necesidad de estandarización. Es deseable que cualquier sistema de conexión o firewall sea capaz de establecer una red privada virtual con cualquier otro en cualquier parte del mundo. Cuando la tecnología de VPN surgió, no existía un estándar para configurar este tipo de conexiones, y algunos proveedores crearon un mecanismo, llamado swIPe (software IP encription) pero no era el único, existían otras variantes pero no eran compatibles ya que se hacían portables para una arquitectura en particular.

Para que la conectividad provista por las VPN sea ampliamente aprovechada, los diferentes sitios deben poder ser capaces de comunicarse con mecanismos compatibles e independientes de la plataforma usada, aunque utilicen diferentes productos. La estandarización puede resolver estos problemas.

Actualmente, el estándar de la Arquitectura de Seguridad para el Protocolo de Internet (IPsec) ha propuesto un ambiente de protocolos de seguridad, que permitirá la interoperabilidad de aquellos proveedores que utilicen las recomendaciones de éste estándar.

Una VPN debe responder a consideraciones de cuatro tipos de tecnologías, de entre los cuales los más importantes actualmente son:

- Mecanismos de encriptado: IPsec, PPTP, T2L, PT2L
- Algoritmos de encriptado: RC2 y RC4, DES y 3DES, IDEA, CAST
- Mecanismos de negociación e intercambio de claves para encriptado: ISAKMP, SKIP
- Algoritmos utilizados para intercambiar claves para el encriptado: RSA, Diffie-Hellman

Todos estos mecanismos deben funcionar en forma coordinada para poder integrar una eficiente funcionalidad para una VPN.

Los Firewalls para Internet son un requerimiento muy importante en el momento de considerar una conexión a una red pública. Si sumamos a esta solución la funcionalidad de una red privada virtual se pueden extender los horizontes de una red local ofreciendo ambos servicios en uno: conectividad privada. Las VPNs no desplazan a los Firewalls, son parte de ellos: un Firewalls es responsable de implementar la política de seguridad de la red privada de una organización como parte del perímetro

de defensa; con el uso de redes privadas virtuales, los Firewalls podrán aplicar estas políticas sobre conexiones de red privadas hacia sitios remotos.

Control de Acceso y Filtros: Una de las funciones más importantes de un firewall es el filtrado o control de acceso de toda la información que sea recibida en los distintos puntos de acceso a la red interna o a los sistemas finales, que son administrados por aquél. El filtrado de datos permite controlar la transferencia segura de datos basado principalmente en: la dirección de donde provienen los datos, la dirección de destino de los datos y los protocolos de transporte y aplicación utilizados. Esta función puede ser implementada en diferentes niveles de la arquitectura de red, con lo cual se logran diferentes niveles de granularidad, es decir, qué tan minucioso es el control de seguridad efectuado. Sobre la base del nivel donde se efectúe el filtrado, la función se implementará en diferentes dispositivos1. Los niveles mencionados son tres2: filtrado de paquetes, control de acceso de conexiones y filtrado de datos de aplicación.

Filtrado de paquetes (a nivel de red): Los filtros de paquetes operan al más bajo nivel de abstracción en el cual, los datos son transmitidos en paquetes y analizados como tales. En la familia de protocolos TCP/IP, los filtros son aplicados al nivel de transporte (TCP, UDP) y al nivel de red (IP). Este mecanismo es implementado por lo general en los sistemas intermedios (gateways o routers) que conectan la red interna con la red pública. Cada paquete que ingresa a la red es interceptado y analizado por la función de filtrado, implementada por un filtro de paquetes en estos dispositivos intermedios. Suelen ser llamados Router de Filtrado de Paquetes o Gateways de Filtrado de Paquetes. El filtro rechaza o reenvía los paquetes al destinatario original, según reglas especificadas en Listas de Control de Acceso (ACL), que son almacenadas en el router o gateway, basadas en los datos de los encabezados de los paquetes TCP e IP. Básicamente los datos analizados son las direcciones IP y puertos TCP de origen y destino de los paquetes. Un filtro de paquetes no mantiene información de contexto para los paquetes que sean parte de una conexión; todos los paquetes son tratados de forma independiente, sin ser relacionados con ningún otro.

La principal ventaja del filtrado de paquetes es que permite proveer, en un único sitio o punto, una protección particular para la red entera. Además es transparente a los usuarios de la red ya que no requiere configuración alguna en los sistemas que interconecta ni realizar tareas especiales de transmisión u otro tipo, lo que ofrece una estructura flexible en el sentido de que puede ser modificada o re-estructurada sin necesidad de modificar el resto de la red.

Aunque existen algunas desventajas como posibles problemas de desempeño que pueden ser clasificados en tres categorías [Peri]: número de campos examinados, posición del campo en el paquete, demora del proceso. Esto afecta el espacio necesario para almacenar las reglas, el número de comparaciones y la complejidad del algoritmo.

El núcleo de un filtro de paquetes consiste de un lenguaje de descripción que permite expresar reglas de políticas de seguridad orientadas a paquetes. Las reglas definidas hacen referencia a entidades, es decir que identifica dispositivos o sistemas por medio de sus direcciones IP. La sintáxis de estos lenguaje no está estandarizada por lo que diferentes productos permiten expresar las reglas de diferentes formas.

Para ser efectivo, un filtro debe permitir expresar reglas utilizando comodines y rangos de valores para referirse a más de un host o dispositivo. Por ejemplo “permitir los paquetes destinados al host 130.15.214.23 pero sólo entre los puertos 1000 y 1050 (130.15.214:1000..1050)”; y “negar todos aquellos paquetes provenientes de la red 170.210.122.0 (170.210.122.*:*)”.

También debe considerarse el espacio necesario para almacenar las reglas ya que existen múltiples caminos que pueden tomar los paquetes hasta llegar al dispositivo filtrador. De aquí surge, también, la necesidad de algoritmos de búsqueda de reglas. Todos estos aspectos afectan el desempeño del filtro afectando también el desempeño de la red.

La función de filtrado de paquetes puede implementarse en varios sitios de la red interna. La forma más directa y simple es utilizar un router que la soporte.

Un router tendrá dos interfaces, una que conecte a la red externa y la otra a la red interna. Los filtros pueden aplicarse en una de las dos interfaces, o en ambas. Además puede aplicarse al tráfico de entrada como al de salida, o a ambos. Estas características varían con los diferentes routers. Tales consideraciones reflejan diferentes políticas más o menos flexibles, con más o menos puntos de control. Una buena política a respetar es que si un paquete ha de ser rechazado, que sea cuanto antes. Otra posible opción es efectuar el filtrado independientemente de la interfaz de red.

Una alternativa es utilizar filtros basados en hosts, tales como screend de Digital Equipment Corporation disponible para algunos sistemas operativos; ipfilterd de SGI Systems y Karlbridge. Otra herramienta es IPTables/NetFilter, la cuarta generación de filtros de paquetes para Linux. La primer generación fue ipfw, creada para BSD UNIX y portada para Linux. Uno de los objetivos de NetFilter es proveer una infraestructura de filtrado de paquetes dedicada que los usuarios y desarrolladores pudieran instalar como agregado en el kernel de Linux.

Filtrado de paquetes con NAT: Es posible efectuar el filtrado de paquetes junto con la Traducción de Direcciones de Red sin causar dificultades a ninguna de las dos funciones. La función de filtrado de paquetes se diseña ignorando por completo cualquier traducción de direcciones que se lleve a cabo ya que ésta última se realiza entre la entrada / salida de datos en el borde de la red y el filtrado de paquetes. Las direcciones captadas por el filtro serán las direcciones origen y destino reales.

Control de Acceso de Conexiones: Este mecanismo controla y retransmite conexiones TCP manteniendo registro del estado de todos los paquetes que agrupan tal conexión, de forma que solo aquellos hosts externos confiables puedan establecer conexiones con aquellos dispositivos habilitados a ofrecer un servicio a tales usuarios. De la misma forma es posible restringir las conexiones originadas en la red interna con destino a ciertos sitios de la red externa. Esta función es realizada por un proceso proxy instalado en un gateway que interconecta la red interna con la red pública. Estos dispositivos son llamados gateways a nivel de circuitos.

Una alternativa a mantener el contexto de cada paquete es utilizar tablas dinámicas basadas en las banderas SYN/ACK del encabezado de los paquetes TCP. En esta forma, la tabla de reglas se genera a medida que un host interno solicita una conexión con un sitio externo por lo que el gateway asume la política de reenviar solo aquellos paquetes entrantes que pertenezcan a conexiones iniciadas desde el interior y rechazar aquellas iniciadas en el exterior (similar a la estrategia lograda con NAT dinámico). Mediante el uso del proxy, los sistemas internos no podrán establecer conexiones directas con el exterior sino por intermedio del proxy; quien solicite una conexión, se conectará a un puerto TCP del gateway, luego el proxy determinará si la conexión es permitida o no, basado en un conjunto de reglas de acceso que utilizan información del encabezado del paquete TCP, luego (si la conexión fue aceptada) el gateway crea una conexión al dispositivo interno final. En este caso, el gateway retransmitirá todos los paquetes involucrados en la conexión.

Estos gateways pueden implementar algunos mecanismos de control de acceso tales como autenticación e intercambio de mensajes de protocolo entre cliente y proxy para establecer ciertos parámetros del circuito. El control de acceso de conexiones no es del todo transparente ya que los usuarios deben ser configurados para dirigir todas sus solicitudes al dispositivo que implemente esta función.

La ventaja del mecanismo de filtrado a nivel de circuitos es que provee servicios para un amplio rango de protocolos aunque requiere software especial en el cliente, lo que lleva al problema de que la seguridad basada en hosts no es escalable (con una arquitectura de seguridad perimetral). A medida que crece la red, la administración de la seguridad de los clientes se hace más compleja por lo que demora más tiempo llevarla a cabo y propensa al error; esto si no se efectúa un control central e implementado de forma distribuida.

Filtrado de Datos de Aplicación: Este mecanismo interpreta los datos encapsulados en los paquetes correspondientes a protocolos de aplicación particulares para determinar si deben o no deben ser procesados por la aplicación correspondiente, ya que pueden contener datos que afecten el buen funcionamiento de las mismas. La función de seguridad ofrecida por este mecanismo es mucho más segura que las anteriores. Son implementados por servicios proxies instalados en gateways, llamados gateways a nivel de aplicación. Proveen una barrera de seguridad entre los usuarios internos y la red pública. Los usuarios de la red interna se conectan al filtro de datos de aplicación, quien funciona como intermediario entre diferentes servicios de la red externa y el usuario interno.

Son implementaciones de propósito especial que intentan ofrecer servicios de seguridad a las aplicaciones que procesen tales datos. Son específicos de la aplicación, es decir que se necesita un proceso proxy para cada aplicación. Esto presenta una desventaja de implementación. Aunque solo algunos programas o protocolos de aplicación necesitan ser analizados (por Ej. FTP y protocolos de correo electrónico, ICMP) ya que otros no presentan peligros de seguridad. El correo electrónico puede ser dirigido a través de estos dispositivos, sin importar que tecnología se utilice en el resto del Firewall. También hay que tener en cuenta que el tipo de filtrado usado depende de las necesidades locales. Un sitio con muchos usuarios de PC debería analizar los archivos que reciba por posibles virus. Además presentan otra ventaja, que en algunos ambientes es bastante crítica: el registro de todo el tráfico de entrada y salida es simple implementar.

Planes de seguridad: Para mantener una visión clara e integral de las políticas de seguridad a definir, es útil establecer un plan de seguridad que ofrezca un marco de guías generales para tales políticas. De esta forma, las políticas individuales serán consistentes con toda la arquitectura de seguridad

Un plan de seguridad debe definir:

- La lista de servicios que serán ofrecidos por la red de la organización
- Qué áreas de la organización proveerán tales servicios
- Quién tendrá acceso a esos servicios
- Cómo será provisto el acceso
- Quién administrará esos servicios
- Cómo serán manejados los incidentes
- ...entre otros.

Al igual que un plan de seguridad ofrece un marco de diseño para una política de seguridad, éstas se definen a diferentes niveles de especificación o abstracción lo que ofrece una visión más clara y coherente del esquema de seguridad completo resultante. Cada iteración o nivel, especifica requerimientos de seguridad más detallados enfocados en diferentes aspectos. Las diferentes políticas se refieren a: seguridad del sitio, acceso a servicios de red, diseño del Firewall, políticas específicas del sistema.

Política de seguridad del sitio: La política de seguridad del sitio es una política global destinada a la protección de los recursos de información de la organización. Incluye desde escáners hasta el acceso remoto a unidades de discos. Es una política de alto nivel que especifica lineamientos y requerimientos generales como por ejemplo:

- La información es vital para la economía de la organización
- Se realizará todo esfuerzo rentable para asegurar la confidencialidad, integridad, autenticidad,

disponibilidad y utilidad de la información,

- La protección de la confidencialidad, integridad, y disponibilidad de recursos de información es prioridad de todos los empleados en todos los niveles de la compañía

A partir de esta política de seguridad surgen políticas específicas del sitio que cubren el acceso físico a la propiedad, acceso general a sistemas de información y acceso específico a los servicios de esos sistemas. La política de acceso a servicios de red es formulada en este nivel.

Política de Acceso a Servicios de Red: La Política de Acceso a Servicios de Red es una política de alto nivel, específica de alguna característica; define aquellos servicios que serán permitidos o explícitamente denegados de la red privada, la forma en la que estos servicios serán usados y las condiciones de las excepciones a esta política. Se enfoca en la restricción y uso de los servicios de la red interna, también incluye todos los otros accesos externos a la red tales como accesos telefónicos y conexiones SLIP y PPP. Esto es importante ya que algunas restricciones en el acceso a los servicios de la red puede llevar a los usuarios a tratar de utilizar otros que pueden crear puntos débiles de acceso a ataques. Esta política debe ser diseñada antes de que el firewall sea implementado. La política debe ser realista y sólida. Una política realista provee un balance entre proteger a la red de riesgos conocidos y proveer al usuario acceso razonable a los recursos de la red. Una política sólida restringe los servicios previendo todos los posibles puntos de acceso a tal servicio. Una medida común asumida por una política de acceso a servicios de red es restringir el acceso a un sitio desde Internet, pero permitir el acceso desde el sitio a Internet, o permitir acceso desde Internet sólo a algunos sistemas seleccionados. Éste último tipo de acceso debe ser permitido sólo si es necesario y debe ser combinado con características de autenticación avanzada.

Política de Diseño de Firewall: Es una política de bajo nivel que describe cómo el Firewall controlará el acceso a los servicios restringidos como se definió en la política de acceso a servicios de red. La política de diseño es específica de cada Firewall. Define las reglas utilizadas para implementar la política de acceso a servicios de red. Debe ser diseñada en relación a, y con completo conocimiento de características tales como las limitaciones y capacidades del Firewall, y las amenazas y vulnerabilidades asociadas con las tecnologías utilizadas (como TCP/IP). Los Firewalls generalmente implementan una de dos políticas de diseño básicas:

- Permitir todo servicio, a menos que sea expresamente restricto, o
- Denegar todo servicio, a menos que sea expresamente permitido.

La primer política es menos deseable, ya que ofrece más vías por las cuales puede accederse a un servicio, evitando el Firewall, mientras que la segunda es más fuerte y segura, aunque es más restrictiva para los usuarios. Ésta última es la clásicamente usada en todas las áreas de seguridad de la información.

Por lo tanto, dependiendo de los requerimientos de seguridad y flexibilidad, ciertos tipos de Firewalls son más apropiados que otros, haciendo muy importante que la política sea considerada antes de implementar un Firewall. De otra forma, el Firewall podría no cubrir las funcionalidades esperadas.

Políticas específicas del sistema: Es implementada por el sistema mediante el uso de funciones de control de acceso. Generalmente establece el permiso de acceso a ciertos recursos para ciertos individuos de la organización.

Para ser efectiva, una política requiere visibilidad, lo que favorece a la implementación de la misma ayudando a asegurar que sea comunicada a través de la toda la organización. Además, debe ser integrada y consistente con otras directivas existentes, leyes, guías, procedimientos, y la misión global de la empresa.

APENDICE E: Sistema de Gestión de la Seguridad de la Información (SGSI)

Los SGSI son un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001. El término se denomina en Inglés "*Information Security Management System*" (ISMS).

El concepto clave de un SGSI es para una organización del diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno.

La ISO/IEC 27001 por lo tanto incorpora el típico "Plan-Do-Check-Act" (PDCA) que significa "Planificar-Hacer-Controlar-Actuar" siendo este un enfoque de mejora continua:

- Plan (planificar): es una fase de diseño del SGSI, realizando la evaluación de riesgos de seguridad de la información y la selección de controles adecuados.
- Do (hacer): es una fase que envuelve la implantación y operación de los controles.
- Check (controlar): es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.
- Act (actuar): en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.

La mejor definición de SGSI es descrito por la ISO/IEC 27001 y ISO/IEC 27002 y relaciona los estándares publicados por la International Organization for Standardization (ISO) y la International Electrotechnical Commission (IEC).

El punto de partida es el planeamiento (Plan) del sistema de gestión. A continuación, ha de ejecutarse lo planeado (Do), lo que incluye tanto la implementación del sistema degestión como su ejecución. Tras la puesta en marcha del sistema, se inician las actividades de monitorización y revisión del mismo (Check). Como resultado de ambas,se identificarán e implantarán mejoras en el sistema (Act). Un SGSI debe permitirnos conocer los riesgos a los que están sometidos nuestros datos,información y servicios, y asumirlos, minimizarlos, transferirlos o controlarlos medianteuna operativa definida, documentada y conocida por toda la organización, que a su vezdebe ser revisada y mejorada de forma continua.

Seguidamente, describiremos cada una de estas cuatro fases, pero comenzaremos revisando una serie de recomendaciones que se deberían tener en cuenta antes de iniciar el establecimiento del SGSI.

Recomendaciones para implementar un SGSI

Antes de iniciar la puesta en marcha de un SGSI, es conveniente tener presente la necesidad, cuando no la obligación legal, de realizar ciertos planteamientos, disponer de ciertas herramientas y llevar a cabo determinadas actividades que son esenciales para garantizar la eficacia posterior del SGSI.

- En primer lugar haremos referencia al compromiso de la Dirección. Como en cualquier otra iniciativa de este calado, el respaldo por parte de la Dirección es una condición necesaria para el éxito real de la misma. De hecho, este requerimiento se recoge en el estándar mismo y no se conforma con la mera declaración: se exige demostrar su implicación en el proceso. Es especialmente importante, a este respecto, la responsabilidad que tiene la Dirección de revisar en profundidad el SGSI (al menos una vez al año), como veremos más adelante.
- Especial importancia tiene disponer de un sistema de gestión documental . La documentación es una actividad clave en cualquier SGSI. Los requisitos del sistema de gestión documental no deben ser demasiado elevados, pero como mínimo éste ha de permitir definir y gestionar los flujos de aprobación de los documentos y controlar el acceso y el tratamiento de los documentos definidos para cada rol contemplado en el modelo organizativo del SGSI.
- También es imprescindible tener un inventario de activos actualizado y operativo. Se entiende por activo cualquier elemento que tenga valor para la organización (instalaciones, equipos, aplicaciones, servicios, etc.). Por ello, cualquier proyecto encaminado a disponer un sistema de inventario versátil y fácil de mantener e integrar con otros sistemas es una magnífica palanca para el éxito del SGSI.
- Otra herramienta esencial para el establecimiento de un SGSI es un sistema de gestión de incidencias de seguridad. Es la herramienta habitual del servicio de atención a los usuarios (CAU), y debería bastar con adaptarlo a los flujos de gestión de incidencias de seguridad que definamos en nuestro SGSI. También aquí, la orientación hacia estándares de buenas prácticas en gestión de servicios, como por ejemplo ITIL, constituye una sinergia a tener en cuenta.
- Cualquier SGSI debe incluir la adecuada gestión de la normativa legal que en cuestión de sistemas de información está obligada a cumplir la organización. En consecuencia, es recomendable tener en marcha el cumplimento de la normativa aplicable antes de poner en marcha el SGSI.
- En un nivel más táctico, es deseable disponer de una política de seguridad para la organización, si no explícitamente definida, al menos tácita. Asimismo, será de gran ayuda la experiencia previa en análisis de riesgos.
- Finalmente, en un ámbito más técnico, constituye un buen punto de partida toda experiencia relativa a la realización de auditorías técnicas de seguridad sobre sistemas, redes y aplicaciones (hacking ético), así como en la ejecución de proyectos de implantación de medidas de seguridad.

Planificar y diseñar el SGSI según la Norma ISO-IEC 27001 implica:

- *Establecer alcance del SGSI*. Es el primer paso. Hay que decidir qué parte de la organización va a ser protegida. Evidentemente puede ser la organización completa, pero es perfectamente válido y muy recomendable comenzar por un área de la organización que sea relevante o importante, por ejemplo, en el caso de un banco, comenzar por el servicio de banca electrónica.
- *Establecer las responsabilidades*. Se asignará un responsable de seguridad, que coordine las tareas y esfuerzos en materia de seguridad. Será el que actúe como foco de todos los aspectos de seguridad de la organización y cuyas responsabilidades cubran todas las funciones de seguridad. En muchas organizaciones será necesario designar un comité de seguridad que trate y busque soluciones a los temas de seguridad, resuelva los asuntos interdisciplinarios y que apruebe directrices y normas.
- *Definir política de seguridad*. Este paso es fundamental. La política de la organización es la que va a sentar las bases de lo que se va a hacer, mostrará el compromiso de la dirección con

el SGSI y servirá para coordinar responsabilidades y tareas.

- *Realizar análisis de riesgos*. El análisis de riesgos es la piedra angular de un SGSI. Es la actividad cuyo resultado nos va a dar información de dónde residen los problemas actuales o potenciales que tenemos que solucionar para alcanzar el nivel de seguridad deseado. El análisis de riesgos debe ser proporcionado a la naturaleza y valoración de los activos y de los riesgos a los que los activos están expuestos. La valoración del riesgo debe identificar las amenazas que pueden comprometer los activos, su vulnerabilidad e impacto en la organización, determinando el nivel del riesgo.
- *Seleccionar los controles*. Una vez que se sabe dónde están los puntos débiles en la gestión de la seguridad, se escogen los controles necesarios para eliminarlos o al menos, reducir la probabilidad de que ocurran algún incidente o el impacto que tendría en caso de que algo ocurriera. En principio los controles se escogerán de los detallados en el Anexo A de la Norma.
- *Establecer el plan de seguridad*. Debido a que serán numerosas las actuaciones que se pretenderá realizar, debe establecerse un plan con los plazos, los recursos y las prioridades a la hora de ejecutarlas.

Fase de Planeamiento (*plan*)

El primer paso de la fase de planeamiento para establecer un SGSI es definir el ámbito de aplicación del proyecto, su alcance. No tiene por qué ser todo o nada. De hecho, es recomendable empezar con pasos cortos. Hay que tener en cuenta que la definición del ámbito del SGSI es clave, ya que determina la complejidad inicial del proyecto. Si, por ejemplo, el ámbito no incluye usuarios finales, no será necesario analizar los riesgos existentes en activos tales como sus puestos de trabajo o las redes de acceso que utilizan. También es evidente que la definición del alcance afecta a la estimación de las necesidades de recursos que conllevará el proyecto de implantación del SGSI.

Se definirá explícitamente, si no existía ya, la política de seguridad que orientará a la organización en cuestión de fijación de objetivos y principios de actuación en todo lo relativo a seguridad de la información, en el tratamiento de los requerimientos legales o contractuales relativos a la seguridad de la información, y en el establecimiento de los criterios con los que se va a evaluar y tratar el riesgo. Es un documento clave y por ello debe ser aprobado por la dirección.

CICLO PDCA (*"Plan, Do, Check, Act"*)

Es indispensable definir el modelo organizativo que soportará el funcionamiento del SGSI. Incluirá la definición del conjunto de roles, así como las funciones y responsabilidades correspondientes a cada rol. Un buen modelo buscará el compromiso entre responsabilidad y operatividad, de forma que las decisiones se tomen siempre al nivel más adecuado: la organización debe ser capaz de dar respuesta ante los incidentes de seguridad habituales en el día a día y reaccionar con eficacia ante incidentes de seguridad graves.

Ejemplo de Modelo Organizativo del SGSI

La figura más relevante del modelo organizativo será el Comité de Seguridad, máximo órgano decisor del SGSI, integrado por directivos de todas las áreas implicadas directamente en la seguridad. Son claros candidatos Tecnologías de la Información, Oficial Mayor, Asesoría Legal y Recursos Humanos. También son parte esencial del Comité de Seguridad el Responsable de Seguridad, encargado de la planificación, coordinación y ejecución de las actividades de seguridad de la información en toda la organización, y el Auditor Interno. Por supuesto, el modelo organizativo incluirá a los responsables de las diferentes áreas técnicas (Sistemas, Infraestructuras y Desarrollo), como responsables de la ejecución de las actividades de seguridad de la información en sus áreas respectivas.

La actividad más definitoria de esta fase es el análisis de riesgos . A fin de conocer con el mayor rigor posible los riesgos a los que están expuestos los activos que deseamos proteger, es necesario llevar a cabo un proceso sistemático de estimación de los riesgos a los que está expuesta nuestra organización. El análisis de riesgos un proceso en el que generalmente conviene contar con técnicos expertos.

El análisis de riesgos tendrá como resultado el tratamiento que la organización dará a cada uno de los diferentes riesgos, teniendo como referencia la política de seguridad y la normativa aplicable. Es lo que el estándar denomina selección de controles , y lleva asociada la identificación de indicadores de eficacia de las medidas de tratamiento de los riesgos. No se debe minimizar la importancia de esta última tarea, ya que está en la base del ciclo PDCA. Los indicadores aportarán información sobre la eficacia de nuestro SGSI y deben, de esta forma, ayudarnos a reorientarlo al final de cada ciclo.

En relación con la selección de controles, la norma ISO/IEC 27002 constituye un buen punto de partida a la hora de definir qué controles deseamos implantar. De hecho, la norma ISO/IEC 27001 obliga a redactar un documento de aplicabilidad, en el cual se deben justificar la no aplicabilidad de aquellos controles que se decida no tener en consideración y la aplicabilidad de aquellos que es necesario tratar.

Este es también el momento de determinar si se desea obtener la certificación de nuestro SGSI. El proceso de certificación es un proceso relativamente dilatado, de ciclos de tres años. Por supuesto, tiene pros y contras. Entre los primeros, podemos mencionar que la obligación de someterse a auditorías anuales supone un acicate para mejorar la gestión del SGSI o también que permite obtener

una acreditación nacional (con alcance internacional), contribuyendo positivamente a la imagen de la organización. En sentido opuesto, debe tenerse presente que requiere una dedicación adicional a las exigencias derivadas del propio SGSI y que supone un coste económico.

Por último, mencionaremos de nuevo la importancia del compromiso de la dirección en toda esta fase, ya que el tratamiento que se dará a los diferentes riesgos (que se plasmará en un plan de acción) supone o bien aportar los recursos necesarios para implantar las salvaguardas contempladas en dicho plan de acción o para transferir el riesgo a un tercero o bien asumir (aceptar explícitamente) la responsabilidad de los daños que podrían causar los riesgos residuales , aquellos para los que no se va a implantar salvaguarda alguna ni se van a transferir a terceros.

Fase de Ejecución (*do*)

La ejecución del SGSI tiene dos vertientes claras: lo que podríamos llamar el día a día y la puesta en marcha de mejoras.

El día a día lo ocupan las tareas de gestión de las operaciones del SGSI y de los recursos asignados al SGSI para el mantenimiento de la seguridad de la información. Corresponden al funcionamiento controlado de la maquinaria. Incluye la ejecución de los procedimientos y medidas previstos para la detección y respuesta de los incidentes de seguridad.

CICLO PDCA (*"Plan, Do, Check, Act"*)

Entre los requerimientos menos aplaudidos a la hora de mantener vivo un SGSI se encuentra la obligación de mantener debidamente documentados los múltiples procedimientos operativos de gestión de la seguridad. Por ejemplo: cómo se gestionan los incidentes de seguridad, cómo se autorizan y revocan los privilegios de acceso, cómo se llevan a cabo las actualizaciones de software o cómo se bascula al centro de respaldo. Dado el esfuerzo requerido, es muy recomendable planificarlo también a corto, medio y largo plazo.

También forman parte del día a día el desarrollo de programas de formación y concienciación continua en relación con la seguridad de la información y dirigidos a todo el personal.

La otra cara de esta fase es la de la puesta en marcha de mejoras. Una vez que, tras el análisis de riesgos, se han identificado los principales riesgos a los que se hallan expuestos nuestros activos y seleccionado los controles a aplicar, ha de elaborarse un plan de acción. Este plan incluirá todos los proyectos que se consideran adecuados para implantar las salvaguardas seleccionadas. Es aconsejable distribuir los proyectos en el tiempo, agrupándolos en corto, medio y largo plazo, según

criterios tales como su complejidad, urgencia y disponibilidad de recursos.

El plan de acción (o de tratamiento de riesgos) debe priorizar las acciones, incluir las necesidades de recursos y sus responsabilidades. Y, obviamente, debe contemplar la implementación de las métricas que permitan medir la eficacia de los controles seleccionados.

Fase de Monitorización (*check*)

La necesidad de monitorizar el funcionamiento del SGSI está en su base. Algunas de las actividades de monitorización se realizan de forma continua y otras son puntuales. Deben ser continuas, por ejemplo, la detección de incidentes de seguridad, la supervisión de los recursos empleados en la gestión de la seguridad de la información o el registro de cualesquiera eventos que hayan supuesto o puedan suponer algún impacto sobre la efectividad del SGSI.

CICLO PDCA (*"Plan, Do, Check, Act"*)

Pero muchas otras actividades de vigilancia se realizan de forma puntual y es por ello muy recomendable planificarlas. Destacaremos las siguientes:

- Medir con la periodicidad definida la efectividad de los controles para verificar que se cumple con los requisitos de seguridad. Es recomendable utilizar una herramienta de seguimiento flexible en la generación de informes y orientada a integrarse con un cuadro de mando. Por supuesto, es importante automatizar las medidas cuando sea posible y eficiente hacerlo.
- Realizar auditorías internas a nuestro SGSI (la norma recoge la figura del Auditor Interno, como se mencionó al describir el modelo organizativo).
- Realizar las auditorías exigidas por la legislación aplicable. El caso más evidente es el de las auditorías exigidas por la Ley Orgánica de Protección de Datos de Carácter Personal.
- Si se ha optado por certificar nuestro SGSI, es obligatorio realizar también la auditoría externa y las revisiones que exige la empresa certificadora.
- Revisar los resultados de las anteriores auditorías de seguridad, incidentes de seguridad, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas por parte de la dirección para garantizar que el alcance definido al comienzo sigue siendo el óptimo, constatar la eficacia creciente del SGSI y validar las medidas correctoras.

Fase de Mejoras (*act*)

Corresponde a esta fase la puesta en marcha de las mejoras identificadas a partir de las actividades de verificación mencionadas anteriormente.

Estas mejoras pueden ser tanto acciones preventivas como correctivas, pero orientadas siempre hacia la solución definitiva del problema. En este sentido, juega un papel importante el análisis de la causa raíz, aquella que constituye la razón de fondo del incidente que queremos resolver.

CICLO PDCA *("Plan, Do, Check, Act")*

Las mejoras introducidas son asimismo medidas de seguridad y debe, por tanto, verificarse que alcanzan los objetivos previstos. De la misma forma, deben ser adecuadamente documentadas y comunicadas a las partes interesadas.

De especial relevancia para el éxito del ciclo de mejora es la óptima ejecución de la revisión por la Dirección (recogida en el apartado 7 de la ISO/IEC 27001). Consiste en una revisión periódica en la que se presentan a la Dirección una foto suficientemente completa del SGSI y propuestas de mejora, de forma que la Dirección tome las decisiones que considere oportunas sobre análisis de riesgos, cambios en procedimientos y controles de seguridad, recursos necesarios o indicadores de eficacia. El conjunto de decisiones adoptadas es la entrada fundamental para la fase de planeamiento que abrirá el ciclo PDCA siguiente.

BIBLIOGRAFÍA

- Envenenamiento ARP. Instituto Nacional de Tecnologías de Comunicación. www.Inteco.es
- Guía de preparación para el examen de certificación CCNA. Oscar Gerometta
- Esteganografía El arte de ocultar información. Instituto Nacional de Tecnologías de Comunicación. www.Inteco.es
- Administración de Redes GNU/Linux. Antonio Perpínan, Fundación Código Libre Dominicano.
- Seguridad de Sistemas GNU/Linux. Antonio Perpínan. Fundación Código Libre Dominicano.
- Honeypots: Instituto Nacional de Tecnologías de Comunicación. www.Inteco.es
- Implantación de un SGSI y Certificación ISO 27001 en la Administración Pública 2010. Manuel Cabrera Silva, José María Vinagre, Paul Jabbour, Fernando Román
- Programa de estudio de Cisco CCNA 4
- Curso de Gestión de la Seguridad de la Información. Instituto Nacional de Tecnologías de la Comunicación (INTECO) http://www.inteco.es
- Programa de estudio Enterprise Security and Risk v1.0 y v2.0
- Aspectos Avanzados de Seguridad en Redes. Joaquín García Alfaro, Xavier Perramón Tornil
- Programa de estudio de Redes Inalámbricas de Cisco Systems
- Programa de estudio de Cisco CCNA 3.1
- Fundamentos y aplicaciones de Seguridad en Redes WLAN. Marcombo, 2006
- Técnicas de Defensa: Mecanismos comunes bajo variantes del sistema operativo Unix. Juan Pablo Sarubbi Universidad Nacional de Luján
- Análisis Forense de Sistemas GNU/Linux, Unix. David Dittrich
- Manual de Metodología abierta de testeo de seguridad (OSSTMM). ISECOM
- Manual de Metodología de Programación Segura (SPSMM). ISECOM
- ISO 17799
- Redes Linux con TCP/IP. Pat Eyler
- Programa de capacitación de Telefónica de España, Introducción a la Telemática y a las Redes de Datos.
- Seguridad en Redes cableadas e inalámbricas. Universidad Tecnológica Nacional Facultad Regional Santa Fe
- Redes inalámbricas: IEEE 802.11. Enrique de Miguel Ponce, Enrique Molina Tortosa, Vicente Mompó Maicas
- Análisis de Redes y Sistemas de Comunicaciones. Xavier Hesselbach Serra, Jordi Altés.
- Programa de estudio en Seguridad Informática de Microsoft Virtual Academy
- Tópicos y preguntas de las certificaciones: CompTia Network+ N10-003, CompTia Security+ SY0 201, Wireless Security Professional PW0-200, Ethical Hacker EC0-350, Certified Network Security Administrator ML0-220
- Otros recursos en Internet incluyendo Wikipedia.org