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!

GUÍA DEL HACKING (mayormente) INOFENSIVO

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!