```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º                SAQUEADORES EDICION TECNICA N§8  10-3-97                   º
º                             Segunda Epoca                                 º
ÇÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¶
º                   Fanzine del underground informatico                     º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼

ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍËÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º  Disponible en  º  http://www.geocities.com/SiliconValley/park/7574/      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
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÊÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```


"I didn’t invent the Unix security problem. I just optimized it."

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
01. CONTENIDOS                                                            º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 02. PRESENTACION                                                          º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Aqui estamos de nuevo :-) estamos batiendo records de velocidad. Habiamos calculado que cada numero de la revista nos iba a costar sacarlo por lo menos dos meses y gracias a nuestros estupendos colaboradores, estamos consiguiendo un ritmo de un numero al mes (GUAU----) Y no solo eso, sino que cada vez sacamos mas articulos y la revista va engordando, en este numero ya hemos superado los 100K de informacion, SIIII y ya empieza a costar encontrar los articulos de los numeros anteriores.

Pero tranquilos porque vamos a sacar un indice de todos los articulos, y vamos a ampliar algunos de ellos. Y quiero decir ampliar, NO volver a publicar, o sea, sera un articulo sobre el mismo tema, pero mucho, mucho mas detallado. (Y corregidos algunos peque¤os deslices :-)

No os hago esperar mas y aqui os dejo el numero ocho.

El Editor

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 03. CLAVES DE DOBLE USO                                                  º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Introduccion:

El contenido de este documento requiere unos conocimientos tecnicos medios, por eso no me voy a parar en explicar detalles ni conceptos basicos. Si hay algo en este texto que no comprendes es mejor que busques otros textos mas acordes con tu nivel. Aunque no creo que te cueste mucho cojer la idea central.

La tecnica que vamos a explicar, no va a requerir unos conociminetos altos en estos temas, es muy general y no requiere mucha destreza para ser aplicada. No es una tecnica de alto nivel, simplemente lo que nos facilitara sera una primera entrada en el sistema, el resto es cosa vuestra. Por eso a pesar de ser sencilla, solo debe ser usada cuando se sepa que hacer una vez dentro.

Metodo:

La mayoria de los sistemas informaticos que hay en internet, son de acceso publico o contienen informacion para un grupo amplio de clientes. Por eso en casi todos los ordenadores conectados a internet hay una cuenta publica, como la famosa cuenta "guest", unos sencillos menus de bienvenida, o una peque¤a presentacion. La mayoria de estas cuentas, tienen un shell restringido o unos lentos menus, que limitan mucho nuestras posibilidades de entrar realmente el sistema.

Para conseguir acceso real al sistema hay dos tecnicas basicas, conseguir salir del shell restringido, o la tecnica que aqui vamos a explicar, usar el nombre de acceso de esa cuenta restringida para acceder al sistema en si.

El truco es el siguiente, para acceder a esa cuenta publica, normalmente nos facilitan un login y un password, o a veces simplemente un login sin password. El quiz de la cuestion, es que un sistema en internet, no solo tienen una forma de acceder a el, sino que tienen un gran numero de puertos de acceso. Si el login que nos dan para esa cuenta de demostracion funciona en una conexion telnet, porque no va a funcionar en una conexion ftp, o en un rlogin, o en rsh?.

Pues resulta que en algunos sitios si que funciona, y en esos maravillosos casos, el shell restringio ya no aparece, sino que tenemos el acceso total al sistema.

Por ejemplo, la mayoria de las bbs en internet, tienen una conexion telnet, pero en algunas de ellas con el mismo login y password de la bbs, puedes acceder mediante ftp, o hacer un rlogin, etc...

Tambien hay servidores web, que necesitan un password de acceso, pero, ¨has probado ese mismo password en una conexion telnet al mismo ordenador?. Pruebalo y te llevaras muchas sorpresas. Hay administradores realmente torpes.

Generalmente se accedera con un nivel muy bajo, por eso se necesitan unos conociemientos altos en hacking, porque el verdadero trabajo empieza ahora. Pero lo importante es que ya estas dentro, y con las manos

libres para probar todo lo que quieras.

Segun nuestra experiencia esta tecnica tiene una efectividad de aproximadamente, un 5% de los ordenadores que tienen una cuenta publica, pero esta efectividad se dispara en ordenadores de universidades, donde tiene una efectividad de hasta el 10% o 20%. Yo creo que son unos porcentajes bastante buenos, para una tecnica tan simple.

Ademas esta tecnica es casi-universal, funciona en todos los sistemas operativos practicamente. Por muy seguro que sea el sistema, si esta mal configurado seguro que hay una brecha de seguridad, y si el administrador es tan torpe de dejarnos un peque¤o hueco abierto, por el entraremos.

Donde:

Los ordenadores donde probablemente exista una cuenta publica de facil acceso son:

-Universidades y centros educativos; con cuentas como ’catalog’, ’indice’, ’consultas’, etc...

-Bibliotecas y hemerotecas; con cuentas como ’hemero’, ’biblio’, ’libros’, etc...

-BBS y servicios de correo publico; con cuentas como ’bbs’, ’nuevo’, ’new’, ’prueba’, etc...

-OPACs (Online Public Acces Catalog); con cuentas como ’opac’, ’public’, etc..

-Organismos publicos; con cuentas como ’publico’, ’dudas’, etc...

-Proveedores de internet.

-Sites warez; con cuentas como ’warez’, ’gamez’, ’anon’, etc...

-Etc...

Habia pensado en publicar una lista de ordenadores donde funciona esta tecnica, pero Eljaker, no me ha dejado. A si que no os lo vamos a poner tan facil y os la vais a tener que currar un poco para encontrar estos lugares.

Os deseo buena suerte en la busqueda del saber...

El Duke de Sicilia

NOTA Este fue uno de los textos que fue presentado como candidato a ser expediente secreto. Como veis no tiene nada de especial y por eso no ha habido problemas para publicarlo. Los que esperaban informacion super-criptica y trucos infalibles de los super-hackers, a lo mejor se han desilusonado, pero es que ese tipo de informacion tan peliculera que todos esperabais, normalmente nunca sale a la luz publica. (Esa es una de las razones de que desechasemos la idea de hacer los expedientes)
*Los que tuvieron la oportunidad de leer el expediente original habran notado que le texto a cambiado un poco, aunque la idea central sigue siendo la misma.

EOF

ÉÍÍÍ»
º 04. RUMORES I º
ÈÍÍÍ¼

Hola y bienvenidos.

Este texto NO es una guia de como ser hacker ni un articulo de opinion
(aunque este relacionado con ambas cosas) sino que pretende ser una
aclaracion y una guias fundamental sobre diversos temas que aqui en
Espa¤a han levantado rumores falsos y/o equivocados.

¨Quien deberia leerlo?

Cualquiera que este desconcertado o confuso por la avalancha de rumores,
textos prehistoricos "recocinados" como actuales o pretendidos intentos de
investigacion que no son mas que traducciones chapuceras, sobre algunos de
los siguientes temas:

Introduccion

PGP
+ ¨Tiene backdoors el PGP?
+ ¨Es ilegal utilizar el PGP?
(aka ¨Pueden enchironarme los yankis?)
+ ¨Es seguro el PGP?
(aka ¨puedes romper la seguridad del PGP? --Yo si!!)

E-mail
+ ¨Puedo contagiarme de un virus por e-mail?
(aka Good Times panik)
+ ¨Que son los sniffers?
+ ¨Es verdad que hay un monton de tipos que husmean todos los ficheros
transmitidos por e-mail?
(aka La pesadilla de los Warez)

En el siguiente capitulo trataremos del Irc, la Paranoia..etc.
(ver lista al final de este fichero)

INTRODUCCION

Esto es Espa¤a... y Espa¤a es diferente (aunque no se que nacionalidad tiene
quien lee esto), vamos a rebufo de los americanos que aportan todas las
innovaciones tecnologicas, tratamos de ponernos a su nivel pero no sabemos
como empezar ni donde, asi que recurrimos a textos de los a¤os 80, listas
de telefonos ya desconectados, trucos que funcionaban hace 10 a¤os....
No todo es culpa nuestra...

Ellos tienen ATT, Sprint, MaBell y nosotros Telefonica
Ellos tienen a Marylin Monroe y nosotros a Marta Sanchez
Ellos tienen a Al Capone y nosotros al Dioni
Ellos tienen $ y nosotros P*ta.

La verdad es que partimos con demasiada desventaja...;>

Lo unico en lo que destacamos es en nuestra credulidad e histerismo, fulano
coloca un mensaje con la mayor idiotez y nos lo tragamos o nos da un ataque
de nervios, nos reimos de los que abrigan el ordenador en invierno "para
que no coja virus" y nos tragamos que por leer un mensaje podemos ser
contagiados.

Asi que este documento pretende acallar rumores, dejar las cosas claras y que la gente sepa a que atenerse.

PGP

El PGP (Pretty Good Privacy by Phil Zimmerman) es como ya sabreis un sistema de encriptacion que se ha convertido en el mas popular entre los usuarios de todo el mundo, para saber como funciona te remito a su documentacion que es muy completa.

¨Porque lo debo usar?
Hay paises (China, Iran, USA...) en los que los ciudadanos no tienen privacidad y deben procurarse los medios para conseguirla, en otros (los llamados paises libres) el Estado siempre quiere entrometerse en nuestros asuntos y debemos impedirselo. Deberias usar siempre PGP ya que representa el espiritu de Internet porque...

- Si solo encriptan pocas personas se fijan en ellas y las vigilan
- Si encriptan muchas personas algunos de los mensajes se preguntan: "¨Porque ha encriptado ESTE?" y siguen ese mensaje.
- Si TODAS las personas **encriptan** TODOS los mensajes, entonces.....
  Jaque Mate (hasta que sean capaces de romper el PGP rapidamente)

Encriptar te beneficia a ti y beneficia a los demas. Es el espiritu de Internet.

+ ¨Tiene backdoors el PGP?

Mucho se ha escrito de este tema, principalmente debido a un texto _humoristico_ que la ignorancia y el histerismo hispano transformaron en un dogma.
Phil Zimmerman no fue obligado por la NSA a poner una backdoor en el PGP
Phil Zimmerman no fue obligado por la NSA a poner una backdoor en el PGP

¨Esta ya claro?

Tenemos que saber que el codigo fuente de las distintas versiones del PGP esta disponible, esto no es garantia puesto que no todos somos expertos pero es que los usarios internacionales NO utilizan el PGP de Zimmerman sino un PGPxxui siendo xx el n§ de version y ui las siglas de Unofficial International, es decir una version desarrollada por otra persona y NO aprobada directamente por Zimmerman (principalmente por motivos legales)

Que quede claro que *no es imposible* que tengamos una version del PGP con backdoor pero eso depende de que fuente obtengamos el PGP, lo preferible es conseguirlo de lugares fiables y no de terceras fuentes que pueden haber decidido ’alterar’ el PGP por algun motivo.

+ ¨Es ilegal utilizar el PGP?

Con nuestra habitual falta de sentido comun se ha llegado a correr el rumor de que "te pueden meter en la trena si mandas un mensaje encriptado a USA". Los hechos:

- La exportacion de criptografia (pese a una reciente liberalizacion) ha estado sujeta siempre a leyes restrictivas.
- El soft de encriptacion desarrollado en USA NO puede ser exportado sin

permiso
- Usarlo FUERA DE USA NO ES DELITO, recuerda, el delito es la EXPORTACION
- Para remediar esto se han desarrollado las versiones Ui (Unofficial International) del PGP, que al ser creadas fueras de USA no estan sujetas a las fascistas leyes yankis.
- El problema de las patentes.
El MIT PGP (El PGP que se utiliza en USA actualmente) utiliza la libreria RSAREF que tiene un monopolio en USA sobre los sistemas de encriptacion basados en clave publica, las versiones Ui mas recientes incorporan otra libreria que es compatible con RSAREF pero no esta sujeta a licencia, recuerda, en USA cualquier sistema de llave peblica *debe* usar la libreria RSAREF (por algo tiene un monopolio)

Supongo que con esto te habra quedado claro que los delitos pueden ser:
- Exportar material criptografico _desde_ USA
- Usar la RSAREF en USA sin tener licencia para ello (uso comercial)
- Usar en USA un sistema de llave publica no basado en la libreria RSAREF

NOTA: Hay paises en los que la encriptacion en si es un DELITO (como Francia) cada pais tiene una legislacion respecto a permitir a sus ciudadanos cifrar las comunicaciones.

Y ya esta, nada de mandar o recibir mensajes (excepto Francia) o crear llaves, nada de eso es delito ni siquiera en USA (y menos aqui donde los legisladores piensan que el PGP es algun partido politico)

+ ¨Es seguro el PGP?

Si no quieres que alguien se entere de algo NO LO DIGAS, (puede que pensarlo sea comprometido tambien), el PGP es un sistema *muy fiable* pero no es invulnerable, basicamente el problema no es el criptoanalisis sino la alteracion de llaves publicas (o del mismo PGP) y la perdida de tu llave secreta y su passphrase.
Descifrar un mensaje de PGP consiste en resolver un problema de factorizacion de nemeros primos, eso lleva mucho tiempo utilizando computadoras muy potentes (si los n§s son grandes), a menos que alguien descubra un sistema nuevo no es rentable intentar descifrar el PGP.
(¨De que te sirve descubrir el dia 15 algo que iba a pasar el dia 10?)
(¨O gastarte millones en descifrar un mensaje en el que pone:" Esto es solo una PGP prueba"?)

Por lo tanto no te preocupes, a no ser que todas las Agencias de Seguridad vayan a por ti nadie se va a molestar en intentar descifrar tus mensajes, presta mas atencion a la seguridad de tu llave secreta, a tener una copia del PGP fiable y a que nadie sustituya tu clave publica por otra con la cual pueda interceptar los mensajes que te envian. Esos temas vienen explicados en la documentacion del PGP.

¨Entonces que pasa con el PGP?

Pasa que algun IDIOTA (si, con mayusculas) se dedico a poner mensajes en newsgroups, Fido.. (otros idiotas ponen solo uno y escarmientan) alardeando de **poder romper el Pgp** , hay que ser muy deficiente para creer que un individuo sin preparacion ni conocimientos ninguno va a conseguir lo que los mas brillantes criptoanalistas no han podido hacer (ni los miles de usuarios del PGP) pero al parecer este tipo era lo suficientemente cretino como para creerselo (encima era espa¤ol, que cruz)
No me acuerdo muy bien de la idiotez que decia pero estaba relacionado con las firmas, al parecer cambiaba la id de usuario en un editor de texto abriendo el fichero de firmas y decia -voila! ya esta, ahora parece que lo ha firmado quien yo he puesto y no el firmante original.

Una payasada que le parecia genial y que supuestamente habia pasado desapercibida a todo el planeta menos a el.
La realidad es que si chequeamos la firma un BAD SIGNATURE asin de grande nos informa de que la firma modificada es FALSA y es que hay que distinguir entre poder cambiar algo y que ese cambio sea aceptado como legitimo.

Que quede claro, el PGP no es invencible pero esta a prueba de ataques de paletos, si el paleto lo usa mal entonces es cuando se la pueden liar A EL.

E-mail

+ ¨Puedo contagiarme de un virus por e-mail?

Otro de los "timo-rumores" que han corrido por ahi, decia que si alguien recibia un mensaje con el Subject: Good Times que no lo abriese porque se instalaba un virus en el ordenador, como de costumbre el analfabetismo informatico y la falta de sentido comun hicieron el resto y hubo desaprensivos que se "jartaron" de enviar mensajes con dicho subject para partirse de risa ante el temor de las victimas.

Habra que recordar que un "virus" no tiene poderes magicos, que es un programa como cualquier otro y que un programa tiene que *ejecutarse* para que haga algun efecto (bueno o malo), leer un mensaje es *inofensivo* (lo maximo es que nos metieran una bomba ANSI pero ya es traerlo de los pelos). Por supuesto si que hay que tener cuidado con los "attach" puesto que son ficheros que pueden estar infectados (o ser un virus en si) asi como con cualquier download pero si tenemos unos buenos y actualizados antivirus (mejor 2 o 3 que no uno solo) no hay problema. Ni Internet ni las BBS destacan por tener archivos infectados, los sites con material virico son minoria y destacan claramente que contienen sus archivos.

Por lo tanto. Do not panic!

+ ¨Que son los sniffers?

Son programas que "monitorizan" la red, por ejemplo buscan palabras previamente definidas en los mensajes que rutan, como aqui todo se saca de quicio ya hay quien piensa que todos los proveedores montan sniffers.
El sentido comun indica que:
- Usar un sniffer (salvo consentimiento del implicado de manera expresa) es ILEGAL porque viola el derecho a la privacidad en las comunicaciones.
- Si un proveedor tiene un sniffer es MAS que probable que lo haya montado algun "loco" de la informatica que trabaja para el y lo haya hecho por su cuenta y riesgo (porque le guste cotillear)
- Con MILLONES de mensajes circulando diariamente los routers y proveedores tienen mas cosas que hacer que chequear tus mensajes.

Quien si puedes imaginarte que lo hace a gran escala es nuestra ""amiga"" la NSA pero ni podemos evitarlo (puedes desarrollar un "codigo" o encriptar tus mensajes con PGP pero no evitar que lo monitorizen) ni la NSA tiene por mision buscar palabras como "warez", "soft pirata" o "imagenes de guarras", su guerra es otra.
Por supuesto es ilegal. Denuncialos si quieres (y si puedes).

+ ¨Es verdad que hay un monton de tipos que husmean todos los ficheros transmitidos por e-mail?

Siguiendo con los sniffers y abonado por la detencion de una red de piratas

en Barcelona y Tenerife a los que interceptaban el e-mail, los alborotadores de siempre empezaron a decir que se interceptaban todos los "attach" y que luego alguien los descodificaba y que se guardaban logs y......

Y los membrillos de siempre entre el: -Ay, no me digas! y el -Hala, que dices, eso no puede ser!

Como de costumbre ni si ni no sino todo lo contrario.

No hay costumbre de interceptar mensajes con attach, ni de guardar logs de los mensajes con attach, lo cual no quiere decir que alguien en alguna parte no lo haga pero SI NO SE SOSPECHA no es mas que un gasto inutil de tiempo y recursos.
Puedes tener alguna posibilidad si estas en relacion con organizaciones terroristas, racistas... a los cuales la policia vigile (hablamos de los yanquis y de las agencias de inteligencia como el Mossad o el M15, la Guardia Civil esta para otras cosas) pero desde luego ningun organismo se encarga de seguir tu "attach" de la playmate del mes a tu amigo Manolo y tomar nota de ello.

NOTA: El CESID no se considera una agencia de inteligencia aunque recibe informes.

Tip: Los unicos que tienen recursos son los yanquis, no te metas en tratos con las organizaciones a los que ellos vigilan porque te pillaran a ti.

-Eso es todo amigos!.

El resto es:

IRC
+ ¨Si utilizo un script pueden machacarme el HD?
+ Extra ¨Que hacer cuando te piden que pulses Alt+F4? :D

Paranoia
+ ¨Que grado de paranoia es bueno?
+ ¨Que es eso del daemon de 1Mb?

El Documento y el Autor
Rollo legal
Ultima hora

Todo en el siguiente capitulo

By Paseante. Febrero 1.997

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 05. RUMORES II                                                            º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Hola y bienvenidos.

Este fichero es la 2¦ parte de un texto destinado a calmar ansias, aclarar rumores y sosegar la vida del internauta espa¤ol (la politica puede seguir crispada..no problemo)

Vamos pues, tras solventar algunas dudas sobre PGP y E-mail, ahora toca:

IRC
 + ¨Si utilizo un script pueden machacarme el HD?
 + Extra ¨Que hago cuando me dicen:"Pulsa Alt+F4 para ver las imagenes X"?

Paranoia
 + ¨Que grado de paranoia es bueno?
 + ¨Que es eso del daemon de 1Mb?

El Documento y el Autor

Rollo Legal

Ultima Hora

IRC

Internet Relay Chat (ya se que lo sabeis) uno de los recursos Inet mas utilizados (y en alza imparable), hay muchos programas de Irc e incluso plugins para Netscape pero el programa mas "historico" es posiblemente el mIrc de Khaled Mardam.
El mIrc tiene muchisimas opciones y entre ellas el dotarte de un lenguaje con el cual puedes crear scripts que automaticen ciertas acciones, de ello vamos a tratar.

+ ¨Si utilizo un script pueden machacarme el HD?

Los scripts son comodos y te permiten "jugar con ventaja" pero no todo el mundo quiere aprenderse el lenguaje para crearlos o tiene ganas de ponerse a hacerlos asi que utilizan scripts que otros autores han creado.

Y aqui viene el peligro, por esta vez SI es cierto y tiene fundamento que hay scripts (bastantes) con backdoors que permiten acciones no deseadas por el usuario que utiliza el script (y que se suelen activar mandando un codigo), estas acciones pueden ser expulsarte del canal, dar +op a alguien o con mas mala leche hacer algo en tu ordenador (como j*der el HD)

Ante esto los mas radicales optan por utilizar el mIrc ’a pelo’ con lo cual sacrifican el uso de scripts a la seguridad. Las malas noticias es que no hace falta que uses scripts para que ’te la peguen’ con una backdoor puesto que algunas versiones del mIrc traen backdoors ’de serie’

Tip: Khaled Mardam es un tipo chistoso, no solo nos cuela backdoors de tanto en tanto sino que ademas prueba a hacer click sobre su nariz en la foto que viene con el mIrc.

Las alternativas si queremos usar scripts de manera segura pasan por:

- Repasar nosotros o un colega el codigo del script (si sabemos lo suficiente)
- Utilizar scripts que lleven tiempo en rodaje y de los que no se hayan detectado backdoors
- Vigilar de donde obtenemos el script.
- No usar scripts nuevos o nuevas versiones de scripts antiguos a menos que confiemos en el tipo que los hace.
- No usar Irc (solo para los mas extremistas)

Y ahora de regalo extra para todos los usuarios de Pc:

+ ¨Que hago cuando me dicen:"Pulsa Alt+F4 para ver las imagenes X"?

La enica respuesta valida es: Lo siento, mi teclado esta bloqueado para desbloquearlo necesito que TU pulses en el TUYO Ctrl+Alt+Supr .

Tip: Si acto seguido responde:"Ya esta, ya lo he hecho" no le creas, esta mintiendo. :D

Paranoia

La paranoia es consustancial al hacker o a cualquiera que se mueva en ambientes underground, algunos opinan que cualquier grado de paranoia es bajo, en todo caso recuerda la letra de Nirvana:

Just because you’re paranoid don’t mean they’re not after you.

+ ¨Que grado de paranoia es bueno?

No podemos pasarnos todo el dia pensando que la portera esta a sueldo del CESID, una cosa es ser conscientes del poder y recursos que tiene el Estado y las grandes compa¤ias y otra muy diferente es creerse cualquier cosa que nos cuenten. Las reglas para que no pases de ser un n§ mas a convertirte en un "peligro nacional" las dicta el sentido comun:

- No llames la atencion (no vayas de fanfas)
- No seas Robin Hood, meterse con los debiles es mas facil
- Si te metes con los fuertes preparalo todo con antelacion, la diferencia de recursos a su favor puede equilibrarse con la planificacion que les lleves de ventaja.
- Y recuerda, pueden ser malos pero son pacientes.

+ ¨Que es eso del daemon de 1Mb?

Uno mas (y van...) de los bulos que corren es que Telefonica tiene en Infovia un proceso daemon que (-atencion a la payasada!) "corta de manera aleatoria las transmisiones mayores de 1MB", esto no solo ha sido motivo de mensajes en Espa¤a sino que al parecer una revista??¨¨ lo publico (supongo que sera un boletin hecho por un aficionado de 3¦)

Lo unico que ocurre es que la estabilidad de Infovia y de nuestras lineas telefonicas no es optima y ello se hace mas evidente en una transmision larga que en una corta (dicho sea en vulgo: es mas facil tener errores estando 2 horas conectado que estando 10 minutos)
Los usuarios de a pie igual se creen que Infovia solo sirve para traer paginas Web de pocos kb, sin embargo HAY MUCHAS transferencias de GRAN volumen, Infovia mueve TERABYTES de informacion de manera diaria, si cortase transmisiones de mas de 1MB estaria machacando a sus clientes mas importantes. (Y dicho sea de paso ¨que ganaria con ello?)

Otra posible fuente de problemas lo tienen aquellos que utilizan la linea principal para llamar con el modem (conectando telefono y modem a la vez) gracias a los nuevos servicios de Timofonica como el de -Llamada en Espera- puede ocurrir que en medio de una transmision comience a sonar el telefono mientras el modem detecta los ring, el final suele ser que no se establece la llamada telefonica y encima perdemos la conexion modem.
(Lo cual hace mucha gracia si te pilla al final de una transferencia de 4MB y te inclina a creer en 'meigas')

El Documento y el Autor

He escrito ya varios "¨docs?, ¨ensayos?, ¨textos?.." sobre aspectos de Internet y las comunicaciones en los que me parecia que podia aclarar dudas e instruir a la gente que estaba interesada en esos temas y no sabia como empezar, no tienen ninguna pretension salvo ayudar a la gente y establecer asi una cadena de solidaridad (que potito ;))
No tienen periodicidad ni n§ de version ni nada parecido, para escribirlos me guio por los temas en los que veo que hay gente interesada y en los que creo poder aportar mi granito de arena.

- Formato

El que utilizo habitualmente.
2 ficheros Txt en formato Ascii
1 fichero file_id.diz para que si lo subes a una BBS tenga descripcion.
Todo comprimidito en .zip

- Autor

Yo NO soy un hacker ni un pirata ni profesor de informatica en la Uni ni siquiera pertenezco al CESID, soy un tipo sencillo que sabe algo de informatica, que esta interesado en los temas "underground" y que sobre todo intenta buscar y aprender de la gente que sabe mas que yo (mucha).
Tengo sentido comun y se donde encontrar algo de informacion. Eso es casi todo.
Como siempre puedes escribirme insultando, alabando, puntualizando, solicitando, preguntando..Paseante es <paseante@thepentagon.com>
Como siempre no te aseguro que recibas una respuesta.

Rollo Legal

Este es un texto freeware, distribeyelo en BBS, en CDs, en FDs, ponlo en tu pagina Inet o pasaselo a un amigo (que este interesado en el tema) a mi no me importa ni necesitas pedirme permiso.
En cuanto a las modificaciones si que me gustaria saber quien, como y porque modifica este texto, parece mucho pero no es mas que un mensaje que diga: Hey tio, voy a cambiar tal x tal que esta ya desfasado.

Por supuesto no me hago responsable de las consecuencias que pueda traerte el leer, seguir o imprimir este texto (salvo que ganes pasta, entonces vamos a medias). Si tras leer este texto tienes un accidente tampoco es culpa mia.
En resumen: Te sabras lo que haces.

Ultima Hora (14 Febrero 1.997)

Pues por diversas razones (trabajo, estudios..) mi pagina va a sufrir un apagon "indefinido" :(por lo cual las personas que pasaban por alli

(-Hey gracias a todos!) ya no podran recoger mis opiniones y textos, eso no supone que no vaya a seguir produciendo, podeis chequear mis textos en el ftp de RedIris o en las BBS que sabeis.
Espero volver a ponerme en breve con una pagina para que podais recoger de alli el "material" y nos sirva de punto de encuentro..necesito algo de tiempo.

Y gracias tambien a los que han intentado 'hackear' mi pagina, cria cuervos... ;). (¨Creo que no lo consiguio nadie, me equivoco?)

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

By Paseante. Febrero 1.997

Paseante <paseante@thepentagon.com>

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 06. HACKERS Y NEWBIES                                                     º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

HACKERS Y NEWBIES.
Para saqueadores.

Permitidme que me presente. Soy Criptero, y no tengo ningun miedo a reconocer que soy un novato entre hackers.
A pesar de que llevo varios a¤os intercambiando correo regularmente en FIDO, y que me manejo bien en INET, no me reconozco los suficientes conocimientos para considerarme un hacker.

Me he decidido a escribir, porque alguien tiene que hacerlo, sobre las relaciones entre los expertos y los que no lo son dentro de la COMUNIDAD de hackers. Si es que tales relaciones existen.

En primer lugar, me gustaria saludar a los funcionarios del ministerio del interior que leen esta revista.

Aparte de ellos, que lo hacen por obligacion, el resto de nosotros lo hacemos por placer, porque nos apetece, porque es nuestro mundo. Porque nos encanta conocer mas y mas, porque somos curiosos, y tambien porque nos gusta esa sensacion de PODER...

Cualquier reto intelectual, por simple que sea, es un juego que deseamos jugar. Cualquier ordenador es juego que ofrece un gran reto. Muchos novatos no entienden esto. Situan el placer en el fin, mas que en el camino recorrido. Solo quieren saber lo extrictamente necesario para llegar cuanto antes. Son/somos irritantes.
Claro que nadie nos ha advertido que podemos ser de otro modo.

Por otro lado muchos hackers parecen olvidar que el deseo de saber, aunque alocado, es precisamente lo que les llevo a ser lo que son. Que se puede canalizar la dispersion de los novatos hacia cosas utiles para los expertos, que a la vez sirvan para aprender a los mas nuevos.

¨Te molesta un novato que te pregunta una y otra vez como se hace hacking? Bueno, creo que la respuesta correcta es...
¨Y QUE PUEDES HACER TU POR MI?
En principio te puede parecer que no gran cosa. Pero hay un monton de labores rutinarias que un novato esta deseando hacer con tal de estar dentro. Con un poco de imaginacion los usos de un novato son ilimitados:
Se despertara dichoso para vigilar un area de chat a las tres de la ma¤ana si con eso se traba tu confianza.
Mantendra con gusto tus cuentas de correo fantasmas si con ello es capaz de entender tal o cual cosa.
En fin, los usos de un novato son ilimitados. UTILIZADNOS !!!

Quizas asi comencemos a desterrar esa fama de comunidad de personajes intelectualoides incapaces de relacionarse y lleguemos, quizas, algun dia, si ello es posible, si nos acompa¤a la suerte, a la conclusion de que LOS HACKERS ESPA¥OLES TIENEN CONCIENCIA DE CLASE.

Cripte+o

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 07. RED TELEFONICA CONMUTADA I                                           º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼


       _/_/_/_/            Red Telefonica Conmutada            \_\_\_\_
      _/_/_/_/                  Primera parte                   \_\_\_\_
     _/_/_/_/                                                    \_\_\_\_
    _/_/_/_/                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.

DEFINICIONES
ÄÄÄÄÄÄÄÄÄÄÄÄ

Bueno, antes de entrar en materia creo que es conveniente aclarar algunas definiciones. Mucha gente piensa que los phreakers son gente que se dedica a conseguir realizar llamadas gratuitas o mas baratas. Pero no es asi.

Un phreaker es una persona que le gusta jugar con la red telefonica, ya sea para conseguir llamar gratis, o simplemente desviar llamadas, y todo aquello que se os ocurra. Incluso en ocasiones es interesante saber como pagar mas por una llamada, como cuando tienes un conocido molesto y quieres hacerle una putada.

Una vez aclarado esto, espero que nadie se desilusione porque en este articulo no se hable de como llamar gratis. Pero puede que os lleveis algunas sorpresas.

ESTRUCTURA DE LA RED TELEFONICA
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ

En un principio la RTC (Red Telefonica Conmutada) se constituia de centrales y equipos analogicos. Actualmente, se encuentra en proceso de digitalizacion.

Existen diversas estrategias de digitalizacion que no merecen la pena ser contadas, pues lo que nos interesa es la situacion actual, y como estara en un futuro. Si a alguien le interesa la historia de telefonica y como estaba estructurada la red hace unos a¤os, que lo solicite, y se estudiara.

Bueno, a lo que ibamos. Actualmente la red telefonica ha evolucionado a un sistema digital, conociendose ahora como la RD, o Red Digital, pasando en un futuro a la RDI o Red Digital Integrada. La estructura de la RD, asi como de cualquier otra red telefonica puede dividirse en dos redes: Red de Transito Nacional y Red de Acceso.

La Red de Transito Nacional es la encargada de encaminar las comunicaciones entre los diversos puntos de la geografia espa¤ola. Existen dos tipos de centrales en esta red: las centrales terciarias y las secundarias. En un principio, se digitalizan las centrales. En la actualidad se han definido 25 areas nodales. En estas areas se establecen parejas de centrales nodales que actuan en doblete, haciendo desaparecer gran parte de las centrales secundarias.

La Red de Acceso se compone de Centrales Autonomas Digitales, y son las que dan acceso al nivel de transito. Estas poseen unas unidades de concentracion remotas compuestas de Concentradores y Unidades Remotas de Abonados, que se encargan de proporcionar los servicios y facilidades a los abonados que estan conectados.

En un futuro se prevee la digitalizacion de todas las centrales telefonicas. Estas se interconectaran entre si, usando el Sistema de Se¤alizacion por Canal Comun n§7 para la se¤alizacion entre centrales. El interfaz con el abonado

seguira siendo analogico.

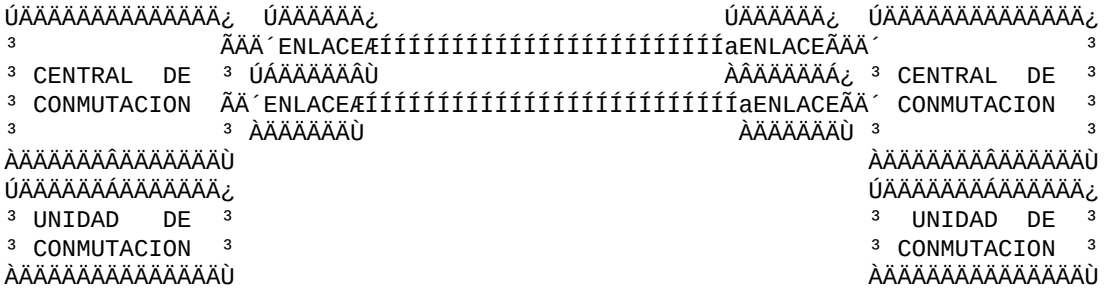
SE¥ALIZACION

Llegados a este punto, conviene aclarar que es la se¤alizacion. La definicion de sistema de se¤alizacion que podreis encontrar en cualquier libro sobre telefonia es: "conjunto de informaciones que deberan intercambiar los diferentes elementos de una red de telecomunicacion para establecer, supervisar, mantener y liberar una conexion".

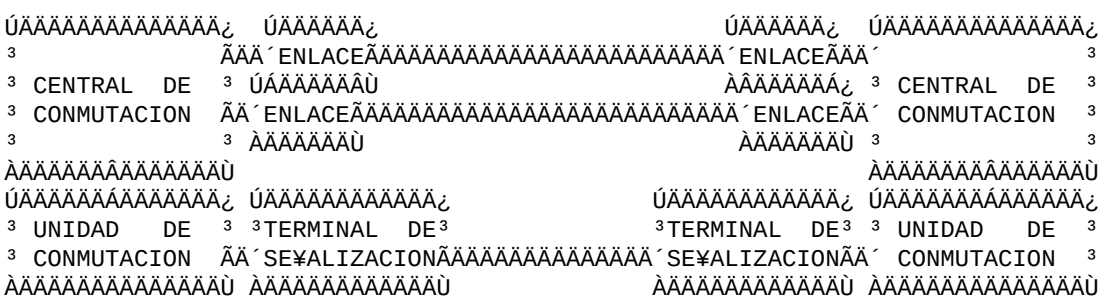
En otras palabras, mediante la se¤alizacion es como las centrales saben a quien llamamos segun el numero que marquemos, como se encuentra la linea, el coste de la llamada, etc. (Esto se pone interesante:)).

La se¤alizacion se puede realizar bien por canal asociado, bien por canal comun. Por canal asociado, la informacion se transmite por el mismo canal por el que se esta llevando a cabo la comunicacion. Es el usado hasta ahora en la RTC. (Puede sernos muy util). Cuando se habla de se¤alizacion por canal comun, nos referimos a cuando se establece un circuito aparte por el que se transmite toda la informacion relativa a varios grupos de abonado.

SE¥ALIZACION POR CANAL ASOCIADO



SE¥ALIZACION POR CANAL COMUN



Como se puede suponer, la se¤alizacion por canal comun ofrece mayor seguridad que la se¤alizacion por canal asociado, pues el abonado no dispone de las facilidades que el sistema de canal asociado permite para intervenir la se¤alizacion.

Veamos ahora como funciona la se¤alizacion por canal asociado, que es la usada en la RTC, y como veremos, la que nos puede servir por el momento.

SE¥ALIZACION ABONADO-CENTRAL

Es la se¤alizacion que se produce entre el equipo de abonado (telefono, modem, etc.). Las se¤ales que aparecen entre el abonado y la central se caracterizan por ser simples y fiables, como vamos a comprobar. Estas se¤ales se clasifican en cuatro tipos:

* Se¤ales de supervision o estado.
* Se¤ales de direccion.
* Se¤ales de informacion.
* Se¤ales de tarificacion.

Estas se¤ales se producen en lo que se denomina el bucle de abonado. Este bucle lo componen el circuito de linea de la central, el par de hilos telefonico y el equipo terminal de abonado.

El bucle de abonado permanece constantemente alimentado por una corriente continua, por lo que la se¤alizacion se realiza en funcion de las variaciones del nivel de corriente y de su sentido.

Cuando el telefono esta colgado, se dice que el bucle esta en reposo o abierto, pues la impedancia del equipo de abonado es muy alta. En estas condiciones la corriente en linea es casi nula, de 3 mA.

Al descolgar el equipo, la impedancia disminuye sensiblemente, obteniendose una corriente de 21 a 60 mA. Entonces se dice que el bucle esta activo o cerrado.

La central detecta esta caida en la impedancia, interpretandola como un deseo de realizacion de llamada.

Pasemos ahora al analisis de los diversos tipos de se¤ales:

Se¤ales de supervision o estado
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ

Son siempre en corriente continua.

* El abonado descuelga
  Se detecta por la caida de la impedancia en la linea.
  Si se produce en la central de origen, se provoca el arranque de los organos necesarios para recibir la informacion de direccion.
  Si es en la central destino, provoca el paso de la comunicacion a conversacion.

* El abonado cuelga
  Se detecta por el aumento de la impedancia en la linea. Provoca la liberacion de los organos ocupados en la comunicacion.
  Si cuelga el abonado llamado, se produce una temporizacion de 30 s. en la central origen, con el fin de liberar los organos si el abonado llamante no ha colgado pasado dicho plazo. (Esto puede ser muy util, ya veremos para que).

Existen otro tipo de se¤ales de supervision, que seran tratadas en otros articulos.

Se¤ales de direccion
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ

Son las que especifican el numero de abonado al que llamamos. Este numero se compone, salvo para servicios especiales, siempre de 8 cifras. Puede parecer raro en un principio, pero el numero completo de un abonado se compone de su prefijo de zona mas su numero de abonado. Ya sabemos que no es preciso marcar el prefijo en una misma provincia, pero nos es util para explicar que son siempre 8 cifras.

Si al prefijo le quitais el 9, comprobareis que la/s cifra/s restantes, sumadas al numero de abonado son 8 cifras. Lo mismo sucede con los telefonos moviles o los telefonos 900...

Bueno, estas se¤ales dependen del sistema de marcado que tengamos en nuestro telefono. El sistema de marcado es de dos tipos:

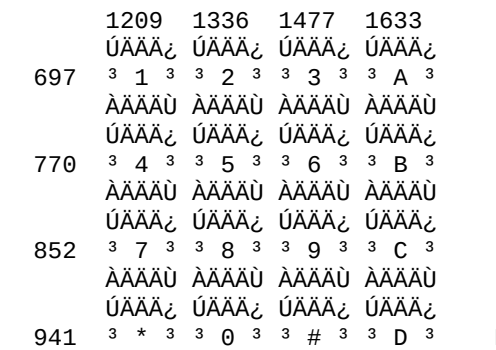
* Informacion decadica
  Es el que nos podemos encontrar en los clasicos telefonos de disco y

en algunos de teclado. Su funcionamiento se basa en abrir y cerrar el bucle tantas veces como indique el digito que hemos marcado, 10 veces si se trata del 0. Estas aperturas y cierres de bucle se efectuan a una frecuencia de 10Hz.

Este sistema esta actualmente siendo retirado.

* Informacion multifrecuencia

Es el que todos vosotros posiblemente tengais ya en vuestras casas. Se basa en el envio de la combinacion de dos frecuencias entre ocho posibles por cada digito.



Este es el esquema con las frecuencias utilizadas en Hz.

Se¤ales de informacion

Son tonos audibles o mensajes grabados previamente (como el popular "El numero marcado no existe", etc). Informan al abonado sobre el progreso de la llamada o las causas por las que no ha podido progresar.

Estas se¤ales suelen ser enviadas desde la central hasta el abonado. Las se¤ales mas habituales son las siguientes:

* Tono de invitacion a marcar

Indica al abonado que origina la llamada que puede empezar a marcar el numero. Se emplea una se¤al de 400 Hz permanente.

* Corriente de llamada

Es una se¤al de 75 Vef initerrumpidos de corriente alterna a 25 Hz. Se usa para hacer sonar el timbre del abonado llamado.

* Tono de llamada

Se¤al enviada al abonado que llama que indica que ya se ha seleccionado al abonado llamado. Se emplea la misma frecuencia que en el tono de invitacion a marcar, pero con una cadencia prefijada.

* Tono de ocupado

Se¤al de 400 Hz con una cadencia determinada que se usa para indicar al abonado que llama que el abonado llamado no tiene su linea libre.

* Tono de congestion

Otra se¤al de 400 Hz con otra cadencia usada para indicar que es imposible establecer la comunicacion debido a dificultades tecnicas.

* Tono de nivel muerto

Y otra se¤al de 400 Hz con otra cadencia para indicar que el abonado llamado no existe.

A continuacion se muestra una tabla en donde se muestran todos los tonos con sus respectivas frecuencias y sus cadencias.

```
                               ³     Cadencia (ms)    ³
                         ÚÄÄÄÄÄÅÄÄÄÄÄÄÄÄÄÄÄÂÄÄÄÄÄÄÄÄÄÄÄÄ´
                         ³ Hz  ³ Emision  ³  Silencio ³
    ÚÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÅÄÄÄÄÄÅÄÄÄÄÄÄÄÄÄÄÅÄÄÄÄÄÄÄÄÄÄÄ´
    ³ Invitacion a marcar   ³ 400 ³ Continuo ³         0 ³
    ³ Llamada               ³ 400 ³     1500 ³      3000 ³
    ³ Ocupado               ³ 400 ³      200 ³       200 ³
    ³ Congestion            ³ 400 ³    3x200 ³ 2x200+600 ³
    ÀÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÁÄÄÄÄÄÁÄÄÄÄÄÄÄÄÄÄÁÄÄÄÄÄÄÄÄÄÄÄÙ

      Cuando decimos 2x200+600 nos referimos a la siguiente secuencia:

         200ms   200ms       200ms   200ms       200ms   600ms

      Ú> tono -> silencio -> tono -> silencio -> tono -> silencio Ä¿
      ÀÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÙ
```

EL PRIMER MONTAJE
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ

Este primer montaje no va a conseguir que podamos llamar gratis, ni siquiera mas barato, pero permitira irnos introduciendo en materia. Ademas, este montaje puede sernos util en algunos casos, pero ahora puede que solo nos sirva para fardar ante los amigos.

Se trata de aplicar lo visto por el momento de se¤alizacion en la realiza- cion de un montaje practico.

Vamos a realizar un circuito que nos permitira emular las se¤ales multi- frecuencia de un telefono que trabaje de esta forma. Con el podremos marcar sin tener la necesidad de usar el teclado numerico del propio aparato.

El montaje se basa en la utilizacion del circuito TCM5087, tal y como lo usan algunos telefonos convencionales.

Su esquema es como sigue:

```
      [Bateria]      ÚÄÄÄÄÄÄÄ¿
         +9V ÄÄÄÄÄÄÄÄ´6      ÃÄÄ<ÄÄ14ÄÄÄÄÄ1 2 3
                     ³       ÃÄÄ<ÄÄ13ÄÄÄÄÄ4 5 6 Lineas de teclado numerico
                     ³       ÃÄÄ<ÄÄ12ÄÄÄÄÄ7 8 9
           ÄÄÄÄÄÄÄÄÄÄ´16     ÃÄÄ<ÄÄ11ÄÄÄÄÄ* 0 #
 [Altavoz]   A       ³       ÃÄÄ<ÄÄ3ÄÄÄÄÄÄÙ ³ ³
           ÄÄÂÄÄÄÄÄÄÂÄ´1     ÃÄÄ<ÄÄ4ÄÄÄÄÄÄÄÄÙ ³
             ³     ³ ³       ÃÄÄ<ÄÄ5ÄÄÄÄÄÄÄÄÄÄÙ
             ³     ÀÄ´15    7ÃÄÄÄ
             ³       ³       ³  X [Cristal de 3.579545 MHz]
             ³       ³      8ÃÄÄÄ
             ³       ÀÄÄÄÄÄÄÄÙ
            GND       TCM5087
  (-Ve de la bateria)
```

Este circuito tambien puede ser realizado sustituyendo el TCM5087 por dos pastillas 555 en circuito monoestable. Aunque prefiero el uso de este circuito, pues a parte de ser un montaje mas barato, es mas sencillo y mas cercano a los equipos telefonicos.

Bueno, esto ha sido todo por esta vez, pero no desespereis, en proximos articulos abordaremos temas mas interesantes sobre el sistema telefonico y sus usos (y abusos).

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

ÿÿÿ

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 08. AVISOS, NOTICIAS, PETICIONES, ETC...                                    º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

1. Nos han llegado algunos articulos curiosos, pero que a pesar de tratar temas underground no son temas del underground informatico o tecnologico y por ello no podemos publicarlos. Lo siento, pero esta publicacion no pretende tratar temas como la fabricacion de explosivos, la sintesis de drogas, el uso de armas, o tecnicas para estafar, etc... Por eso solo publicaremos articulos relacionados con el underground informatico o con las nuevas tecnologias, con temas como la telefonia, el hacking no informatico (VMB, faxes, etc...) electronica y informacion de ese estilo.

2. Estamos pensando en la posibilidad de crear una lista de distribucion para la revista, pero la verdad es que nos faltan medios. Si alguien conoce alguna forma de crear una de estas listas de forma barata y segura, que nos escriba y nos cuente como hacerlo.

3. Como dijimos hace un par de meses, la revista tambien iba a empezar a tratar temas tecnicos aunque no fuesen directamente hacking, cracking, o phreacking. Por eso aunque seais novatos en estos temas, seguro que conoceis algun tema que seria de interes para la comunidad underground. Hay temas como la criptografia, la programacion, etc... que son muy interesantes y que queremos que sean tratados en la revista. A si que si os animais ya sabeis donde encontrarnos.

4. el_duke1@hotmail.com

5. Pero hay una novedad en el sistema, y es que vamos a empezar a usar el PGP. No va a ser obligatorio pero si muy recomendable que para consultas "serias" se use esta llave:

```
-------------------llave--------------llave----------------llave--------------
Type Bits/KeyID    Date       User ID
pub  1024/3359D401 1997/02/11 el duke de sicilia

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

mQCNAzMAj4EAAAEEAJyNgoO6YzU+PZvbwsSH9AHhNNtLPyPF15rUtb9TcH/82rzv
3l6wETMcwNX/4dumsKDjz3iwl5JN+V5AYiIg4JDi5otbrkk6imjtMUMSXnsriw9a
0noSvw9guDC+JR8NDNPS+M8PpdcFBtQIv88oJF3JLWO/P9m6XX1rjOwzWdQBAAUR
tBJlbCBkdWtlIGRlIHNpY2lsaWE=
=R8Us
-----END PGP PUBLIC KEY BLOCK-----
-------------------llave--------------llave----------------llave--------------
```

6. Tambien estamos pensando en hacer una edicion especial de la revista que se llamara "SAQUEADORES INTERNACIONAL" donde haremos una seleccion de los mejores articulos y a¤adiremos tambien alguno mas. Y os preguntareis cual es la novedad, pues resulta que como sera internacional, pues no habra mas remedio que hacerla en ingles :-/

Ya tenemos un peque¤o grupo de traductores y colaboradores que se manejan bien en este idioma, pero no nos vendria mal un par de traductores mas y tambien algunos articulos escritos en ingles. A si que si conoceis a algun hacker americano que este dispuesto a escribir un articulillo para nosotros, avisadnos :-)

7. Y si alguien se siente con fuerzas de intentar este proyecto, en otros idiomas, pues nada, adelante, contais con nuestro apoyo.

8. Buscamos un servidor de ftp para distibuir la publicacion, si alguien conoce algun sistema en el que nos permitan tener un directorio con todos los numeros de la revista, para acceso publico, que nos lo diga.

9. Necesitamos encontrar a los autores de un MAGNIFICO curso sobre cabinas telefonicas, llamados CAR&BER, la ultima informacion que tenemos sobre ellos es que publicaron este curso en la bbs "Global BBS VMail-Fido <-> VirtualMail Gateway (70:343/14)" Por lo que suponemos que seran de Barcelona. Cualquiera que tenga alguna informacion sobre ellos o sobre donde conseguir el curso completo que se ponga en contacto con nosotros. (Se gratificara :)

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 09. ADMINISTRADORES                                                        º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

¨Que hacker no se ha preguntado quien hay detras del sistema que pirateais? ¨Que tipo de gente hay detras del sistema que estoy hackeando? Como os podeis imaginar, en funcion del tipo de actividad que realice la entidad, estara el tipo de gente que la maneja el sistema y su actitud. No es lo mismo ser un guru vicioso de la informatica y administrador del sistema UNIX de su universidad que un currante que solo quiere que se hagan las dos para irse a comer. Para ser verdaderos cazadores, debeis conocer la anatomia de las vuestras victimas, dejando un poco de lado los detalles tecnicos del ¨como?.

Desde el sistema operativo UNIX, que estan en el 100% de las universidades, los administradores de las universidades son en la mayoria de los casos becarios que como aquel que dice se han caido del nido y no saben en lo que realmente se meten (entre los que yo una vez estuve). Es una "pena" que las universidades no le dan importancia a este puesto y aprovechan para meter normalmente estudiantes o ex-estudiantes recien licenciados de menos de 28 a¤os que con el titulo de ingeniero informatico, son el genio de su pueblo y verdaderos fanfarrones que se merecen todo lo que les pase (aparte de lo que me cuentan, conozco personalmente a administradores de dos universidades distintas y son todos iguales). A esta gente, les gusta la administracion de los sistemas operativos y creen que el UNIX, es el invento del siglo XX y quieren ser los "jefecillos" de lo que es una pieza realmente importante de la universidad. Aprenden lo que concierne a seguridad a la brava, y acaban apuntandose a listas de mailing y consultando paginas web sobre hacking con lo que siempre van un paso por detras del pirata informatico. Y empieza a las tres semanas o un mes, consiguiendo de otro administrador o de internet un self-script que comprueba los ficheros de sistema a ver si alguien ha accedido o intentado acceder de forma ilegal al sistema, en este punto les empieza a caer el pelo, se cargan de extres y se vuelven paranoicos (si no acaban pasando de todo), y terminan siendo unos verdaderos administradores.
Si aguantan, sin pasar de todo, esta suele ser la primera experiencia profesional de los administradores de la empresa privada. Un sistema como este es realmente una perita en dulce para hackear ya que posee todos los recursos informaticos que se puede esperar de un sistema pero si alguien hackea alguna universidad, por favor, por lo menos no manipuleis los trabajos de los sufridos estudiantes, que son al final las verdaderas victimas.

En la gran empresa privada, por la informacion que tengo, no dan ninguna facilidad al acceso exterior, evitando incluso dar a conocer la propia existencia de ese acceso. En el caso de los bancos, que utilizan protocolos de comunicaciones muy peculiares o "extra¤os" cortando asi por lo sano.
Por ejemplo, en el BBV utilizan en todas sus sucursales por muy peque¤as que sean una inocente red Novell en entorno OS/2, pero acceden con la central de Tres Cantos en Madrid a traves de una emulacion VT3270 pero bajo un gran secretismo sobre todo lo concerniente a las comunicaciones. Yo estuve trabajando dos meses como tecnico informatico configurando las redes de sus sucursales y no supe ni pude acceder a ningun tipo de informacion al respecto y solo teniendo todas las claves de acceso (que cambian todos los dias) puedes hacer algo propio del hacker. Detras de todo este tinglado estan uno o varios departamentos (entre los que se lanzan, unos a otros, los problemas que surgen), compuestos por tecnicos que confian plenamente en los sistemas de seguridad que han adoptado, para ellos impolsible cualquier intromision ajena al propio banco en su sistema. Los bancos son unos usureros y explotadores y en realidad, un verdadero reto para la el hacker (y no imposible).

Faltan los peque¤os sistemas pero que no merece la pena y son poco atractivos para el

hacker. Ya que estos forman parte de una mediana empresa, compuesta por currantes y que esta continuamente luchando por no desaparecer.

Estos son dos ejemplos sobre los que yo tengo mas experiencia. Existen aparte otras empresas (no tan grandes como los bancos) pero que son el objetivo normal de los hackers. Pero si os fijais al final el administrador peligroso, siempre sera un tecnico/os con estudios en la universidad en la que algo hizo ya sea como becario o el trabajo de fin de carrera relacionado con la seguridad informatica y que al final ha aprendido a la brava y con un maestro estilo Karate Kid que le ese¤e los secretos y misteros del submundo o gracias a la informacion sobre hacking que circula inevitablemente en la Red. Frente la poca preparacion en seguridad informatica en las carreras informaticas.

Lex Luthor

EOF

ÉÍÍ»
º 10. LAS MEJORES PUBLICACIONES EN INGLES // INDICE DE LA REVISTA COTNO   º
ÈÍÍ¼

Esta seccion se ha echo un poco pesada en numeros anteriores, con el interminable indice de la Phrack, pero por fin hemos terminado y vamos a empezar en serio, comentando y recomendando las que a nuestro parecer son las mejores publicaciones en ingles.

En este numero vamos a hablar de la COTNO, "Communications of The New Order", realizada por en grupo TNO, "The New Order", algunos de sus miembros mas conocidos son estos:
Disorder
Edison
Major
Voyager
DeadKat
Karb0n
Panther Modern
Cavalier
Jewish Lightning
Nuklear Phusion

Esta es una de las mejores publicaciones que se pueden encontrar en la red. Es ralativamente actual y trata principalmente de hacking y phreacking. Tiene un nivel tecnico relativamente alto, pero por eso precisamente sus articulos son totalmente aplicables al hacking real.

El grupo TNO es norteamericano (como no) y ultimante algunos de sus miembros han tenido algunos problemas con la justicia, y probablemente no aparezcan nuevos numeros de esta maravilla. :‘-(

PUNTUACION: 9 (sobre 10)

* Articulos recomendados

Y ahora el indice:

Communications of The New Order
Issue #1
Summer, 1993

TABLE OF CONTENTS
~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~

Communications of The New Order
Issue #2
September/October 1993

Table of Contents
~~~~~~~~~~~~~~~~~

Communications of The New Order
Issue #3
November/December 1993

Table of Contents
~~~~~~~~~~~~~~~~~

Communications of The New Order
Issue #4
Spring/Sumer 1994

Table of Contents
~~~~~~~~~~~~~~~~~

Communications of The New Order
Issue #5
Fall 1994

Table of Contents
~~~~~~~~~~~~~~~~~

Communications of The New Order
Issue #6
Fall 1995

Table of Contents
~~~~~~~~~~~~~~~~~

Creo que el numero 7 no ha llegado a salir, a si que aqui acaba esta seccion.

EOF
~~~~~~~~~~~~~~~~~

ÉÍÍÍ»
º 11. CONCEPTOS VIRICOS º
ÈÍÍÍ¼

Esta es una recopilacion de los terminos mas usados cuando intentemos seguir un curso de virus o cuando se hable de ellos etc...

Activacion: El "efecto" del virus. La mayoria de los virus de hecho no tienen
^^^^^^^^^^^ ningun efecto, y se limitan a reproducirse (utilizando a veces tecnicas de proteccion). Este "efecto" puede ser destructivo, tonto, gracioso, o cualquier otra cosa. Puede dispararse por datos del sistema, como fecha u hora, por la llamada a una determinada funcion del sistema, por el numero de infecciones, y un largo etcetera.

Anti-Debugging: Un conjunto de peque¤as tecnicas destinadas a dificultar al
^^^^^^^^^^^^^^^ maximo posible el debugging de un virus (o un programa). No son infalibles, aunque pueden dar algun que otro dolor de cabeza al que se ponga a estudiar el virus. (tambien usadas en juegos y programas)

Anti-Dissasembly: Un grupo de tecnicas que tienen por objeto impedir que se
^^^^^^^^^^^^^^^^^ desensamble el virus mediante el uso de algun desensamblador, incluyendo en aquel, codigo para "confundirlo". (tambien usadas en juegos y programas)

Background: Se habla de background cuando un programa (o un virus),
^^^^^^^^^^^ se esta ejecutando "paralelamente" al programa ejecutandose : Por ejemplo al DOS.

Boot Sector: El primer sector del disco. Contiene la BPB (Bios Parameter Block)
^^^^^^^^^^^^ una tabla referente al formato y tipo del disco, y un peque¤o pro_ grama que es el encargado de Bootear (en discos de sistema) o del men_ saje "Non-system disk or disk error" (en discos sin sistema). Ademas, si se trata de un disco duro, el primer sector del disco contiene una tabla de particion, que a su vez contiene los sectores en que se encuentran los boot sectors de cada una de las particiones del disco, ademas de otra informacion referente a ellas.

Bug: Error en un programa, que produce que este funcione mal. Tambien se
^^^^ aplica a los virus. (Un bug en un virus podria hacer, por ejemplo, que este infectara mal los EXEs y los destruyera, etc.)

Carrier: Asi llamado el file ejecutable generado al ensamblar el source
^^^^^^^^ original de un virus.

CMOS: Un tipo de memoria que sobrevive a los apagados de la maquina. Contiene
^^^^^ informacion de configuracion (ver Setup) como los tipos de disco, de monitor, etc. (Solo existe en ATs) Algunos virus (muy pocos) la cambian para invertir el orden de booteo (de A:;C: a C:;A:) e impedir que se bootee de un disco limpio.

Debugger: Un programa para estudiar el funcionamiento de otros programas.
^^^^^^^^^ (Tambien sirve para estudiar virus).

Directory Stealth: Una tecnica de ocultamiento que consiste en substraer el
^^^^^^^^^^^^^^^^^^ size del virus del size mostrado por el comando DIR de DOS. (A los virus que solo utilizan Dir-Stealth se los suele llamar semi_ stealth)

Disinfect-On-The-Fly: Una tecnica de (file) stealth que consiste en
^^^^^^^^^^^^^^^^^^^^^ directamente desinfectar el file cuando se considera que este va a ser inspeccionado (por ejemplo cuando es abierto). Suele

ir acompa¤ada de Infection-On-Close (pues si no seria inefectivo).

Disassembler: Programa para producir codigo fuente en base a un ejecutable.
^^^^^^^^^^^^

Disparador: Se llama disparador a la parte del codigo del virus que se encarga
^^^^^^^^^^ de evaluar si se cumplen o no las condiciones para que el virus se
active.

Fast Infector: Un tipo de virus que se distingue por la velocidad con la
^^^^^^^^^^^^^ que se dispersa. Esto se logra infectando no solo cuando el file
es corrido sino cada vez es accedido por algun medio (abierto, leido,
etc.)

FAT: File Allocation Table. El "mapa" mediante el cual el DOS mantiene
^^^^ registro de que clusters estan usados y a que file pertenecen, etc.

File Stealth: En contraposicion a Dir-Stealth. Un virus que implementa
^^^^^^^^^^^^ distintas tecnicas para pasar desapercibido, tecnicas mas avanza_
das que el ocultamiento del size en el DIR.

Full Stealth: Un virus en el cual las tecnicas de stealth estan tan bien
^^^^^^^^^^^^ implementadas e integradas que la existencia del virus pasa
desapercibida cuando este esta activo en memoria. Se logra mediante
la intercepcion de un monton de funciones del sistema, y hay stealth
que son incluso indetectables a nivel de BIOS (via int 13h)

Generador de virus: Un programa para hacer virus. Para utilizarlo solo se
^^^^^^^^^^^^^^^^^^ necesita un conocimiento muy basico del tema.

Header EXE: Una estructura que se encuentra al principio de todos los EXE, y
^^^^^^^^^^ mediante la manipulacion de la cual los virus son capaces de
infectarlo. Contiene informacion necesaria para correr el EXE.

Hoste: (s) Programa parasitado por el virus, programa infectado. (Ver
^^^^^^ Overwriting y Parasitico)

Infection-On-Close: Infectar al cerrar un archivo, en lugar de cuando este
^^^^^^^^^^^^^^^^^^ es corrido.

MCB: Memory Control Block. Una estructura de DOS para la alocacion de memoria,
^^^ que es manipulada por los virus para quedar residentes de una manera
lo menos sospechosa posible. Los virus que utilizan esta tecnica
para su alojamiento en memoria o bien disminuyen el size total
reportado o bien son reconocibles por un ultimo bloque, perteneciente
al "sistema" (en realidad del virus).

Multipartito (o multiparticion): Un virus que es simultaneamente de Boot y de
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ file. Suelen ser mas complejos que sus contra_
partidos solo de file o solo de boot, y la interaccion entre la parte
de boot y la de file suele ser compleja, y dar mejores resultados en el
funcionamiento del virus.

New Header EXE: Ampliacion del header de los EXE comunes en los EXE de
^^^^^^^^^^^^^^^ Windows.

No-Residente: (a) Un virus en el que el proceso de infeccion es llevado
^^^^^^^^^^^^ a cabo cuando el virus es corrido. Son menos efectivos que los
residentes, y su funcionamiento impide realizar tecnicas de stealth.
(Aun asi son considerados respetables, no como los overwriting, pues
aun pueden tener un cierto grado de exito en su dispersion).

Overwriting: Un virus que al infectar destruye al programa infectado. Este
^^^^^^^^^^^^ tipo de virus no tiene mucha proyeccion, y se lo considera muy
primitivo.

Parasitico: Un virus que conserva al programa infectado, para poder correrlo
^^^^^^^^^^^ luego como si no lo estuviera.

Polimorfismo: Una tecnica de ocultamiento que apunta a que sea imposible
^^^^^^^^^^^^^ descubrir al virus mediante scanning, variando de tal forma el codigo
de infeccion a infeccion que es imposible extraer una string. Esto se
hace encriptando el codigo del virus y "variabilizando" la rutina de
encripcion tanto como sea posible.

Residente: (a) Un virus que, cuando es corrido, se carga en memoria y
^^^^^^^^^^ a partir de ahi, queda en el background, hasta que es llamado a la
superficie y alli infecta.

Root: Directorio Raiz, el primer directorio.
^^^^^

Sector: Uno de los "pedazos" en que los discos estan divididos. Para el BIOS
^^^^^^^ los sectores son "fisicos" y se los referencia mediante 3 coordenadas;
lado, pista, sector (lado 0, pista 0, sector 1, p.ej). El DOS utiliza
sectores logicos, que son referenciados mediante un numero. (Sector 0)
Y existe la correspondencia (lado 0, pista 0, sector 1 == Sector 0).

Setup: El famoso setup. Un programa cargado en la BIOS, desde donde se maneja
^^^^^^ la configuracion del sistema (Por ejemplo la cantidad de sectores del
disco rigido, o la fecha del sistema, etc).

SFT: System File Table. Una tabla con informacion referente a un file abierto.
^^^^ Se utiliza para todo tipo de propositos en los virus, ya que la
informacion que contiene es muy variada y muy valiosa.

Stealth: Genericamente, se llama stealth a un virus que utiliza alguna tecnica
^^^^^^^^ para no ser notado. Existen varias de estas tecnicas.

String: Cadena que se utiliza para reconocer un file infectado. Es una PARTE
^^^^^^^ del virus, NO todo el virus. Generalmente se hacen strings de las ruti_
nas de infeccion. Al hacer virus polimorficos, se trata justamente de
que no exista una cadena comun entre infeccion e infeccion.

Toolkit: Una libreria para incluir en un virus, y conferirle a este la
^^^^^^^^ potencia de alguna tecnica avanzada como polimorfismo o tunneling.
(Notese que no existen ni podran existir toolkits de stealth ya
que este tipo de tecnicas estan muy ligadas al dise¤o general del
virus, y no pueden ser "aisladas" en un toolkit).

Troyano: Programa especialmente hecho para causar da¤o. Se los suele confundir
^^^^^^^^ con los virus, aunque no tienen NADA que ver, excepto el hecho de que
los troyanos hacen da¤o, y algunos virus hacen da¤o.

Tunneling: Una tecnica de proteccion, de tipo anti-anti-virus, que consiste
^^^^^^^^^^ basicamente en pasar "por debajo" de los antivirus residentes, que
monitorean la actividad "rara". Se obtiene el address original de la
int que se piensa puede estar monitoreada, y se usa este address
para accederla.

Virus: (s) Un codigo ejecutable capaz de reproducirse a si mismo a traves de
^^^^^^ sistemas y computadoras. Se los clasifica primariamente por el tipo de
reproduccion (Boot Sector, File, Cluster), y luego por la utilizacion
de tecnicas de ocultamiento y proteccion (Stealth, Polimorfico, etc).

Virus de boot: Un tipo de virus. Se reproduce poniendose en el boot sector
^^^^^^^^^^^^^^ de los discos, y luego de haberse instalado en memoria, corre el
boot sector original.

Virus de file: Este tipo de virus se reproduce infectando los files del disco.
^^^^^^^^^^^^^^ Se dividen en infectores de COM, de SYS, y de EXE. (y ultimamen_
te de EXE de windows).

Virus de cluster: Un tipo de virus relativamente nuevo y oscuro. Para infectar
^^^^^^^^^^^^^^^^^ no modifica el file, sino sencillamente la entrada de direc_
torio del archivo. Solo existe UN virus de este tipo, el celebre Dir-2.

Bithunter

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 12. CURSO DE HACKING EMPEZANDO DESDE CERO IV                               º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Ya tenemos aqui la cuarta entrega de esta serie, despues de un peque¤o lapso para aclarar dudas volvemos al trabajo, y vamos a seguir explicando los pasos iniciales en este mundillo.

Conocimientos:

Despues de explicar donde empezar nuestras primeras andanzas, despues de explicar los conceptos basicos, despues de esbozar la etica del hacker, vamos a seguir con otro tema de inicio. La eterna pregunta:

¨QUE TENGO QUE SABER PARA SER UN HACKER?

Y la pregunta es esta exactamente, ya que alguien es un hacker por sus conocimientos no por sus actos, alguien es un hacker cuando sabe como hackear, incluso aunque nunca haya hackeado. (Valga la redundancia)

Pues antes de todo, para ser un hacker hay que tener un domino total y absoluto de la informatica, si te has comprado el ordenador hace 6 meses, a menos que seas un genio, me parece que te va acostar mucho ser un hacker a corto plazo. Y con conocimientos de informtica, no me refiero a sabe programar ni nada por el estilo (aunque es recomendable) conocimientos de informatica, es mas o menos, saber de todo, es decir, si te hablan de redes saber algo de redes (lo basico) si te hablan de virus, saber lo que son y como funcionan, es decir, no hay que ser un experto en nada, pero si que hay que saber de todo un poco.

Y una vez que se ha conseguido una cultura general informatica aceptable llega el momento de especializarse. Los campos que tiene que controlar a la perfeccion, cualquier hacker que se precie deben ser:

-Sistemas operativos UNIX, el 90% de los ordenadores en internet, y un gran porcentaje de las empresas, usan algun tipo de UNIX, desde Linux hasta AIX pasando por HP/UX, IRIX, etc... Por eso tienes que manejarte en un sistema UNIX como lo harias en tu propio ordenador, y ¨cual es la mejor forma de manejarte asi? pues sencillo, usando un unix en tu casa y ¨que unix puedo usar en mi casa? pues el linux es muy recomendable, pero si te puedes permitir otro unix, pues adelante.
-Conociemiento de programacion en algun lenguaje, preferiblemete C, ya que es un lenguaje muy extendido, sobre todo en los unix, como no. Tambien hay otros lenguajes como perl y ensamblador que seria muy interesante conocer.
-Conocimientos de redes, internet es una red, las empresas suelen tener redes internas, los grandes ordenadores suelen estar en redes, por eso la mejor forma de hackear es a traves de una red.
-Conociemientos de telefonia, la mejor forma de conectar con una red es atraves de un modem y de la liena telefonica, por lo tanto, tienes que conocer que pasa entre tu y tu objetivo.
-Tambien tienes que controlar al 100% los protocolos mas comunes de internet, como el ftp, el http, el smtp, etc...
-Y por supuesto tiene que conocer el manejo de todas las herramientas

de uso habitual, como son el cliente irc, el war-dialer, el
programa de telnet, etc...

Herramientas:

Basicamente cualquier pack de conexion a redes viene con unas herramientas
suficientes para el hackeo. Pero si se quiere conseguir un mejor
dominio de la situacion habra que usar unas herrameintas especiales
para cada tarea.

Lo ideal son las herramientas de conexion y manejo de redes que vienen
incorporadas de serie en la mayoria de los UNIXes del mercado (incluido
linux) ya que es mucho mas comodo trabajar de unix a unix, que de dos
a unix, y nada que decir de las patateras y muy bonitas visualmnete
herramientas para windows95.

Pero bueno, no vamos a meternos con nadie y vamos a poner una lista
de herramientas genericas, sin fijarnos en el sistema operativo bajo
el que funcionan:

-Un war-dialer, hace unos a¤os esta herramienta era casi imprescindible,
ahora con el precio y las posibilidades de internet, tampoco es
necesario perder tiempo buscando ordenadores cuando tenemos a nuestra
disposicion una red con millones de ellos. Pero el war-dialing sigue
siendo una forma bastante buena de encontrar sistemas virgenes y
muy faciles de hackear y simpre es interesante conocer posibles objetivos
en tu propia ciudad.

-Un programa de telnet, sin uno de estos en internet vas a tener poco
que hacer. Y es que un cliente telnet, no solo sirve para hacer una
conexion telnet clasica (puerto 23) sino que tambien sirve para
conectarse a otros puertos y usar otros servicios, que usan el estandar
telnet para hacer sus conexiones, como son el smtp (puerto 25) el
pop (puerto 113) las news (puerto 513) el ftp (puerto 21) o incluso
el propio http usado para la web (puerto 80)

-Un programa de ftp que permita el uso de comandos, imprescindible, tanto
para el hacking, como para el acceso a los sites warez. :-)

-Un navegador de web, esto no es imprescindible para el hacking, pero
si muy util para buscar buenos textos.

-Un escaneador de puertos, pues eso un programa que se encargue de
deciros que puertos de la maquina o maquinas elegidas, estan abiertos
al publico.

-Un crackeador de ficheros de password de unix, aunque tambien es
recomendable uno para novell.

-Y por supuesto las tipicas herramientas de diagnostico de redes,
como un capturador de paquetes, un medidor de trafico, algun sniffer,
etc...

-Y totalmente indispensable, la ultima version del doom para acabar con el
estres. (Y si es posible hacerlo en red, mejor :-)

Sitio:

Ya explicamos cuales eran los mejores lugares para hackear, y ahora vamos a explicar los mejores lugares DESDE DONDE hackear, es decir, donde conectarse a la red. Por supuesto quedan decartados lugares como tu casa, la casa de tu amigo o la de tu primo. El primer requisito a la hora de hackear es usar un telefono limpio.

Los lugares que reunen esta caracxteristica esencial son pocos, estan entre otros:
-Las salas de acceso a internet que ofrecen algunas universidades o institutos. Son un lugar idoneo para el hacking, y generalmente no suele haber problemas, aunque en muchas hace falta ser estudiante de ese centro para poder acceder a ellas.
-Los cafes internet o sitios por el estilo. El problema de estos sitios es que generalmente carecen de las herramientas necesarias para un hackin comodo y tambien suele haber muchos "curiosos".
-Las cabinas de telefono. Sin duda son el lugar mas anonimo, desde el que se puede hackear, tienen algunos inconvenientes, pero garantizan un total anonimato. (El tema de las cabinas sera tratado con mas detalle en el proximo numero)
-Algun ordenador ajeno, si no tienes miedo a ser pillado in fraganti urgando en el ordenador de alguien, esta puede ser tu opcion. Simplemnete cuelate en la casa o en la oficina de alguien y usa su ordenador para hackear. El problema de este sistema es que multiplica el riesgo y las consecuencias legales del hacking.
-Pinchando la linea de alguien. Hay algunos texto rondando por ahi que explican como hacerlo, por eso voy a ser breve. El truco consiste en colarte en un edificio, abrir la caja de las conexiones telefonicas del edificio, y pinchar una de las lineas. Es sencillo, pero al igual que en el caso anterior, si te pillan, la condena puede ser doble.

Y aqui terminamos, el proximo numero, massss...

El duke de Sicilia

EOF

É͸»
º 13. MENSAJES Y PREGUNTAS DE LOS LECTORES º
È͸¼

Inauguramos esta nueva seccion de la revista, para que vuestras felicitaciones, quejas y preguntas puedan ser conocidas por todos los lectores de la saqueadores. Aqui van los mas interesantes de estos ultimos meses:

De: Merjimenez
Para: Eljaker
Tema: Redes Novell

>Me interesa mucho darme un paseo por la rambla de la red novell de mi trabajo.
>¨Alguien ha investigado el tema? ¨Hay alguna manera de entrar como supervisora
>sin conocer el pasword?

Pues las redes novell estan bastante investigadas, en internet hay mucha informacion sobre el tema. Incluso creo recordar que hay algo en espa¤ol sobre el tema.

Para orientarte mas o menos, tienes varias opciones para conseguir lo que quieres:
-Poner un sniffer o un capturador de teclas, y interceptar el password del administrador. Si no tienes conocimientos para hacerte tu uno, en internet hay varias herramientas creadas especificamente para ello.
-Buscar en las listas de bugs y exploits, alguno que afecte a las redes novell y que te permita hacer lo que quieres. Aunque si no estas muy metida en estos temas a lo mejor te cuesta encontrar algo. En espa¤ol hay poca cosa, intenta en los buscadores con palabras como exploit, bug, novell, cert, bugtrack, o palabras relacionadas con el tema.
-Conseguir el fichero de passwords y con un crackeador intentar conseguir la clave del administrador. Por supuesto puedes encontrar crackeadores en internet.

De: Javier
Para: El Duke de Sicilia
Tema: Login Hacker

>Resulta que me he echo con el telefono del modem de un almacen
>perteneciente a una gran red (tipo Prica, Continente, etc), y quiero entrar
>en el sistema, conecto con un programa terminal DOS, tipo FRODO, y paratir
>de ahi me pide el Login y el Password, un numero indeterminado de veces,
>o sea que no tiene log, ¨que programas hay para automatizar la entrada de
>passwords desde un listado?, como el aparecido en el n§ 2 de esta revista.

Lo primero enhorabuena por haber encontrado ese chollo, porque si no tiene logs, tarde o temprano podras con el :-)

Pues hay pocos programas para hacer eso, y que sean faciles de encontrar pero conozco uno muy bueno, que es el "THC LOGIN HACKER" del grupo aleman THC (The Hackers Choice) Es una herramienta potentisima, y muy buena, tiene unas detalladas instrucciones en ingles, pero es un poco dificil de configurar, porque funciona mediante scripts, pero en cuanto le cojas el truco, vas a flipar.

Tambien tienes la opcion de programarte tu un programa a medida, aunque

supongo que te sera mas comodo bajarte el Login Hacker.

Para los que tengan interes en esta herramienta y en el resto de los buenisimos trabajos del grupo THC, podeis encontrar la mayoria de sus obras en:

ftp.paranoia.com/pub/zines/THC/

Sobre todo os recomiendo su publicaccion (THC_MAG) y su war-dialer THC-SCANNER.

De: ThE_WiZArD
Para: Eljaker
Tema: Sobre phreacking (Las preguntas del millon :)

1§ ES POSIBLE LLARMAR GRATIS A INTERNET A TRAVES DE INFOVIA ??

Si, pero: ES ILEGAL :-))))

[Bueno, y tambien hay un par de servidores que ofrecen conexiones de prueba gratuitas, pero son un poco molestas de usar. Pero el telefono lo pagas por webos]

2§ HAY MUCHO PELIGRO DE KE TE COJAN ?? CUALES SON LAS PRECAUCIONES TENER EN CUENTA?

Hay MUCHO peligro y altas posibilidades de que te cojan, y las precauciones son simples, no hacerlo desde tu casa, utilizar un telefono limpio, no abusar mucho, cambiar de lugar cada pocos usos y sobre todo: "BE PARANOID"

3§ KUAL ES EL MEJOR METODO (Las bluebox quizas??)

El boxing en Espa¤a es casi imposible, y lo que es posible es muy inseguro y facil de pillar. La unica posibilidad medianamente segura es que otro pague la llamada, y aun asi, tampoco te aseguro que no te cojan o que funcione.

Venga, y los que tengan dudas de interes general, que escriban.

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 14. COMO PILLAR LAS CLAVES (LLAVES O KEYS) DE CANALES DE IRC              º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Apodo: Inmortal
E-Mail: xxxxx@xxxxx (solo para el grupo)
Nivel Tecnico: Medio-Bajo
Titulo: Como pillar las claves (llaves o keys) de canales de Irc.
Estilo y Tema: Hacking Irc.

Hola a todos, soy Inmortal y os voy a decir como se pueden pillar las claves que algunas personas suelen poner en los canales de Irc. Lo primero es deciros que material necesitamos:
- Mirc o Pirch 4.7x o superior (16 o 32bits)
- Un Link Looker o el Script para Mirc llamado 7th Sphere que incluye el Link Looker (7th Sphere en http://www.7thsphere.com).

Nota: No he visto ni probado Link Lookers para Pirch asi que mejor que uses Mirc a no ser que tengas un Link Looker que funcione con Pirch.
Pues bien, una vez tengamos eso, nos conectamos al Irc (se supone usando el 7th Sphere) y buscamos el canal que queremos acceder y tiene una clave, ej.:
Tecleamos para meternos en un canal:

```
/join #xxxxx
Unable to join #xxxxx (requires the correct *key)
```

* Esto dice que necesitamos la clave.

Entonces nos metemos en otro canal, #hackers ;-) por ejemplo, entonces en la barra de menus del Mirc vamos al menu 7thSphere (esta escrito en codigos ASCII) y pulsamos War Menu (si no estamos en el), ahora aparecen opciones distintas en el menu, una de ellas "Link Looker", vamos a ese menu y pulsamos en el submenu ON. Ahora esperamos a que nos salga un mensajito asi:

```
--------------------------------------------------------------------- NetSplit
ÿffffd7 irc.xxx.xxx
---------------------------------------------------------------------
[Shift+F5] to load the Takeover Bot.
[Shift+F6] to switch the Takeover Bot to the split server.
[Shift+F7] to load Nick Collide Bots onto the split server.
[Shift+F8] to view currently Split servers.
---------------------------------------------------------------------
```

Esto nos dice que el servidor irc.xxx.xxx tiene un *netsplit, y nos conectamos a el con la orden:

```
/server irc.xxx.xxx 6667 (donde irc.xxx.xxx es el servidor con netsplit)
```

* Un netsplit es cuando un servidor se separa de todos los demas por cualquier motivo (fallo, arreglo, renovacion...).

Una vez conectados en el servidor con Netsplit nos metemos en el canal que tiene la clave, entonces veremos como el canal "no existe" y nosotros lo creamos, ahora viene la marcha!

Si quereis ser discretos quitaros el Op para que no sospechen porque si espera un rato volveremos a ver que todo comienza a restaurarse con respecto a los de servidores, se restauran topics, lista de bans, Ops y como no "claves" jejeje. Pues seguimos dentro y ya tenemos la clave! No ha sido tan dificil, no? :)

Unos consejos para conservar la clave:

- Una vez el servidor se restaure (Ops, Bans, Topics, Claves...) y tengamos la clave, apuntadla o memorizarla RAPIDAMENTE y salid del servidor o conectaros a otro que sea un *link de este y meteos en el canal con la clave asi:

/join #xxxxx clave

Entonces entramos como si fueramos del canal y supieramos la clave de hace tiempo. Asi no sospecharan ni cambiaran la clave. :-)

* Un servidor Irc puede estar formado por muchos servidores, a cada uno se le llama "link", para ver los links de un servidor Irc debemos poner la orden:

/links

Espero que os haya gustado la leccion y escribire otra mas:

- Como tirar a alguien de Irc e incluso de SU CONEXION. :) Bye!

- Inmortal -

EOF

ÉÍÍ»
º 15. CONTESTADORES AUTOMATICOS º
ÈÍÍ¼

Hola, soy Red_Cool, y he escrito este texto (o mejor dicho recopilado) para todos los que odian esa cosa, que siempre te dice: "deje su mensaje despues de la se¤al".
Ademas de ser incomodo, tambien puede ser divertido para nosotros. :-)))))

nOtA: el autor no se hace responsable de la utilizacion que se le pueda dar a este texto.

Un gran porcentaje de personas poseen contestadores automaticos en sus casas (-que asco!), en algunos modelos se tiene la posibilidad de acceder a los mensajes grabados, y otras opciones por medio de tonos (DTMF) en forma remota, o sea llamando desde otro telefono y usar el teclado del telefono para ver el estado de nuestro contestador.

¨Porque no llamar al contestador de nuestro vecino que tanto odiamos y escuchar los mensajes grabados?.

Es una buena diversion, aparte es algo como para empezar con el Phreaking, y a familiarizarse con los codigos de acceso, ya que si pretendemos acceder a algun PBX generalmente tenemos que poner un codigo de acceso.
Obviamente para acceder a estas funciones tenemos que ingresar un codigo de acceso a travez de tonos, estos codigos pueden variar entre 2 y 5 digitos, cuanto mayor cantidad de funciones tenga el contestador mas digitos tendra el codigo de acceso.

La marca mas difundida de contestadores, es:
- PANASONIC -

La mayoria de la gente tiene los modelos de Panasonic que solo utilizan codi-gos de 2 digitos, facil de buscar el codigo solo va de 0-99 (100 codigos)
Para hacerlo es aun mas facil, con enviar la siguiente combinacion ya hemos enviado todos los codigos:

01122334455667788991357902468036925814715937049483827261605172959628408529
639974197531864209876543210

Pero si consideramos que generalmente los modelos Panasonic no usan digitos del 0 al 9, solo algunos, solo se deberia enviar una combinacion como la si-guiente o algo parecida:

33556636653

Una vez que ingresamos el codigo correcto, el contestador nos va a tirar una serie de BEEPs y se queda esperando a que le mandemos un comando, que para los modelos panasonic mas convencionales son:

1 - Retrocede un mensaje
2 - Avanza al proximo mensaje
3 - RESET
5 - PLAY
6 - Room monitoring
7 - Record receive message
9 - End receive message
0 - Discontect answering machine
* - Skip Message

Funcion *: Nos permite pasar por alto el mensaje de recepcion, y empezar a grabar el mensaje o enviar el codigo al contestador.

Funcion 1: Retrocede al mensaje anterior y lo reproduce

Funcion 2: Avanza al proximo mensaje que hay grabado.

Funcion 3: Resetea el contestador, vuelve al mensaje 0 y cuando dejemos uno sobreescribe los mensajes grabados, etc.

Funcion 5: Reproduce los mensajes que hay grabados en el contestador automatico.

Funcion 6: Nos permite escuchar lo que esta sucediendo a donde llamamos, ya que el constestador habilita el microfono que tiene incorporado, esta funcion no sirve de mucho, solo para saber si hay alguien hablando en la casa o algun otra boludez.

Funcion 7: Esta es una de las mas interesantes, nos permite grabar el mensaje que se envia al recibir una llamada. Aca tenemos varias cosas para hacer, una es grabarle alguna chorrada, otra es llamar a un lugar donde mandan Putas a domicilio y pedirle que manden a una puta a la casa de algun 'AMIGO' y decirle que llamen al n£mero del contestador. En el contestador debemos grabar algo asi como:

- Si si, yo hice la llamada (o alguna cosa paracida).

Esto para que resulte hay que llegar a hacerlo muy bien, calcular bien los tiempos y tener un poco de suerte (o nada) :-))

Otra cosa para hacer es: si tenemos a algun amigo que viva en otro pais es arreglaro para que haga una llamada con cobro revertido (via operadora) a ese n£mero y dejar grabado:

- Hola? <PAUSA> SI, si acepto la llamada.
o
- Hello? <PAUSA> Yes I accept the Call.

Esto es para alguien que odiemos, porque si lo hacemos unas cuantas veces, el pobre cabron va a tener un "poquito" de recargo en la factura del telefono.

Funcion 8: Esta funcion se usa despues de la 7, con esto le indicamos al contestador que hemos terminado de grabar el mensaje de recepcion.

Funcion 0: Desconecta el Contestador automatico, pero no es una desconecsion total, ya que si llamamos y dejamos sonar 15 veces el contestador se vuelve a encender automaticamente.

////////////////////// Otras marcas de contestadores \\\\\\\\\\\\\\\\\\\\\\\\

Estas funciones son para algunos modelos de contestadores AT&T y por ahi tambien funcionan con algun otra marca:

1 Retroceder
2 Repetir
3 Avance
4 Grabar mensaje de recepcion (De nuevo para terminar de grabar)
5 Stop
6 Grabar Mensajes
8 Play >
9 Desconecta el contestador
0 Anuncio de la fecha y la hora

/\/

Si el contestador tiene mas de 2 digitos en el codigo, ya se complica un poco mas, pero hay que tener en cuenta que muy poca gente utiliza los contestadores en forma remota, mas de uno no sabe que es eso, asi que ninguno se calienta en cambiarle el codigo (en algunos no se puede cambiar), asi que siempre hay que probar con los que vienen por default:
1111,0000,1234,9999 y codigos asi.

Algunos de los contestadores mas nuevos tienen una funcion muy interesante, que es la de programar al contestador para que cada vez que nos dejan un mensaje nos llame a un n£mero y nos lo pase, si podemos acceder a uno de estos contestadores, que tienen 4 o 5 n£meros de codigo, podriamos programarlo para que llame a algun n£mero Internacional, y asi entrar a dejarle mensajes, y es mejor si le podemos llegar a ver la cara al tipo cuando reciba la factura al fin del bimestre :)

Espero que con esto os divertais bastante, y os pongais en practica para sacar codigos.!

+++Red_Cool+++

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 16. EL BUG DEL MES                                                        º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Este apartado casi se nos olvida este numero, y es que como nadie manda material para este apartado, pues siempre tenemos que hacerlo a ultima hora y con prisas. Bueno, pues por falta de tiempo en este bug del mes nos vamos a tener que limitar a describir el bug, y poco mas. A si que a los que esperaban un jugoso exploit todo bien explicadito, me parece que se van a desilusionar, y esperar hasta el proximo numero.

Y si la proxima vez quereis algo mas jugoso, pues moved el culo y mandarnos vuestros exploits. Pero eso si, hemos echo caso a la gente que nos pedia bugs recientes y os hemos traido uno de hace pocos meses. (Gracias a Eljaker y a Valfadir por mandarnos informacion sobre el)

Sistemas: IRIX
Versiones: 5.2 - 6.3
Descripcion: Bug del sistema de logs

Los IRIX tiene un avanzado sistema de logs y de seguridad en los logins, uno de estos servicios de seguridad viene representado por la variable LOCKOUT que hace que una cuenta con un numero determinado de intentos de acceso incorrectos se bloquee. Este sistema no es nada nuevo y es un sistema bastante efectivo. Pero en el caso de los IRIX los desarrolladores han metido la gamba hasta el fondo :-)

Los datos relacionados con la variable LOCKOUT se almacenan en el directorio /var/adm/badlogin, a cada cuenta con intentos fallidos le corresponde un fichero de 1 byte que es el numero de intentos fallidos. (por ejemplo si la cuenta es ’guest’ pues apareceria un fichero llamado guest de un byte de longitud)

Pero el problema esta ahi, porque el sistema crea un fichero con el nombre de la cuenta a la que se ha intentado acceder, o sea lo que se ha tecleado en el prompt ’login:’ ¨Entonces si tecleamos el nombre de una ruta, que pasara?

Pues efectivemnete ahi esta el agujerazo, si tecleamos algo como esto:

```
        login: ../../../etc/estamos_dentro
        Password:
        UX:login: ERROR: Login incorrect
```

Habras creado un fichero de un byte llamado /etc/estamos_dentro (Y cada vez que intentemos este mismo ’login:’ el primer byte del archivo especificado se incremetara en 1)

Ademas de pegarle un susto de muerte al administrador creando ficheros por todos sus directorios con nombres raros, este bug tiene multiples utilidades.

Con el truco NO se pueden sobreescribir ficheros (cagen) pero si que podemos incrementar el primer byte. Esto puede tener multiples utilidades y puede ser usado para crear varios exploits, a mi se me han ocurrido un par de usos, pero ninguno suficientemente bueno.

Si a alguien se le ocurre algun sistema de explotar este defecto, que nos lo diga.

El Duke de Sicilia

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 17. DESPEDIDA                                                             º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Bien, veo que ya han terminado, ¨desean ustedes tomar algo de postre?

No, entonces cerramos el Bar :-)

Se despide el editor

"No subestimes el poder del lado oscuro de la fuerza"

-FINAL DEL NUMERO 8-

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

EOF