Ingeniería Inversa del Software – Parte I – Herramientas básicas

Por fin ha llegado el tan ansiado primer número de DIFISEC, la revista sobre seguridad informática que escribimos los alumnos de la Facultad de Informática de SS y con él ha llegado también el primer número de esta sección que pretende llamar la atención de los informáticos sobre la importancia de la seguridad vista desde el lado de la inseguridad.

Los primeros artículos que escribiré tratarán sobre la Ingeniería Inversa del Software (IIS) que no es otra que la temida y desconocida disciplina tabú que trata sobre la alteración del comportamiento de los programas compilados modificando su código fuente o variables manejadas.

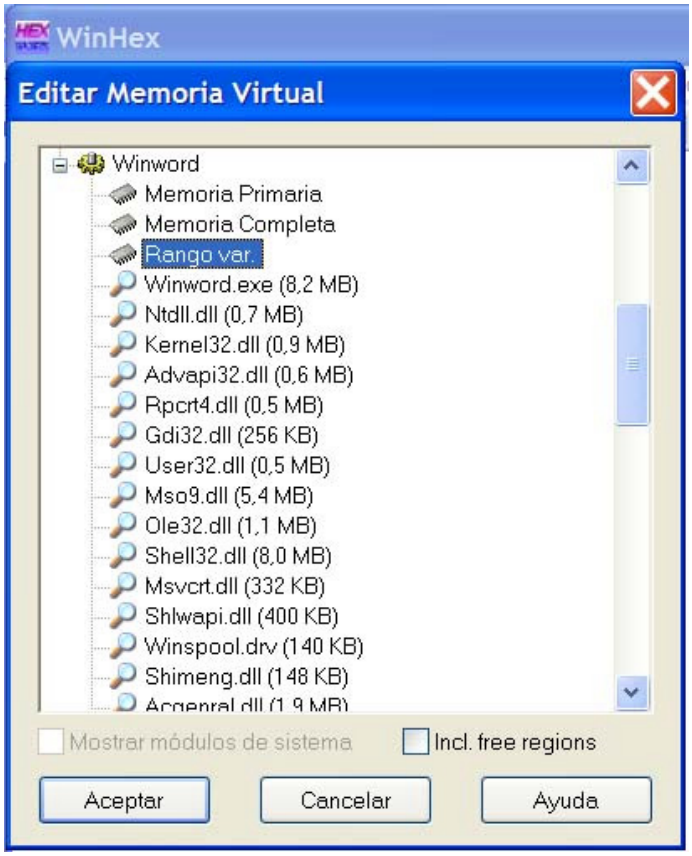
Seguro que más de uno de mis lectores se ha preocupado más de una vez por la seguridad de su código frente a los crackers; y, posiblemente también, la mayoría de ellos ha llegado a la conclusión de que no merece la pena preocuparse porque no pueden concebir ninguna idea capaz de luchar contra la IIS. Es normal que todos nos sintamos inútiles y maniatados frente a temas que nos son desconocidos. Para dar una luz sobre esta oscura disciplina, pretendo explicar en una serie de artículos las ideas en que está basada. Todas ellas son muy sencillas, tal y como veremos en los próximos meses. En cuanto esté publicada esta primera serie de escritos, todos nosotros seremos capaces de modificar el comportamiento de cualquier programa y de esta manera podremos crear código más seguro frente a otra gente con conocimientos similares a los nuestros.

Para empezar a realizar cualquier trabajo, siempre es necesario saber que herramientas se necesitan y qué se puede hacer con ellas. Nuestro caso no es una excepción, por supuesto, y por ello esta primera concatenación de palabras intentará tratar este asunto con la profundidad que se merece.

Una utilidad bastante usada por los crackers más expertos es el editor de memoria. Este tipo de programas permiten localizar y modificar el valor de variables que se encuentran en la memoria RAM del sistema. Como todos sabemos, en estas variables se almacenan todos los datos que maneja un programa, incluso la información sobre si un programa está registrado o cuantos días de prueba quedan.

Aquí no se va a entrar en detalles sobre qué hacer o cómo emplear las herramientas descritas, ya que extendería demasiado el artículo restándole claridad. Eso se tratará más adelante en sucesivos números de esta sección.

El editor de memoria que yo suelo emplear es el WinHex, el cual se puede configurar para que funcione en castellano. En la siguiente figura se puede observar como permite seleccionar que parte de la memoria se va a analizar.



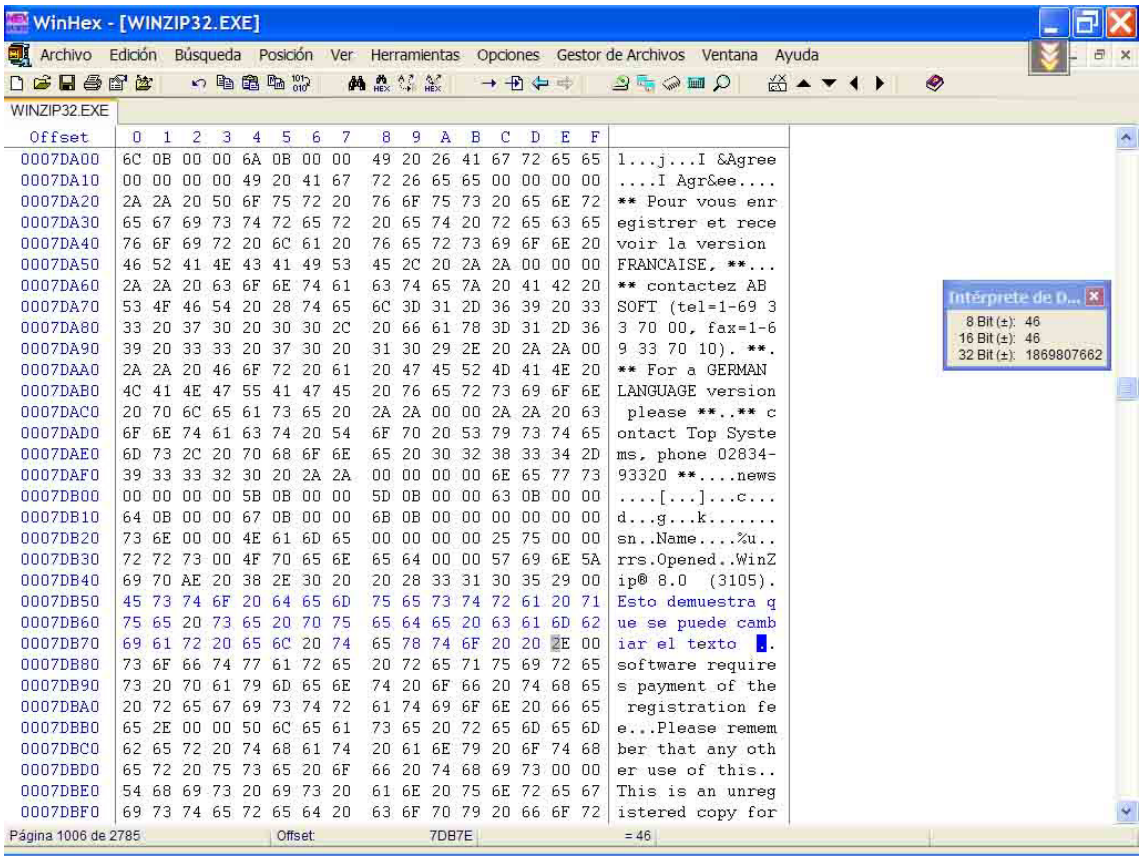
Otra de las utilidades básicas en la IIS es el editor hexadecimal, ese gran desconocido del que todos hemos salido corriendo en cuanto lo hemos visto. Por supuesto, usar un editor hexadecimal sin saber que tienes que cambiar puede ser tan desesperante como tener que hacer cola para no esperar. En fin, como ya veremos, nosotros siempre que lo usemos sabremos de antemano que valores modificar y con qué nuevas secuencias de códigos hexadecimales sustituirlos.

El empleo más típico de este tipo de software es “retocar” de manera perdurable las instrucciones en lenguaje máquina que emplean los programas que ya han sido compilados. Sin ello, sería necesario crackear los códigos de cada programa cada vez

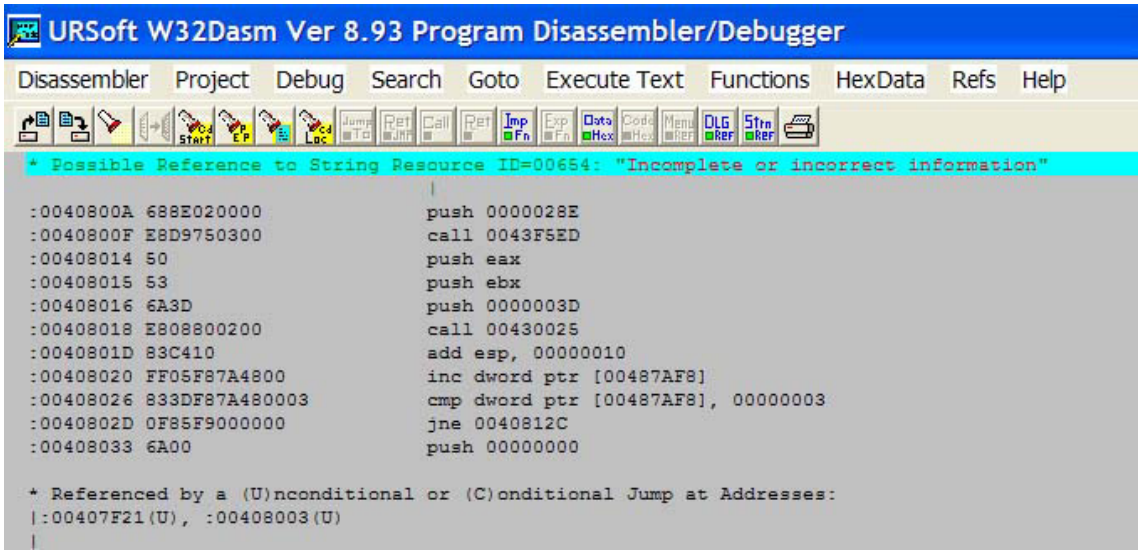
que se quisieran volver a emplear, pues, como ya sabemos, los datos y códigos almacenados en memoria son volátiles y se pierden al cerrar el proceso que los emplea.

El editor hexadecimal que yo suelo emplear es también el WinHex ya que tiene la posibilidad de modificar tanto la memoria como los archivos físicos. ¡Que le voy a hacer si siempre he sido partidario de usar la menor cantidad posible de programas diferentes para realizar la mayor cantidad posible de tareas!

En la siguiente imagen se puede observar el aspecto que presenta cualquier editor hexadecimal:



Para acabar con las herramientas software más importantes y básicas de la IIS mencionaré también el depurador o debugger, otro de los grandes incomprendidos por los no-iniciados. Próximamente dedicaré todo un articulo a este arma tan temido tanto por los desarrolladores como por los crackeadores. Por lo tanto no entraré ahora a detallar sus tipos ni funcionamiento, solo mencionaré que sirve para sacar el código ensamblador de cualquier programa y modificar su comportamiento de manera temporal, al menos en principio. Mi preferido es el W32Dasm porque es el más potente de usar, aunque los hay más sencillos de usar. A continuación se muestra su aspecto:



Esta utilidad software es la más imprescindible y compleja de todas las empleadas en la IIS, por lo que siempre se intentará evitar su uso. Esto es posible gracias a la herramienta más importante de todas las que ha podido desarrollar el hombre a lo largo de toda la historia de la humanidad y, aunque parezca mentira, no me refiero ni a la boina ni a las discotecas, sino a la lógica, el raciocinio o el entendimiento. Esta ha sido la herramienta que ha permitido al ser humano llegar a desarrollarse más que cualquier otro ser viviente del planeta Tierra y, además, ha sido la principal impulsora de todas las revoluciones tecnológicas de la historia. Resulta realmente lamentable que la sociedad actual ya no sea capaz de valorarla como se merece. Aunque parece que todo está ya inventado y es perfecto, esto no es así. En realidad nuestra tecnología no es más que un cúmulo de parches y apaños mal hechos. ¿Cómo se puede explicar que un sistema operativo falle cada dos por tres?¿Cómo es posible que tantas naves espaciales exploten a escasos segundos del despegue?¿A quién le parece lógico que un dispositivo de corte eléctrico como es un diodo, imprescindible para controlar que la corriente eléctrica circule en un solo sentido, cuando se encuentra con una diferencia de potencial inversa de valor mayor al que puede soportar, en ver de estropearse abriendo su circuito, lo haga cortocircuitándose para dejar circular toda esa corriente, que antes retenía, a su libre albedrío? La base tecnológica que tenemos es realmente desastrosa y está en nuestras manos cambiarla, pero para eso necesitamos usar el raciocinio en vez de someter nuestras mentes a la inteligencia o la sabiduría, que solo son importantes para tener una referencia de los fallos existentes y poder evitarlos. Gran parte de los conocimientos existentes en la tecnología actual son vagos, opacos y muchas veces están basados en meras paralogías que somos incapaces de identificar porque nos las

enseñan como axiomas irrefutables, a la vez que indemostrables. Lo único exacto que incluyen son sus bases matemáticas. Posiblemente algún día se superará de nuevo esta época de mentes planas y conoceremos una tecnología más eficaz, a la vez que eficiente. Los ciclos de la historia están de mi lado y estoy seguro de la mayoría de nosotros lo veremos. Es nuestra labor contribuir a ello acostumbrándonos a usar la cabeza para algo más que almacenar conocimientos, en el mejor de los casos.

En el próximo número hablaré de cómo nos puede ayudar la lógica en el tema que estamos tratando. Id abriendo vuestras mentes hasta entonces.

Un saludo a todos y que tengáis un bonito día,

Joxean Nieto