aRC-FL-Cracking 001 (01/08/2003)

Iniciación

(por Furious Logic [aRC])

Advertencia

Antes de poner en práctica el presente documento y cualquier material asociado al mismo, sea éste naturaleza tangible o intangible usted debe estar totalmente de acuerdo con todos los términos y condiciones siguientes:

Del software

Cualquier software se proporciona tal como está, sin ninguna garantía expresa ni implícita de ningún tipo.

aRC no garantiza ni asume responsabilidad alguna en cuanto a la integridad o exactitud de cualquier información contenida en el software.

Ni los miembros ni los colaboradores ni los invitados aRC se hacen responsables por el uso que se le pueda dar al software.

Al examinar, copiar, ejecutar, instalar o utilizar el software, el lector está aceptando su total conformidad con todos los términos y condiciones enunciados.

Del documento

Al abrir este documento, el lector acepta incondicionalmente su total y exclusiva responsabilidad legal, de acuerdo a las leyes vigentes en su país, por el uso de las técnicas experimentales, educativas y/o de investigación aquí vertidas en materia de programación especializada de computadoras.

En caso de discrepar con alguno de los puntos descritos, deberá eliminar inmediatamente el presente documento y todo material asociado al mismo.

Agradecimientos

A aquellos "amigos" que nos alquilaron nuestra primera computadora allá por los 90's y que se burlaron de nuestra ignorancia, porque no sabíamos ni siquiera encender ese extraño "artefacto". Ellos nos dieron esta motivación que, lejos de toda falsa modestia, nos inspiró a prometer: "Algún día demostraremos que podemos aprenderlo todo y ser los mejores en ello".

A FontLab 3.00F de FontLab Developers Group por permitirnos asignar permiso completo a las fuentes true type protegidas contra copia y a Acrobat Distiller 5.0 de Adobe Systems por su excelente resultado en la creación del documento electrónico en formato PDF.

A todas las semillas sembradas que empiezan a germinar y desarrollarse en la *Scene* con entusiasmo y fuerza. ¡Felicitaciones a todos ustedes compañeros de estudios! No se rindan ante la adversidad porque el conocimiento nos da libertad contra la que nuestros detractores atentan a diario. No existe peor tortura para un investigador, que aprenderlo todo tan solo para su beneficio personal y sin poder disfrutar del enorme privilegio e incomparable placer de compartir lo aprendido con alguien más. Ustedes, lectores recién iniciados, están por recorrer un maravilloso camino que nunca dejará de brindarnos grandes alegrías ni dejará de sorprendernos con nuevos conocimientos mientras transitemos por él.

A los amigos y colegas que, durante los tiempos más difíciles, nos apoyaron desinteresadamente fortaleciendo nuestra decisión por sobreponernos. Gracias a quienes jamás aceptaron la censura que intentaron imponernos.

Objetivos

Mostrar al recién iniciado, que existe un largo camino por recorrer y que puede ser recorrido únicamente si está dispuesto a aprender con ahínco.

Despejar la mente informática de frases como: "Yo se más que los demás", a fin de que esté preparada para recibir caudales de información que de otra manera no podría asimilar.

Enseñar al novato, a leer, leer, leer, leer, leer, leer... por sí mismo.

Terapia de la aversión

¿Filosofía? Así es. Si usted es de los "no se puede", mejor olvídese de este asunto. Aquí no existen los "no se puede". Libere su mente de lo que cree saber porque es muy probable que esté equivocado. El cracking no se aprende en un curso universitario ni mediante charlas de capacitación sobre tecnología ni con los cursos de arquitectura de sistemas que ciertas universidades distribuyen en 5 ciclos académicos. Usted tiene que investigarlo todo. Utilizamos la Terapia de la Aversión que consiste en enfrentarnos repetidamente a todo aquéllo que parezca infundirnos pánico o nos cree algún sentimiento de rechazo (informáticamente hablando). En buen castellano, usted tiene que aprender a programar. Contrariamente a lo que algunos crackers sostienen, nosotros le exigimos que sea un programador y no nos venga con eso de que "Yo se hacer sistemas de Facturación", que para nuestros propósitos es no saber nada. Recuerde esto: Usted no sabe nada, pero puede aprenderlo todo. Es su decisión. Lo desafiamos a pasar la prueba de fuego del cracking junto con sus demás compañeros.

¿Por qué cree que no existen muchos crackers latinos? Una revista mencionó que un peruano estudia un promedio de 400 horas al año, un chileno 1,500 horas y un chino unas 2,500 horas. Asistir a clases no necesariamente es estudiar. Depende de nosotros el cambiar esta bochornosa realidad.

Napoleón Bonaparte era capaz de leer un libro, dictar una carta y jugar una partida de ajedrez con total concentración para cada una de las tareas al mismo tiempo. El cracking requiere realizar varias tareas a la vez manteniendo la secuencia de todas ellas.

Para muestra: Una de nuestras herramientas de trabajo, llamada SoftIce 4.05 ocupa unos 11 MB, es decir unos 11,264 KB. Este es un programa de origen estadounidense. Entre tanto, uno de sus competidores muy poco utilizado, de nombre TRW2000 recién en su versión 1.23 ocupa unos 860 KB, es más versátil que el anterior e incluso tiene mejor aspecto. Es de origen chino.

No hay más que decir al respecto, sino solamente que en el mundo informático se debe probar lo que se dice; es decir, debemos aplicar el método científico. Cualquier afirmación debe ser demostrada con argumentos técnicos. Frases como: "todos sabemos que esto es así" solo muestran incongruencia y falta de criterio ante nuevos conceptos. Pruébenos sus conocimientos con el método experimental o científico. Sí, ese método de 6 pasos que se enseña en el curso de Investigación Científica. Aquel método cuyos resultados siempre deben ser los mismos, reproduciendo las mismas circunstancias para que la hipótesis pueda alcanzar el rango de tesis o teoría. No tema aprender nuevas especialidades. La nueva generación en la *Scene* ha cambiado demasiado, muchas veces perdiendo el deseo de hacer "aquella tarea" por sí mismos. Enfrente sus temores uno a uno.

Posiblemente esté pensando en hackers, crackers, phreakers y piratas informáticos. Brevemente, debemos aclararle que, los dos primeros, son personas que tienen el conocimiento, habilidad y deseo incomparable e incontenible de explorar completamente cualquier sistema informático para aprender y/o mejorar su funcionamiento. La diferencia estriba en que el hacking se especializa en el uso de este sistema, mientras que el cracking se concentra en el contenido de los programas. El phreaking se especializa en comunicaciones incidiendo mayormente en la electrónica.

El pirata informático NO entra en ninguna de estas categorías, porque es un delincuente común. No obstante, existen hackers, crackers y phreakers que utilizan sus habilidades para cometer delitos. Son ellos los que dan mala reputación a los verdaderos hackers, crackers y phreakers. Tal es el caso de los hackers que, violando el código de ética universal, entran a un sistema para destruirlo o sabotearlo. Estos individuos TAMBIÉN SON LLAMADOS CRACKERS, no obstante, esta segunda acepción del término, es diametralmente opuesta al cracking al que nos referimos en estas páginas.

Demás está decir que el investigador informático es una mezcla de cracker, hacker e incluso phreaker, alguien que investiga y aprende todo lo que esté fuera de su alcance tan solo para disfrutar de la libertad que el aprendizaje le proporciona.

Nosotros le instamos a convertirse en un invesigador y no limitarse solo a la especialidad del cracking o del hacking. No obstante, el presente tutorial le enseñará específicamente cracking.

Un genio utiliza su locura para hacer grandes proezas. Un loco utiliza su genialidad para causar grandes desastres.

Técnica de estudio

Nuestra mejor recomendación es aprender lo suficiente como para enseñar a otros. Así, usted aprenderá mucho más de lo que imagina si alcanza el nivel para la enseñanza.

Ya se habrá dado cuenta que aplicamos esto, también en nuestra vida ajena al underground.

En resumen, siga estos pasos:

1. Escuchar. Los canales IRC por ejemplo.
2. Leer. Si no puede comprar libros, Internet es la solución o de lo contrario conviértase en un "ratón de biblioteca".
3. Escribir. Sí, es verdad que la información está en el libro, pero su mente asimilará mucho más si usted vuelve a escribir lo aprendido con sus propias palabras. No mande hacer el trabajo en el cybercafé de enfrente. ¡Piense por sí mismo!
4. Practicar. ¿Qué es lo que se practica? -La teoría- ¿y qué va a practicar si no tiene una sólida base teórica? En la práctica está implícita la teoría. No existe práctica si no existe teoría.
5. Enseñar. Ésta es la mejor parte. Las preguntas de sus alumnos desafiarán sus conocimientos y lo instarán a aprender más allá de sus límites.

Términos frecuentes

API

(1) Siglas de *Application Program Interface*, "interfase de programas de aplicación".
(2) Parte del sistema operativo que proporciona funciones (pequeños programas) para uniformizar la forma como son ejecutadas las tareas más comunes que se realicen en él. Las APIs residen todo el tiempo en el sistema operativo, por lo que, al utilizarlas en nuestros programas, no es necesario agregar ninguna librería sino solo las referencias a ellas.

Bug

(1) Anglicismo que se traduce como "insecto". "Error persistente en el software o el hardware" (Alan Freedman, "*Bug*", *Diccionario de computación*).
(2) En los primeros años de las computadoras, cuando no existían las computadoras personales sino solamente los mainframes o supercomputadoras, era necesario refrigerar los sobrecalentados sistemas con ranuras de ventilación además de enormes ventiladores. En cierta ocasión, un sistema empezó a fallar inexplicablemente. Se realizaron todos los diagnósticos de hardware y software. Todo parecía normal hasta que, en una minuciosa revisión ocular dentro de uno de los servidores se encontró un insecto (un bug). A partir de ese momento se acuñó el término *bug*, para referirse a un error de hardware o de software.

Codificar

(1) Programar, encriptar.
(2) Cuando el contexto es programación ensamblador, se refiere a convertir códigos mnemónicos en su equivalente valor hexadecimal o binario.

Código fuente

(1) Instrucciones originales de un programa hecho por usted, en un lenguaje cualquiera.
(2) Listado de instrucciones obtenidas al desensamblar un programa que usted no programó.
(3) El código fuente se refiere a cualquier lenguaje y no necesariamente al lenguaje ensamblador.

Compresor

(1) Programa que reduce la cantidad de bytes que ocupa un archivo de cualquier tipo. WinACE, WinRAR, WinZIP son algunos ejemplos de programas compresores de archivos.
(2) Existen compresores especiales que solamente compactan archivos ejecutables que se autodescomprimen cada vez que son ejecutados. Generalmente se les conoce como compresores de ejecutables. UPX, PECompact, Yoda, Aspack, Neolite, Pklite32, etc.

Depurador

(1) Traducción del término inglés *debugger* (literalmente quitar "bugs")
(2) Acompaña a los compiladores serios para que el programador pueda determinar los posibles errores en sus creaciones.
(3) Programa para hacer el seguimiento por instrucciones de un programa a crackear.
(4) Algunos depuradores son TRW2000, SoftIce, OllyDebug, TWX2002 y Hackman, entre otros.

Desensamblar

(1) Obtener el código fuente en lenguaje ensamblador de un programa específico.
(2) Existen muchos desensambladores con diferentes características. Los más conocidos son W32Dasm e IDA Pro.

Ensamblar

(1) Generar un ejecutable a partir de un código fuente en ensamblador.
(2) Los ensambladores más utilizados son Turbo Assembler (TASM) y MacroAssembler (MASM).
(3) Adicionalmente, recomendamos al lector poner especial atención en el proyecto HLA (*High Level Assembler*, "Ensamblador de Alto Nivel"), creado por Randall Hyde para dictarse como primer curso de programación en Cal Poly y UC Riverside. Con una sintaxis similar a Pascal o C++ ha dado resultados positivos. Visite http://webster.cs.ucr.edu para obtener más información.
(4) También, destaca GoAsm de Jeremy Gordon en http://www.godevtool.com con ejemplos y completa documentación disponible. Genera código optimizado en velocidad y tamaño.

Hexadecimal

(1) Sistema numérico de base 16 que utiliza los dígitos 0 al 9 y las letras A,B,C,D,E,F para identificarse. A,B,C,D,E,F significan 10,11,12,13,14,15 en nuestro sistema decimal.
(2) A partir de ahora es vital para usted, manejar el sistema hexadecimal.

Lamer

(1) Si no sabe que es un lamer es porque usted es un lamer.
(2) Término peyorativo (insultante) para señalar al individuo común que...
  (2.1) ... descarga cientos de manuales, pero no lee ninguno.
  (2.2) ... se jacta de poder "nukear" en el IRC autodenominándose "hacker" por ese simple hecho.
  (2.3) ... sólo sigue los tutores de cracking de otros para luego decir que crackea sin ayuda.
  (2.4) ... cree que Bill Gates es el inventor de Internet.
  (2.5) ... cree que Linux Red Hat es solo para redes por que su nombre lo dice: "Red".
  (2.6) ... Tiene los programas necesarios e innecesarios para crackear, pero no crackea nada.

Lenguaje de alto/bajo nivel

(1) El microprocesador sí que es imparcial. Nunca acepta los "creo que sí" ni los "seguramente" ni los "supongo" ni los "todos sabemos". Simplemente acepta hechos concretos, ó es 1 ó es 0 (sistema binario), es SÍ o es NO, sin mayor complicación que esto. Excepto que nosotros no "hablamos" en binario. A ver traduzca esto:

  ```
  11111001
  ```

  y también esto:

  ```
  F9
  ```

  ¿No entendió verdad? (No, no significa pulsar F9). Por esta razón se llama lenguaje de bajo nivel, porque está más abajo, más cerca al entendimiento del microprocesador que al del ser humano. El primero es lenguaje binario o de máquina; el segundo, es lenguaje ensamblador.

(2) Los seres humanos hablamos español (inglés, francés o árabe, para el caso no importa). No pretenderá que su computadora entienda: **"Computadora, haz un programa que descomprima ejecutables y córrelo en la holocubierta número 5"**. Ese sería un lenguaje de muy alto nivel y no existe aún. A ver traduzca esto:

```
Write ("Hola mundo");
```

¿Esto si lo entendió verdad? Al menos lo puede deducir y por ello se llama lenguaje de alto nivel, porque está más arriba, más cerca a la comprensión del ser humano que a la del microprocesador. Ejemplos de ello son: Pascal, C++, Basic, FoxPro, Clipper (o si prefiere Delphi, C Builder, Visual Basic, Visual FoxPro, Visual Objects).

Lenguaje de máquina

(1) Lenguaje de muy bajo nivel en el que se comunican los microprocesadores de manera nativa.
(2) No es el lenguaje ensamblador (códigos mnemotécnicos), es lenguaje binario (uno/cero, activo/inactivo, sí/no, encendido/apagado, under/lamer, linux/winxp).

Lenguaje ensamblador

(1) Traducción del inglés *Assembler Language*.
(2) Debido a la necesidad de un idioma común entre los microprocesadores y los seres humanos, sin llegar a ser lenguaje binario o de máquina, se inventaron los códigos mnemónicos que son codificados a hexadecimal y luego convertidos a binario para que el microprocesador nos comprenda.
(3) MNEMOTECNIA: "Procedimiento de asociación mental para facilitar el recuerdo de algo".

Lista muerta

(1) Traducción para el inglés *Death List*.
(2) En la jerga cracking, este término se utiliza para denominar al listado en ensamblador obtenido a partir de un desensamblador. Lista muerta porque es estática, es decir, no se está ejecutando. Por el contrario, los depuradores trabajan con listas activas.
(3) JERGA: Conjunto de términos empleados en una profesión u oficio cuyo significado es único en el contexto en que se utilizan. No confundir con el lenguaje vulgar.

Parchar

(1) Traducción para el término inglés *Patch*.
(2) Modificar las instrucciones de un archivo cualquiera no necesariamente ejecutable.
(3) Generalmente esta modificación se realiza directamente en hexadecimal con la ayuda de un editor apropiado o a través de un programa creado para tal fin.

Tracear o Trazar

(1) Términos "spanglish" para *Trace*, "seguir".
(2) Ejecutar un programa instrucción por instrucción en cualquier lenguaje.
(3) La denominación apropiada para este sistema es Seguimiento y no "tracear" ni "trazar".

Windoze, Winbugs, Windown, Micro$$oft Window$$

(1) No hay más remedio que usar esto por ahora y esos son algunos de sus nombres "para los amigos de confianza".

Requisitos

Al menos dos dedos de frente. Y si se acaba de medir la frente con la mano, debiera preguntarse qué hace aquí porque esto solo era un expresión alegórica. Están aventajados los de cabeza grande. Pondremos a trabajar ese "cerebrazo".

Capacidad para leer libros sin "figuritas". Y cuando decimos libros, nos referimos a manuales, revistas, cientos y miles de páginas para aprender. Si va a aprender algo, tiene que ser el mejor en ello. Si va a ser un mediocre, mejor retírese y dedíquese a otros menesteres menos complicados.

Aprender a programar. Empiece con Pascal, nada de lenguajes para arrastrar botones y cuadros hacia una pantalla. Continúe con C/C++ y luego aprenda lenguaje ensamblador.

Sus primeras herramientas

(1) Un compilador. Turbo Pascal. La última versión es la 7.1.
(2) Un desensamblador. W32 Dasm. La última versión es la 8.93.
(3) Un editor hexadecimal. Hackers View. La última versión es la 6.82. Es mejor conocido como Hiew.
(4) Un administrador de archivos. Nada de explorador de windown ni nada parecido. Eso no sirve. Busque Total Commander. La última versión es la 5.50. Si prefiere, puede utilizar algún otro programa similar y con las mismas características de Total Commander. En los siguientes capítulos le explicaremos porqué hemos elegido Total Commander.
(5) Manuales de las APIS de windown.
(6) Diccionarios inglés/español. A menos que conozca inglés técnico como segunda lengua, existen enormes locales repletos de libros, llamados librerías. Busque una y cómprese un buen diccionario inglés-español de varios tomos. El libro es el mejor amigo del under.
(7) Babylon Translator. Un buen traductor residente siempre es útil.
(8) Un buen cuaderno en donde anotar organizadamente todo lo que aprenda.
(9) Una buena taza de café negro como petróleo crudo, para no dormirse por el "agotamiento mental" que pudiera sobrevenirle. (''La cafeína puede ser perjudicial para su salud'')

Direcciones en donde buscar:

http://www.anticrack.de (Herramientas y documentos para cracking)
http://www.exetools.com (Herramientas para cracking)
http://www.crackstore.com (Herramientas para cracking)
http://www.ghisler.com (Administrador de archivos Total Commander)
http://www.babylon.com (Afamado traductor Babylon Translator)
http://arc3000.web1000.com (Página oficial de aRC)

O consulte en los canales IRC especializados que se mencionan en la parte final de este primer capítulo. Algunos crackers romperán la tradición de solo decirle: ¡Busca tu solo! y probablemente les ayudarán en sus inicios. Claro, si es que tienen tiempo disponible y sus preguntas son concretas.

También existen muchos canales en Undernet, Efnet, IRCHispano solo piense en palabras relacionadas con cracking e intente unirse a supuestos canales con esos nombres (cracking, cracker, crackers, crackersnewbie, win32asm, cracktools, crackmaster, etc.)

De acuerdo, haga su primer crack aquí

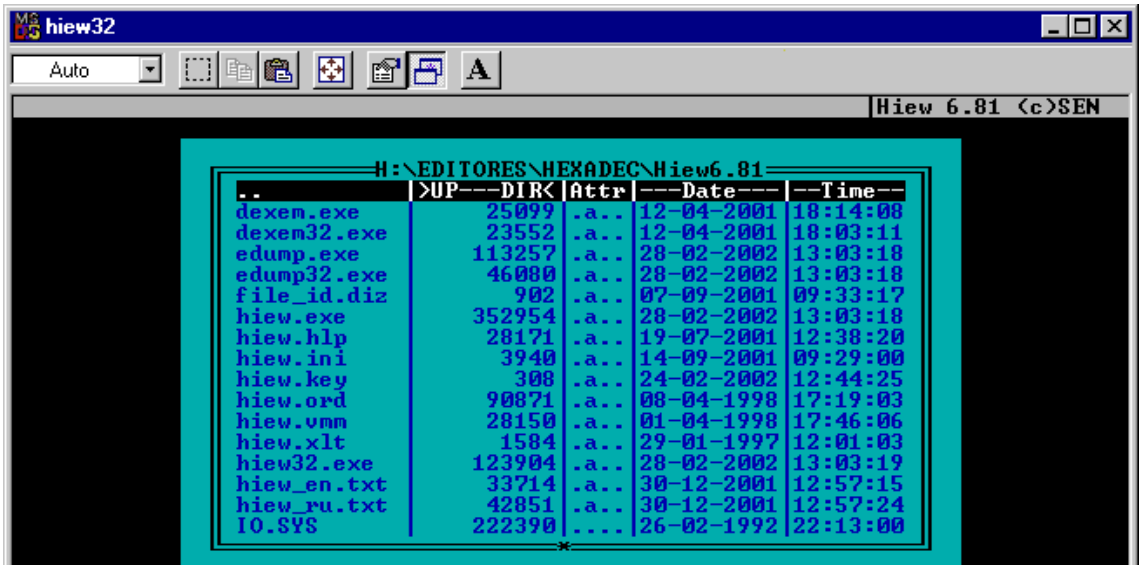
Qué impaciente es usted, debió esperar hasta aRC-Cracking 002. Pero en fin, si desea crackear algo en su primera clase, manos a la obra.

Este tipo de cracking es del tipo patch. Es definitivamente muy simple. Siga las instrucciones atentamente. No nos responsabilizamos por los daños que un lector desatento pueda causar a su computadora.

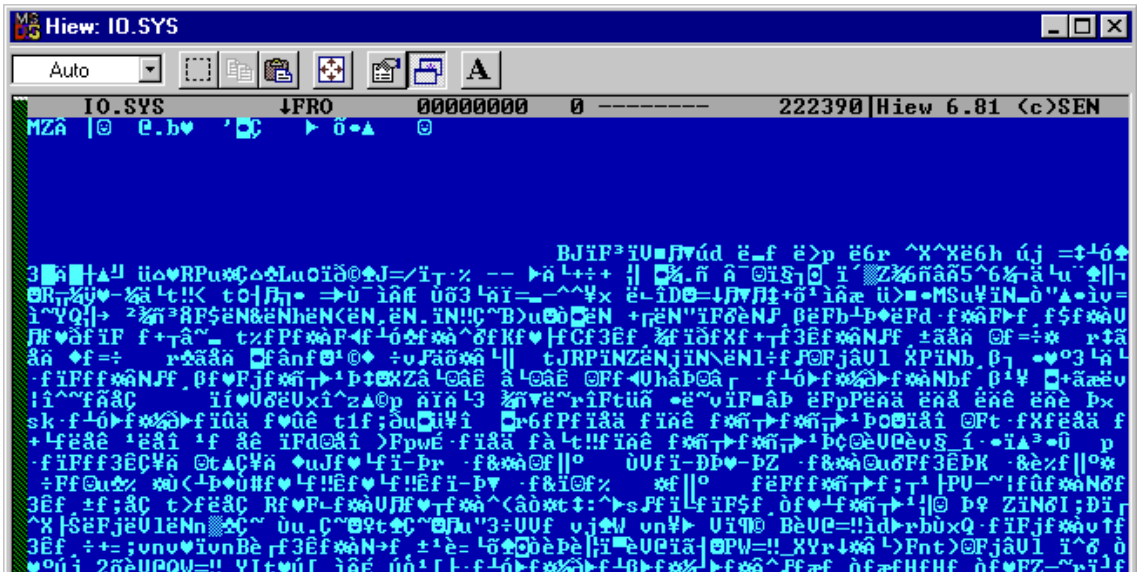
Herramientas necesarias: `Hiew`
Víctima: Archivo `io.sys`
Objetivo: Cambiar el mensaje de carga del sistema: `Iniciando windows...`

1. Quite todos los atributos del archivo `io.sys` que está en `c:\`. (Si no sabe cómo hacerlo, mejor lleve un curso acelerado de Windows antes de meterse en cosas para gente adulta).
2. Ahora copie `io.sys` hacia el directorio en donde instaló `Hiew`.

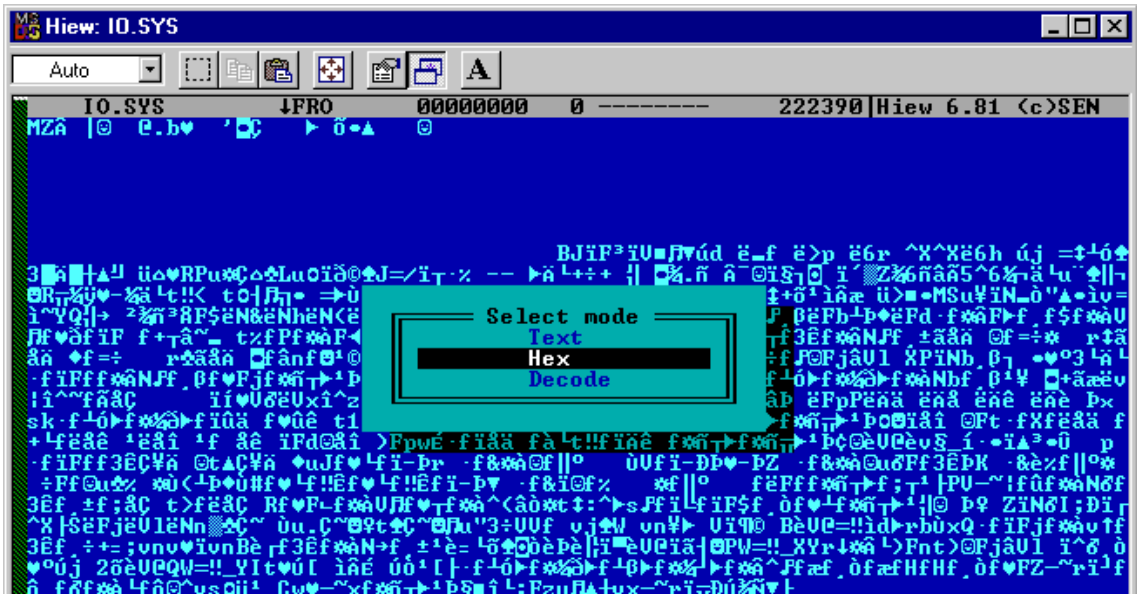
3. Cargue **Hiew** y verá una ventana como ésta: (si prefiere puede maximizarla pulsando **ALT+ENTER**)



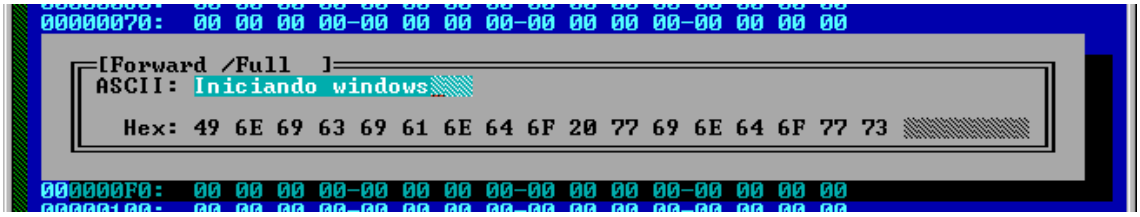
4. Seleccione con las teclas de cursor, el archivo **io.sys** y pulse **ENTER**. Ahora verá la pantalla:



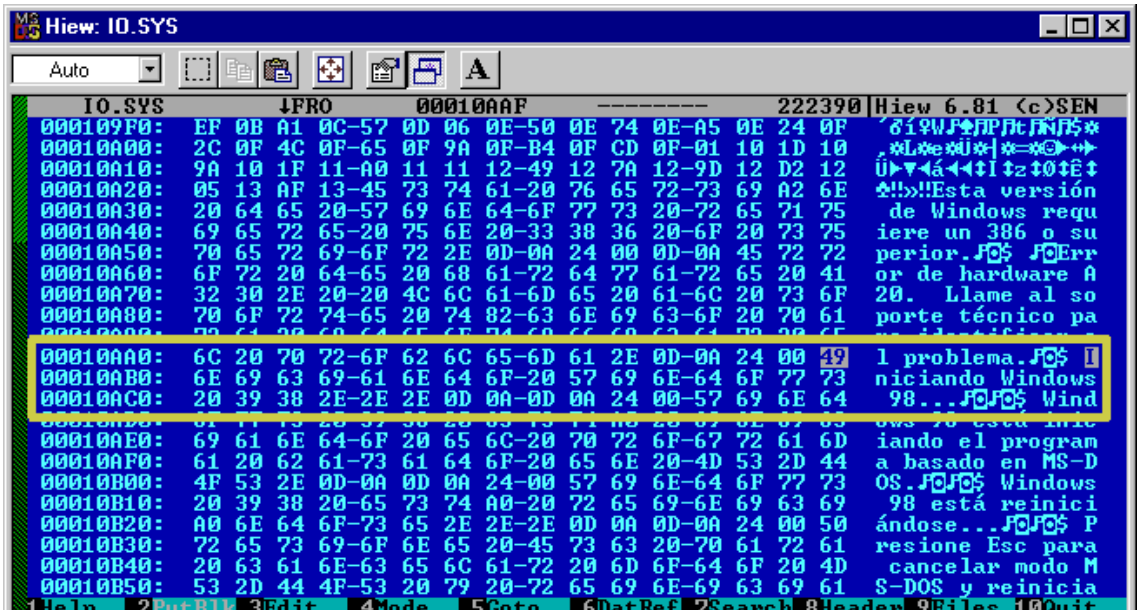
5. Pulse **F4** (**Mode**) y seleccione **Hex** para cambiar de modo de vista a hexadecimal. Presione **ENTER**.



6. Pulse **F7** (**Search**) y en el recuadro **ASCII** escriba **Iniciando windows** y presione **ENTER**.



7. El programa ubicará su cadena de texto en la zona central de la pantalla. Usted verá lo siguiente: ¡Excelente! Hemos encontrado la referencia al mensaje. Ahora editaremos. Nota para "felices"

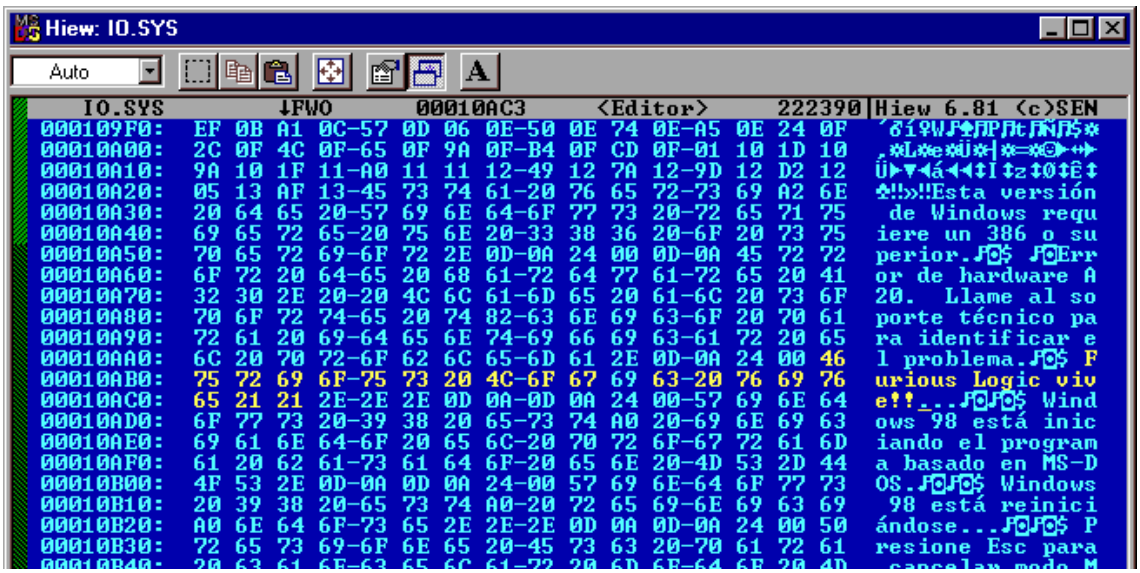


usuarios de 95/ME/2000/XP: El mensaje completo <u>EN NUESTRO CASO</u> es:

```
Iniciando windows 98...
```

Consta de 23 caracteres porque también se cuentan los espacios y los puntos. Todos tienen su equivalente en hexadecimal.

8. Pulse **F3** (**Edit**). Aún NO podemos empezar a escribir porque el cursor parpadeante está en la zona hexadecimal. Pulsamos **TAB** para trasladarnos hacia la zona **ASCII**. Ahora sí podemos empezar a escribir: **Furious Logic vive!!...** o cualquier mensaje de no más de 23 caracteres. Si nos sobran espacios los rellenamos con la barra espaciadora. Recuerde: no más de 23 caracteres. Nos quedará así:



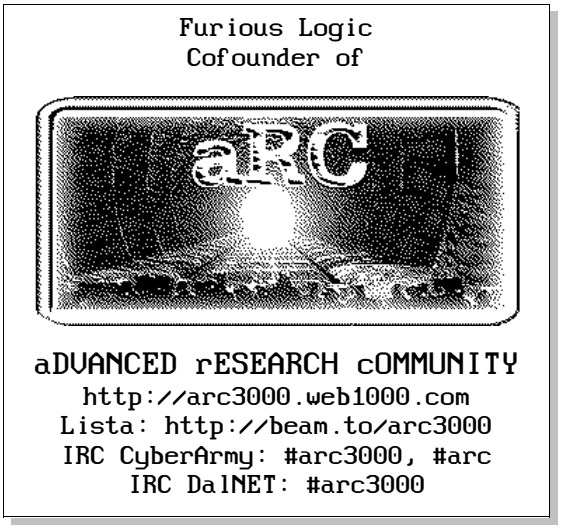
9. Note que mientras escribe, en el lado izquierdo de la pantalla (la zona hexadecimal) automáticamente se van modificando los valores hexadecimales apropiados.
10. Ahora pulsamos **F9** (**Update**) y luego **ESC** ó **F10** (**Quit**) para salir de **Hiew** y retornar a windoze.
11. Copie el archivo **io.sys** modificado hacia **c:** sobreescribiendo el que ya existe allí.
12. Active TODOS los atributos del archivo **io.sys** que acaba de modificar (Si llegó hasta este paso no dudamos que sabrá cómo hacerlo).
13. Si todo ha resultado satisfactorio. Reinicie su computadora y verá un nuevo mensaje al cargar el sistema, aunque solo aparecerá unos pocos segundos.
14. Observación: NUNCA elimine el archivo **io.sys** de **c:** porque es un archivo que está grabado en una zona especial del disco duro. Si lo elimina, NO es posible restaurarlo con un simple copiado.
15. Hemos recibido consultas acerca de cómo realizar el mismo procedimiento con los pseudo sistemas operativos Winbugs ME, XP y 2000. Para todos ellos, les recordamos seguir el procedimiento particular arriba descrito, pero adaptándolo a las circunstancias. Siempre será un archivo el que contenga el mensaje de carga del sistema. Eso es lo único que cambia. En algún caso, es posible que el mensaje se encuentre grabado en el sector de arranque del disco de carga.

En suma, acaba de realizar su primer crack, aunque no es tan primitivo como parece, porque es un método que está en plena circulación. Sin embargo, aún no es un crack. Como dijera años atrás nuestro buen amigo Bishop, dondequiera que se encuentre: **"Para ser crack tiene que ser automático (un programa que haga los cambios), no manual"**. ¡Gracias amigo Bishop por haber opacado nuestra pequeña victoria! Sin esa frase, nunca hubiésemos aspirado a aprender más.

Derechos de autor

El autor puede ser contactado en:

IRC CyberArmy /server -m irc.cyberarmy.com: #arc3000, #arc
IRC DalNet: #arc3000
Email: furiouslogic@eml.cc



"Porque buscamos la libertad que sólo en el conocimiento podemos encontrar"